

# Quantum<sup>®</sup>

## User's Guide

# Quantum Scalar *i*40 and Scalar *i*80



Scalar i40 and Scalar i80 User's Guide, 6-66545-06 Rev A, June 2011, Product of U.S.A.

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

#### **COPYRIGHT STATEMENT**

Copyright 2011 by Quantum Corporation. All rights reserved.

Your right to copy this manual is limited by copyright law. Making copies or adaptations without prior written authorization of Quantum Corporation is prohibited by law and constitutes a punishable violation of the law.

#### **TRADEMARK STATEMENT**

Quantum, the Quantum logo, and Scalar are registered trademarks of Quantum Corporation, registered in the U.S.A. and other countries.

Preserving the World's Most Important Data. Yours., StorageCare, and Vision are trademarks of Quantum.

LTO and Ultrium are trademarks of HP, IBM, and Quantum in the U.S.A. and other countries. All other trademarks are the property of their respective companies.

Specifications are subject to change without notice.



# Contents

---

---

## Preface

	<b>xxi</b>
Worldwide End-User Product Warranty . . . . .	xxviii

---

## Chapter 1

Description	1
Overview . . . . .	1
Library Components . . . . .	2
Front Panel . . . . .	2
Robotic System and Barcode Scanner . . . . .	3
Magazines . . . . .	4
Power Supply . . . . .	8
System Control Board . . . . .	8
Tape Drives . . . . .	9
Standard Features . . . . .	12
User Interface . . . . .	12
Partitions . . . . .	12
Control Path Modification . . . . .	12
Support for WORM . . . . .	13
Licensable Features . . . . .	13
Capacity on Demand (COD) . . . . .	13
Advanced Reporting . . . . .	14
Encryption Key Management . . . . .	15

<b>Chapter 2</b>	<b>Unpacking the Library</b>	<b>17</b>
<b>Chapter 3</b>	<b>Understanding the User Interface</b>	<b>21</b>
	Operator Panel . . . . .	21
	Operator Panel Layout and Functions . . . . .	22
	Navigating and Editing on the Operator Panel . . . . .	27
	Web Client . . . . .	28
	Tips . . . . .	28
	Sorting Information In Tables . . . . .	29
	Web Client Layout and Functions . . . . .	29
	Web Client Home Page . . . . .	31
	System Summary . . . . .	31
	Subsystem Status . . . . .	32
	Menu Trees . . . . .	33
<b>Chapter 4</b>	<b>Configuring the Library</b>	<b>37</b>
	Using the Setup Wizard . . . . .	39
	Default Configuration . . . . .	40
	Configuring Network Settings . . . . .	40
	Library Host Name . . . . .	41
	DHCP . . . . .	42
	IP Addresses . . . . .	42
	Default Gateway, Subnet Mask, Network Prefix, and DNS Addresses . . . . .	43
	Configuring SNMP Settings . . . . .	44
	Registering External Management Applications . . . . .	44
	Enabling SNMP Versions . . . . .	46
	Enabling SNMP Authentication Traps . . . . .	46
	Modifying the SNMP Community String . . . . .	47
	Downloading the SNMP MIB . . . . .	47
	Setting the Date, Time, and Time Zone . . . . .	48
	Setting the Date and Time Manually . . . . .	49
	Setting the Date and Time Using the Network Time Protocol . . . . .	49
	Setting the Time Zone . . . . .	50
	Setting Daylight Saving Time . . . . .	51

Working With Partitions . . . . .	51
Automatically Creating Partitions . . . . .	53
Manually Creating Partitions . . . . .	54
Modifying Partitions . . . . .	56
Deleting Partitions . . . . .	57
Viewing the Current Partitions . . . . .	58
Changing Access to Partitions . . . . .	59
Taking a Partition Online or Offline . . . . .	59
Configuring Cleaning Slots . . . . .	61
Configuring I/E Station Slots . . . . .	63
Configuring Tape Drive Parameters . . . . .	65
Configuring Control Paths . . . . .	67
Adding or Upgrading Licensable Features . . . . .	69
About License Keys . . . . .	69
Viewing Your License Keys . . . . .	70
Viewing Installed Licenses . . . . .	70
Obtaining a License Key . . . . .	70
Applying a License Key . . . . .	71
Working With E-mail Notifications . . . . .	72
Creating E-mail Notifications . . . . .	73
Modifying E-mail Notifications . . . . .	74
Deleting E-mail Notifications . . . . .	75
Configuring the Library E-Mail Account . . . . .	76
Setting Customer Contact Information . . . . .	78
Configuring the Service Port . . . . .	78
Working With Local User Accounts and Passwords . . . . .	79
Using the Web Client Default Administrator Account . . . . .	80
Privilege Levels . . . . .	81
Creating Local User Accounts on the Web Client . . . . .	82
Modifying Local User Accounts on the Web Client . . . . .	83
Deleting Local User Accounts on the Web Client . . . . .	84
Enabling and Creating Passwords on the Operator Panel . . . . .	84
Disabling Passwords on the Operator Panel . . . . .	87
Modifying Passwords on the Operator Panel . . . . .	87
Resetting Passwords on the Operator Panel . . . . .	88
Working With LDAP User Accounts (Remote Authentication) . . . . .	88
Local Authentication vs. Remote Authentication . . . . .	88
LDAP Server Guidelines . . . . .	89

Configuring Secure LDAP on the Library . . . . .	90
Configuring LDAP on the Library . . . . .	90
Testing LDAP Settings . . . . .	94
Configuring Kerberos . . . . .	94
Generating the Kerberos Service Keytab File . . . . .	96
Setting the Session Timeout . . . . .	97
Configuring System Settings . . . . .	98
Unload Assist . . . . .	98
Logical Serial Number Addressing. . . . .	99
Manual Cartridge Assignment . . . . .	100
SNMP . . . . .	101
SMI-S . . . . .	101
Power Save . . . . .	101
Configuring Security Settings . . . . .	103
Network Interface . . . . .	103
SSH Services . . . . .	104
Internet Control Message Protocol (ICMP) . . . . .	104
Remote Access Via Web Client . . . . .	105
Remote Service Login . . . . .	105
SNMP V1/V2 . . . . .	105
SSL . . . . .	106
Saving and Restoring the Library Configuration . . . . .	107
Saving the Library Configuration . . . . .	107
Restoring the Library Configuration . . . . .	108
Registering the Library. . . . .	109
Changing Operator Panel Home Screen View . . . . .	109
Changing to Alternate Home Screen. . . . .	109
Returning to Default Home Screen . . . . .	110

---

**Chapter 5**

<b>Advanced Reporting</b> . . . . .	<b>111</b>
Advanced Reporting Features . . . . .	112
Required Firmware . . . . .	113
Working with Control Path Failover (CPF) . . . . .	113
Prerequisites . . . . .	113
Configuring CPF . . . . .	114
Forcing CPF . . . . .	116
Using Advanced Reporting Reports . . . . .	118

- Configuring the Drive Resource Utilization Report . . . . . 119
- Configuring the Media Integrity Analysis Report. . . . . 121
- Using Advanced Reporting Templates. . . . . 123
- Loading and Reloading Advanced Reporting Data . . . . . 124
- Deleting Advanced Reporting Data. . . . . 125
- Saving and E-mailing Advanced Reporting Data Files . . . . . 125
- Working with the Media Security Log . . . . . 126
  - Configuring Media Security . . . . . 127
  - Viewing, Saving, and E-mailing Media Security Log . . . . . 128
- Viewing the Media Usage Log . . . . . 129
- Automatically E-mailing Advanced Reporting Reports and Logs . . . . 130
  - Creating a Recipient . . . . . 131
  - Modifying a Recipient. . . . . 134
  - Deleting a Recipient . . . . . 134

---

**Chapter 6 Performing Library Operations 135**

- Logging In . . . . . 136
  - Simultaneous Logins . . . . . 136
  - Logging in for the First Time. . . . . 136
  - Logging in Using the Operator Panel . . . . . 137
  - Logging in Via the Web Client . . . . . 137
  - Logging in When LDAP or Kerberos is Enabled . . . . . 138
- Logging Out . . . . . 138
- Shutting Down, Restarting, Turning Off, and Removing Power. . . . . 139
  - Shutting Down the Library . . . . . 140
  - Restarting the Library . . . . . 142
  - Turning Off the Library . . . . . 143
  - Completely Removing Library Power. . . . . 144
  - Emergency Power-off Procedure. . . . . 144
  - Taking the Library Offline . . . . . 145
- Unlocking and Opening the I/E Station . . . . . 145
- Releasing Magazines . . . . . 148
  - Releasing Magazines via the User Interface. . . . . 149
  - Releasing Magazines Manually . . . . . 150
- Performing Media Operations . . . . . 151
  - Importing Tape Cartridges . . . . . 152
  - Bulk Loading Tape Cartridges . . . . . 155

Moving Tape Cartridges . . . . .	156
Exporting Tape Cartridges . . . . .	158
Loading Tape Drives . . . . .	160
Unloading Tape Drives . . . . .	161
Cleaning Tape Drives . . . . .	163
Valid Cleaning Cartridges . . . . .	164
About AutoClean . . . . .	164
Enabling AutoClean . . . . .	165
Importing Cleaning Cartridges . . . . .	165
Exporting Cleaning Cartridges . . . . .	167
Manually Cleaning Tape Drives . . . . .	169
Taking a Tape Drive Online or Offline . . . . .	172

---

**Chapter 7 Encryption Key Management 175**

About the EKM License . . . . .	176
Configuring Scalar Key Manager (SKM) on the Library . . . . .	176
Step 1: Upgrade Firmware . . . . .	176
Step 2: Install the EKM License Key on the Library . . . . .	176
Step 3: Install SKM on a Server or Servers . . . . .	177
Step 4: Configure Encryption Settings and Key Server Addresses . . . . .	177
Step 5: Install TLS Communication Certificates on the Library . . . . .	179
Step 6: Run EKM Path Diagnostics . . . . .	179
Step 7: Configure SKM Partitions and Generate Data Encryption Keys . . . . .	179
Step 8: Save the Library Configuration . . . . .	182
EKM Path Diagnostics . . . . .	182
Description . . . . .	182
Failure Scenarios . . . . .	183
Running Manual EKM Path Diagnostics . . . . .	183
Enabling Automatic EKM Path Diagnostics . . . . .	184
Viewing Tape Drive Encryption Settings . . . . .	185
Scalar Key Manager Functions Available on the Library . . . . .	185
Installing TLS Certificates on the Library . . . . .	186
Generating Data Encryption Keys . . . . .	191
Sharing Encrypted Tape Cartridges . . . . .	195
Exporting Encryption Certificates . . . . .	197



Importing Encryption Certificates . . . . . 198  
 Exporting Data Encryption Keys . . . . . 199  
 Importing Data Encryption Keys . . . . . 201  
 Accessing the SKM Server Logs . . . . . 202  
 Using the SKM Encryption Key Import Warning Log . . . . . 202

**Chapter 8**

**Getting Information About the Library . . . . . 205**

Viewing Library Information . . . . . 206  
 Viewing System Information . . . . . 206  
 Viewing the Location of the Robot . . . . . 207  
 Viewing the Library Configuration Report . . . . . 210  
 Saving and E-mailing the Library Configuration Record . . . . . 212  
     Saving the Configuration Record . . . . . 213  
     E-mailing the Configuration Record . . . . . 213  
 Viewing the Network Settings Report . . . . . 214  
 Viewing the Logged in Users Report . . . . . 215  
 Viewing the All Slots Report . . . . . 215  
 Viewing, Saving, and E-mailing Library Logs . . . . . 217  
     Cleaning Log . . . . . 217  
     Diagnostic Tickets Log . . . . . 218  
     Media Security Log (with Advanced Reporting License) . . . . 219  
     Media Usage Log (with Advanced Reporting License) . . . . 219  
     SKM Encryption Key Import Warning Log (with EKM License) . . 219  
     Tape Drive Log . . . . . 220  
 Viewing Library Information on the Operator Panel . . . . . 221  
     Viewing Partition Information . . . . . 221  
     Viewing Tape Drive Information . . . . . 222  
     Viewing Network Settings . . . . . 222  
     Viewing the Date, Time, and Time Zone . . . . . 223  
     Viewing Licenses . . . . . 223  
 Using Advanced Reporting Features . . . . . 223  
 Viewing the Open Source License Agreement . . . . . 223  
 Viewing the Copyright Statement . . . . . 224

<b>Chapter 9</b>	<b>Installing, Removing, and Replacing Components</b>	<b>225</b>
	Taking ESD Precautions . . . . .	226
	Connecting Library Cables . . . . .	227
	Installing the Rack Mount Kit (Rail Kit) . . . . .	229
	Supported Rack Types . . . . .	229
	Space Requirements . . . . .	230
	Tools Required . . . . .	230
	Rack Mount Kit Contents . . . . .	230
	Installing the Rack Mount Shelves . . . . .	232
	Installing the Library In a Rack . . . . .	241
	Removing the Library From a Rack . . . . .	243
	Installing the Library in a Desktop Kit . . . . .	244
	Kit Contents . . . . .	246
	Tools Required . . . . .	246
	Space Requirements . . . . .	247
	Procedure . . . . .	247
	Removing the Library from a Desktop Kit . . . . .	252
	Removing and Replacing the Front Bezel . . . . .	253
	Required Tools . . . . .	253
	Bezel Replacement Kit Contents . . . . .	253
	Bezel Replacement Procedure . . . . .	253
	Replacing the Chassis . . . . .	258
	Required Tools . . . . .	258
	Procedure . . . . .	259
	Removing and Installing a Filler Plate . . . . .	269
	Removing and Installing a Tape Drive Filler Plate . . . . .	269
	Removing and Installing a Power Supply Filler Plate . . . . .	269
	Removing and Replacing a Magazine . . . . .	271
	Required Tools . . . . .	271
	Magazine Replacement Kit Contents . . . . .	271
	Creating a Backup Map of Cartridge Locations . . . . .	271
	Removing the Magazine from the Library . . . . .	272
	Installing the Magazine . . . . .	273
	Removing and Installing a Power Supply . . . . .	276
	Replacing a Power Supply in a Single-Power-Supply System (Scalar i40 and Scalar i80) . . . . .	277

	Adding or Replacing a Redundant Power Supply on the Scalar i80 278	
	Removing and Replacing the System Control Board . . . . .	279
	Replacing the System Control Board . . . . .	279
	Installing Library Firmware . . . . .	281
	Restoring the Library Configuration . . . . .	283
	Manually Reconfiguring the Library . . . . .	284
	Removing and Replacing a Tape Drive . . . . .	286
	Preparing Partitions and Control Paths . . . . .	287
	Removing a Tape Drive from the Library . . . . .	288
	Installing a Tape Drive . . . . .	288
	Packaging the Library for Moving or Shipping . . . . .	292
	Packaging Kit Contents . . . . .	292
	Creating a Backup Map of Cartridge Locations . . . . .	292
	Procedure . . . . .	293
	Replacing the Y-tray with Robot . . . . .	298
<hr/>		
<b>Chapter 10</b>	<b>Updating Firmware</b>	<b>299</b>
	Updating Library Firmware . . . . .	299
	Updating and Autoleveling Tape Drive Firmware . . . . .	304
	About Tape Drive Firmware Autoleveling . . . . .	305
	Uploading Tape Drive Firmware Used in Autoleveling . . . . .	306
	Deleting Tape Drive Firmware Used in Autoleveling . . . . .	308
	Initiating Tape Drive Firmware Autoleveling . . . . .	310
<hr/>		
<b>Chapter 11</b>	<b>Troubleshooting</b>	<b>311</b>
	About Diagnostic Tickets . . . . .	312
	Viewing, Closing, and Resolving Diagnostic Tickets . . . . .	313
	Closing Diagnostic Tickets Automatically . . . . .	316
	Capturing Snapshots of Library Information . . . . .	317
	Troubleshooting Library “Not Ready” Messages . . . . .	318
	“Not Ready” Messages on the Operator Panel . . . . .	318
	“Not Ready” Messages on the Web Client . . . . .	318
	Retrieving Tape Drive Logs . . . . .	320
	Interpreting LEDs . . . . .	320

Front Panel LEDs . . . . .	321
System Control Board LEDs . . . . .	322
Tape Drive/Sled LEDs . . . . .	323
Power Supply LED . . . . .	324
Running the Installation and Verification Test (IVT) . . . . .	325
Running the IVT Diagnostic Subtests Individually – Robotics, Tape Drive, and Magazine Tests . . . . .	327
Running the Random Move Test . . . . .	329
Performing Library Diagnostics . . . . .	330
Resetting a Tape Drive . . . . .	331
Robotics Get/Put Test . . . . .	332
Resetting Factory Defaults . . . . .	333

---

<b>Chapter 12</b>	<b>Working With Cartridges and Barcodes</b>	<b>335</b>
	Handling Tape Cartridges Properly . . . . .	336
	Write-Protecting Tape Cartridges . . . . .	337
	Barcode Label Requirements . . . . .	337
	Supported Barcode Formats . . . . .	338
	Installing Barcode Labels . . . . .	339

---

<b>Appendix A</b>	<b>Specifications</b>	<b>341</b>
	Physical Specifications . . . . .	341
	Capacity . . . . .	342
	Environmental Specifications . . . . .	343
	Air Clearance Requirements . . . . .	343
	Library Power Specifications . . . . .	344
	Power Consumption and Heat Output . . . . .	345
	Communication Interfaces . . . . .	346
	Supported Tape Drives . . . . .	346
	Supported Media . . . . .	347







# Figures

---

Figure 1	Front Panel . . . . .	2
Figure 2	Scalar i40 Internal Layout and Magazine Slot Location Coordinates6	
Figure 3	Scalar i80 Internal Layout and Magazine Slot Location Coordinates7	
Figure 4	Scalar i40 Back Panel Components . . . . .	10
Figure 5	Scalar i80 Back Panel Components . . . . .	11
Figure 6	Packaging . . . . .	18
Figure 7	Removing the Robot Restraint . . . . .	20
Figure 8	Operator Panel User Interface - Home Screen . . . . .	22
Figure 9	Operator Panel User Interface - Alternate Home Screen . . . . .	23
Figure 10	Using the Buttons to Set the Date and Time. . . . .	28
Figure 11	Web Client User Interface - Home Page . . . . .	30
Figure 12	Operator Panel Menus . . . . .	34
Figure 13	Web Client Menus . . . . .	35
Figure 14	LDAP Setup Example. . . . .	93
Figure 15	Setup - Drive Settings Screen . . . . .	114
Figure 16	Setup - Control Path Screen . . . . .	115

Figure 17	Tools - Drive Operations Screen for CPF . . . . .	116
Figure 18	Force CPF Screen. . . . .	117
Figure 19	Template and Report Data Functions . . . . .	123
Figure 20	Report Data Buttons. . . . .	125
Figure 21	Saving and E-mailing the Report Data . . . . .	126
Figure 22	Shutdown in Progress Message . . . . .	140
Figure 23	Ready to Power Down Message . . . . .	141
Figure 24	Ready to Power Down Message . . . . .	141
Figure 25	Series of Restart Messages . . . . .	142
Figure 26	I/E Station Unlocked Message. . . . .	146
Figure 27	I/E Station Locked Message . . . . .	147
Figure 28	Magazine Unlocked Message . . . . .	149
Figure 29	Magazine Locked Timer Message . . . . .	149
Figure 30	Magazine Release Latch Access . . . . .	151
Figure 31	Configuring Encryption Settings and Key Server Addresses . 178	
Figure 32	Configuring Partition Encryption . . . . .	180
Figure 33	Enabling Automatic EKM Path Diagnostics. . . . .	184
Figure 34	Checking and Installing TLS Certificates . . . . .	187
Figure 35	Accessing the Encryption Partition Configuration Screen	193
Figure 36	Changing Encryption Method to Allow Application Managed 194	
Figure 37	Changing Encryption Method Back to Enable Library Managed195	
Figure 38	Exporting Encryption Certificates . . . . .	197
Figure 39	Importing Encryption Certificates. . . . .	198
Figure 40	Exporting Encryption Keys . . . . .	199
Figure 41	Importing Data Encryption Keys . . . . .	201
Figure 42	Connection Locations . . . . .	228
Figure 43	Rack Mount Shelf Depth Requirements . . . . .	233



Figure 44	Assembling the Left and Right Rack Mount Shelves . . . . .	234
Figure 45	Rail Adapter Types . . . . .	235
Figure 46	Assembling the Left-Hand Rack Mount Shelf . . . . .	236
Figure 47	Installing the Rack Mount Shelves . . . . .	238
Figure 48	Tightening the Rack Mount Shelves . . . . .	239
Figure 49	Location for Installing the Clip Nut or Cage Nut . . . . .	241
Figure 50	Magazine Release Latch Access Holes . . . . .	242
Figure 51	Securing the Scalar i40 and Scalar i80 in the Rack . . . . .	243
Figure 52	Desktop Kit, Scalar i40 and Scalar i80 . . . . .	245
Figure 53	Magazine Release Latch Access Holes . . . . .	248
Figure 54	Location of Rubber Feet on Bottom of Library . . . . .	249
Figure 55	Installing side panels . . . . .	251
Figure 56	Installing Top Cover . . . . .	252
Figure 57	Bezel Screw Locations on Bottom of Library . . . . .	255
Figure 58	Bezel Screws . . . . .	256
Figure 59	Scalar i80 Pull/Push Locations . . . . .	257
Figure 60	Components to Remove . . . . .	261
Figure 61	Removing the Y-tray Restraints . . . . .	262
Figure 62	Restraining the Y-tray . . . . .	264
Figure 63	Reinstalled Components . . . . .	267
Figure 64	Filler Plates Installed . . . . .	270
Figure 65	Magazine Release Latch Access Holes . . . . .	273
Figure 66	Proper Orientation (Right-Side Magazine) . . . . .	274
Figure 67	Removing/Installing the Magazine Bezel . . . . .	275
Figure 68	Single Power Supply System . . . . .	276
Figure 69	Redundant Power Supply System . . . . .	277
Figure 70	Ethernet Port Locations on the SCB . . . . .	281
Figure 71	Acceptable Installation Locations for Full-Height Tape Drives 289	

Figure 72	Installing a Tape Drive . . . . .	290
Figure 73	Restraining the Y-tray . . . . .	295
Figure 74	Scalar i40 Packaging . . . . .	296
Figure 75	Scalar i80 Packaging . . . . .	297
Figure 76	Tools - Update Library Firmware Screen . . . . .	301
Figure 77	Front Panel LEDs . . . . .	321
Figure 78	System Control Board LEDs . . . . .	322
Figure 79	Fibre Channel Tape Drive LEDs . . . . .	324
Figure 80	Power Supply LED . . . . .	325
Figure 81	Barcode Label Orientation . . . . .	340



# Tables

---

Table 1	Front Panel Features . . . . .	2
Table 2	Operator Panel Functions . . . . .	24
Table 3	Web Client Screen Elements . . . . .	31
Table 4	Scalar i80 I/E Slot Configuration . . . . .	64
Table 5	Fibre Channel Tape Drive Configurable Settings . . . . .	66
Table 6	Encryption Methods . . . . .	181
Table 7	Base Library . . . . .	341
Table 8	Library Installed in a Desktop Kit . . . . .	342
Table 9	Tape Alert Flag Severity Codes . . . . .	349
Table 10	Tape Drive Tape Alert Flag Descriptions . . . . .	350





# Preface

---

This manual introduces the Quantum Scalar® i40 and Scalar i80 and discusses:

- System operations
- Configuration
- Web and operator panel interface
- Installation and replacement
- Basic troubleshooting

---

## Audience

---

This manual is written for Scalar i40 and Scalar i80 operators, system administrators, and field service engineers.

---

## Document Organization

---

Following is a brief description of chapter contents.

- [Chapter 1, Description](#) provides a physical description of the library, its components, and major features.
- [Chapter 2, Unpacking the Library](#) describes how to prepare a space and unpack the library.
- [Chapter 3, Understanding the User Interface](#) describes the appearance and function of the operator panel and Web client.

- [Chapter 4, Configuring the Library](#) provides instruction and description for all the configurable features of the library.
- [Chapter 5, Advanced Reporting](#) describes the features available with the Advanced Reporting license.
- [Chapter 6, Performing Library Operations](#) explains how to run the library from the operator panel and Web client.
- [Chapter 7, Encryption Key Management](#) describes the features available with the Encryption Key Management (EKM) license.
- [Chapter 8, Getting Information About the Library](#) describes all of the reporting features on the library.
- [Chapter 10, Updating Firmware](#) describes how to upgrade library firmware and install and autolevel tape drive firmware.
- [Chapter 9, Installing, Removing, and Replacing Components](#) provides detailed instruction on how to install, remove, and replace all the physical components of the library.
- [Chapter 11, Troubleshooting](#) describes the library's troubleshooting tools, including diagnostic tickets, LEDs, and tests.
- [Chapter 12, Working With Cartridges and Barcodes](#) provides basic information about how to label and care for media used in the library.
- [Appendix A, Specifications](#) provides physical, environmental, power, and other specifications about the library, tape drives, and media.
- [Appendix B, Tape Alert Flag Descriptions](#) lists all the Tape Alerts you may encounter in a diagnostic ticket.
- [Appendix C, Disposal of Electrical and Electronic Equipment](#) provides information on disposing and recycling.

The document concludes with a glossary and index.

## Notational Conventions

This manual uses the following conventions:

Convention	Example
File and directory names, menu commands, button names, and window names are shown in bold font.	<b>/data/upload</b>
Menu names separated by arrows indicate a sequence of menus to be navigated.	<b>Utilities &gt; Firmware</b>

The following formats indicate important information:

---

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

---



---



---

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

---



---



---

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

---

- Right side of the system — Refers to the right side as you face the component being described.
- Left side of the system — Refers to the left side as you face the component being described.

## Product Safety Statements

Quantum will not be held liable for damage arising from unauthorized use of the product. The user assumes all risk in this aspect.

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

The *System, Safety, and Regulatory Information Guide* is located on the Scalar i40 and Scalar i80 documentation and training CD.

---

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

---

---

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

---

---

**警告** 操作本产品前，请先阅读本文件及系统、安全与法规资讯指南中的指示与警告说明。

---

---

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

---

---

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

---

---

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

---

---

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

---

---

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

---

---

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

---



---



---

**ПРЕДУПРЕЖДЕНИЕ** всеми инструкциями и предупреждениями, приведенными в данном документе и в *Справочном руководстве по устройству, технике безопасности и действующим нормативам*.

---



---



---



---

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

---



---



---



---

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

---



---

## Related Documents

The following Quantum documents are also available for Scalar i40 and Scalar i80 systems:

Document No.	Document Title
6-66546-xx	<i>Scalar i40 and Scalar i80 Quick Start Guide</i>
6-66547-xx	<i>Scalar i40 and Scalar i80 Release Notes</i>
6-00618-xx	<i>System, Safety, and Regulatory Information</i>
6-66773-xx	<i>Scalar i40 and Scalar i80 Basic SNMP Reference Guide</i>
6-00423-xx	<i>Quantum Intelligent Libraries SCSI Reference Guide</i>
6-01317-xx	<i>Quantum Intelligent Libraries SMI-S Reference Guide</i>
6-66531-xx	<i>Scalar Key Manager User's Guide</i>

For the most up to date product information and documentation, see:

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

## SCSI-2 Specification

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

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

---

## Contacts

---

Quantum company contacts are listed below.

### Quantum Corporate Headquarters

To order documentation on the Scalar i40 or Scalar i80 or other products, contact:

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

### Technical Publications

To comment on existing documentation send e-mail to:

[doc-comments@quantum.com](mailto:doc-comments@quantum.com)

### Quantum Home Page

Visit the Quantum home page at:

<http://www.quantum.com>

---

## Getting More Information or Help

---

## Quantum. Global Services

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

Accelerate service issue resolution with these exclusive Quantum StorageCare services:

- **Service and Support Web site** – Register products, license software, browse Quantum Learning courses, check backup software and operating system support, and locate manuals, FAQs, firmware downloads, product updates and more in one convenient location. Benefit today at:

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

- **Telephone Support** – Find contact information for your location at:

<http://www.quantum.com/ServiceandSupport/Contacts/ProductSelect/Index.aspx>

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

<http://www.quantum.com/osr>

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

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

- **Quantum Vision** – Quantum Vision software enables simplified monitoring and reporting of Quantum DXi disk-based systems and Scalar tape libraries. Especially powerful for customers with multiple disk systems or a combination of Quantum disk and tape libraries working together, Vision puts you in control to make better decisions that will prevent issues, manage resources efficiently, and improve uptime. Vision can aggregate data across multiple systems, provide system status, and display trend information all from a single console. More quantum Vision information can be found at:

<http://www.quantum.com/Products/Software/QuantumVision/Index.aspx>

- **Latest Library Firmware** - You can view a listing of the latest version of library firmware on the following Web site:  
<http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI40/Index.aspx> and click the **Firmware** tab.

If your library has an internet connection, you can log into your library to view the latest firmware version available. Click **Tools > Update Library Firmware**. The screen displays the firmware currently loaded on your library and the latest available firmware.

Follow instructions in [Chapter 10, Updating Firmware](#) to upgrade Firmware. For further assistance, or if training is desired, contact the Quantum Customer Support Center.

---

## Worldwide End-User Product Warranty

---

For more information on the Quantum Worldwide End-User Standard Limited Product Warranty:

<http://www.quantum.com/pdf/QuantumWarranty.pdf>



# Chapter 1 Description

---

This chapter covers the layout and basic functionality of the library, including:

- [Overview](#)
- [Library Components](#)
- [Standard Features](#)
- [Licensable Features](#)

---

## Overview

The Scalar i40 and i80 tape libraries automate 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.

See [Appendix A, Specifications](#) for library capacity and a list of tape drives and media supported by the Scalar i40 and Scalar i80 libraries.

# Library Components

## Front Panel

[Figure 1](#) illustrates the features of the operator panel. The picture shows the Scalar i40, but the features are the same on the Scalar i80. These features are described in [Table 1](#).

Figure 1 Front Panel

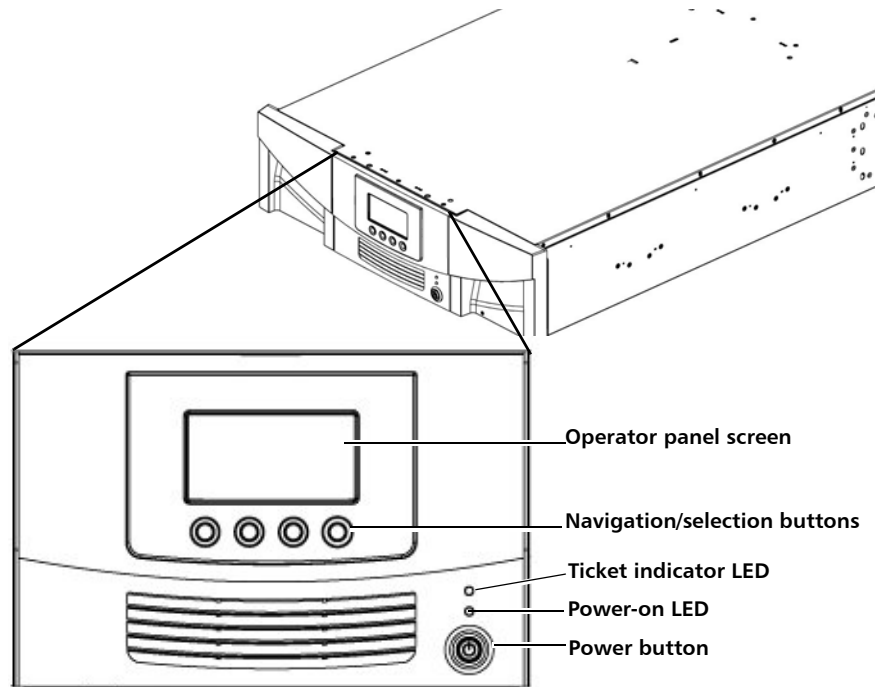


Table 1 Front Panel Features

Feature	Description
Operator panel screen	The operator panel displays library status information and allows you to access the library menus. These menus allow you to view or change the library settings and run diagnostic tests. For more information, see <a href="#">Operator Panel</a> on page 21.

Feature	Description
Four navigation/selection buttons	These buttons, in combination with the operator panel display, are used to scroll through screens and select options or commands. The functionality of these buttons changes depending on the currently displayed operator panel screen.
Ticket indicator LED	Indicates whether a diagnostic ticket exists on the library. See <a href="#">Front Panel LEDs</a> on page 321 and <a href="#">About Diagnostic Tickets</a> on page 312 for more information.
Power-on LED	Indicates whether library power is on or off. See <a href="#">Front Panel LEDs</a> on page 321 for more information.
Power button	Turns the library on or off. Turning off the library using the power button turns off the robot and operator panel, but power still runs to the power supplies. See <a href="#">Shutting Down, Restarting, Turning Off, and Removing Power</a> on page 139 for instructions on how to shut down the library safely.

## 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 and out of slots and tape drives.

A barcode scanner is attached to the library's robotic hand. This barcode scanner automatically identifies the slots and cartridges in the library, if the cartridges are fitted with acceptable barcode labels.

Each tape cartridge must contain a unique, matching-readable barcode that the barcode scanner reads during the inventory process. During the inventory process, the barcode scanner reads the barcode labels on the tape cartridges and empty slots to identify the types of tape cartridges that are installed in the library.

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 12, Working With Cartridges and Barcodes](#).

Robots can only be replaced by a Quantum Support technician.

---

## Magazines

---

Magazines are removable and contain storage and import/export station slots for cartridges. Each magazine has 20 slots, arranged in four columns of five slots each. The Scalar i40 contains two magazines; the Scalar i80 contains four. The right magazines provide up to five slots each for use as an import/export (I/E) station. For more information on I/E stations, see [Configuring I/E Station Slots](#) on page 63.

---

**Note:** Cartridges are gently restrained within the magazine by a detent found on the left side of each individual magazine bin slot. To manually remove a cartridge, pull a cartridge from the front or push on the cartridge from the rear of the magazine via an “access hole.” Be gentle to avoid any bending of the top magazine cover sheet metal.

---

The library will run if one or more magazines is open or removed; however, it runs at reduced speed. The library will not move a cartridge to an open or removed magazine, but it will move a cartridge to any of the other installed magazines.

You can open the magazines using library software or manually. For information, see [Releasing Magazines](#) on page 148.

For information on removing and replacing magazines, see [Removing and Replacing a Magazine](#) on page 271.

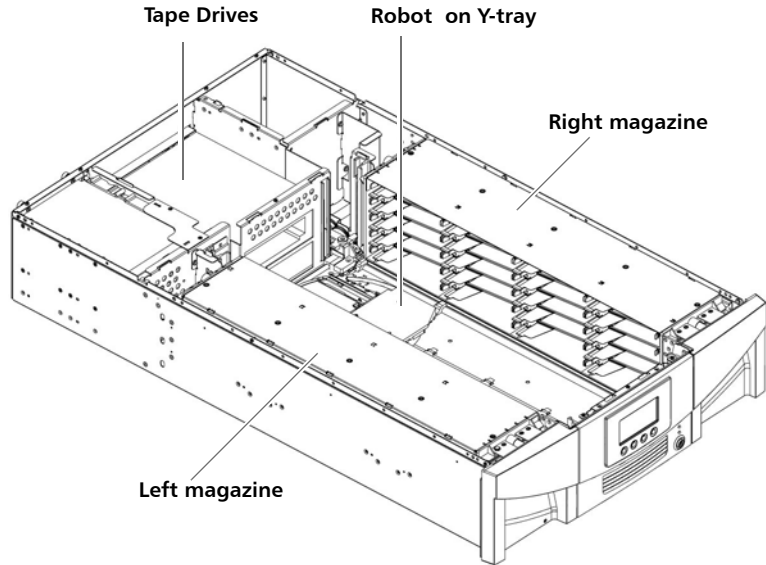


## Magazine Slot Location Coordinates

Each slot in the installed magazine is numbered with location coordinates. The library location coordinate contains three digits as follows: [Magazine],[Column],[Slot]. [Figure 2](#) and [Figure 3](#) show the magazines and list all of the location coordinates.

- **Magazine** — Library magazine level is represented by the first digit of a library coordinate. In a Scalar i40, there is only one level of magazine. The coordinate is always zero. In a Scalar i80 library, the bottom magazines are indicated by a zero; the top magazines are indicated by the number 1.
- **Column** — 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 8.
- **Slot** — Slots (both storage and I/E station) are represented by the third digit of the library location coordinate. Within each magazine column, slots are numbered from 1 to 5, starting at the top of the magazine.

Figure 2 Scalar i40 Internal  
Layout and Magazine Slot  
Location Coordinates



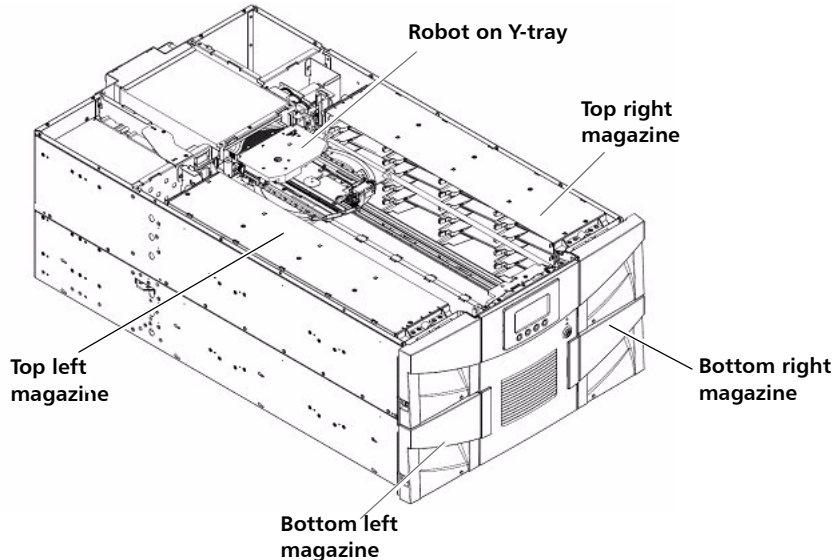
**Left Magazine**

0,1,1	0,2,1	0,3,1	0,4,1
0,1,2	0,2,2	0,3,2	0,4,2
0,1,3	0,2,3	0,3,3	0,4,3
0,1,4	0,2,4	0,3,4	0,4,4
0,1,5	0,2,5	0,3,5	0,4,5

**Right Magazine**

0,5,1	0,6,1	0,7,1	0,8,1
0,5,2	0,6,2	0,7,2	0,8,2
0,5,3	0,6,3	0,7,3	0,8,3
0,5,4	0,6,4	0,7,4	0,8,4
0,5,5	0,6,5	0,7,5	0,8,5

Figure 3 Scalar i80 Internal  
Layout and Magazine Slot  
Location Coordinates



**Top Left Magazine**

1,1,1	1,2,1	1,3,1	1,4,1
1,1,2	1,2,2	1,3,2	1,4,2
1,1,3	1,2,3	1,3,3	1,4,3
1,1,4	1,2,4	1,3,4	1,4,4
1,1,5	1,2,5	1,3,5	1,4,5

**Top Right Magazine**

1,5,1	1,6,1	1,7,1	1,8,1
1,5,2	1,6,2	1,7,2	1,8,2
1,5,3	1,6,3	1,7,3	1,8,3
1,5,4	1,6,4	1,7,4	1,8,4
1,5,5	1,6,5	1,7,5	1,8,5

**Bottom Left Magazine**

0,1,1	0,2,1	0,3,1	0,4,1
0,1,2	0,2,2	0,3,2	0,4,2
0,1,3	0,2,3	0,3,3	0,4,3
0,1,4	0,2,4	0,3,4	0,4,4
0,1,5	0,2,5	0,3,5	0,4,5

**Bottom Right Magazine**

0,5,1	0,6,1	0,7,1	0,8,1
0,5,2	0,6,2	0,7,2	0,8,2
0,5,3	0,6,3	0,7,3	0,8,3
0,5,4	0,6,4	0,7,4	0,8,4
0,5,5	0,6,5	0,7,5	0,8,5

---

## Power Supply

---

The Scalar i40 and Scalar i80 libraries support single power configurations consisting of a single AC line input and single DC power supply. The Scalar i80 library supports a redundant power configuration consisting of a dual AC line input and dual DC power supplies.

If you have a Scalar i80 and are only using one power supply, the power supply should be installed in the upper power supply slot, and a filler plate must cover the empty power supply slot (see [Figure 5](#) on page 11). If you are using redundant power, you can hot add or hot swap a power supply (power to the library remains on while you add or exchange the hardware).

The Scalar i40 power supply cannot be installed in a Scalar i80. However, the Scalar i80 power supply works in either the Scalar i40 or the Scalar i80.

---

---

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

---

---

The power system consists of the following components:

- Power supply
- AC power cord

The power supply has one status LED. For more information, see [Power Supply LED](#) on page 324.

For information on removing and replacing power supplies, see [Removing and Installing a Power Supply](#) on page 276.

---

## System Control Board

---

The system control board (SCB) contains the library firmware, all configurable settings, license keys, and SKM TLS certificates. It 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 SCB has two Ethernet ports:

- Left port — For remote management (Web client)
- Right port — For service only. In rare cases, you may need to change the IP address of the port if it conflicts with your library IP address (see [Configuring the Service Port](#) on page 78).

See [Figure 4](#) on page 10 and [Figure 5](#) on page 11 for port locations.

The SCB contains one LED, in addition to two LEDs on each Ethernet port (for a total of 5 LEDs). For more information, see [System Control Board LEDs](#) on page 322.

For information on removing and replacing the SCB, see [Removing and Replacing the System Control Board](#) on page 279.

---

## Tape Drives

---

Every library configuration must contain at least one tape drive.

See [Appendix A, Specifications](#) for a list of tape drives and media supported by the Scalar i40 and Scalar i80 libraries.

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 51.

Tape drives are installed into tape drive slots in the rear of the library. If a tape drive slot is empty, a filler plate must cover the empty slot (see [Figure 5](#) on page 11).

---

**Caution:** Filler plates are required to maintain proper library cooling. Do not run the library with uncovered slots.

---

SAS tape drives have one status LED. Fibre Channel tape drives contain a status and a link LED. For more information on tape drive LEDs, see [Tape Drive/Sled LEDs](#) on page 323.

All tape drives contain only one cable connector.

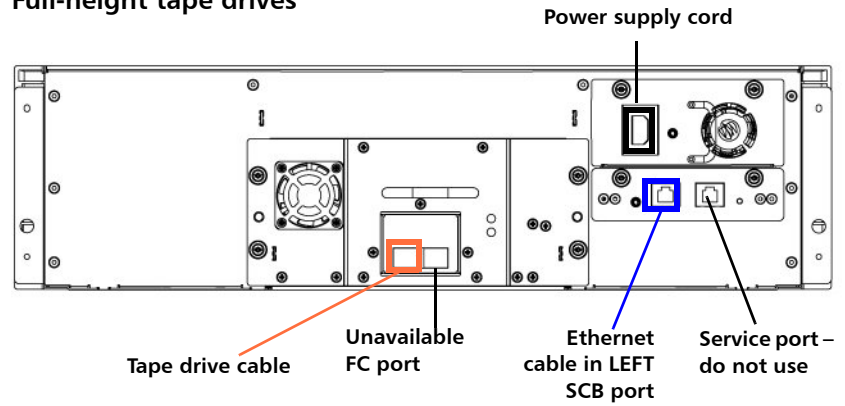
For information on removing and replacing tape drives, see [Removing and Replacing a Tape Drive](#) on page 286.

### Installed Tape Drive Location Coordinates

Installed tape drives have a two-digit location coordinate. These are the coordinates shown in the library configuration report. The first digit is always zero. The second digit indicates the location of the tape drive relative to the other tape drives. The bottommost tape drive has location coordinates [0,1], the next-to-bottom has location coordinates [0,2], and so on.

Figure 4 Scalar i40 Back Panel Components

### Full-height tape drives



### Half-height tape drives

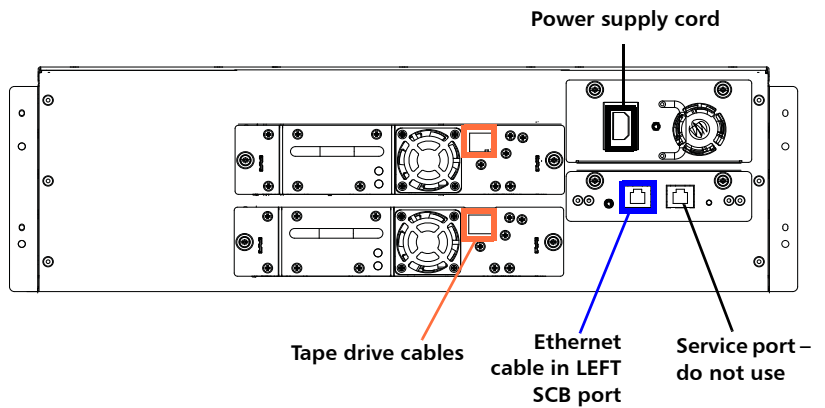
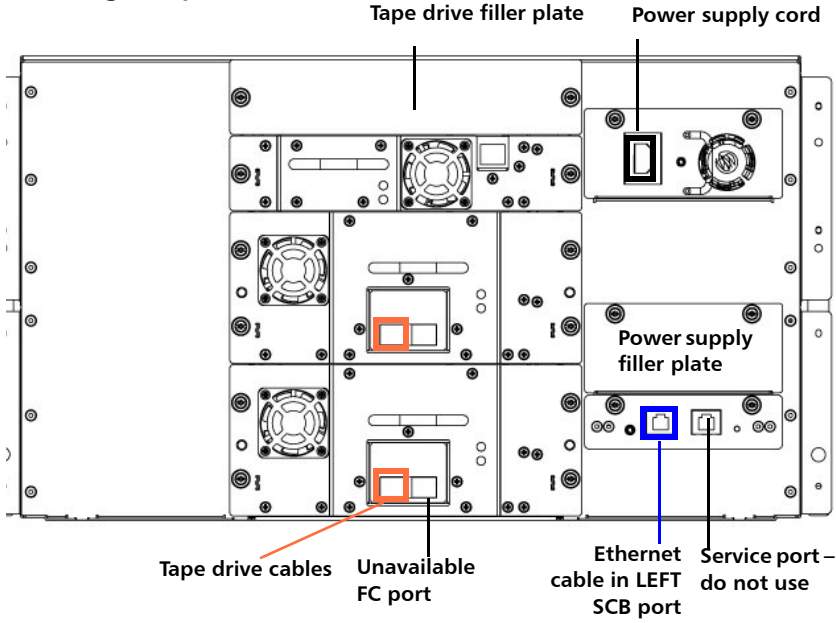
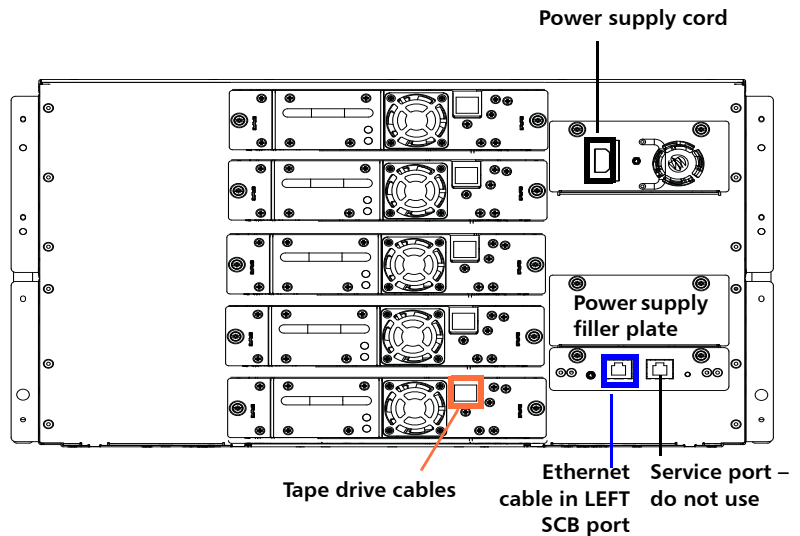


Figure 5 Scalar i80 Back Panel Components

**Full-height tape drives**



**Half-height tape drives**



---

## Standard Features

This section describes several features of Scalar i40 and Scalar i80 libraries.

---

### User Interface

---

The operator panel is located on the front of the library 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 each contain a different user interface and functionality.

See [Chapter 3, 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. If one of the resources is not available due to a failure or other cause, the other partitions and their assigned components are still available. Partitions can also be used to control access to portions of the library by granting permissions to user accounts to access certain partitions (see [Privilege Levels](#) on page 81 and [Creating Local User Accounts on the Web Client](#) on page 82).

For more information on partitions, see [Working With Partitions](#) on page 51.

---

### Control Path Modification

---

The control path tape drive is used to connect a partition to a host application. Only one tape drive can be selected as the control path at one time. By default, the first tape drive assigned to a partition is designated as the control path. In the event that the control path connection to the host application fails, you can select a new control path for the partition. See [Configuring Control Paths](#) on page 67.



---

## Support for WORM

---

Scalar i40 and Scalar i80 tape libraries support WORM (write once, read many) technology. 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:

- [Capacity on Demand \(COD\)](#)
- [Advanced Reporting](#) - includes custom reports and logs and Control Path Failover functionality.
- [Encryption Key Management](#)

For information on how to obtain and install a license key, see [Adding or Upgrading Licensable Features](#) on page 69.

---

## Capacity on Demand (COD)

---

All Scalar i40 and Scalar i80 library configurations ship with the purchased number of slots pre-activated. After the initial purchase of your library, you can activate any remaining inactive slots in your library by purchasing a COD license upgrade.

- The Scalar i40 base configuration has 25 slots activated (these slots comprise the first 5 magazine columns starting from the left front magazine column going clockwise). You can buy a COD license to activate the remaining 15 slots.
- The Scalar i80 base configuration has 50 slots activated (these slots comprise the first 5 magazine columns starting from the left front magazine column going clockwise). You can buy a COD license to activate the remaining 30 slots.

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

---

## Advanced Reporting

---

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.

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

**Control Path Failover (CPF)** - Provides support for configuring the HP LTO-5 drive for control path failover. When control path failover is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever the primary control path drive fails or is inoperable

**Reports** - Listed below are report names. You can view, configure, send via e-mail, and save and reuse report configurations as templates. In addition, you can automatically e-mail any of the reports to designated recipients at specified, scheduled times.

- **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 Tape Alert count for various combinations of tape drives, tape cartridges, and Tape Alert flags. This can help you determine if a problem is due to a specific tape drive or tape cartridge.

**Logs** - Listed below are available logs:

- **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.

For information on how to use the advanced reporting features, see [Advanced Reporting](#) on page 111.

---

## Encryption Key Management

---

The Encryption Key Management (EKM) license enables tape drive transparent encryption using library-managed encryption. The EKM license applies to the entire library, regardless of how many slots are licensed. If you increase the number of slots in your library, your existing license applies to your new library configuration. For more information about EKM, see [Chapter 7, Encryption Key Management](#).





## Chapter 2

# Unpacking the Library

---

Choose a location in which to install the library that is as free from dust as possible. Dust can damage or degrade performance of library components and media.

Refer to the following sections of this manual for important information that you need when installing and setting up your library:

- [Environmental Specifications](#) on page 343
- [Taking ESD Precautions](#) on page 226

---

**Note:** Unpack the library as close to the installation location as possible.

---

- 1 Inspect the outer library packaging for damage. If there is any damage evident on the library packaging, do not continue with the installation and contact Quantum customer support.
- 2 Open the library packing box and remove the kit tray containing the accessory kit and the rail kit (see [Figure 6](#)). Some configurations come with tape drives installed in the library, and some come with tape drives packaged separately. If yours comes with tape drives packaged separately, remove them and set aside for installation later.



---

**WARNING:** Two people are required to safely lift the library out of its packaging or into a rack.

---

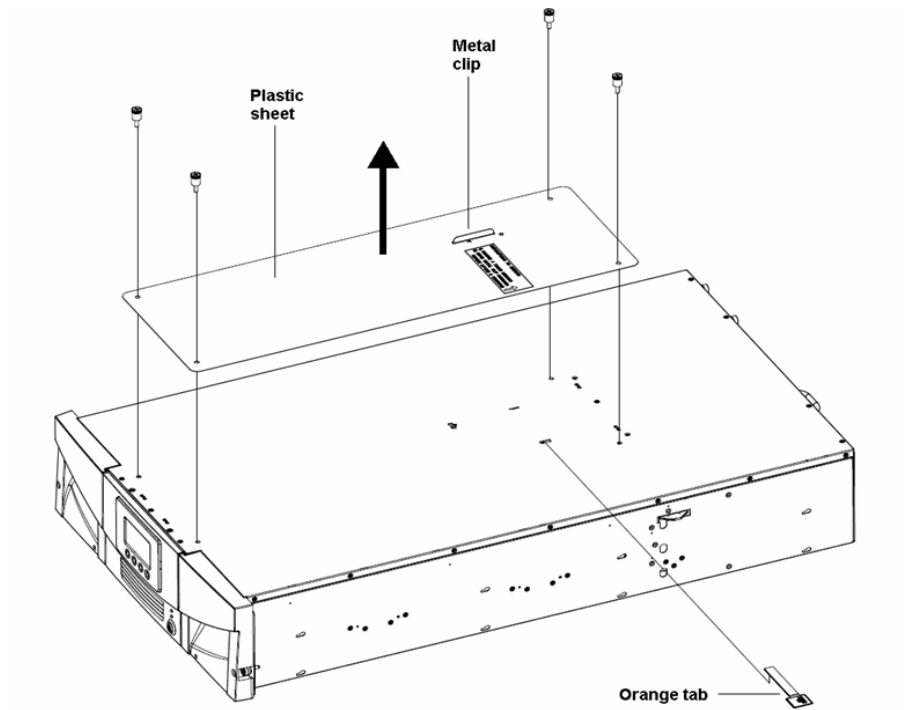
---

**Caution:** Lift the library chassis at the sides. Avoid putting the weight of the library chassis on the front bezel.

---

- 6 Remove the anti-static wrapping from the library. Keep the anti-static wrapping intact so that you can use it later if needed.
- 7 Save the packing box, packaging material, and anti-static wrapping in case you need to move or ship the library in the future.
- 8 Remove the Y-tray restraint. The Y-tray restraint consists of four (4) thumbscrews, a plastic sheet, a small metal clip, and underneath the plastic sheet, an orange restraint tab—located on the top cover of the library. See [Figure 7](#).
  - a Unscrew and remove the four thumbscrews from the top cover (see [Figure 7](#)). Save the thumbscrews in case you need to move or ship the library in the future.
  - b Remove the plastic sheet and metal clip and discard. You will not need to use them again.

Figure 7 Removing the Robot Restraint



- c Remove the orange shipping restraint tab and discard. You will not need to use it again.

---

**Note:** The Y-tray may stay at the top of the library, or it may move downward toward the floor of the library. If it moves downward, you will hear the gears turning as it moves. This is normal.

---

- 9 Once you remove the Y-tray restraint, you may cover the holes in the library top cover with stickers, which are provided in the accessory kit for this purpose. This step is optional and is intended to prevent small objects from accidentally falling into the library through the holes.
- 10 Remove the protective plastic sheet covering the front panel display.





# Chapter 3

## Understanding the User Interface

---

The user interface for the Scalar i40 and Scalar i80 libraries is available in two formats: the operator panel and the Web client. Operations on the library can be performed locally on the operator panel or remotely on your computer using the Web client.

Both the operator panel and the Web client 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, it is recommended that you use the Web client rather than the operator panel to perform most library operations.

This chapter covers:

- [Operator Panel](#)
- [Web Client](#)
- [Menu Trees](#)

---

## Operator Panel

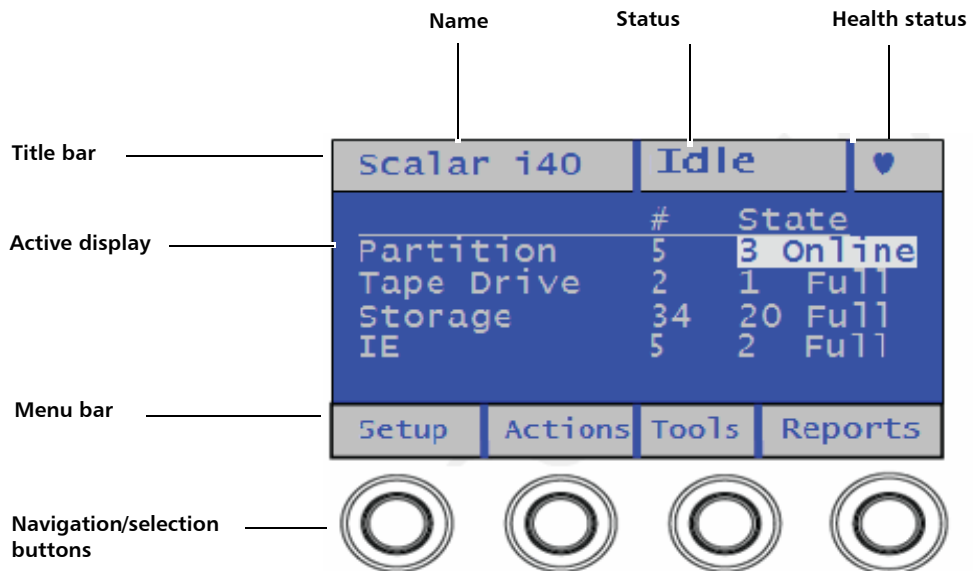
The operator panel is located on the front panel of the physical library. The operator panel screen contains a menu bar with operations that correspond to the four physical buttons below it. The menu operations and button functions change with each screen.

The operator panel home screen refreshes every 5 seconds to provide up-to-date information about library performance.

## Operator Panel Layout and Functions

You can choose your desired operator panel home screen that displays on the local user interface—the default home screen or the alternate home screen that allows easy I/E unlock access. [Figure 8](#) and [Figure 9](#) depict these screen options; [Table 2](#) describes the operator panel functions.

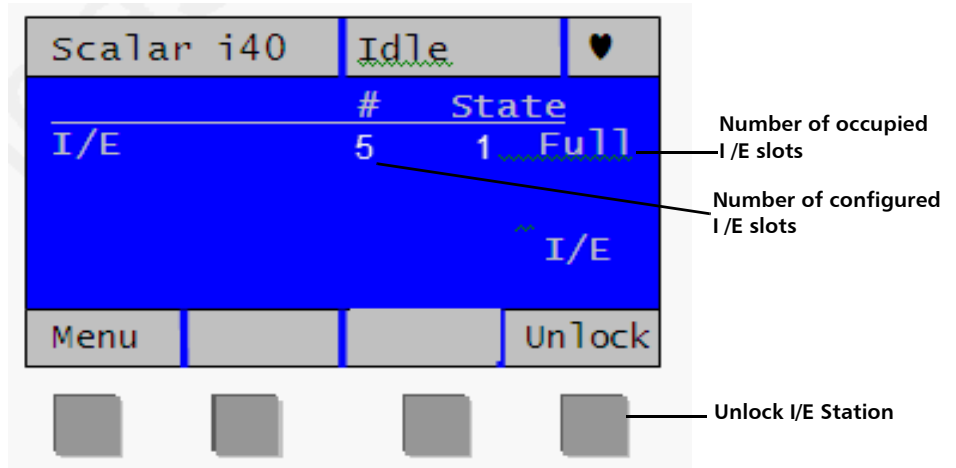
Figure 8 Operator Panel User Interface - Home Screen



You can choose to change the view of the home screen for easy I/E unlock access. Refer to [Changing Operator Panel Home Screen View](#) on page 109.

Figure 9 Operator Panel User Interface - Alternate Home Screen

### Scalar i40



### Scalar i80

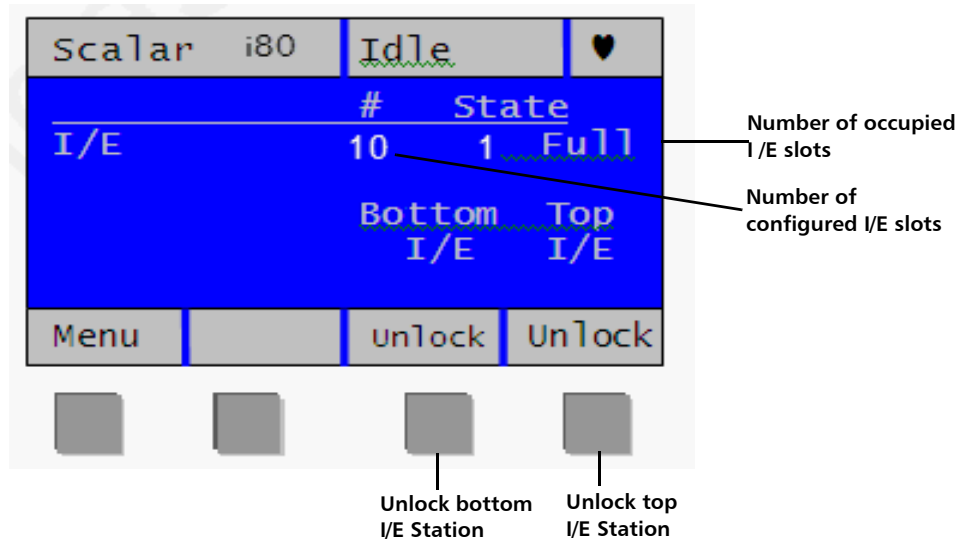





Table 2 Operator Panel  
Functions

Operator Panel Element	Description
Title bar	The title bar is present on every screen, and contains three fields: name, status, and health status.
Name	<p>The name field displays a description of the current view. It changes depending on the menu selection.</p> <ul style="list-style-type: none"><li>• On the home screen, the field displays the library type (Scalar i40 or Scalar i80).</li><li>• On active pages, the field displays the name of the main menu (Setup, Actions, Tools, Reports).</li><li>• When a message displays, the field displays the message type (Success, Completed, Information, FAILURE, NOTICE). Failure messages will blink.</li></ul>

Operator Panel Element	Description
Status	<p>The status field displays the current state or operation being performed by the robot. If the robot is not idle, the status will blink. status can be any of the following:</p> <ul style="list-style-type: none"> <li>• Initializing — The is currently in the process of initializing.</li> <li>• Autoleveling — The robotics hardware is being autoleveled.</li> <li>• Homing — The robot is performing a home operation.</li> <li>• Teaching — The robot is performing a teach operation.</li> <li>• Calibrating — The robot is performing a calibration operation.</li> <li>• Scanning — The robot is performing an inventory operation.</li> <li>• Unlocking — The robot is in the process of unlocking a magazine.</li> <li>• Move Media — The robot is moving media from one location to another.</li> <li>• Loading — The robot is in the process of moving a tape to load into a tape drive.</li> <li>• Unloading — The robot is in the process of unloading a tape drive and returning it to the source location.</li> <li>• Idle — The robot is ready and idle.</li> <li>• Not Ready — The robotics system is not ready.</li> </ul>

Operator Panel Element	Description
Health status	<p>The health status field displays an icon representing the health of the library.</p> <p> <b>Heart</b> — Library is in good health (no open or unopened diagnostic tickets are present).</p> <p> <b>Triangle</b> — Library health is degraded (library contains open or unopened low- or high-priority diagnostic tickets).</p> <p> <b>Exclamation point</b> — Immediate attention is required (library contains open or unopened urgent diagnostic tickets).</p>
Active display	<p>The active display provides information or menu items according to the selected menu item or operation.</p> <p>The default home screen displays the number and state of partitions, tape drives, storage slots, and I/E slots.</p> <p>The alternate home screen displays the number and state of the I/E slots, and provides access to unlock I/E stations.</p>
Menu bar	<p>The menu bar displays the function associated with each of the navigation/selection buttons. The button function changes with each menu. Common functions are navigation (up, down, left, right, next) and menu selection (select, apply, exit, yes, no, cancel).</p>
Navigation/ Selection Buttons	<p>The physical buttons enable you to navigate menus and start and stop library operations according to the functions listed in the button bar. Not all buttons are functional for every operation. See <a href="#">Navigating and Editing on the Operator Panel</a> on page 27 for more information.</p>

## **Navigating and Editing on the Operator Panel**

You use the four navigation/selection buttons exclusively to move through the menus and commands on the operator panel.

From the default home screen, the menu bar lists the four main menu headings. From the alternate home screen, you can select Menu to return to the default home screen to access the four main menu headings.

Press the button corresponding to a menu item to bring up the list of sub-menu items. The item you are currently on is highlighted. Press the buttons corresponding to **Up**, **Down**, **Left**, or **Right** to navigate to a desired menu item. As you move through the items, the highlighting moves with you so you always know which item you are on. Press the button corresponding to **Select** to select a highlighted item or action. This in turn brings up either another sub-menu, a screen where you can modify settings or perform operations, or a screen displaying information.

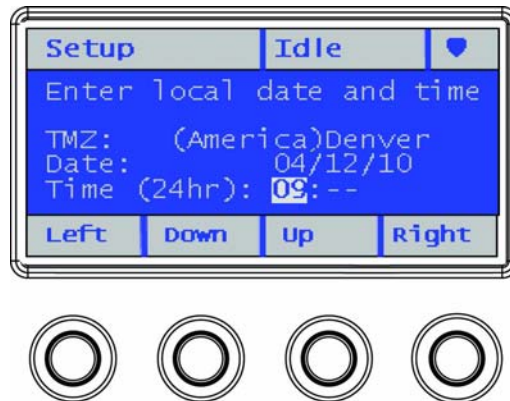
To edit a modifiable field, such as date, time, licenses, IP address, and so on, use the **Left** and **Right** buttons to move through the field, one segment at a time (for license keys and passwords, you will move one digit or letter at a time). Use the **Up** and **Down** buttons to change the value of each segment. When you reach the value you want, press the **Right** button. As you press **Right**, the value fills in and you go to the next segment. To edit a previous entry, press the **Left** button until you reach the entry and edit as before. For multiple fields, continue to press **Right** after each entry until you reach the last entry. At this point, the **Right** button designation changes to **Apply**. Press the **Apply** button. The new information displays. Press **Exit** to exit. For an example, see [Figure 10](#) on page 28.

To scroll through a list of items, or to edit letters and numbers, you can press the appropriate button repeatedly to scroll one item at a time, or you can hold the button down for fast scrolling through the available options.

To exit a screen, press the **Exit** button.

To cancel an operation without saving any changes, press the **Cancel** button. If you are in the middle of making changes, repeatedly press the **Left** button until you are back at the first field on the screen, then press the **Cancel** button.

Figure 10 Using the Buttons to Set the Date and Time



## Web Client

The Web client interface is accessible from supported Web browsers (see [Supported Internet Browsers](#) on page 347).

To access the library from a remote location, the library must be connected to your network via an Ethernet connection. Simply enter the library's IP address in your Internet browser bar to access the Web client. See [Configuring Network Settings](#) on page 40 for information on setting the network configuration settings for remote use.

### Tips

Keep the following tips in mind when using the Web client:

- You must disable Web browser popup blockers to use the Web client interface and the library's online Help. Add the Scalar i40 or Scalar i80's Internet Protocol (IP) address to the list of trusted/allowed sites on your Scalar i40- or Scalar i80-supported browser, so the Web client pages will automatically refresh.
- Do not use your Internet browser **Back** button to navigate the Web client pages. Instead, use the buttons provided within the Web client.



- Optimum screen resolution for viewing using a Windows operating system is 96 DPI. If your resolution is set higher, certain screen messages may not display as intended. To change screen resolution, show the desktop, right click to display the **Properties** window, and click **Settings > Advanced**.
- 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. Clicking the close button (X) in the upper-right corner of the Web client closes the browser window but does not log you out.

---

## Sorting Information in Tables

---

You can sort information displayed in tables if the table column heading is bold. Click the column heading and the information will sort. Click again to toggle from ascending to descending.

---

## Web Client Layout and Functions

---

[Figure 11](#) on page 30 shows the Web client interface. [Table 3](#) on page 31 explains the Web client interface elements.

Figure 11 Web Client User Interface - Home Page

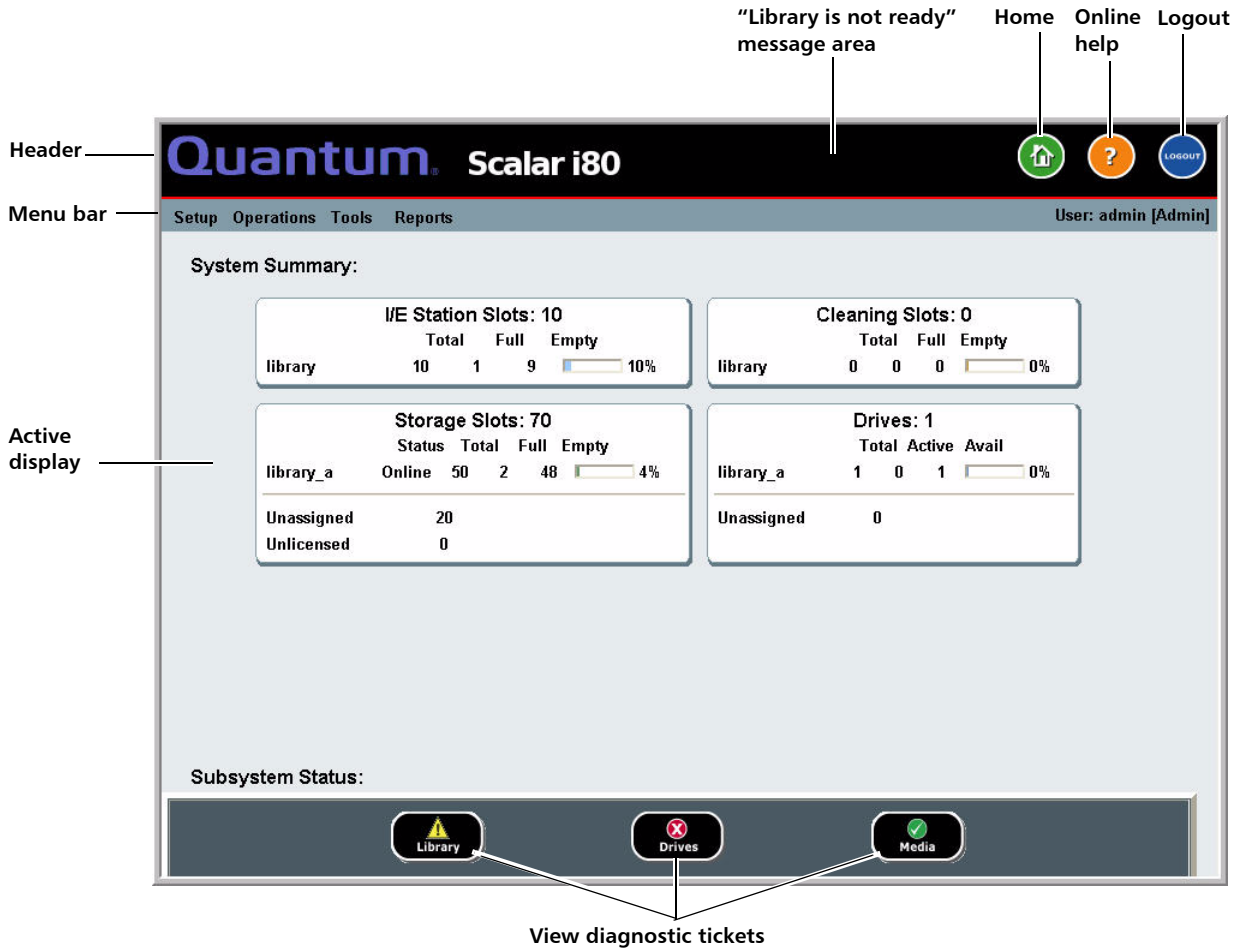





Table 3 Web Client Screen Elements

Web Client Element	Description
Header	<p>The header is present on all pages and contains the library type (Scalar i40 or Scalar i80) and three buttons:</p> <ul style="list-style-type: none"> <li> <b>Home</b> — Brings you to the home page.</li> <li> <b>Help</b> — Displays the online help.</li> <li> <b>Logout</b> — Logs out of the current session.</li> </ul> <p>A message in the header alerts you when the robot is not ready to perform library functions. See <a href="#">Troubleshooting Library “Not Ready” Messages</a> on page 318 for more information on “Library Not Ready” messages displayed in the header.</p>
Menu bar	<p>Displays the available menu choices. The choices vary depending on login privileges.</p> <p>The far right of the menu bar also displays the name of the logged-in user, with the associated privilege level indicated in brackets.</p> <p>If a menu item selected has a sub-menu, then &gt; is displayed to the right of the item.</p>
Active display	<p>The active display provides information or menu items according to the selected menu item or operation.</p>

## Web Client Home Page

The home page displays status and health information in the active display portion of the window (see [Figure 11](#) on page 30). See [System Summary](#) and [Subsystem Status](#) below for more information.

## System Summary

The system summary is available on the home page of the Web client.

It provides tabular data on the capacity of the library's partitions, slots, and tape drives. It also displays whether partitions are online or offline (in the Storage Slots section). The current user's login privileges determine which partitions are displayed (see [Privilege Levels](#) on page 81).

---

## 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 diagnostic tickets that report problems in the subsystems.

The three subsystems are:

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

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

-  **Green (check mark)** — No diagnostic tickets exist, or, if any tickets do exist, they have all been closed.
-  **Yellow (exclamation point)** — The library contains open or unopened, low- or high-priority diagnostic tickets.
-  **Red ("X" mark)** — The library contains open or unopened urgent diagnostic tickets.

If the color of a subsystem button is red or yellow, you can click the button to display the corresponding **Diagnostic Tickets** screen. This screen lists library, drives, or media tickets, depending on which button was selected. See [About Diagnostic Tickets](#) on page 312 for more information.

## Menu Trees

The following menus organize operations and commands into logical groupings:

- The **Setup** menu consists of commands that users with administrator privileges can use to set up and configure various aspects of the library, including partitions, I/E station slots, cleaning slots, control paths, network settings, drive settings, users, notifications, date and time, licenses, library registration, and e-mail.
- The **Operations/Actions** 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, lock or unlock the I/E station, log out, and shut the library down. The menu is called **Actions** on the operator panel and **Operations** on the Web client.
- The **Tools** menu consists of commands that you can use to maintain your library such as viewing diagnostic tickets, generating diagnostic logs, identifying drives, configuring the internal network, saving and restoring the library configuration, setting system and security settings, and updating firmware, and performing library diagnostics.
- The **Reports** menu provides various kinds of library information.

Administrators have access to all menu commands, but users' privileges are more limited.

[Figure 12](#) lists the operator panel menus. [Figure 13](#) lists the Web client menus.

Figure 12 Operator Panel  
Menus

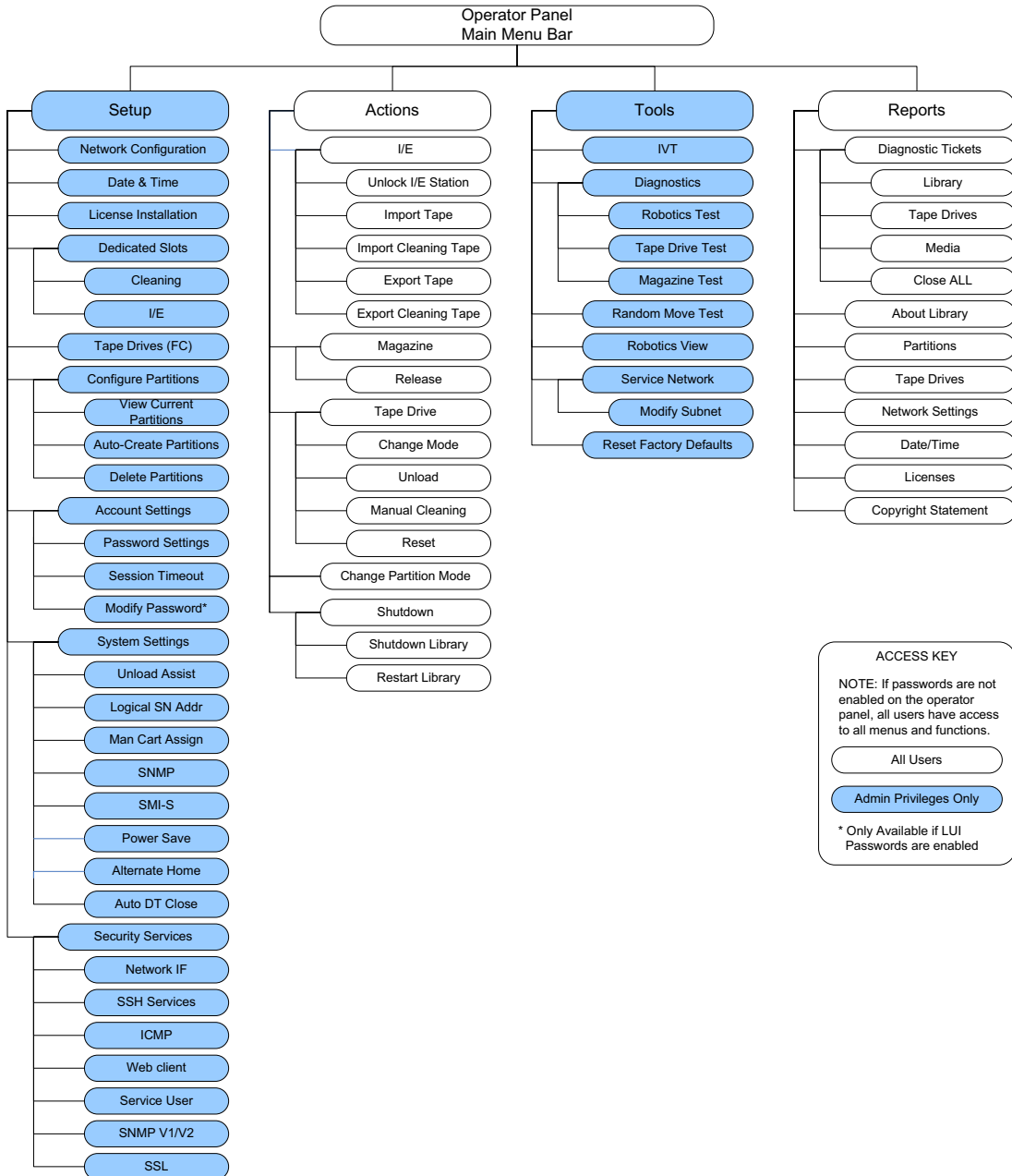
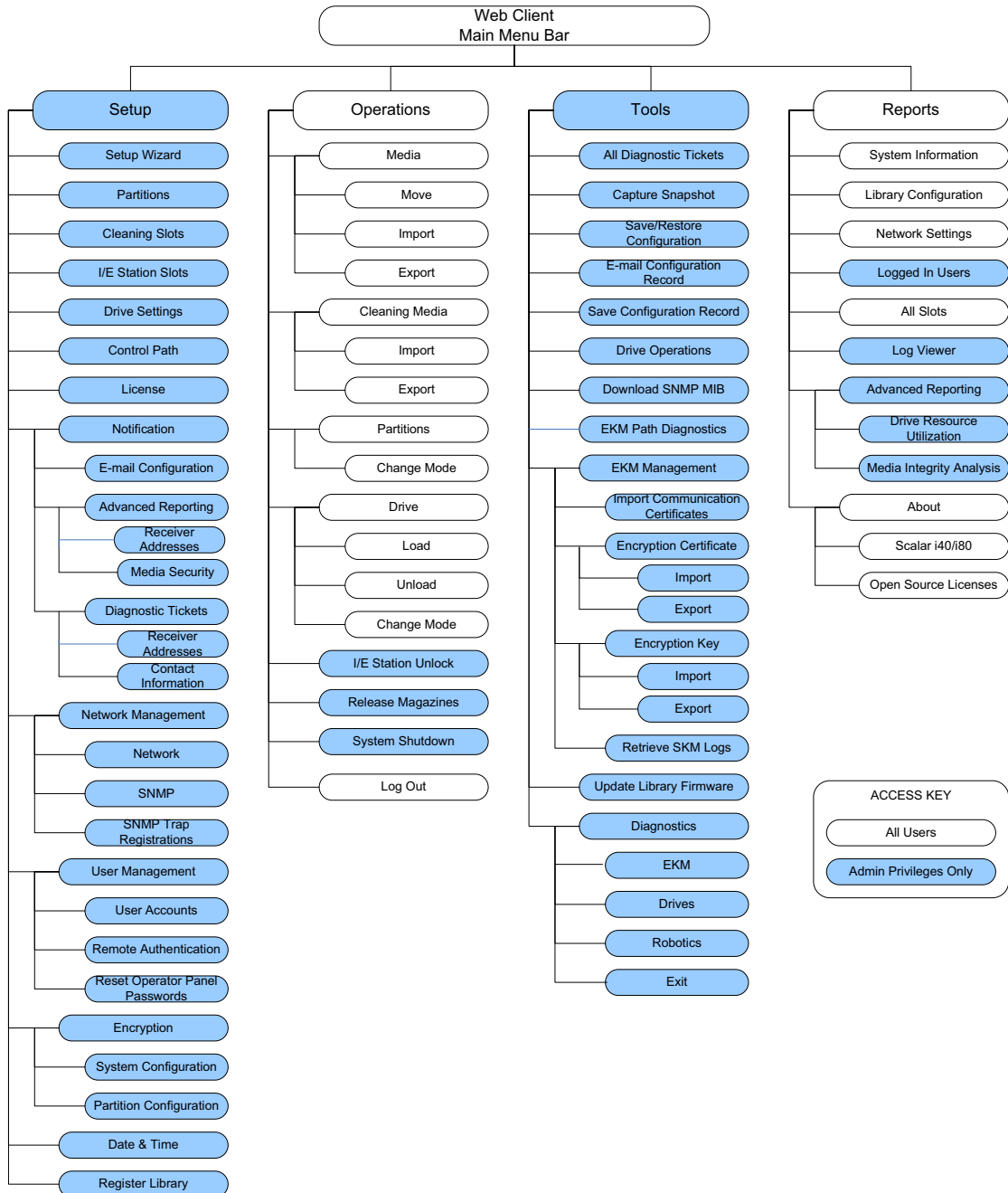
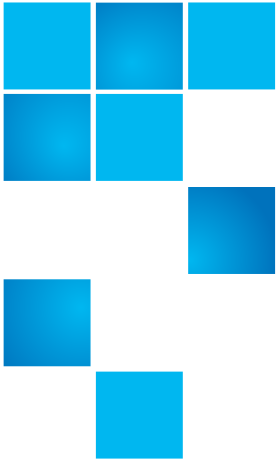


Figure 13 Web Client Menus









## Chapter 4

# Configuring the Library

---

A Setup Wizard is available to assist you with the initial configuration of the library. The Setup Wizard, however, contains only a subset of configuration tasks. The operator panel and Web client menus provide access to all configuration options that are included in the Setup Wizard and many that are not.

This chapter covers the Setup Wizard and all of the other configuration options. Paths to open the appropriate screens on both the operator panel and the Web client are given for each task. (For complete menu trees, see [Menu Trees](#) on page 33.)

---

**Note:** These 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.

---

---

**Caution:** Always save the library configuration after modifying a configurable item. This will allow you to restore the most current settings if necessary. See [Saving and Restoring the Library Configuration](#) on page 107.

---

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

---

This chapter covers:

- [Using the Setup Wizard](#)
- [Configuring Network Settings](#)
- [Configuring SNMP Settings](#)
- [Setting the Date, Time, and Time Zone](#)
- [Working With Partitions](#)
- [Configuring Cleaning Slots](#)
- [Configuring I/E Station Slots](#)
- [Configuring Tape Drive Parameters](#)
- [Configuring Control Paths](#)
- [Adding or Upgrading Licensable Features](#)
- [Working With E-mail Notifications](#)
- [Configuring the Library E-Mail Account](#)
- [Setting Customer Contact Information](#)
- [Configuring the Service Port](#)
- [Working With Local User Accounts and Passwords](#)
- [Working With LDAP User Accounts \(Remote Authentication\)](#)
- [Setting the Session Timeout](#)
- [Configuring System Settings](#)
- [Configuring Security Settings](#)
- [Saving and Restoring the Library Configuration](#)
- [Registering the Library](#)
- [Changing Operator Panel Home Screen View](#)

## Using 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 displays when you first install your library. It displays only once, with the following exceptions: it will also display after SCB replacement, resetting factory defaults, or downgrading library firmware.

When the Setup Wizard displays on the operator panel, you must either complete the Setup Wizard or cancel out of it. If you cancel, you accept the library's default configuration (see [Default Configuration](#) on page 40). You can modify the configuration at any time later using the Setup Wizard on the Web client, or by using the Setup menu options from the operator panel or Web client.

### Operator Panel

The Setup Wizard on the operator panel is covered in detail in the *Scalar i40 and Scalar i80 Quick Start Guide*.

### Web Client

To access the Setup Wizard, click **Setup > Setup Wizard**. Work through several screens that enable you to add licenses; set date, time, and time zone; configure cleaning slots; configure I/E station slots; and auto-create partitions.

## Default Configuration

The library comes with a default configuration, which you can modify at any time. The default configuration is as follows:

Feature	Default Configuration
Library host name	library
Network settings	IPv4, DHCP enabled IPv6 disabled
Number of partitions	Equal to the number of unique tape drives — based on interface type (Fibre Channel or SAS) and drive generation (LTO-4, LTO-5) — not currently assigned to a partition. Storage slots are divided equally among the partitions.
Number of I/E station slots	5
Number of cleaning slots	0

## Configuring Network Settings

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

---

**Note:** Changing the network settings may interrupt the library connection and library communication. Your current browser session may become invalid. If this happens, you must close your browser and then restart it to reconnect to the library with your new configuration settings.

---

**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 left-most Ethernet port of the system control board (SCB) located on the back of the library (see [Figure 4](#) or [Figure 5](#) on page 11). Make sure the other end of the Ethernet cable is installed in the appropriate LAN port on your LAN.

---

You can configure the following network settings:

- [Library Host Name](#)
- [DHCP](#)
- [IP Addresses](#)
- [Default Gateway, Subnet Mask, Network Prefix, and DNS Addresses](#)

Some settings are only available on the Web client; others are only available on the operator panel, as described below.

---

## Library Host Name

---

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

You can view, but not modify, the host name on the operator panel. To modify the host name, you must use the Web client.

### Web Client

- 1 Select **Setup > Network Management > Network**.
- 2 Type a name in the **Host Name** field, and click **Apply**.

---

## DHCP

---

DHCP is enabled by default. When DHCP is enabled, the library obtains an IP address automatically. If DHCP is disabled, you must manually enter an IP address, default gateway, and subnet mask/net prefix. You can enable/disable DHCP from the operator panel or Web client.

### Operator Panel

Select **Setup > Network Configuration**.

### Web Client

Select **Setup > Network Management > Network**.

---

## IP Addresses

---

The library can support both IPv4 and IPv6 network settings at the same time. For more details, see the bullets below.

---

**Caution:** If you change the IP address on your library, make sure to change it on any host applications that access the library.

---

---

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

---

- **IPv4 Addresses** — The library always supports IPv4 network settings. The library can support either a DHCP-obtained or a static IPv4 address.

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** — IPv6 is disabled by default and can only be enabled/disabled via the operator panel. Once enabled, you must use the Web client to modify the address. Unlike IPv4, the library can support both DHCP-obtained and static IPv6 addresses at the same time.

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.

You can configure IPv4 addresses on the operator panel or Web client. You can set the library to use IPv6 via the operator panel, but you must use the Web client to configure a static IPv6 address.

## Operator Panel

- 1 Select **Setup > Network Configuration**.
- 2 Modify the IP address using the method described in [Navigating and Editing on the Operator Panel](#) on page 27.

## Web Client

Select **Setup > Network Management > Network**.

---

### Default Gateway, Subnet Mask, Network Prefix, and DNS Addresses

---

These settings have specific configuration requirements, as follows:

- **Default Gateway** — The IP address of the default gateway for your portion of the Ethernet network. For IPv4, this setting can only be changed if DHCP is disabled.
- **Subnet Mask (IPv4 only)** — Available only if DHCP is disabled.
- **Network Prefix (IPv6 only)**. Can be entered only on the Web client.
- **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.

## Operator Panel

- 1 Select **Setup > Network Configuration**.
- 2 Modify the fields using the method described in [Navigating and Editing on the Operator Panel](#) on page 27.

## Web Client

Select **Setup > Network Management > Network**.

---

# Configuring SNMP Settings

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

For more information about SNMP, see the *Scalar i40 and Scalar i80 Basic SNMP Reference Guide* (6-66773-xx).

For information on integrating MIBs with an SNMP management application, contact your network management application vendor.

---

## 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** — User Datagram Protocol for IPv4.
  - **UDP6** — User Datagram Protocol for IPv6.
  - **TCP** — Transmission Control Protocol for IPv4.
  - **TCP6** — Transmission Control Protocol for IPv6.
- **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 [Default Gateway, Subnet Mask, Network Prefix, and DNS Addresses](#) on page 43.
- **Port** — the port number of the external application you want to register. The default port number for an external application is 162.

You can only perform these functions from the Web client.

## Web Client

- 1 Select **Setup > Network Management > SNMP Trap Registrations**.
- 2 Click one of the following buttons to perform these actions:
  - **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** — Deletes a selected IP address and port number.
  - **Test** — This test simply sends the traps; it does not check to see if they were received. You must check the external management applications to verify that the traps were received.

---

## Enabling SNMP Versions

---

The library supports SNMP v1, v2c, and v3.

You can enable or disable support for SNMP v1 and v2c. They are enabled by default. 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.

### Operator Panel

- 1 Select **Setup > Security Services > SNMP V1/V2**
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Press **Exit**.

### Web Client

- 1 Select **Setup > Network Management > SNMP**.
- 2 Select the **SNMP V1 and V2c** check box (under **New Settings**) to enable SNMP v1 and v2c. Clear the **SNMP V1 and V2c** check box to disable SNMP v1 and v2c.

---

## Enabling SNMP Authentication Traps

---

The library allows you to 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 the external management application, indicating the authentication failure. SNMP authentication traps are disabled by default.

## Web Client

- 1 Select **Setup > Network Management > SNMP**.
- 2 Select the **SNMP Authentication Traps** check box (under **New Settings**) to enable SNMP authentication traps. Clear the **SNMP Authentication Traps** check box to disable SNMP authentication traps.

---

## 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.

You can modify the SNMP community string from the Web client only.

## Web Client

- 1 Select **Setup > Network Management > SNMP**.
- 2 Enter a new community string in the **SNMP Community** text box under **New Settings**.
- 3 Click **Apply**.

---

## Downloading the SNMP MIB

---

The SNMP Management Information Base (MIB) is for library customers, partners, third-party management software developers, and other parties interested in integrating the Scalar i40 and Scalar i80 with commercial management frameworks. The Scalar i40 and Scalar i80 libraries support SNMP by publishing a MIB that can be queried to obtain the status of the library and many of its individual components.

Administrators can download the SNMP MIB from the library. The MIB can then be installed on an SNMP external management application.

For more information about the library MIB, see the *Scalar i40 and Scalar i80 Basic SNMP Reference Guide* (6-66773-xx) or contact Quantum Support.

For information on integrating MIBs with an SNMP management application, contact your network management application vendor.

### Web Client

- 1 Select **Tools > Download SNMP MIB**.
- 2 Save the file to a known location.

---

## Setting the Date, Time, and Time Zone

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

If you enable NTP, you must also configure the IP address of at least one NTP server. Contact your network administrator for NTP server IP address information.

You can configure the date and time on both the operator panel and the Web client. You can view the time zone on the operator panel, but must use the Web client to change it. You can only configure NTP settings on the Web client.

---

**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.

---

---

## Setting the Date and Time Manually

---

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.

### Operator Panel

- 1 Select **Setup > Date & Time**.
- 2 Modify the date and time using the method described in [Navigating and Editing on the Operator Panel](#) on page 27.

### Web Client

- 1 Select **Setup > Date & Time**.
- 2 Refer to the library Web client online help for detailed instructions. To view the help, click the **Help** icon in the upper right corner of the screen.



---

## 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 (or host names, if DNS is configured) of at least one NTP server must be configured on the library. Contact your network administrator for NTP server IP address information.

---

---

**Caution:** Using two NTP servers can cause incorrect time calculations. You should use either one NTP server, or more than two, but not exactly two.

---

---

Details on NTP settings include:

- At least one NTP server must be configured and available.
- NTP is enabled on the **Date & Time** screen. When NTP is enabled, you cannot manually configure date and time. For more information on setting date and time manually, see [Setting the Date and Time Manually](#) on page 49.
- You can enter an IP address (or host name, if DNS is configured) for the NTP servers.
- NTP server IP addresses must be entered in the proper format. See [Configuring Network Settings](#) on page 40 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.

### Web Client

- 1 Select **Setup > Date & Time**.
- 2 Refer to the library Web client online help for detailed instructions. To view the help, click the **Help** icon in the upper right corner of the screen.



---

## Setting the Time Zone

---

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

If your time zone does not appear on the list, or if 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 via the Web client.

## Web Client

- 1 Select **Setup > Date & Time**.
- 2 Refer to the library Web client online help for detailed instructions. To view the help, click the **Help** icon in the upper right corner of the screen.



---

## Setting Daylight Saving Time

---

If you selected your time zone from the drop-down list (see [Setting the Time Zone](#) on page 50), 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.

## Web Client

- 1 Select **Setup > Date & Time**.
- 2 Refer to the library Web client online help for detailed instructions. To view the help, click the **Help** icon in the upper right corner of the screen.



---

# 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.

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 (Fibre Channel or SAS) and media generation (LTO-4, LTO-5). When you automatically create partitions, you add to the number of existing partitions. You can create partitions automatically on either the operator panel or the Web client. For more information, see [Automatically Creating Partitions](#) on page 53.
- **Manually** — An administrator can create partitions one at a time. Creating partitions manually gives you more control over resource allocation. When you manually create partitions, you add to the number of existing partitions. You can only create partitions manually on the Web client. For more information, see [Manually Creating Partitions](#) on page 54.

You can modify a partition if you need to change its settings. For example, the partition name, emulation type, media barcode format (to report to host), and number of assigned tape drives and slots can be modified. For information on modifying partitions, see [Modifying Partitions](#) on page 56.

When a partition is no longer needed, it can be deleted. For information on deleting partitions, see [Deleting Partitions](#) on page 57.

Administrators can create, delete, and control access to all library partitions. Users can be given access to only certain partitions and denied access to others. For information on changing partition access for users, see [Changing Access to Partitions](#) on page 59.

Details on partitions include:

- A partition consists of one tape drive and one slot at a minimum. The tape drive or slot cannot be shared with another partition.
- The default configuration for the library is one partition per unique tape drive installed in the library, based on interface type (Fibre Channel or SAS) and media generation (LTO-4, LTO-5).
- 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.
- The minimum number of partitions is one (the minimum may be higher when automatically creating partitions; see [Automatically Creating Partitions](#) on page 53 for details).



- Import/export (I/E) station slots are shared between all partitions. Partitions take temporary ownership of I/E station slots performing certain operations, such as importing and exporting cartridges.

---

## Automatically Creating Partitions

---

Automatic partitioning assigns available library resources proportionately among the partitions, grouping tape drives according to their interface type (Fibre Channel or SAS) and media generation (LTO-4, LTO-5).

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 56 and [Deleting Partitions](#) on page 57.

You can select the number of partitions to create. The maximum number of partitions that you can create is equal to the number of tape drives in the library that are not currently assigned to a partition. The minimum number of partitions you can create automatically is the number of unique tape drives — based on interface type (Fibre Channel or SAS) and media generation (LTO-4, LTO-5) — not currently assigned to a partition. For example, if your library contains two tape drives, a Fibre Channel HP LTO-4 and a Fibre Channel HP LTO-5, two partitions is the minimum because the tape drive generations are different.

You cannot mix tape drive interface types or media generations within a partition when creating partitions automatically. If you wish to do so, you must create the partition manually (see [Manually Creating Partitions](#) on page 54).

When the library automatically creates partitions, it assigns the first tape drive in the partition as the control path. You can change the control path at any time. See [Configuring Control Paths](#) on page 67 for more information.

Before automatically creating partitions, verify that all tape drives are unloaded and that all cartridges are in their appropriate storage slots. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 161.

## Operator Panel

- 1 Select **Setup > Configure Partitions > Auto-Create Partitions**.
- 2 Use the **Up** and **Down** buttons to select the number of partitions you want to create. (If the **Up** and **Down** buttons are not available, you do not have available resources. Modify or delete partitions to create resources.)
- 3 Press **Apply**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Web Client

- 1 Select **Setup > Partitions**.
- 2 Click **Automatic**. (If the **Automatic** button is not visible, you do not have available resources. Modify or delete partitions to create resources.)

The **Automatically Create Partitions** screen displays.

By default, the library applies the Scalar i40-i80 library emulation type and Standard media barcode format to each partition. You can change these settings by modifying the partition after it has been created (see [Modifying Partitions](#) on page 56).

- 3 Using the **Partitions** drop-down list, select the number of partitions to create.
- 4 Click **Apply**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Manually Creating Partitions

---

You can manually create 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 tape drives in the library.

The library must contain at least one unallocated tape drive and one unallocated slot to manually create a partition. If no unallocated tape drives or slots exist, you must modify or delete partitions to free resources. For more information, see [Modifying Partitions](#) on page 56 and [Deleting Partitions](#) on page 57.

When the library creates partitions, it assigns the first tape drive in the partition as the control path. You can change the control paths at any time. See [Configuring Control Paths](#) on page 67 for more information.

Before creating partitions, verify that all tape drives are unloaded and that all cartridges are in their appropriate storage slots. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 161.

You can create partitions manually only on the Web client.

## Web Client

- 1 Select **Setup > Partitions**.
- 2 Click **Manual**.
- 3 Type a name to describe the new partition into the **Enter Name** text box.
- 4 Select one of the following emulation types from the **Emulation Type** drop-down list:
  - **Scalar i40-i80** (default)
  - **ADIC Scalar i500**
  - **Quantum Scalar i500**
  - **Quantum Scalar i2000**
  - **ADIC Scalar i2000**
- 5 Select one of the following media barcode formats (for reporting to host) from the **Set Media Barcode Format** drop-down list:
  - **Standard Six** — Six character barcode number with or without a one or two-character media ID; for example, "XXXXXX" or "XXXXXXL4". Only the six character barcode is reported to the host.
  - **Plus Six** — Six character barcode number followed by a media ID; for example, "XXXXXXL3". Six character barcode and media ID are reported to the host.

- **Extended** — Five to 15 characters total, including a barcode number and optional media ID. All characters are reported to the host, regardless of having a media ID or not. If a media ID is included, the label must have a five to 13 character barcode followed by a media ID; for example, “XXXXXL2” or “XXXXXXXXXXXXXXXXL2”. If a media ID is not included, the label must have a five to 15 character barcode; for example, “XXXXX” or “XXXXXXXXXXXXXXXXXX”.
  - **Media ID Last** — Five to 13 character barcode number followed by media ID; for example, “XXXXXXXXXXXXXXXXL4”. The media ID is reported to the host last.
  - **Media ID First** — Five to 13 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”.
  - **Standard (default)** — Five to 15 characters total, including a barcode number and optional media ID. The media ID is not reported to the host. If a media ID is included, the label must have a five to 13 character barcode followed by a media ID; for example, “XXXXXL3” or “XXXXXXXXXXXXXXXXL3”. If a media ID is not included, the label must have a five to 15 character barcode; for example, “XXXXX” or “XXXXXXXXXXXXXXXXXX”.
- 6 Type the number of slots to assign to the new partition into the **Enter Number of Slots** text box.
  - 7 Under the **Select Drives** section, assign one or more available tape drives to the partition by selecting the check box located to the left of the tape drive.
  - 8 Click **Apply**.
  - 9 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Modifying Partitions

---

You can modify partition settings any time after a partition is created. For example, you can modify the name, emulation type, media barcode format, and number of assigned tape drives and slots.

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

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 [Configuring Control Paths](#) on page 67.

Before modifying partitions, verify that all tape drives are unloaded and that all cartridges are in their appropriate storage slot location. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 161.

You can modify partitions only on the Web client.

### Web Client

- 1 Select **Setup > Partitions**.
- 2 Select a partition and click **Modify**.
- 3 Modify any of the settings. For a description of what each setting means, see [Manually Creating Partitions](#) on page 54.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Deleting Partitions

---

A partition can be deleted when it is no longer needed. After a partition is deleted, its resources (tape drives and slots) become unassigned and can be used to create new partitions or added to existing partitions.

Before deleting a partition, unload cartridges from the tape drives within the partition and then export all cartridges from the partition. Remove the cartridges from the I/E station after exporting them. For information on unloading tape drives, see [Unloading Tape Drives](#) on page 161. For information on exporting cartridges, see [Exporting Tape Cartridges](#) on page 158s. You can also remove cartridges by releasing the magazine and removing them by hand (see [Releasing Magazines](#) on page 148). If you do this, be sure to only remove cartridges assigned to that partition (see [Viewing the Library Configuration Report](#) on page 210).

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 any library operations. For information on how to assign a user to another partition, see [Changing Access to Partitions](#) on page 59.

---

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

---

You can delete partitions on both the operator panel and the Web client.

### Operator Panel

- 1 Select **Setup > Configure Partitions > Delete Partition**.
- 2 If more than one partition is configured on the library, use the **Up** and **Down** buttons to select a partition from the list.
- 3 Press **Delete**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

### Web Client

- 1 Select **Setup > Partitions**.
- 2 Select a partition and click **Delete**.
- 3 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

### Viewing the Current Partitions

---

You can view basic details about all of your partitions, including online/offline status, control path tape drive, number of tape drives in the partition, number of storage slots, and number of I/E station slots available to the partition.

## Operator Panel

- 1 Select **Reports > Partitions** (alternatively, select **Setup > Configure Partitions > View Current Partitions**).
- 2 If more than one partition is configured on the library, select a partition and press **Select**.

## Web Client

You can view partition information in several places:

- Library home page (see [Web Client Home Page](#) on page 31)
- Library configuration report (see [Viewing the Library Configuration Report](#) on page 210).
- Partition modification screen (select **Setup > Configure Partitions**, select a partition, and click **Modify**).

---

## Changing Access to Partitions

---

An administrator can control which partitions a specified user can access by modifying the user's account on the Web client. For more information, see [Working With Local User Accounts and Passwords](#) on page 79.

## Web Client

Select **Setup > User Management > User Accounts**.

---

## 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 local or remote user interface.

Changing the partition mode changes whether or not the specified partition is online or offline to the host application. Changing a partition mode using the library interface may affect your host application. See your host application documentation for more information.

---

**Note:** The library automatically turns partitions offline when performing certain operations, and turns them back online again when the operation successfully completes. If the operation fails, the partitions will remain offline until you manually turn them back online again.

---

---

**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.

---

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

- When you access the **Change Partition Mode** screen, you will see only partitions to which you have been given access.
- When changing the partition mode from online to offline, all host application commands in progress at the start of the mode change are completed.

You can change partition modes from the operator panel or the Web client.

## Operator Panel

- 1 Select **Actions > Change Partition Mode**.

The partitions are displayed, along with their online/offline status.

- 2 If more than one partition is configured on the library, use the **Up** and **Down** buttons to select a partition.
- 3 Press **Modify**.
- 4 Uses the **Up** and **Down** buttons to change the mode.
- 5 Press **Apply**.



## Web Client

- 1 Select **Operations > Partitions > Change Mode**.

In the partition table under **Mode**, the **Current** column indicates the current mode of the partition. The **New** column contains an **Online/Offline** button. The button toggles between modes.

---

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

---

- 2 In the partition table, identify the partition that requires a mode change.
- 3 Click the **Online/Offline** button to toggle to the desired mode.
- 4 Click **Apply**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Configuring Cleaning Slots

Cleaning slots are used exclusively to store cleaning cartridges. Configuring one or more cleaning slots enables the library's AutoClean feature for all partitions in the library. When AutoClean is enabled, the library is notified by a tape drive when cleaning is required, and the library automatically cleans the tape drive using a cleaning cartridge.

You can configure cleaning slots during the initial library configuration or at any time in the future as long as there are licensed slots available in the library.

If no licensed slots are available, you must purchase additional slots or modify or delete a partition to free existing slots (see [Working With Partitions](#) on page 51). Cleaning slots are not assigned to specific partitions. They are shared by all partitions within a library.

A maximum of four cleaning slots can be configured. Zero cleaning slots are configured by default.

Cleaning slots do not need to be configured if you clean tape drives manually. For more information about manual tape drive cleaning, see [Manually Cleaning Tape Drives](#) on page 169. In addition, you do not need to configure cleaning slots if you use host-based cleaning. Cleaning slots are not visible to the host application. To use host-based cleaning, configure zero cleaning slots in the library and set up your host application to manage the cleaning process. See your host application documentation for more information.

---

**Note:** If you decrease the number of cleaning slots from what is currently configured, the extra slots become unassigned and available to use as storage slots in new or existing partitions. For information on how to assign available storage slots, see [Manually Creating Partitions](#) on page 54, and [Modifying Partitions](#) on page 56.

---

---

**Note:** If the library contains zero import/export (I/E) station slots, you will not be able to import or export cleaning cartridges. See [Configuring I/E Station Slots](#) on page 63 for more 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.

---

## Operator Panel

- 1 Select **Setup > Dedicated Slots > Cleaning**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select a value from zero to 4.
- 4 Press **Apply**.
- 5 Press **Exit**.
- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Web Client

- 1 Select **Setup > Cleaning Slots**.
- 2 Under the **New Settings** column, select the number of cleaning slots to configure.
- 3 Click **Apply**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

# 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.

I/E station slots can be configured as either I/E station slots or storage slots. I/E station slots are used to import and export cartridges and are shared by all partitions. Storage slots are used to store data cartridges and cleaning cartridges and are assigned to a single partition.

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. You can view the Library Configuration Report to determine how I/E slots are configured. For more information, see [Viewing the Library Configuration Report](#) on page 210. For instructions on deleting cleaning slots, see [Configuring Cleaning Slots](#) on page 61.

You cannot configure I/E station slots if cartridges are currently loaded in the I/E station(s). Remove all cartridges from the I/E station(s) before attempting the following procedure.

Each I/E station is configured as a complete unit. When configuring an I/E station, all the slots in the I/E station are configured the same way. The Scalar i40 and Scalar i80 are configured with 5 I/E station slots by default.

On the Scalar i40, you can configure 0, 5, or 20 I/E station slots. Configured I/E station slots are located in the right magazine—for 5, the right front 5 are configured. On the Scalar i80, you can configure 0, 5, 10, 20, 25, or 40 I/E station slots. The table below lists slots that will be configured based on setting selected.

---

Table 4 Scalar i80 I/E Slot Configuration

Setting Selected	Slots Configured
5	Right top front 5
10	Right top front 5 Right bottom front 5
20	Right top 20
25	Right top 20 Right bottom front 5
40	Right top 20 Right bottom 20

You can configure zero I/E station slots. However, configuring zero I/E station slots has the following consequences:

- You cannot import and export data or cleaning cartridges using I/E stations.
- You cannot manually clean tape drives with a cleaning cartridge using the operator panel.
- You will need to bulk load and bulk unload cartridges, disrupting library operations (see [Bulk Loading Tape Cartridges](#) on page 155).

---

**Note:** Before using the I/E station to load and unload cartridges, you need to unlock the I/E station, which allows you to slide the magazine out just far enough to access the I/E station slots (see [Unlocking and Opening the I/E Station](#) on page 145).

---

---

**Caution:** Empty I/E station slots before changing the I/E configuration to avoid tape cartridge ownership confusion.

---

---

## Operator Panel

- 1 Select **Setup** > **Dedicated Slots** > **I/E**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select a value.
- 4 Press **Apply**.
- 5 Press **Exit**.
- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Web Client

- 1 Select **Setup** > **I/E Station Slots**.  
The **I/E Station Configuration** screen displays. The **Current Settings** column lists the number of I/E station slots that are currently configured.
- 2 Under the **New Settings** column, select the number of I/E station slots to configure.
- 3 Click **Apply**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

# Configuring Tape Drive Parameters

You can configure Fibre Channel tape drive loop ID, topology, and speed using the operator panel or the Web client. On the Web client, you can also view the actual topology and speed, plus the tape drive's world-wide node name (WWNN) and other information about the tape drives.

You cannot configure SAS tape drive settings. A SAS tape drive's SAS address is automatically and uniquely generated based on a unique World Wide Name (WWN) that the drive receives when it is configured. You can view SAS tape drive settings (but not change them) on the Web client.

---

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

---

Table 5 Fibre Channel Tape Drive Configurable Settings

Setting	Description
Loop ID	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 is assigned a default loop ID of 61. The tape drive installed in the 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.
Requested Topology*	The requested topology connection mode can be set to one of the following: <ul style="list-style-type: none"> <li>• Auto (LN) — Auto-configure trying L-Port first</li> <li>• Loop (L) — Force L-Port</li> <li>• Point to Point — Force N-Port</li> <li>• Auto (NL) — Auto-configure trying N-Port first (default)</li> </ul>
Requested Speed*	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 the tape drive.  When you set the speed to 4 Gb/s or 8 Gb/s on the Web client, a caution message displays informing you that the speed selection may not be applicable to all FC tape drives installed in the library. Acknowledge the message by clicking <b>OK</b> .

\* If the requested FC topology and speed settings are not supported, the next appropriate settings are negotiated. On the Web client, the **Setup - 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."

---

## Operator Panel

- 1 Select **Setup > Tape Drives (FC)**.
- 2 If more than one Fibre Channel tape drive is installed, use the **Up** and **Down** buttons to select a tape drive and press **Select**.
- 3 Use the **Up** and **Down** buttons to select the item to configure (Speed, Topology, or Loop ID) and press **Modify**.
- 4 Use the **Up** and **Down** buttons to scroll through the list of options until you reach the one you want, then press **Apply**.
- 5 Continue to modify as above. When finished, press **Exit**.
- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Web Client

- 1 Select **Setup > Drive Settings**.
- 2 View the SAS tape drive settings, if desired.
- 3 Make changes to any of the Fibre Channel tape drive settings by using the drop-down lists to select new values.
- 4 Click **Apply**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

# Configuring Control Paths

A control path is the connection between a partition and host application. The control path connection is made through a designated tape drive.

When you create a partition, the library automatically assigns the first tape drive in the partition as the control path. You can modify the control path at any time.

Only one tape drive can be selected as the control path per partition. In the event that the tape drive control path connection to the host application fails, you can manually select a different control path tape drive for the partition.

---

**Note:** You might need to modify settings in your host application as a result of modifying the control path. See your host application documentation for more information.

---

You can only configure control paths via the Web client.

### Web Client

- 1 Select **Setup > Control Path**.
- 2 If more than one partition exists, select a partition and click **Next**.
- 3 To select a new control path for the partition, select a tape drive from the list of tape drives.
- 4 To delete the control path for the partition, locate the tape drive that is currently selected as the control path and clear the selection.
- 5 Click **Apply**.
- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

**Note:** You can configure a control path failover drive if you have an Advanced Reporting license and HP LTO5 tape drives. See [Working with Control Path Failover \(CPF\)](#) on page 113

---



## Adding or Upgrading Licensable Features

You can increase the functionality of your library by purchasing licenses for the following upgrades:

- Capacity on Demand (COD)
- Advanced Reporting - includes custom reports and logs and Control Path Failover (CPF) functionality.
- Encryption Key Management (EKM)

For more information about these features, see [Licensable Features](#) on page 13.

A license key can be applied to only one library and is tied to the library's serial number. If the license is not installed when you receive your library, you will receive a *License Key Certificate* that contains an authorization code and instructions on how to obtain your license key from the Quantum Web site. Once you install the license key on the library, the feature becomes available.

### About License Keys

Details about license keys include:

- An authorization code to obtain a license key can be used one time only.
- A license key consists of 5 characters randomly selected from the following allowable characters: a-h, j-n, p-t, v-z, 2-9, and the ampersand character (@). Alpha characters are always lower case.
- 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 library chassis or system control board (SCB)).

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

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

---

## Viewing Your License Keys

---

To see the licenses you have purchased and obtained, go to the following Web site: <http://www.quantum.com/licensekeys>. The license history for each feature is listed (feature licensed, authorization code, and date license key was obtained).

---

## Viewing Installed Licenses

---

To see which licenses are installed on your library, go to the following screens:

### Operator Panel

Select either of the following

- **Reports > Licenses**
- **Setup > License Installation**

### Web Client

Select **Setup > License**.

---

## Obtaining a License Key

---

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

- 1 Contact your Quantum technical sales representative to submit your order for the feature or upgrade.
- 2 Upon receipt of your order, Quantum will mail you a license key certificate containing your authorization code.

- 3 On your library, locate the serial number. You will need the serial number to retrieve your license key from the Web site. To locate the serial number:
  - On the operator panel, select **Reports > About Library**.
  - On the Web client, select **Reports > About > Scalar i40/i80**.
- 4 Access the License Key Management Web site: <http://www.quantum.com/licensekeys>.
- 5 Enter the information requested on the screen to obtain your license key.

You are now ready to apply the license key to the library. See [Applying a License Key](#) on page 71.

---

## Applying a License Key

---

Once purchased, you can apply a license key to the library.

---

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

---

## Operator Panel

---

**Note:** Entering a license key on the operator panel is difficult. It is recommended that you use the Web client, if possible.

---

- 1 Select **Setup > License Installation** and press **Select**.  
The **Current Licenses** screen is displayed.
- 2 Select **Add**.  
The Enter License Key screen is displayed. Five blank digits appear on the screen. The first digit is highlighted.
- 3 Use the **Up** and **Down** buttons to scroll through the list of letters and numbers until you reach the letter or number you want. Press the **Right** button to advance to the next digit. Repeat for the remaining digits.
- 4 When all the digits are entered correctly, press **Apply**.
- 5 Press **OK**.

- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

### Web Client

- 1 From the Web client, select **Setup > License**.
- 2 Type the new license key in the **Enter New License Key** text box.
- 3 Click **Apply**.
- 4 Refresh your Internet browser. Adding a license can sometimes affect menu display. Refreshing the browser updates all the menus.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Working With E-mail Notifications

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

Before you can configure e-mail notifications, you must configure the library's e-mail account so that the library can send notifications to the designated recipients. See [Configuring the Library E-Mail Account](#) on page 76 for information on how to configure the e-mail account.

The library supports a maximum of 20 e-mail notification recipients, including the default Quantum Support e-mail notification. See [Creating E-mail Notifications](#) on page 73 for information on setting up additional e-mail notifications.

If an e-mail notification is no longer needed, you can delete it. For information on how to delete an e-mail notification, see [Deleting E-mail Notifications](#) on page 75.

There are three e-mail notification filter levels:

- All Tickets — Notifies e-mail recipients of all tickets.
- High and Urgent tickets only — Notifies e-mail recipients of high-severity and urgent tickets.
- Urgent tickets only — Notifies e-mail recipients of urgent tickets only.

The library comes with one default e-mail notification recipient, for Quantum Support. The filter level and e-mail address of the default technical support notification cannot be modified, but the notification can be enabled or disabled. It is disabled by default.

Users with administrator privileges 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.

You can view and configure e-mail notifications from the Web client only.

---

## Creating E-mail Notifications

---

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

To set e-mail notifications, you need to provide the e-mail address and filter level setting for the recipient. For more information on filter levels, see [Working With E-mail Notifications](#) on page 72.

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

You can create e-mail notifications on the Web client only.

## Web Client

- 1 Select **Setup > Notification > Setup**.

The **Setup - System E-mail Notifications** screen displays. The screen lists all e-mail notifications that have been created.

- 2 Click **Create**.

The **Create System E-mail Notification** screen displays.

- 3 In the **Select Filter Level** drop-down list, select the filter level to assign to the e-mail notification. For more information on filter levels, see [Working With E-mail Notifications](#) on page 72.
- 4 In the **Enter E-mail Address** text box, type the e-mail address that you want to receive e-mail notifications.

---

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

---

- 5 In the **Enter E-mail Comment** text box, type a comment (optional).

---

**Note:** Only letters, numbers, spaces, and hyphens are allowed in this fields. Do not use any special characters—like commas, apostrophes to name a few.

---

- 6 Click **Apply**.
- 7 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Modifying E-mail Notifications

---

Administrators can modify existing e-mail notification settings at any time after the e-mail notification is created.

---

**Note:** The e-mail address of the default technical support notification (**techsup@quantum**) cannot be changed, but the notification can be enabled or disabled.

---

You can modify e-mail notifications on the Web client only.

## Web Client

**1** Select **Setup > Notification > Setup**.

The **Setup - System E-mail Notifications** screen displays. The screen lists all the e-mail notifications that have been created.

**2** Select an address to modify, and click **Modify**.

The **Modify System E-mail Notification** screen displays.

**3** Modify any of the following settings:

- Under the **New Settings** column, select the **Enabled** check box to enable e-mail notification. Clear the **Enabled** check box to disable e-mail notification.
- Under the **New Settings** column, select a new filter level from the **Filter Level** drop-down list. For more information on filter levels, see [Working With E-mail Notifications](#) on page 72.
- In the **E-mail Address** text box, type a new e-mail address.
- In the **E-mail Comment** text box, type a new comment.

---

**Note:** Only letters, numbers, spaces, and hyphens are allowed in this fields. Do not use any special characters—like commas, apostrophes to name a few.

---

**4** Click **Apply**.

**5** Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Deleting E-mail Notifications

---

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

---

**Note:** The default **techsup@quantum.com** e-mail notification cannot be deleted, but the notification can be enabled or disabled. It is disabled by default.

---

You can delete e-mail notifications on the Web client only.

### Web Client

- 1 Select **Setup > Notification > Setup**.
- 2 Select an e-mail notification and click **Delete**.  
A confirmation dialog box displays.
- 3 Click **OK**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## 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 the IP address, valid login account (optional), and valid password (optional) of your SMTP server. E-mail account settings are not case-sensitive.

---

**Note:** You may use a host name for the SMTP server instead of an IP address only if the library is set up to use Domain Name System (DNS) servers. See [Default Gateway, Subnet Mask, Network Prefix, and DNS Addresses](#) on page 43 for more information.

---

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.

You must have administrator privileges to configure the e-mail account.

You can configure the library e-mail account from the Web client only.

### Web Client

- 1 Select **Setup > Notification > E-mail Account**.  
The **Setup - E-mail Account** screen displays.



- 2 In the **SMTP server** text box, type the IP address or host name of the SMTP server.

---

**Note:** IP addresses may be entered using the IPv4 dot notation or using the IPv6 format. IPv4 addresses must be entered in dot notation (for example, 192.168.0.1). IPv4 address text boxes do not allow values exceeding 255 for dot-separated values.

---

- 3 In the **Sender e-mail address** text box, type an e-mail address for the SMTP server (for example, scalar\_i40@mycompany.com). The sender address indicates the originator of the e-mail message.
- 4 For **Send snapshot with e-mail notifications**, do one of the following:
  - To attach a library snapshot file to e-mail notifications, select the check box.
  - To not attach a library snapshot file to e-mail notifications, clear the check box.

---

**Note:** **Send snapshot with e-mail notifications** instructs the library to automatically attach a library snapshot file (ASCII format) to most e-mail notifications. This feature is turned off by default. Library snapshot files can also be sent to specified e-mail addresses using the capture snapshot operation. The capture snapshot operation allows you to create the snapshot in ASCII format. See [Capturing Snapshots of Library Information](#) on page 317.

---

- 5 For **Authentication**, do one of the following:
  - If you do not need to configure login account and password authentication settings, clear the **Authentication** check box. Continue with [Step 6](#).
  - If you need to configure login account and password authentication settings, select the **Authentication** check box. The **Login Account**, **Password**, and **Confirm Password** text boxes display. Do the following:
    - a In the **Login Account** text box, type the name of a valid account on the SMTP server (for example, john.user).



- 3 Click **Apply**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Configuring the Service Port

There are two Ethernet ports on the SCB. The left port is for customer use for remote access via the Web client, and the right port is for service use only. The default service port IP address is **192.168.177.1**.

You should never change the service port subnet unless it happens to conflict with the subnet configured for the customer port. Incorrectly setting the service port subnet could impact connectivity of the customer port and network traffic attached to the customer port, even when the service port is disconnected. If there is a subnet conflict you must change the service port subnet to avoid ambiguity between the two interfaces.

The instructions below explain how to change the IP address on the service port. You can only change the subnet (third octet) of the IP address: 192.168.xxx.1. The other sections must remain as they are. You may choose a number from 1 to 255.

You can only configure the service network from the operator panel.

### Operator Panel

- 1 Select **Tools > Service Network**.

Under “Modify Subnet” the three-digit octet of the IP address is highlighted.

- 2 Use the **Up** and **Down** buttons to scroll to the desired subnet, and press **Apply**.

For more information on scrolling, see [Navigating and Editing on the Operator Panel](#) on page 27).

---

**Note:**

---

- 3 Press **OK**.

- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Working With Local User Accounts and Passwords

Administrators can create and modify two types of local user accounts: user and administrator. These users have different library privilege levels and can access different things. The Web client requires user accounts and user logins; the operator panel does not. You can configure the operator panel to run with logins required. You can also configure the library to use Lightweight Directory Access Protocol (LDAP) accounts.

This section covers:

- [Using the Web Client Default Administrator Account](#) on page 80
- [Privilege Levels](#) on page 81
- [Creating Local User Accounts on the Web Client](#) on page 82
- [Modifying Local User Accounts on the Web Client](#) on page 83
- [Deleting Local User Accounts on the Web Client](#) on page 84
- [Enabling and Creating Passwords on the Operator Panel](#) on page 84
- [Disabling Passwords on the Operator Panel](#) on page 87
- [Resetting Passwords on the Operator Panel](#) on page 88

You must have administrator privileges to create, modify, and delete local user accounts.

---

### Using the Web Client Default Administrator Account

---

The library ships with a default administrator account for use on the Web client. The default administrator account has the following settings:

- User name: **admin**
- Password: **password**.

The first time you access the library via the Web client, when you see the **Login** screen, type **admin** in the **User name** text box and type **password** in the **Password** text box. As soon as you complete the initial library setup, you should change the password on the default administrator account. For information on changing passwords, see [Modifying Local User Accounts on the Web Client](#) on page 83.

---

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

---

---

**Note:** If you misplace the password for the default administrator account, contact Quantum Support (see [Getting More Information or Help](#) on page xxvii).

---

---

## Privilege Levels

---

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.

---

**Note:** If passwords are not enabled on the operator panel, all users have access to all privileges. See [Enabling and Creating Passwords on the Operator Panel](#) on page 84.

---

Three types of users are defined in Scalar i40 and Scalar i80 libraries:

- **Administrators** have access to the entire physical library and all of its partitions. The library ships with a default administrator account. The user name for the default administrator account is **admin** and the password is **password**. You cannot modify or delete the user name for the default administrator account, but you can modify the password. If you misplace the password for the default administrator account, contact Quantum Support.

For security purposes, an administrator can prevent a service user from logging on to the library remotely, from either the Web client or over the Ethernet service port. The service user will still be able to log in to the library from the operator panel interface. For more information, see [Remote Service Login](#) on page 105.

- **Users** have access to portions of the **Actions, Operations, and Reports** menus. Users cannot access the **Setup** and **Tools** menus. Users can perform functions within a partition (such as performing cartridge and tape drive operations), but cannot perform operations that affect the physical library (such as creating or deleting partitions).
  - On the Web client, users can only perform operations and view reports within partitions to which they have been granted access.
  - On the operator panel, users can perform actions and view reports for all partitions.
- **Service users** have access to the entire physical library and all of its partitions as well as to service-only functions. Each library has only one service user account. When a service user logs in, all other active users are automatically logged out.

---

## Creating Local User Accounts on the Web Client

---

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

### Web Client

1 Select **Setup > User Management > User Accounts**.

2 Click **Create**.

The **Create User Account** screen displays.

3 **Enter User Name** - Type a name for the local user account. User names are limited to 1–12 lower-case letters, numbers, and underscores (\_). For example: john\_usa.

4 **Enter Password** - Type a password for the local user 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\_19.

5 **Confirm Password** - Retype the password.

- 6 **Select Privilege** - Select a local user account privilege level by selecting either Admin or User. For more information on users and administrators, see [Privilege Levels](#) on page 81.
- 7 If the new local user account was given *user* privileges, click **Next**.  
The **Create User Account - User Name** screen displays, where **User Name** is the name of the user account. This screen lists all library partitions.
- 8 Select the library partitions that you want the user to access.
- 9 Click **Apply**.
- 10 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Modifying Local User Accounts on the Web Client

---

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 (see [Deleting Local User Accounts on the Web Client](#) on page 84).

### Web Client

- 1 Select **Setup > User Management > User Accounts**.  
The **Setup - Users** screen displays.
- 2 Select a user account and click **Modify**.  
The **Modify User Account** screen displays, where **User Name** is the name of the local user account.
- 3 **Enter your Admin password** to verify you have privileges to modify the account.
- 4 **Enter new password for selected user name:** - Optionally, type a new password. 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**.
- 5 **Confirm new password for selected user name:-** Retype the password.
- 6 **Select Privilege:-** Optionally, change privilege level.

- 7 If the user account has user privileges and you want to modify partition access, click **Next**.

The **Modify User Account - User Name** screen displays, where **User Name** is the name of the user account. This screen lists all library partitions, with the user's assigned partitions checked.

- 8 Modify any of the partition selections.
- 9 Click **Apply**.
- 10 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Deleting Local User Accounts on the Web Client

---

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

---

**Note:** You cannot delete the default administrator account.

---

### Web Client

- 1 Select **Setup > User Management > User Accounts**.

The **Setup - Users** screen displays.

- 2 Select a user account and click **Delete**.

A confirmation dialog box displays.

- 3 Click **OK**.

- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Enabling and Creating Passwords on the Operator Panel

---

If you do not set passwords on the operator panel, all users will have access to all functions, including administrator and service functions. If you want to restrict access to some users, you must set passwords on the operator panel.



Passwords on the operator panel are disabled by default. Once you enable and configure passwords on the operator panel, all users must enter a password on the operator panel to log in. In addition, the service login is automatically enabled and users with user or admin privileges cannot access service functions. The service password is only available to Quantum Support personnel.

Passwords on the operator panel are completely different and separate from passwords on the Web client. On the Web client, you can create and set up to 18 unique user accounts with different user names, passwords, privileges, and partition access. On the operator panel, only three unique accounts names are allowed, and the user names and privileges cannot be changed (the only things you can change are the passwords on the user and admin accounts). The accounts and corresponding privilege levels are:

Account	Privilege Level
admin	Administrator
user	User
service	Service — Only service users may use this account. You <i>cannot</i> change the password for this account.

See [Privilege Levels](#) on page 81 for a description of administrator and user privileges.

In order to use logins and passwords, you must set the passwords for at least the admin account. You can only do this via the operator panel.

You can enable just the admin password (and NOT the user password). However, you cannot enable just the user password.

## Operator Panel

You start out by creating the admin account password. Once created, you are logged out and need to log back in using the **admin** password. Then you can create the **user** account password.

- 1 Select **Setup > Account Settings > Password Settings**.

**Admin Password** is highlighted.

- 2 Press **Modify**.  
**Disabled** is now highlighted.
- 3 Press the **Up** button to change the setting to **Enabled**.
- 4 Press **Apply**.
- 5 You are prompted to create the password. The password is a 4-digit code (no letters or other characters). The first digit of the code is highlighted. Use the **Up** and **Down** buttons to select a number for the first digit, then press **Right** to go to the second digit. As you move off the digit you created, it displays as a # symbol so that only the digit you are working on displays actual numbers. If you need to view or change a digit, press the **Left** button.
- 6 When you are finished creating the admin password, press **Right** until the **Validate Password** prompt appears. Re-enter the password the same way you created it. When finished, press **Apply**.  
A confirmation screen displays.
- 7 Press **OK**.  
The library logs the session out and the operator panel displays the login screen, with the User ID of **admin** highlighted.
- 8 Press **Apply** to go to the password line.
- 9 Using the directional buttons, enter the admin password you created and press **Apply**.
- 10 Select **Setup > Account Settings > Password Settings**.
- 11 Press the **Down** button to highlight **User Password** and press **Modify**.  
**Disabled** is highlighted.
- 12 Press the **Up** button to change the setting to **Enabled**.
- 13 Press **Apply**.
- 14 Create and validate the user password the same way you created the admin password above.
- 15 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Disabling Passwords on the Operator Panel

---

If you no longer want to use passwords on the operator panel, you can disable them. Once you disable the admin password, the user password is also automatically disabled. You can only do this on the operator panel.

### Operator Panel

- 1 Select **Setup > Account Settings > Password Settings**.  
**Admin Password** is highlighted.
- 2 Press **Modify** to modify the Admin password.  
**Enabled** is now highlighted.
- 3 Press the **Down** button to change the setting to **Disabled**.
- 4 Press **Apply**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Modifying Passwords on the Operator Panel

---

Once passwords are created, you can modify them.

### Operator Panel

- 1 Select **Setup > Account Settings > Modify Password**.
- 2 Use the **Up** and **Down** buttons to select **admin** or **user**.
- 3 Press **Apply**.
- 4 Enter the current password and press **Apply**.
- 5 Enter a new password and press **Apply**.
- 6 Re-enter the new password to validate it and press **Apply**.
- 7 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Resetting Passwords on the Operator Panel

If you forget your operator panel passwords and cannot log in, you must reset the passwords. Resetting the passwords disables them and deletes both the admin and user passwords. This means that no login is required to access the operator panel. You can re-create the passwords again as needed.

You can only reset operator panel passwords via the Web client.

### Web Client

- 1 Select **Setup > User Management > Reset Operator Panel Passwords**.
- 2 Click **Apply**.

## Working With LDAP User Accounts (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 a Lightweight Directory Access Protocol (LDAP) server. Enabling LDAP allows existing user accounts residing on an LDAP server to be integrated into the library's current user account management subsystem. User account information is centralized and shared by different applications, simplifying user account management tasks.

To use remote authentication, you must enable LDAP on the library. Once LDAP is enabled, users can log into the library using either LDAP or local authentication. To use LDAP authentication, a user must enter a directory service user name and password. The Web client Login screen displays the Remote Authentication login option only when LDAP is enabled. See [Logging in When LDAP or Kerberos is Enabled](#) on page 138.

LDAP logins are only available on the library Web client.

## 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 90).
- **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 partitions 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 90).

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 94). 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

---

You can configure Secure LDAP using one of two 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.

Additionally, if you are using one of these Secure LDAP methods listed above, 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 checking the **Remove TLS CA Certificate** check box. This check box only becomes available once a certificate is installed. The presence of this check box lets you know that a certificate is installed. Refer to [Figure 14 LDAP Setup Example](#) on page 93.

---

## Configuring LDAP on the Library

---

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 [Working With Local User Accounts and Passwords](#) on page 79.

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 94.

## Web Client

### 1 Select **Setup > User Management > Remote Authentication**.

The **Setup - Remote Authentication** screen displays.

### 2 Under Authentication Type, do one of the following:

- To enable LDAP, select **LDAP** and continue with [Step 3](#).
- To disable LDAP, select **Local Only** and continue with [Step 4](#).
- To modify LDAP configuration settings, continue with [Step 3](#).

### 3 Obtain the following LDAP parameters from your network administrator and enter them in the fields provided:

- **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 90.

- **StartTLS** - Optional. See [Configuring Secure LDAP on the Library](#) on page 90.

- **Install TLS CA Certificate** — Optional. See [Configuring Secure LDAP on the Library](#) on page 90.

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

For an example, see [Figure 14](#) on page 93.

- **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 14](#) on page 93

- **Group DN** — The Fully Qualified Distinguished Name that contains the groups.

For an example, see [Figure 14](#) on page 93

- **Library User Group** — The name of the group on the LDAP server associated with library users who have user-level privileges (see [Privilege Levels](#) on page 81 for more information on user privilege levels). This group must exist on your LDAP server (see [LDAP Server Guidelines](#) on page 89).

For an example, see [Figure 14](#) on page 93

- **Library Admin Group** — The name of the group on the LDAP server associated with library users who have administrator-level privileges (see [Privilege Levels](#) on page 81 for more information on user privilege levels). This group must exist on your LDAP server (see [LDAP Server Guidelines](#) on page 89).

For an example, see [Figure 14](#) on page 93

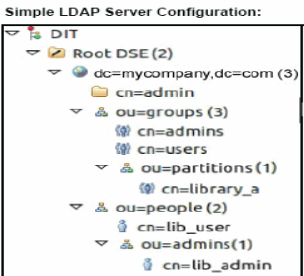
A sample of a completed dialog box is depicted below:



Figure 14 LDAP Setup Example

The LDAP server configuration shown to the right would give the library settings shown in the sample screen below.

Simple LDAP Server Configuration:



```
graph TD
    DIT --> RootDSE[Root DSE (2)]
    RootDSE --> dc[dc=mycompany,dc=com (3)]
    dc --> cn[cn=admin]
    dc --> ou_groups[ou=groups (3)]
    ou_groups --> cn_admins[cn=admins]
    ou_groups --> cn_users[cn=users]
    dc --> ou_partitions[ou=partitions (1)]
    dc --> ou_people[ou=people (2)]
    ou_people --> cn_lib_user[cn=lib_user]
    dc --> ou_admins[ou=admins (1)]
    ou_admins --> cn_lib_admin[cn=lib_admin]
```

### Setup - Remote Authentication

Authenticate logins against a third-party service.

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

#### LDAP Server

Server URI:  *Ex: ldap://hostname:389*

StartTLS:  *Check if your LDAP server supports this extension.*

Install TLS CA Certificate:   *Refer to online help for further details.*

Remove TLS CA Certificate:  *Check to remove the installed certificate.*

Principal:  *A user with search permissions. Refer to your LDAP vendor for syntax.*

Password:

Confirm Password:

#### Authorization

User DN:  *Ex: cn=users,ou=system,dc=mycompany,dc=com*

Group DN:  *Ex: cn=groups,ou=system,dc=mycompany,dc=com*

Library User Group:  *Only members of this group can manage this library.*

Library Admin Group:  *Members of this group are granted the administrator privilege.*

User:  Password:

*Apply any changes to the settings before using this test.  
Test with a user that belongs to both the User and Admin groups.*

4 Click **Apply** to apply any changes.

If you enabled LDAP or modified LDAP settings, the **Test Settings** button is activated.

5 Click the **Test Settings** button to test all the new or changed LDAP settings. See [Testing LDAP Settings](#) on page 94 for more information.

6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## 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** before using this button. Otherwise, any changes you made will be lost and will not be tested.

To test the settings, you must enter a user name and password, then click the 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.

---

## Configuring Kerberos

---

Use Kerberos if you want extra security with remote authentication.

You can configure the Kerberos® settings any time after the initial library configuration. Before you can configure Kerberos, you need to generate the service keytab file on your Kerberos (AD) server. For instructions, see [Generating the Kerberos Service Keytab File](#) on page 96.

You must have administrator privileges to configure Kerberos.

You can only configure Kerberos on the Web client.

### Web Client

- 1 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 49.
- 2 Select **Setup > User Management > Remote Authentication**.  
The **Setup - Remote Authentication** screen displays.

- 3 Under **Authentication Type**, do one of the following:
  - To enable Kerberos, select **LDAP with Kerberos** and continue with [Step 4](#).
  - To disable Kerberos, select **LDAP** or **Local Only** and continue with [Step 6](#).
  - To modify Kerberos configuration settings, continue with [Step 4](#).
- 4 Fill the following Kerberos 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. If you have not already generated this file, do so now. For instructions, see [Generating the Kerberos Service Keytab File](#) on page 96. Then click the **Browse** button to upload the file.
- 5 Configure the LDAP settings as described in [Configuring LDAP on the Library](#) on page 90.
- 6 Click **Apply** to apply any changes.
- 7 If you enabled LDAP or Kerberos, or modified LDAP or Kerberos settings, click the **Test Settings** button to test all the new or changed LDAP settings. See [Testing LDAP Settings](#) on page 94 for more information.
- 8 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Generating the Kerberos 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 2003 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](http://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 kerbtst
```

- 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 Session Timeout

The library automatically logs out a user or administrator when the library has detected no activity for a specified length of time. This always occurs on the Web client, and will occur on the operator panel if passwords are enabled (see [Enabling and Creating Passwords on the Operator Panel](#) on page 84). The default session timeout is 15 minutes. You can change that to 30, 45, or 60 minutes. You can only change this setting on the operator panel.

## Operator Panel

- 1 Select **Setup > Account Settings > Session Timeout**.  
The current timeout setting is highlighted.
- 2 Use the **Up** and **Down** buttons to select the desired timeout.
- 3 Press **Apply**.
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

# Configuring System Settings

You can enable/disable the following system settings on the operator panel:

- [Unload Assist](#)
- [Logical Serial Number Addressing](#)
- [Manual Cartridge Assignment](#)
- [SNMP](#)
- [SMI-S](#)
- [Power Save](#)

---

## Unload Assist

---

When Unload Assist is enabled, the library will unload tape drives when a move command from the tape drive is received. When Unload Assist is disabled, the tape drive must be unloaded prior to a move command, or the move command will fail. This setting is enabled by default.

## Operator Panel

- 1 Select **Setup > System Settings > Unload Assist**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.

- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Logical Serial Number Addressing

---

The library uses the actual tape drive serial numbers by default (logical SN addressing is disabled). Enabling logical SN addressing enables the library to assign logical serial numbers to all tape drives in the library. Specifically, the library assigns a logical serial number to a tape drive in a specific location, not the serial number of the particular tape drive. If the tape drive is then replaced by another tape drive in the same library location, the logical serial number remains the same. From the host application's perspective, the replacement tape drive is the same as the original. This setting is disabled by default.

---

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

---

### Operator Panel

- 1 Select **Setup > System Settings > Logical SN Addr**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Power cycle the library.
- 6 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Manual Cartridge Assignment

---

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

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

The manual cartridge setting is enabled by default. You can only change this setting on the operator panel.

### Understanding Host Application Notification

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

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

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

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

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

### Operator Panel

- 1 Select **Setup > System Settings > Man Cart Assign**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.



- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## SNMP

---

Enables or disables SNMP traffic to the library. This setting is enabled by default.

### Operator Panel

- 1 Select **Setup > System Settings > SNMP**.
- 2 Select the setting you want to modify and press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 When finished making all changes, press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## SMI-S

---

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

### Operator Panel

- 1 Select **Setup > System Settings > SMI-S**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Power Save

---

To help save power, the operator panel goes dark after a period of inactivity on the operator panel (meaning, no buttons have been pressed). The default period is 30 minutes. You can set this period to 15 minutes, 30 minutes, 45 minutes, 60 minutes, or never.

To immediately restore the operator panel screen once it has gone dark, press any of the four navigation buttons on the library.

The operator panel will restore when any of the following happens:

- Any navigation button is pressed.
- The **Assign I/E** screen displays (see [Manual Cartridge Assignment](#) on page 100).
- Tape drives start to autolevel.
- The library receives a signal to shut down.
- Library health (diagnostic ticket) status changes.
- Library ready status changes.

The operator panel will NOT go dark when:

- The library is initializing.
- Tape drives are autoleveling.
- The **Assign I/E** screen is displayed (see [Manual Cartridge Assignment](#) on page 100).
- An operator panel-initiated operation is in progress (such as IVT).
- The Setup Wizard is displayed.
- Passwords are enabled on the operator panel and a user is logged in.
- The power save timeout value is set to NEVER.

## Operator Panel

- 1 Select **Setup > System Settings > Power Save**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select the desired setting and press **Apply**.

# Configuring Security Settings

You can enable/disable the following security settings on the operator panel:

- [Network Interface](#)
- [SSH Services](#)
- [Internet Control Message Protocol \(ICMP\)](#)
- [Remote Access Via Web Client](#)
- [Remote Service Login](#)
- [SNMP V1/V2](#)
- [SSL](#)

## Network Interface

Enables or disables all external access to the library. This setting is enabled by default to allow external access.

### Operator Panel

- 1 Select **Setup > Security Services > Network IF**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## SSH Services

---

Enables or disables Secure Shell (SSH) services, such as SSH, from accessing the library. This setting is enabled by default.

### Operator Panel

- 1 Select **Setup > Security Services > SSH Services**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Internet Control Message Protocol (ICMP)

---

Enables or disables external attempts to discover the library by pinging it (by means of the ICMP Echo packets. This setting is enabled by default.

You may disable this feature if you are using IPv4, but you should NOT do so if you are using IPv6. Disabling this feature disables all IPv6 communication on the Scalar i40 and Scalar i80. There will be no error messages, and the library will appear to be working, but it will not be communicating.

---

---

**Caution:** Do NOT disable ICMP if you are using IPv6!

---

---

### Operator Panel

- 1 Select **Setup > Security Services > ICMP**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Remote Access Via Web Client

---

Enables or disables remote access to the library via the Web client. This setting is enabled by default (meaning remote access is allowed).

### Operator Panel

- 1 Select **Setup > Security Services > Web client**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## Remote Service Login

---

Enables or disables remote service user login (from 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. This setting is enabled by default (meaning remote service login is allowed).

### Operator Panel

- 1 Select **Setup > Security Services > Service User**
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

---

## SNMP V1/V2

---

This topic is discussed in [Enabling SNMP Versions](#) on page 46.

---

## SSL

---

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

Enabling SSL 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. For more information about SMI-S on the library, see [SMI-S](#) on page 101.

Disabling SSL creates an unencrypted connection from a Web browser to the Web client.

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

---

**Note:** Before enabling SSL, make sure you enter a name for the library in the **Host Name** text box when configuring network settings (**Setup > Network Management > Network** on the Web client; see [Library Host Name](#) on page 41). After enabling SSL, use that host 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. This information is used to identify company information in the SSL certificate.

---

### Operator Panel

- 1 Select **Setup > Security Services > SSL**.
- 2 Press **Modify**.
- 3 Use the **Up** and **Down** buttons to select **Enabled** or **Disabled** and press **Apply**.
- 4 Make another selection or press **Exit**.
- 5 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Saving and Restoring the Library Configuration

The library has many configurable items, such as tape drive IDs, partitions, user accounts, import/export (I/E) stations, and cleaning slots. In the event of a hardware failure or firmware upgrade, the save and restore operations can be used to restore the library's configurable items to a previous state. The save/restore operation also saves and restores library firmware and license keys installed on the library.

---

**Note:** The save/restore 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

This operation saves your current library configuration and library firmware.

It is recommended that you save the library configuration after modifying a configurable item and before upgrading firmware. This allows you to restore the most current settings if necessary.

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.

You can only save the configuration from the Web client.

#### Web Client

- 1 Select **Tools > Save/Restore Configuration**.
- 2 Select **Save System Configuration**.

- 3 Click **Apply**.
- 4 When the operation completes successfully, complete the next screens to save the file to a known location.

---

## Restoring the Library Configuration

---

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.

---

**Caution:** After you restore the library's configuration, verify that your drive firmware version reflects the desired firmware level.

---

**Note:** You can also downgrade library firmware to an earlier version using the **Tools > Update Library Firmware** command (see [Updating Library Firmware](#) on page 299). 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.

---

You can only restore the library configuration via the Web client.

### Web Client

- 1 Select **Tools > Save/Restore Configuration**.
- 2 Select **Restore System Configuration**.
- 3 Click **Apply**.
- 4 Use the next screens to browse to the saved configuration file and upload it to the library.  

This operation saves your current library configuration and library firmware.
- 5 Verify the drive firmware level, and if necessary, manually upgrade to the desired firmware level.



---

## Registering the Library

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

You cannot register the library from the operator panel.

### Web Client

Select **Setup > Register Library**.

---

## Changing Operator Panel Home Screen View

From the operator panel, you may choose to change the default home screen to an alternate home screen that facilitates easy I/E unlock access, displays the number of I/E slots and the number of I/E slots that are full.

Changes to the home screen can be made only from the operator panel. Refer to [Figure 9](#) on page 23.

---

### Changing to Alternate Home Screen

---

- 1 Select **Setup > System Settings** and press **Select**.
- 2 Select **Alternate Home** and press **Modify**.
- 3 Select **Up** to choose **Unlock I/E**, and press **Apply**.
- 4 Select **Exit** twice to return to the alternate home screen.

---

**Note:** From the alternate home screen, selecting **Menu** returns you to the default home screen. To return to the alternate home screen, select **Actions > Alternate Home**, and press **Select**.

---

The Alternate Home Screen as shown in [Figure 9](#) displays.

Unlocking the I/E is described in [Unlocking and Opening the I/E Station](#) on page 145.

---

## Returning to Default Home Screen

---

- 1 From the alternate home screen, select **Menu** to return to the default home screen.

The default home screen is displayed temporarily, however upon power cycle will display the alternate home screen until reset permanently.

- 2 To reset to view the default home screen permanently, select **Setup > System Settings** and press **Select**.

- 3 Select **Alternate Home** and press **Modify**.

- 4 Select **Down** and press **Apply**.

Select **Exit** twice to return to the default home screen.



## Chapter 5

# 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 [Adding or Upgrading Licensable Features](#) on page 69.

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.

---

**Note:** You can work with Advanced Reporting Data using only the Web client.

---

This chapter covers:

- [Advanced Reporting Features](#)
- [Working with Control Path Failover \(CPF\)](#)
- [Using Advanced Reporting Reports](#)
  - [Configuring the Drive Resource Utilization Report](#)
  - [Configuring the Media Integrity Analysis Report](#)
  - [Using Advanced Reporting Templates](#)
  - [Loading and Reloading Advanced Reporting Data](#)
  - [Deleting Advanced Reporting Data](#)

- [Saving and E-mailing Advanced Reporting Data Files](#)
- [Working with the Media Security Log](#)
- [Viewing the Media Usage Log](#)
- [Automatically E-mailing Advanced Reporting Reports and Logs](#)

---

## Advanced Reporting Features

The Advanced Reporting license provides the following library features:

**Control Path Failover (CPF)** - Provides support for configuring the HP LTO-5 Fibre Channel (FC) drive for control path failover. To configure a control path failover drive, you must also have an Advanced Reporting license. When control path failover is used, one drive is assigned as the primary control path and another drive as the control path failover (secondary) drive. The control path failover drive is used whenever the primary control path drive fails or is inoperable.

**Reports** - Listed below are Advanced Reporting report names. You can view, configure, send via e-mail, and save and reuse report configurations as templates. In addition, you can automatically e-mail any of the reports to designated recipients at specified, scheduled times.

- **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 report 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 report can help you determine if a problem is due to a specific tape drive or tape cartridge.

**Logs** - Listed below are available logs:

- **Media Security Log** - Lists media that has been removed from the library.
- **Media Usage Log** - Lists media usage information regarding capacity, and read and write errors for media ever mounted in a drive.-

---

## Required Firmware

---

To use all the features of Advanced Reporting, you should install the latest released version of library firmware on your library. For information on installing library firmware, see [Updating Library Firmware](#) on page 299.

---

# Working with Control Path Failover (CPF)

If an HP LTO-5 FC tape drive is the control path for a partition, you can select another HP LTO-5 FC tape drive in that partition for control path failover. This means that if the control path tape drive fails, the failover tape drive becomes the control path for the partition. The failed-over tape drive remains the control path for the partition unless it fails or the library is restarted. When either of these events occurs, the library starts over and attempts to use the original control path tape drive as the control path, and the original failover tape drive for failover.

The control path and failover tape drives are assigned by location in the library, so even if you replace a tape drive with another HP LTO-5 FC tape drive, the library will still fail over or revert to the specified location.

---

## Prerequisites

---

To configure control path failover, you must have the following setup on your library:

- Advanced Reporting License. Refer to [Adding or Upgrading Licensable Features](#) on page 69.
- The control path and failover tape drives must both be HP LTO-5 FC tape drives, and you must have a minimum of two drives in a single partition.
- The control path and failover tape drives must have their topology configured as **Point to Point**. Refer to [Configuring Tape Drive Parameters](#) on page 65.
- The control path and failover tape drives must be connected to an NPIV-enabled switch on the same fabric. They must not be connected to an FC I/O blade.

When control path failover is configured for a partition, the partition uses a virtual port as the control path communication port. The World Wide Port Name (WWPN) for this virtual port is listed in the library's System Information Report in the Library Partitions section under Control Path (see [Viewing System Information](#) on page 206).

## Configuring CPF

You can configure control path failover from the Web client only.

### Web Client

#### 1 Setup the drive topology.

Set the topology for the control path and control path failover tape drives to **Point to Point**. For more information, refer to [Configuring Tape Drive Parameters](#) on page 65.

##### a Select **Setup > Drive Settings**.

The **Setup - Drive Settings** screen displays.

Figure 15 Setup - Drive Settings Screen

Setup Operations Tools Reports

### Setup - Drive Settings

Modify the settings on Fibre Channel drives.

Note: The Actual Topology and Speed can take up to two minutes to be negotiated and returned from a Fibre Channel drive. The values will be unknown until negotiated.

#### Fibre Channel Drives

Partition	Location	State	Type	Loop ID	Requested Topology	Requested Speed	Actual Topology	Actual Speed	Max Speed	WWNN
library_a	0,2	Ready	LTO-5 (Half Height)	63	Point to Point	Auto	Point to Point	8 Gb/s	8 Gb/s	500308C3:88B90004
library_a	0,1	Ready	LTO-5 (Half Height)	61	Point to Point	Auto	Point to Point	8 Gb/s	8 Gb/s	500308C3:88B90000

Page 1 of 1

Drives: 1 through 2

##### b For the appropriate partition, select the Requested Topology of **Point to Point** from the drop down menu.

##### c Click **Apply**.

2 Select **Setup > Control Path**.

The **Control Path** screen displays for that partition.

Figure 16 Setup - Control Path Screen

The screenshot shows the 'Control Path - library\_a (Online)' screen. At the top, there are navigation tabs: 'Setup', 'Operations', 'Tools', and 'Reports'. The user is identified as 'User: admin'. Below the title, there is a descriptive text: 'Select a tape drive to host the library control path for this partition. If an HP LTO-5 FC tape drive is selected as the control path drive, you may select another HP LTO-5 FC tape drive to use as the control path failover drive. Note: To disable a control path or failover drive, click the current selection to deselect it, or make a different selection.' A 'Total Drives: 2' indicator is in the top right corner. The main content is a table with the following data:

Drive Type	Interface Type	Location	Control Path	Failover	Is Active
LTO-5	Fibre	0,2	<input type="radio"/>	<input checked="" type="radio"/>	No
LTO-5	Fibre	0,1	<input checked="" type="radio"/>	<input type="radio"/>	Yes

At the bottom of the screen, there is a pagination control showing 'Page 1 of 1' and a 'Drives: 1 - 2' indicator.

3 Select the **Failover** drive by clicking the **Failover** option.

4 Click **Apply**.

You can also manually force a failover (see [Forcing CPF](#) on page 116).

## Forcing CPF

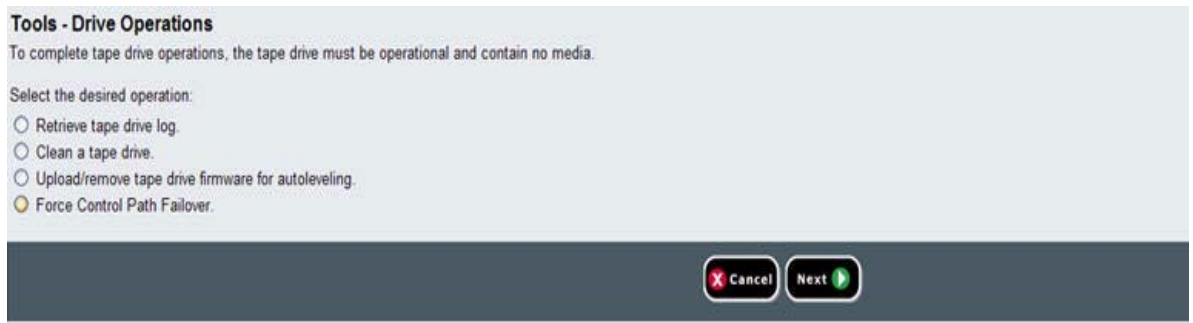
### Web Client

You can manually force a control path failover. You might want to force a failover to check that the control path on the non-active tape drive is operational, or to switch back to the original control path tape drive once the issue that originally caused the failover has been fixed.

- 1 Click **Tools > Drive Operations**.

The **Tools - Drive Operations** screen displays.

Figure 17 Tools - Drive Operations Screen for CPF



- 2 Select **Force Control Path Failover** and click **Next**.

The Force Control Path Failover screen displays (see [Figure 18](#) below). All of the partitions that have control path failover enabled are listed. The location and status of the tape drive that is currently serving as the control path are listed in the Active columns. The location and status of the tape drive that is currently serving as the standby control path are listed in the Standby columns. For each partition, the following information is listed:

Column	Indicates
Active Drive	Location of the current control path tape drive.
Active Status	Ready status of the current control path tape drive.



Column	Indicates
Active Connected	Whether the current control path tape drive is connected and has a working link.
Standby Drive	Location of the standby tape drive.
Standby Status	Ready status of the standby tape drive.
Standby Connected	Whether the standby tape drive is connected and has a working link.

Figure 18 Force CPF Screen



- 3 Select the partition on which you want to force the failover, and click **Apply**.

**Note:** The standby tape drive must be “ready” and “connected” in order to force a failover.

- 4 Click **Apply**.

The new active tape drive location displays in the **Active Drive** column. The new standby tape drive location displays in the **Standby Drive** column.

**Note:** If the new tape drive locations do not display, refresh the browser.

## Using Advanced Reporting Reports

The following notes will help you interpret the data listed on the reports.

- 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 chart displays information for the entire range.) To view all of the data, you need to save or e-mail the data file. See [Saving and E-mailing Advanced Reporting Data Files](#) on page 125.
- 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.
- To see the exact values of each item in the displayed chart, move your mouse so that it “hovers” over the item you wish to see. An information bubble displays with the values listed in it. If you click on a bar, point, or slice, the information bubble locks in place and the hovering feature turns off until you reload the chart. The hovering feature does not work when the value equals zero.
- Values of zero do not appear in Pie charts.

---

## 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

You can only access this report from the Web client.

### Web Client

- 1 From the library menu bar, select **Reports > Advanced Reporting > Drive Resource Utilization**.

The Drive Resource Utilization Report configuration page opens. This may take several minutes.

- 2 Configure the report by specifying the following:
  - **Date Range** — Specifies the range of time covered by the report. Choose Last 7 days; Last 4 weeks (default); Last 3 months; or All History (as far back as there is data in the log file).
  - **Attribute** — Specifies which value is 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. Choose Area, Bar (default), Line, or Pie.
- Type — The chart type. Select one of the following:
  - Rollup (default) — Displays the Grouping on the x-axis and the Attribute amount on the y-axis.
  - Trend — Shows how the Attribute amount changes over time for the selected Grouping.
- Grouping — Specifies which tape drive(s) or partition(s) to include in the report. Select one of the following:
  - All Drives by Coordinate (default) — Presents the sum total of the selected attribute for all tape drives according to their location in the library. If more than one tape drive resided in that location during the selected range, then the attribute values for all the tape drives that resided in that location are combined in the chart.
  - All Drives by Physical SN — Presents the sum total of the selected attribute for all drives according to the physical tape drive serial number.
  - All Partitions — Presents a comparison of all drives grouped by partition in the physical library.
  - Selected Drive by Coordinate — The report chart is based on an individual tape drive location in the library. If more than one tape drive resided in that location during the selected range, then the attribute values for all the tape drives that resided in that location are combined in the chart.
  - Selected Drive by Physical SN — The report chart is based on an individual tape drive identified by its physical drive serial number.
  - Selected Partition — The report chart is based on an individual partition in the physical library.

---

**Note:** See [Installed Tape Drive Location Coordinates](#) on page 9 for an explanation of the location coordinates.

---

**3 Click Next.**

The report is generated and displays on the screen.

---

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

- Date/Time
- Tape drive physical serial number
- Cartridge barcode
- TapeAlert value
- TapeAlert Description

You can only access this report from the Web client.

### Web Client

**1 From the library menu bar, select **Reports > Advanced Reporting > Media Integrity Analysis**.**

The Media Integrity Analysis Report configuration page opens. This may take several minutes.

**2 Configure the report by specifying the following:**

- **Date Range** — Specifies the range of time covered by the report. Choose Last 7 days; Last 4 weeks (default); Last 3 months; or All History (as far back as there is data in the log file).
- **Attributes**—Specifies which values are included in the report, and how they are combined. Select in any combination, including all (default) and none. If you select no attributes, the chart displays the TapeAlert count for the selected Grouping.

- Cartridge Barcode — All relevant tape cartridges.
- Drive Physical SN — All relevant tape drives.
- TapeAlert — The TapeAlert flags that were issued. For a description of all TapeAlert flags, see [Appendix B, Tape Alert Flag Descriptions](#).
- Chart — How the data is displayed in the chart. Choose Area, Bar (default), Line, or Pie.
- Type — The chart type. Select one of the following:
  - Rollup (default) — Displays the number of TapeAlerts for the combination of Grouping and Attributes you selected (default).
  - Trend — Shows the occurrence of TapeAlerts over time.
- Grouping—Specifies which drive(s) or tape cartridge(s) on which to base the report. Choose one of the following:
  - All (default) — All tape drives and tape cartridges for which a TapeAlert was issued during the specified range.
  - Selected Drive by Physical SN — An individual tape drive. Only tape drives which issued a TapeAlert during the specified range appear in the report.
  - Selected Cartridge by Barcode — An individual tape cartridge. Only tape cartridges that were associated with a TapeAlert during the specified range appear in the report.
- Sorting— Specifies how the data will be sorted. Choose from the following:
  - Alphabetical
  - Count (ascending)
  - Last Occurrence (default)

**3 Click Next.**

The report is generated and displays on the screen.

## 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.

You can only work with templates from the Web client.

### Web Client

#### Creating or Accessing a Template

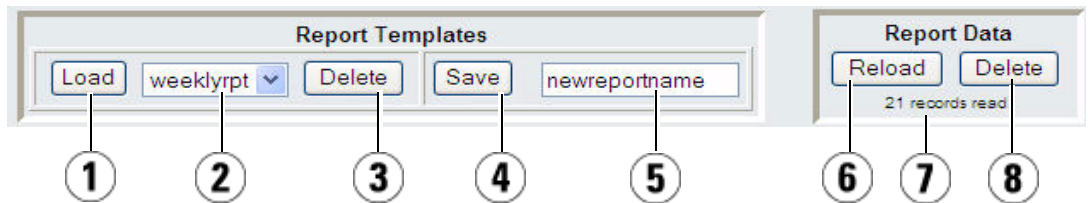
- 1 From the menu bar, select **Reports > Advanced Reporting**, and then select the desired report.

The configuration screen for that report appears.

2

- 3 For a new template, 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.

Figure 19 Template and Report Data Functions



1	Loads the selected template.
2	Template drop-down list.
3	Deletes the selected template.
4	Saves a report configuration as a template.
5	Type name of new report here.
6	Reloads the data from the library log file to the Internet browser.

7	Lists the number of records currently loaded in the Internet browser for this report.
8	Deletes all the Advanced Reporting data.

4 Click **Save**.

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

### Using a Saved 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 screen, 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 example, a TapeAlert occurs), it will not appear in the on-screen 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 on the report's configuration page. This action reloads the entire data for that report, 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 20](#) on page 125).



## 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—see [Figure 20](#) on page 125. This action deletes the data for **both** the Drive Resource Utilization report and the Media Integrity Analysis report.

---

---

**Caution:** Once you delete the data in the log files, you cannot get it back. The **Reload** button does NOT retrieve deleted data! It is recommended that you save all the data for both the Drive Resource Utilization report and the Media Integrity Analysis report before deleting the data (see [Saving and E-mailing Advanced Reporting Data Files](#) on page 125).

---

---

Figure 20 Report Data Buttons



## Saving and E-mailing Advanced Reporting 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.

You can only access this report from the Web client.

### Web Client

- 1 Generate a report.
- 2 Scroll down to the bottom of the report viewing screen to a box titled **Retrieve the Report Data File**. See [Figure 21](#) on page 126.
- 3 To save the report data as a.csv file, click **Save**.

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

Figure 21 Saving and E-mailing the Report Data



## Working with the Media Security Log

---

**Note:** You must have an Advanced Reporting license to use this feature.

---

Media removal is detected by the library when it performs an inventory (at boot up, for example). The media security log lists media that have been removed from the library. You can configure the library to collect any or all of the following media removal events for the log.

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

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

**Expected removal** refers to tape cartridges that were exported properly via the I/E station.

By default, all the options are disabled and the library collects nothing. You must enable at least one of the options for the library to begin collecting data. The log only lists media that is completely removed from the library. It does not list media that moves from one location to another within the library.

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.

You can access and configure this log from only the Web client.

---

## Configuring Media Security

---

You can choose to collect data in a log to list the following conditions that occur in your library:

- Unexpected removal of media after a power-up and reboot
- Unexpected removal of media during library operation
- Expected removal of media from I/E Slots during library operation

Once configured, the library issues diagnostic tickets for the selected conditions, and collects the media removal conditions in the logs. To configure the Media Security, do the following:

You can only access this report from the Web client.

### Web Client

- 1 Select **Setup > Notifications > Advanced Reporting > Media Security**.

The Setup - Advanced Reporting Media Security screen displays.

- 2 Click to enable any or all of the options.
  - Unexpected Removal Detection After Power-Up and Reboot Only
  - Unexpected Removal Detection During Library Operation
  - Expected Removal Detection From I/E Slots During Library Operation

---

**Note:** These options are disabled by default.

---

**3 Click Apply.**

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

- If **Success** appears in the Progress Window, the operation completed successfully. Click Close to close the Progress Window.
- If **Failure** appears in the Progress Window, the operation did not successfully complete.

**4 To view the Media Security Log, select Reports > Log Viewer and then select Media Security Log.**

---

## Viewing, Saving, and E-mailing Media Security Log

---

Using the Web client, you can view, save, or e-mail the Media Security Log.

You can only access this report from the Web client.

### Web Client

- 1 Select Reports > Log Viewer.**
- 2 Select Media Security Log** from the list of logs and click Next.

The report displays in a new window for viewing.

- 3 You can save or e-mail the report** following the on-screen instructions.

---

**Note:** If you want to e-mail the log file to a recipient, type the recipient's name in the text box next to the **E-mail** button, and then click the **E-mail** button. You must have your e-mail notification configured in order to e-mail a log file. See [Configuring the Library E-Mail Account](#) on page 76 for more information.

---

## Viewing the Media Usage Log

The Media Usage Log 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)

You can access and configure this log from only the Web client.

### Web Client

- 1 To view, save, or e-mail the report, select **Reports > Log Viewer**.
- 2 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.

---

**Note:** 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 76.

---

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.

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.

---

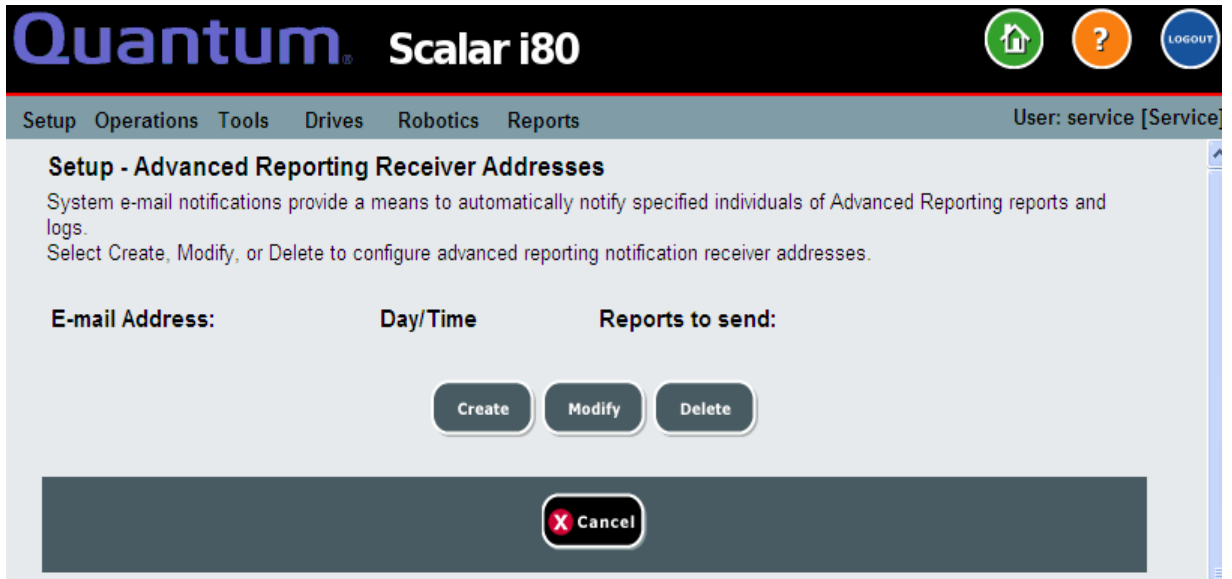
## Creating a Recipient

---

### Web Client

- 1 Select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

The Setup - Advanced Reporting Receiver Addresses screen displays.



## 2 Click Create.

The Setup - Advanced Reporting Receiver Address Configuration screen displays. The screen lists all Advanced Reporting e-mail notifications that have been created, along with the day/time the e-mail is scheduled to be sent, and which reports and logs will be sent.



**Quantum Scalar i80**

Setup Operations Tools Drives Robotics Reports User: service [Service]

### Setup - Advanced Reporting Receiver Address Configuration

Select reports and fill in e-mail address for auto notifications.

Select Reports:  Drive Utilization  
 Media Integrity  
 Media Usage  
 Media Security

Notification Day & Time: Daily 00:00

E-mail Address:

E-mail Comment:

Cancel Apply

- 3 Under **Select Reports**, select the check box of the report(s) and log(s) you want to send.
- 4 Under **Notification Day & Time**, there are two drop-down lists. From the first drop-down list, select the day of the week you want to send the e-mail, or select Daily to send every day. From the second drop-down list, select the time of day to send the e-mail (hourly, using a 24-hour clock).
- 5 In the **E-mail Address** field, enter the recipient's e-mail address.
- 6 In the **E-mail Comment** field, enter a comment that will be sent in the body of the e-mail (optional).

---

**Note:** Only letters, numbers, spaces and hyphens are allowed in this fields. Do not use any special characters—like commas, apostrophes to name a few.

---

- 7 Click **Apply**.
- 8 On the Success window, click **Close**.

- 9 Save the library configuration. For instructions on how to save the library configuration, see [Saving the Library Configuration](#) on page 107.

---

## Modifying a Recipient

---

### Web Client

- 1 Select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

The Setup - Advanced Reporting Receiver Addresses screen displays.

- 2 Click **Modify**.
- 3 Change any of the settings and click **Apply**.
- 4 On the Success window, click **Close**.
- 5 Save the library configuration. For instructions on how to save the library configuration, see [Saving the Library Configuration](#) on page 107.

---

## Deleting a Recipient

---

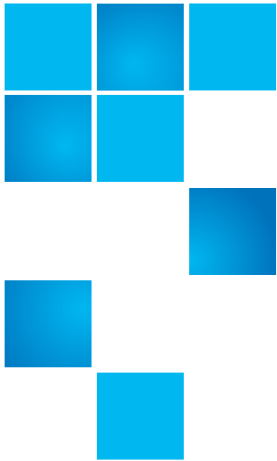
### Web Client

- 1 Select **Setup > Notifications > Advanced Reporting > Receiver Addresses**.

The Setup - Advanced Reporting Receiver Addresses screen displays.

- 2 Select a recipient and click **Delete**.
- 3 On the Confirmation window, click **OK**.

Save the library configuration. For instructions on how to save the library configuration, see [Saving the Library Configuration](#) on page 107.



## Chapter 6

# Performing Library Operations

---

This chapter explains how to access and operate your library. Most of the library functions described here can be found on the **Operations** menu of the Web client, or the **Actions** menu of the operator panel.

This chapter covers:

- [Logging In](#)
- [Logging Out](#)
- [Shutting Down, Restarting, Turning Off, and Removing Power](#)
- [Emergency Power-off Procedure](#)
- [Unlocking and Opening the I/E Station](#)
- [Releasing Magazines](#)
- [Performing Media Operations](#)
- [Cleaning Tape Drives](#)
- [Taking a Tape Drive Online or Offline](#)

## Logging In

All users, service users, and administrators must log in to the library to perform library functions or view library operations. (Exception: If passwords are not configured on the operator panel, login to the operator panel is not required.)

### Simultaneous Logins

Multiple users can be logged in to the library at the same time. The same user can be logged from multiple locations. Note that multiple users logged in from different locations cannot make changes to configuration settings or perform certain library functions simultaneously. The screens are visible, but access is denied. Whichever one is logged in first has access to the screen until they exit the screens.

### Logging in for the First Time

When you first boot up the library, the operator panel does not require you to log in. (In fact, if you do not configure passwords for the operator panel, you never need to log in to the operator panel; see [Enabling and Creating Passwords on the Operator Panel](#) on page 84 for more information.)

To log in to the Web client for the first time:

- 1 Make note of your library's IP address. From the operator panel, select **Reports > Network Settings** to display the IP address.
- 2 Enter the IP address in your Internet browser to bring up the Web client login screen.
- 3 Enter the default user name and password:
  - Default user name: **admin**
  - Default password: **password**
- 4 Click **OK**.

After you log in for the first time, change the password for the default admin account. See [Modifying Local User Accounts on the Web Client](#) on page 83.

---

**Note:** If you misplace the password for the default admin account, contact Quantum Support. For contact information, see [Getting More Information or Help](#) on page xxvii.

---

---

## Logging in Using the Operator Panel

---

If passwords have not been set on the operator panel, you do not need to log in, and all operations are allowed to all users. It is recommended that you set passwords on the operator panel (see [Enabling and Creating Passwords on the Operator Panel](#) on page 84).

If passwords have been set on the operator panel, there are three possible user IDs: admin, user, and service. Log in as follows:

- 1 At the login screen, use the **Up** and **Down** buttons to select **admin**, **user**, or **service**.
- 2 Press **Apply**.
- 3 Enter the first digit of the password using the **Up** and **Down** buttons to scroll to the correct number, then press **Right** to go to the next digit. Enter the rest of the digits in the same way.

---

**Note:** Only the digit you are currently modifying displays an actual number. When you finish one digit and move to the next, the completed digit displays as a cross-hatch symbol (#).

---

- 4 When finished entering all digits, press **Apply**.

---

**Note:** If you misplace the password for the operator panel logins, you can clear operator panel passwords via the Web client (see [Resetting Passwords on the Operator Panel](#) on page 88).

---

---

## Logging in Via the Web Client

---

- 1 Establish an Internet connection to the library by typing the library's IP address into your Internet browser.

If you do not know your library's IP address, you can find it on the operator panel by selecting **Reports > Network Settings**.

- 2 At the login screen, enter a user name and its associated password and click **OK**.

---

## Logging in When LDAP or Kerberos is Enabled

---

When LDAP or Kerberos is enabled, the Web client **Login** screen displays a **Remote Authentication** check box. Log in 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 the Library](#) on page 90.

For more information on Kerberos, see [Configuring Kerberos](#) on page 94.

---

## Logging Out

Logging out secures the library from being accessed by unauthorized users. Log out whenever you have finished accessing the library.

---

**Note:** You will only be able to log out of the operator panel if passwords have been configured (see [Enabling and Creating Passwords on the Operator Panel](#) on page 84).

---

---

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

---

---


**Note:** All users are logged out automatically after a configurable period of inactivity. The default timeout period is 15 minutes, but you can change this (see [Setting the Session Timeout](#) on page 97).

---

### Operator Panel

- 1 Select **Actions > Logout**.
- 2 Press **Yes** to confirm.

## Web Client

- 1 Click the  **Logout** button in the upper right corner of the screen, or select **Operations > Log Out**.
- 2 Click **OK** to confirm.

---

# Shutting Down, Restarting, Turning Off, and Removing Power

It is important to shut down the library properly before turning off the library or completely removing library power.

- 
- Caution:** You should always perform a shutdown before turning off the library or completely removing power. Otherwise, the following could occur:
- The library may not complete closing all data and log files.
  - If you turn off power or unplug the power cord while writing to tape, the data on the tape could become corrupted.
  - If you unplug the power cord, the robot may become frozen in the middle of an operation and unable to move once library power is restored, possibly requiring a service call.
- 

The steps for shutting down, turning off, and completely removing library power are:

- 1 Make sure the connected host applications are not sending commands to the library and that all library operations have stopped.
- 2 Shut down the library using the operator panel or Web client (see [Shutting Down the Library](#) on page 140).
- 3 Turn **OFF** the library by pressing the power button on the front panel (see [Turning Off the Library](#) on page 143).

- 4 Remove library power by disconnecting the power supply cord from the power supply on the back of the library. If there are two power supplies, remove the cords to both. See [Completely Removing Library Power](#) on page 144.

---

## Shutting Down the Library

---

Shutdown shuts down the library's operating system and firmware, closes data and log files, and retracts the picker so that a tape cartridge or the picker fingers are not stuck part way into a tape drive or magazine slot. If the robot was in the middle of a get or put operation, it will attempt to complete the operation before shutting down, by either pushing the cartridge into the destination slot, or removing it completely from the slot and stopping in a safe location from which it can move again once power is restored.

Once the shutdown is complete, you can safely turn off the library by pressing the power button on the front panel (see [Turning Off the Library](#) on page 143).

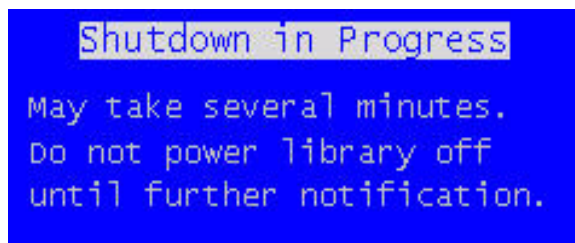
### Operator Panel

- 1 Make sure the connected host applications are not sending commands to the library and that all library operations have stopped.
- 2 Press **Actions > Shutdown > Shutdown Library**.
- 3 Press **Yes** to confirm.

A "shutdown in progress" message displays on the operator panel (see [Figure 22](#)).

---

Figure 22 Shutdown in Progress Message

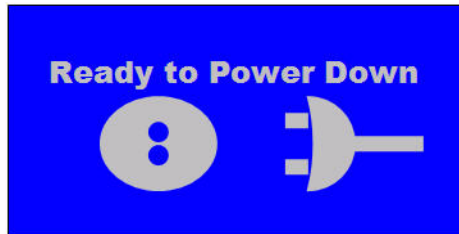




- 4 Wait until the “ready to power down” message displays (see [Figure 23](#)).

---

Figure 23 Ready to Power Down Message



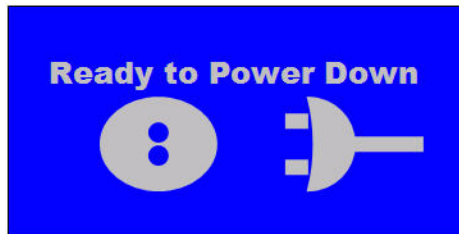
- 5 Turn **OFF** the library by pressing the power button on the front panel.

### Web Client

- 1 Press **Operations > System Shutdown**.
- 2 Select **Shutdown** and click **Apply**.
- 3 Click **OK** to confirm.
- 4 Wait until the “ready to power down” message displays on the operator panel (see [Figure 24](#)).

---

Figure 24 Ready to Power Down Message



- 5 Turn **OFF** the library by pressing the power button on the front panel.

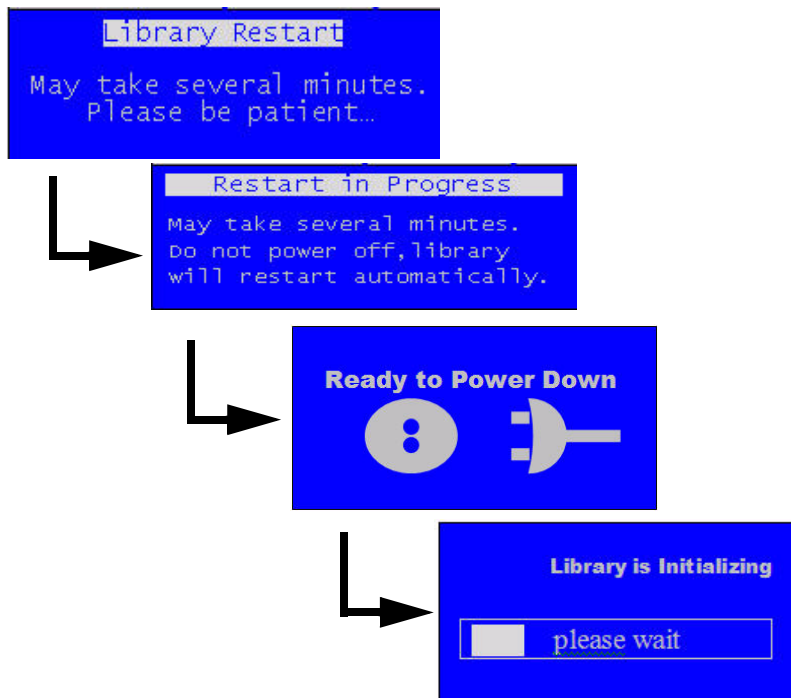
## Restarting the Library

Restart shuts down and then reboots the library's operating system and firmware. During the reboot, the library performs an inventory of the tape drives and magazine slots. If any tape drives or partitions were previously taken offline, restarting the library brings them back online. The reboot takes approximately 5 minutes.

### Operator Panel

- 1 Make sure the connected host applications are not sending commands to the library and that all library operations have stopped.
- 2 Press **Actions > Shutdown > Restart Library**.
- 3 Press **Yes** to confirm.
- 4 Several messages appear on the screen, in the order shown in [Figure 25](#). Do not do anything in response to these messages. The library will restart and initialize on its own.

Figure 25 Series of Restart Messages



## Web Client

- 1 Make sure the connected host applications are not sending commands to the library and that all library operations have stopped.
- 2 Press **Operations > System Shutdown**.
- 3 Select **Restart** and click **Apply**.
- 4 Press **OK** to confirm.
- 5 Several messages appear on the operator, in the order shown in [Figure 25](#) on page 142. Do not do anything in response to these messages. The library will restart and initialize on its own.

---

## Turning Off the Library

---

Turning **OFF** the library means pressing the power button on the front panel.

It is recommended that you perform a shutdown via the Web client or operator panel before turning off the library. If you do not perform a shutdown, the library attempts to complete all shutdown operations before turning off the library. However, it may not have enough time to shut down completely, and operations could be stopped mid-process.

---

**Caution:** You should always perform a shutdown before turning off the library or completely removing power. Otherwise, the following could occur:

- The library may not complete closing all data and log files.
- If you turn off power while writing to tape, the data on the tape could become corrupted.

---

- 1 Make sure the connected host applications are not sending commands to the library and that all library operations have stopped.
- 2 Shut down the library (see [Shutting Down the Library](#) on page 140).
- 3 Turn **OFF** the library by physically pressing the power button on the library's front panel. It can take up to 12 seconds for the power to completely turn off.

---

**Note:** Turning off the library does not completely remove library power (see [Completely Removing Library Power](#) on page 144).

---

---

## Completely Removing Library Power

---

Completely removing library power means disconnecting the power cord from each power supply on the library.

---

**Caution:** You should always perform a shutdown and then turn off library power before completely removing power. Otherwise, the following could occur:

- The library may not complete closing all data and log files.
- If you turn off power or unplug the power cord while writing to tape, the data on the tape could become corrupted.
- The robot may become frozen in the middle of an operation and unable to move once library power is restored, possibly requiring a service call.

---

- 1 Make sure the connected host applications are not sending commands to the library and that all library operations have stopped.
- 2 Shut down the library (see [Shutting Down the Library](#) on page 140).
- 3 Turn **OFF** the library by physically pressing the power button on the library's front panel (see [Turning Off the Library](#) on page 143). Make sure the operator panel turns off or the LED on the SCB turns off.
- 4 Disconnect the power cord(s) from all power supplies on the back of the library. If there are two power supplies, disconnect both cords. Power is completely removed from the library when the LED on each power supply is off.

---

## Emergency Power-off Procedure

---

In an emergency, you may need to turn off power immediately to stop robot motion, bypassing the normal shutdown process.

In an emergency, you can turn off power in one of two ways:

- Press the power button on the front of the library to turn the library **OFF**. It may take up to 4 seconds for all motion to completely stop.

Note that this does not completely remove library power (you need to disconnect the power cords to do that).

- Disconnect the power cord from each power supply on the back of the library. It may take 1 to 2 seconds for motion to completely stop.

---

---

**Caution:** These methods are not recommended except in case of emergency where it is vital that library operations be stopped immediately. If you do not first perform a shutdown as described in the sections above, the following could occur:

- The library may not complete closing all data and log files.
- If you turn off power or unplug the power cord while writing to tape, the data on the tape could become corrupted.
- If you unplug the power cord, the robot may become frozen in the middle of an operation and unable to move once library power is restored, possibly requiring a service call.

---

---

---

## Taking the Library Offline

---

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. See [Taking a Partition Online or Offline](#) on page 59 for instructions.

---

## Unlocking and Opening the I/E Station

The I/E station is locked during normal library operation. To access the I/E station you must first unlock it. When you give the command to unlock the I/E station, the robot physically moves to the unlock mechanism and unlocks it. This takes a few seconds. Once unlocked, you have 30 seconds to open the I/E station before it locks again.

Opening the I/E station consists of pulling outward on the magazine bezel handle until the magazine stops moving. The magazine will automatically stop when the entire I/E station is exposed.

---

**Note:** Because the I/E station is part of the magazine, all storage slots contained in that magazine are unavailable to applications during the time that the I/E station is open.

---

**Note:** On the Scalar i80, if you want to open more than one I/E station, such as when importing multiple tape cartridges, unlock and open both I/E stations before you close either of them. Otherwise, if you open and close one at a time, you must wait for the robot to complete inventory on the one being closed before it can open the other one.

---

For more information about the physical location and capacity of the I/E station, see [Configuring I/E Station Slots](#) on page 63.

## Operator Panel

- 1 If viewing from the default home screen, select **Actions > I/E > Unlock I/E Station**. If viewing from the alternate home screen, select **Unlock**.
- 2 If more than one I/E station is configured on the library, select which I/E station to unlock, and press **Unlock** for the desired selection.

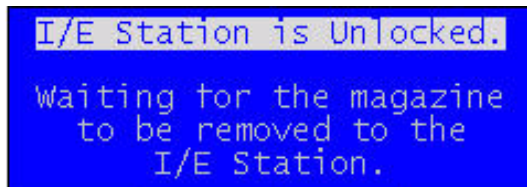
---

**Note:** Only closed I/E stations are listed.

---

- 3 Wait until the robot unlocks the I/E station and the screen displays the **I/E Station is Unlocked** message (see [Figure 26](#)).

Figure 26 I/E Station Unlocked Message

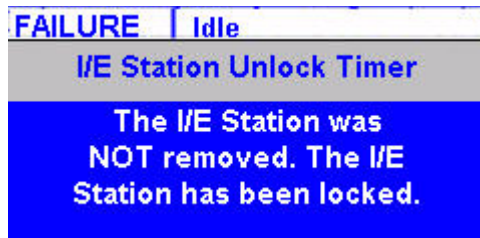


I/E Station is Unlocked.  
waiting for the magazine  
to be removed to the  
I/E Station.

- 4 Within 30 seconds, open the I/E station by pulling outward on the magazine bezel handle until the magazine stops moving.

If you do not open the magazine within 30 seconds, it locks and you receive the following failure message.

Figure 27 I/E Station Locked Message



- 5 When finished, push the magazine in completely.  
The I/E station is now locked.

## Web Client

- 1 Select **Operations > I/E Station Unlock**.
- 2 Select an I/E station to unlock and click **Apply**.

---

**Note:** Only closed I/E stations are listed.

---

- 3 Click **Apply** to confirm, and click OK.

The Progress Window displays. The Progress Window contains information on the action, elapsed time, and status of the requested operation. Do one of the following:

- If **Success** appears in the Progress Window, the I/E station was unlocked. Click **Close** to close the Progress Window. The operator panel displays the status **Unlocking** and then **Idle**.
  - If **Failure** appears in the Progress Window, the I/E station did not unlock.
- 4 Within 30 seconds, pull outward on the magazine bezel handle to open the I/E station.

If you do not open the magazine within 30 seconds, it locks.

5 When finished, push the magazine in completely.

The I/E station is now locked.

---

## Releasing Magazines

Magazines are locked during normal operation. Before you open or completely remove a magazine, you must release it, either via the user interface or manually, as described in:

- [Releasing Magazines via the User Interface](#) on page 149
- [Releasing Magazines Manually](#) on page 150

When you give the command to release a magazine via the operator panel or Web client, the robot physically moves to the unlock mechanism and unlocks it. This takes a few seconds. Once unlocked, you have 30 seconds to open the magazine before it locks again.

---

**Note:** All storage slots contained in an open or removed magazine are unavailable to applications.

---

---

**Note:** If you want to remove more than one magazine, such as when bulk loading tape cartridges, release and remove all the magazines you want to remove before you close any of them. Otherwise, if you remove and replace them one at a time, you must wait for the robot to complete inventory on the one being replaced before it can release another one.

---

---

**Caution:** If the library is turned **ON**, always release the magazines via the user interface. It is easier and will not result in a diagnostic ticket (see [About Diagnostic Tickets](#) on page 312). Additionally, the library makes sure nothing is physically blocking the magazine that could cause damage to library components before allowing you to release it.

---



## Releasing Magazines via the User Interface

Use this method when the library is turned **ON**.

### Operator Panel

- 1 Select **Actions > Magazine**.
- 2 Select a magazine and press **Release**.

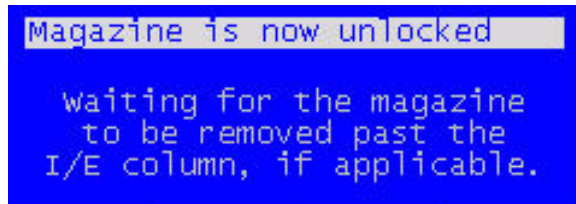
---

**Note:** Only closed magazines are listed.

---

- 3 Wait until the robot unlocks the magazine and the screen displays the **Magazine is now unlocked** message (see [Figure 28](#)).

Figure 28 Magazine Unlocked  
Message



- 4 Pull outward on the magazine bezel handle to slide the magazine out as far as you wish, or remove it completely. Once you slide the magazine back into the slot all the way, it locks again automatically.  
**If** you do not open the magazine within 30 seconds, it locks and you receive the following failure message.

Figure 29 Magazine Locked  
Timer Message



## Web Client

- 1 Select **Operations > Release Magazine**.
- 2 Select a magazine and press **Apply**.

---

**Note:** Only closed magazines are listed.

---

- 3 Click **OK** to confirm.

The Progress Window displays. The Progress Window contains information on the action, elapsed time, and status of the requested operation. Do one of the following:

- If **Success** appears in the Progress Window, the magazine was unlocked. Click **Close** to close the Progress Window. The operator panel displays the status **Unlocking** and then **Idle**.
  - If **Failure** appears in the Progress Window, the magazine did not unlock.
- 4 Within 30 seconds, pull outward on the magazine bezel handle to slide the magazine out as far as you wish, or remove it completely. Once you slide the magazine back into the slot all the way, it locks again automatically.

If you do not open the magazine within 30 seconds, it locks.

---

## Releasing Magazines Manually

---

Use this method when the library is turned **OFF**. If you use this method when the library is turned **ON**, you will receive a diagnostic ticket.

---

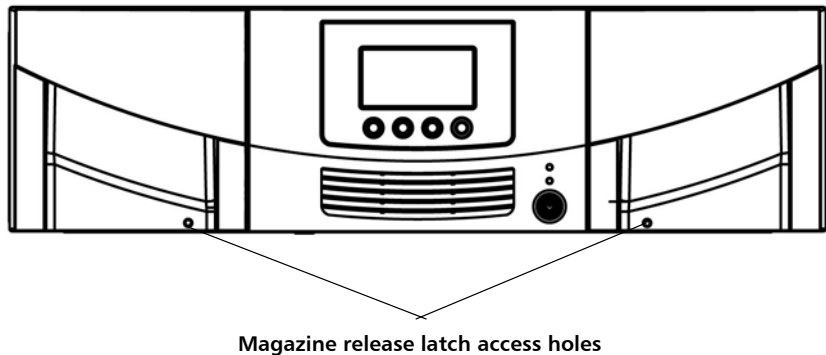
**Caution:** If you use the manual method to remove magazine(s) when the library is turned **ON** you risk a mechanical collision between the magazine and the robotics that could seriously damage components.

---

- 1 Insert an opened paperclip, small screwdriver, or other object (3.5 mm or less in diameter that will not break off) into the access hole in the bottom of the magazine bezel (see [Figure 30](#)).
- 2 Use the tool to depress the release latch (push straight in) while gently pulling the magazine bezel handle to slide the magazine out.
- 3 If the magazine is on the right side, it will only slide out as far as the I/E station. To release the magazine fully:

- On the Scalar i40 and the bottom right magazine of the Scalar i80, reach under the open magazine and insert the tool directly into the access hole in the library chassis to depress the release latch, while pulling outward on the magazine bezel handle.
- On the top right magazine of the Scalar i80, reach under the open magazine and press the release latch directly with your finger, while pulling outward on the magazine bezel handle.

Figure 30 Magazine Release Latch Access



## Performing Media Operations

This section describes how to import, export, load, unload, and move data cartridges in the library. The following section, [Cleaning Tape Drives](#) on page 163, describes how to perform similar operations with cleaning cartridges.

---

**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 Tape Cartridges

---

You can 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.

Tape cartridges must be present in the I/E station and assigned to a partition before you can import them. You will select a partition into which to import the cartridges. 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.

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

---

**Note:** All tape cartridges must have a unique, external barcode label that is machine readable. See [Supported Barcode Formats](#) on page 338 and [Installing Barcode Labels](#) on page 339 for more information.

---

---

**Note:** If your library has zero I/E station slots, you cannot import or export media using the I/E station. See [Configuring I/E Station Slots](#) on page 63.

---

---

**Note:** Importing cartridges using the library interface may necessitate performing an inventory on your host application. You can also import cartridges using your host application. See your host application documentation for more information.

---

---

**Note: Note on importing unassigned tape cartridges:** When the manual cartridge assignment setting is enabled (the default setting), the **I/E Assign** screen automatically displays on the operator panel after you have loaded the cartridges into the I/E station and closed the I/E station. The screen prompts you to assign the cartridges to a specific partition or to the System partition. The cartridges can then be used only by the assigned partition. If you do not wish to assign cartridges to a partition immediately, or you wish to assign them to different partitions via the Web client, you can cancel out of this screen and the cartridges are considered “unassigned.” Alternatively, you can disable manual cartridge assignment (operator panel, **Setup > System Settings > Man Cart Assign**; see [Manual Cartridge Assignment](#) on page 100). In this case, the **I/E Assign** screen does not appear on the operator panel and the cartridges are considered “unassigned.” Unassigned cartridges in the I/E station are available for use by any partition, including the System partition. However, you can only import or move unassigned cartridges into the library when manual cartridge assignment is disabled. Once imported or moved into a partition, the cartridges are considered assigned to that partition and can only be used by that partition.

---

---

**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.

---

The process for importing cartridges includes the following steps:

### Inserting and Assigning Cartridges

- 1 Verify that all tape drives are unloaded and that all cartridges are in their appropriate storage slot locations. Doing this will avoid overloading the library with cartridges.
- 2 Go to the front of the library and insert cartridges into the I/E station.

3 Close the I/E station.

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

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

- a Using the operator panel, select the partition to which you want to assign the cartridges. All unassigned cartridges in the I/E station will be assigned to the same partition.
- b Press **Apply**. (Alternatively, you may press **Cancel** to bypass this step if you wish to assign cartridges to different partitions using the Web client. Note that you must disable manual cartridge assignment from the operator panel before you can import unassigned cartridges, as described in the Note above.)

5 Continue using one of these options:

- [Importing Cartridges via the Operator Panel](#) on page 154
- [Importing Cartridges via Web Client](#) on page 155

## Importing Cartridges via the Operator Panel

You can import one cartridge at a time, or all cartridges at once, using the operator panel.

- 1 Select **Actions > I/E > Import Tape**.
- 2 If the cartridges in the I/E station are assigned to multiple partitions, select the partition into which you want to import.
- 3 If there is more than one cartridge in the I/E station, use the **Up** and **Down** buttons to select a cartridge to import, or select **ALL** to import all cartridges. The **ALL** option is only available if there are enough empty slots in the selected partition to accommodate all the cartridges.
- 4 Press **Import**.

The library imports the tape cartridge(s) into the first empty slot(s) in the partition.

## Importing Cartridges via Web Client

- 1 Select **Operations > Media > Import**.
- 2 If more than one partition exists, select the partition into which you want to import cartridges and click **Next**.
- 3 The **Import Media - Partition (Mode)** screen displays, where **Partition** is the name of the partition and **Mode** is the current mode of the partition. This screen contains a list of cartridges in the I/E station that are ready for import.
- 4 Identify the number of empty storage slots that appear in the **Empty Partition Slots** field. The number of cartridges you can import is limited to the number of empty slots that exist in the partition.
- 5 Select the cartridges to import into the partition.

---

**Note:** You can select all cartridges by selecting the top check box. You can use the **Filter by Barcode** text box to filter the available cartridge barcodes. Click the **Help** button next to the **Find** button for more information about filtering barcodes. In addition, if not all cartridges appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

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

---

- 6 Click **Apply**.
- 7 Click **OK** to confirm it is OK to take the partition offline.

The library imports the tape cartridge(s) into the first empty slot(s) in the partition.

---

## Bulk Loading Tape Cartridges

---

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 210.

Place cartridges in their appropriately configured slot location; for example, cleaning cartridges should not be placed in slots configured for storage.

To perform an initial bulk load, remove the magazine and manually insert tape cartridges directly into storage slots (see [Releasing Magazines](#) on page 148). When finished loading the cartridges, reinstall the magazine and push it in until it is completely closed.

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 Tape Cartridges](#) on page 152.

---

## Moving Tape Cartridges

---

Once a cartridge has been imported into a library and assigned to a partition, it can be moved to a tape drive for data access, to a storage slot for storage, or back to the I/E station for removal from the library.

Details on using the library to move media include:

- 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 63.
- You can move a cartridge from one location to another within a partition. You can also move unassigned cartridges from the I/E station to available locations in the library. If you move an unassigned tape cartridge into a slot in a partition, it will become assigned to that partition and will only be available for use by that partition.

---

**Note:** If you move an unassigned tape cartridge directly from the I/E station to a tape drive, you will not be able to perform an “unload” operation on that tape drive later. The tape drive can only “unload” a cartridge if that cartridge came from a storage slot in the partition. You will need to perform a “move” operation to move the tape drive to a storage slot or back to the I/E station.

---



- Moving cartridges using the library Web client may necessitate performing an inventory on your host system. You can also move cartridges using your host application. See your host application documentation for more information.
- If the partition is online, it will be taken offline before the move is performed and brought back online after the move is complete. You will be asked to confirm that you want to take the partition offline.
- You can select only the partitions to which you have been given access.
- You cannot move media directly from one partition to another.

You can only perform move commands from the Web client.

## Web Client

- 1 Select **Operations > Media > Move**.
- 2 If more than one partition exists, select the partition that contains the cartridge you want to move and click **Next**.

The **Move Media - Partition (Mode)** screen displays, where **Partition** is the name of the partition and **Mode** is the current mode of the partition.

- 3 In the **Select Media** section, select the source cartridge you want to move.

---

**Note:** You can use the **Filter by Barcode** text box to filter the available cartridge barcodes. Click the **Help** button next to the **Find** button for more information about filtering barcodes. In addition, if not all cartridges appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

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

---

- 4 In the **Select Destination** section, select a destination location for the source cartridge.
- 5 Click **Apply**.

6 Click **OK** to confirm it is OK to take the partition offline.

The robot moves the cartridge to the destination. A “success” message displays when the move completes.

---

## Exporting Tape Cartridges

---

The Export Media operation enables you to export data cartridges from storage slots to empty I/E station slots for removal from the library.

Details on exporting cartridges include:

- Exporting cartridges using the library Web client may necessitate performing an inventory on your host application. If the host application has issued a prevent media removal command to the library, you will not be able to use the library Web client to export cartridges. In addition, you can export cartridges using your host application. For more information, see your host application documentation.
- If the partition is online, it will be taken offline before the export is performed, and brought back online after the export is complete. You will be asked to confirm that you want to take the partition offline.
- If your library has zero I/E station slots, you cannot export cartridges. See [Configuring I/E Station Slots](#) on page 63.
- If you have AutoClean enabled, you can also export cleaning cartridges. For information, see [Exporting Cleaning Cartridges](#) on page 167.
- 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 export 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.

---

You can export cartridges using either the operator panel or the Web client.

### Operator Panel

- 1 Select **Actions** > **I/E** > **Export Tape**.
- 2 If more than one partition exists, use the **Up** and **Down** buttons select the partition that contains the source cartridge you want to export, then press **Select**.
- 3 A list of all the tape cartridges in storage slots in the selected partition displays. Use the **Up** and **Down** buttons to select a tape cartridge for export. You may also select **ALL** to export all cartridges; however, the **ALL** option is only available if there are enough empty slots in the I/E station to accommodate all the cartridges in the selected partition.
- 4 Press **Export**.
- 5 When the screen displays confirmation that the export completed, press **OK**.
- 6 Once the operation completes, you may open the I/E station and remove the cartridges (see [Unlocking and Opening the I/E Station](#) on page 145).

### Web Client

- 1 Select **Operations** > **Media** > **Export**.
- 2 If more than one partition exists, select the partition that contains the source cartridge you want to export.

- 3 Click **Next**.

The **Export Media - Partition (Mode)** screen displays, where **Partition** is the name of the partition and **Mode** is the current mode (online or offline) of the partition.

- 4 Note the number of empty I/E station slots that appear in the **Empty I/E Station Slots** field. The number of cartridges you can export is limited to the number of empty I/E station slots. You cannot export cartridges if all I/E station slots are full.

- 5 Select one or more cartridges for export.

---

**Note:** You can use the **Filter by Barcode** text box to filter the available cartridge barcodes. Click the **Help** button next to the **Find** button for more information about filtering barcodes. In addition, if not all cartridges appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

---

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

---

- 6 Click **Apply**.
- 7 Click **OK** to confirm it is OK to take the partition offline.  
The robot moves the cartridge to the I/E station. A “success” message displays when the export completes.
- 8 Once the operation completes, you may open the I/E station and remove the cartridges (see [Unlocking and Opening the I/E Station](#) on page 145).

---

## 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:

- The storage slot and tape drive must be assigned to the same partition.
- The tape cartridge must be compatible with the tape drive.
- If the partition is online, it will be taken offline before the load operation is performed and brought back online after the operation is complete. You will be asked to confirm that you want to take the partition offline.

- You can select only partitions to which you have been given access.
- Default tape drive locations are highlighted if the barcode field is empty or the field is cleared.

You can only load tape drives from the Web client.

## Web Client

- 1 Select **Operations > Drive > Load**.
- 2 If more than one partition exists, select the partition that contains the tape drive you want to unload, and click **Next**.
- 3 The **Load Drive - Partition (Mode)** screen displays, where *Partition* is the name of the partition and *Mode* is the current mode of the partition (online or offline).
- 4 In the **Select Media** section, select the cartridge you want to load into a tape drive.

---

**Note:** You can use the **Filter by Barcode** text box to filter the available cartridge barcodes. Click the **Help** button next to the **Find** button for more information about filtering barcodes. In addition, if not all cartridges appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

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

---

- 5 In the **Select Destination** section, select the destination tape drive.
- 6 Click **Apply**.
- 7 Click **OK** to confirm it is OK to take the partition offline.

---

## 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:

- The tape drive and storage slot must be assigned to the same partition.
- Only drives with media loaded appear on the screen.
- You can select only partitions to which you have been given access.
- If the affected partition is online, it will be taken offline before the unload operation is performed, and brought back online after it is complete.

You can unload media from the operator panel or the Web client.

### Operator Panel

- 1 Select **Actions > Tape Drive > Unload**.
- 2 If more than one tape drive is installed in the library, use the **Up** and **Down** buttons to select a tape drive to unload.
- 3 Press **Unload**.

### Web Client

- 1 Select **Operations > Drive > Unload**.
- 2 If more than one partition exists, select the partition that contains the tape drive you want to unload.
- 3 Click **Next**.

The **Unload Drive - *Partition (Mode)*** screen displays, where *Partition* is the name of the partition and *Mode* is the current mode of the partition. The screen contains a list of all tape drives in the partition that are loaded with a cartridge.

- 4 Select the tape drive you want to unload.

---

**Note:** If not all drives appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

---

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

---

- 5 Click **Apply**.
- 6 Click **OK** to confirm it is OK to take the partition offline.

The library attempts to unload the tape cartridge and move it into the storage slot it was in when it was originally loaded into the tape drive. If that storage slot is full, the library will attempt to move it into another empty slot in the partition. If no empty slots exist, the unload operation will fail. If this happens, you can try to perform a move operation to move the cartridge from the tape drive to an I/E station instead (see [Moving Tape Cartridges](#) on page 156), or free up a storage slot and try the unload operation again.

---

## Cleaning Tape Drives

Tape drives require occasional cleaning. Cleaning cartridges are used to remove accumulated residue from each tape drive's read/write head.

Cleaning slots are used exclusively to store cleaning cartridges. Configuring one or more cleaning slots enables the library's AutoClean feature for all partitions in the library. When AutoClean is enabled, the library is notified by a tape drive when cleaning is required, and the library automatically cleans the tape drive using a cleaning cartridge. For more information about the AutoClean feature, see [About AutoClean](#) on page 164.

You can configure cleaning slots during the initial library configuration or at any time in the future as long as there are licensed slots available in the library. For instructions on how to configure cleaning slots, see [Configuring Cleaning Slots](#) on page 61.

A maximum of four cleaning slots can be configured. Zero cleaning slots are configured by default.

If no licensed slots are available, you must purchase additional slots or modify or delete a partition to free existing slots. For information on how to modify partitions, see [Modifying Partitions](#) on page 56. For information on how to delete partitions, see [Deleting Partitions](#) on page 57. Cleaning slots are not assigned to specific partitions. They are shared by all partitions within a library.

You do not need to configure cleaning slots if you clean tape drives manually. For more information about manual tape drive cleaning, see [Manually Cleaning Tape Drives](#) on page 169.

You do not need to configure cleaning slots if you use host-based cleaning. Cleaning slots are not visible to the host application. To use host-based cleaning, configure zero cleaning slots in the library and set up your host application to manage the cleaning process. See your host application documentation for more information.

---

## Valid Cleaning Cartridges

---

Use universal cleaning cartridges to clean tape drives. If you attempt to clean a tape drive using a non-cleaning cartridge, the library may show that the operation completed, but the tape drive will not be cleaned, and the library will issue a diagnostic ticket.

Universal cleaning cartridges are designated by labels that begin with CLN or CLNU or end with C1, C2, C3, C4, or CU. Examples: CLN123, CLNU123L1, CLN123C1, 123CU, 123C1.

Cleaning cartridges, like all other cartridges imported into the library, must have a unique, external barcode label that is machine readable. See [Supported Barcode Formats](#) on page 338 and [Installing Barcode Labels](#) on page 339 for more information.

---

## About AutoClean

---

Configuring one or more dedicated cleaning slots automatically enables AutoClean (see [Configuring Cleaning Slots](#) on page 61). Cleaning cartridges are stored in 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. For example, if the host application requests the library to move a tape cartridge, and 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, the library issues a diagnostic ticket that tells you 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, the library issues a diagnostic ticket informing you that the tape drive needs cleaning and that a cleaning cartridge needs to be imported (see [Importing Cleaning Cartridges](#) on page 165 and [Exporting Cleaning Cartridges](#) on page 167).

---

## Enabling AutoClean

---

To enable AutoClean, all you need to do is configure at least one cleaning slot in the library. For information on configuring cleaning slots, see [Configuring Cleaning Slots](#) on page 61.

---

## Importing Cleaning Cartridges

---

When AutoClean is enabled (at least one cleaning slot has been configured), you can import cleaning cartridges from the I/E station to designated cleaning slots. For information on configuring cleaning slots, see [Configuring Cleaning Slots](#) on page 61.

When manual cartridge assignment is enabled (the default setting), you cannot import cartridges until you have assigned them to a specific partition or to the System partition. Cleaning cartridges should always be assigned to the System partition. Assigning cleaning cartridges to the System partition makes them available to all partitions in the library. For more information about manual cartridge assignment, see [Manual Cartridge Assignment](#) on page 100.

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

---

---

**Caution:** Some host applications may fail import/export operations when the I/E station contains cartridges that are assigned to another partition. Move cartridges from the I/E station as soon as possible to avoid possible conflicts with the other partitions.

---

---

---

**Note:** If your library has zero I/E station slots, you cannot import or export cleaning media. See [Configuring I/E Station Slots](#) on page 63.

---

---

**Note:** Cleaning cartridges, like all other cartridges used in the library, must have a valid, readable barcode label properly installed (see [Supported Barcode Formats](#) on page 338 and [Installing Barcode Labels](#) on page 339).

---

The process for importing cleaning cartridges includes the following steps:

### Inserting and Assigning Cartridges

- 1 Verify that there is an available, empty slot that is not assigned to a partition. If needed, free up access by modifying a partition (see [Modifying Partitions](#) on page 56).
- 2 Go to the front of the library and insert the cleaning cartridge(s) into the I/E station.
- 3 Close the I/E station.
- 4 If manual cartridge assignment is enabled, the **I/E Assign** screen displays on the operator panel. If manual cartridge assignment is enabled, select the **System** partition.
- 5 Press **Apply**.
- 6 Continue using one of these options:
  - [Importing Cleaning Cartridges via the Operator Panel](#) on page 166
  - [Importing Cleaning Cartridges via the Web Client](#) on page 167

### Importing Cleaning Cartridges via the Operator Panel

- 1 Select **Actions > I/E > Import Cleaning Tape**.

A list of all the cleaning cartridges present in the I/E station displays.

- 2 If more than one cleaning cartridge is present in the I/E station, use the **Up** and **Down** buttons to select a cleaning cartridge to import, or select **ALL** to import all cleaning cartridges. The **ALL** option is only available if there are enough empty cleaning slots in the library to accommodate all the cleaning cartridges.

**3 Press Import.**

The library moves the cleaning cartridge to a previously configured cleaning slot.

## Importing Cleaning Cartridges via the Web Client

**1 Select Operations > Cleaning Media > Import.**

The **Operations - Import Cleaning Media** screen displays. This screen contains a list of the cleaning cartridges in the I/E station. If no cleaning slots are configured, a message displays stating that the library cannot import cleaning cartridges.

**2 Note the number of empty cleaning slots that appear in the Total Empty Cleaning Slots field on the right side of the screen. The number of cleaning cartridges you can import is limited to the number of empty cleaning slots.**

**3 Select one or more cleaning cartridges to import. An error displays if the number of selected cleaning cartridges is more than the number of empty cleaning slots.**

---

**Note:** If not all cartridges appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

---

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

---

## Exporting Cleaning Cartridges

When AutoClean is enabled (at least one cleaning slot has been configured), you can 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 61. For a description of AutoClean, see [About AutoClean](#) on page 164.

---

**Note:** If your library has zero I/E station slots, you cannot import or export cleaning media. See [Configuring I/E Station Slots](#) on page 63.

---

---

**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.

---

The number of cleaning cartridges you can export is limited to the number of empty I/E station slots.

You can export cleaning cartridges from either the operator panel or the Web client.

### Operator Panel

- 1 Select **Actions > I/E > Export Cleaning Tape**.
- 2 Use the **Up** and **Down** buttons to select a cleaning cartridge to export. You may also select **ALL** to export all cleaning cartridges; however, the **ALL** option is only available if there are enough empty slots in the I/E station to accommodate all the cleaning cartridges.
- 3 Press **Export**.

The library moves the selected cleaning cartridge to an I/E station slot.

### Web Client

- 1 Select **Operations > Cleaning Media > Export**.

The **Operations - Export Cleaning Media** screen displays. This screen contains a list of the cleaning cartridges in the library. The media barcode, location coordinates, media type, and cleaning status (usable/expired) are displayed for each cartridge.

- 2 Note the number of empty I/E station slots that appear in the **Empty I/E Station Slots** field on the right side of the screen. The number of cleaning cartridges you can export is limited to the number of empty I/E station slots.

- 3 Select one or more cleaning cartridges to export. An error displays if the number of selected cleaning cartridges is more than the number of empty cleaning slots.

---

**Note:** If not all cartridges appear on the screen, use the **Page 1 of x** arrows to view the additional cartridges.

---

---

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

---

- 4 Click **Apply**.

The library moves the selected cleaning cartridge to an I/E station slot.

---

## Manually Cleaning Tape Drives

---

When a tape drive needs cleaning, it notifies the library. If the library's AutoClean feature is not enabled (meaning, no cleaning slots have been configured), the library generates a diagnostic ticket informing you that the tape drive needs cleaning.

Details about manually cleaning tape drives include:

- 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.
- Be sure to use a valid cleaning cartridge. If you use a data cartridge, for example, the operation may complete but the tape drive will not have been cleaned, and the library will issue a diagnostic ticket. See [Valid Cleaning Cartridges](#) on page 164.
- If you have at least one cleaning slot configured (see [Configuring Cleaning Slots](#) on page 61), the library uses a cleaning cartridge from either the topmost I/E station slot, or a configured cleaning slot. If the cleaning cartridge is in the top I/E station slot and manual cartridge assignment is enabled, assign the cleaning cartridge to the System partition.
  - On the Web client, you can choose to use a configured cleaning slot or the topmost I/E station slot. If two or more cleaning slots are configured and have cleaning cartridges in them, the library chooses which cleaning cartridge to use.

- On the operator panel, the library chooses which cleaning cartridge to use, in this order: 1) topmost I/E station slot, and 2) one of the configured cleaning slots.
- If you have zero cleaning slots configured, you must use a cleaning cartridge in the topmost I/E station slot. If manual cartridge assignment is enabled, assign the cleaning cartridge to the System partition.
- The associated partition is 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 partition offline.
- When the operation is complete, the library moves the cleaning cartridge back to the I/E station slot or cleaning slot.

You can clean tape drives manually at any time using commands on the operator panel or the Web client.

### Operator Panel

- 1 Select **Actions > Tape Drive > Manual Cleaning**.
- 2 If more than one tape drive is in the library, use the **Up** and **Down** buttons to select a tape drive to clean, then press **Clean**.
- 3 When the operation completes, press **OK**.

### Web Client

- 1 Select **Tools > Drive Operations**.
- 2 Select **Clean a tape drive** and click **Next**.
- 3 If more than one partition exists, select the partition that contains the tape drive you want to clean, and click **Next**.

The **Clean Drive - *Partition (Mode)*** screen displays, where *Partition* is the name of the partition and *Mode* is the current mode (online/offline) of the partition. This screen contains a list of tape drives assigned to the partition.

- 4 If you have no cleaning slots configured, skip this step (you will use the top I/E station slot as the source for your cleaning cartridge). If you have at least one cleaning slot configured, you are asked to **Select Cleaning Source**. Select which location to take the cleaning cartridge from:
  - **Use the top I/E slot** — Allows you to use a cleaning cartridge from the topmost I/E station slot. Make sure to install a cleaning cartridge in the topmost I/E station slot. If manual cartridge assignment is enabled, assign the cleaning cartridge to the System partition.
  - **Use configured cleaning tapes** — Allows you to use a cleaning cartridge from a configured cleaning slot. If two or more cleaning slots are configured and have cleaning cartridges in them, the library chooses which cleaning cartridge to use.
- 5 Select one or more tape drives to clean.

---

**Note:** If not all tape drives appear on the screen, use the **Page 1 of x** arrows to view the additional tape drives.

---

---

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

---

- 6 Click **Apply**.
- 7 Click **OK** to confirm it is OK to take the partition offline.

The library moves the cleaning cartridge to the tape drive and cleans it. When finished, it moves the cartridge back to the cleaning slot or I/E station.

## 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. A drive taken offline will remain offline until you bring it back online, or until the library is rebooted. 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 online/offline state follows the tape drive slot, not the particular tape drive (if the tape drive were to be moved to a different slot in the library).
- You can select only tape drives in partitions to which you have been given access.
- If you change the mode of a control path tape drive to offline, a caution dialog displays asking you to confirm the mode change. For information on control path tape drives, see [Configuring Control Paths](#) on page 67.

You can change the tape drive mode from both the operator panel and the Web client.



## Operator Panel

- 1 Select **Actions > Tape Drive > Change Mode**.
- 2 If more than one tape drive is in the library, use the **Up** and **Down** buttons to select a tape drive.
- 3 Press **Modify**.
- 4 Use the **Up** and **Down** buttons to select **Online** or **Offline**.
- 5 Press **Apply**.  
The new mode is displayed.
- 6 Press **Exit**.

## Web Client

- 1 Select **Operations > Drive > Change Mode**.

The **Change Drive Mode** screen displays. This screen lists each tape drive's partition, location, state, current mode, activity, and version.

---

**Note:** If more than four tape drives are installed in the library, use the **Page 1 of x** arrows to view the additional tape drives.

---

- 2 Locate the tape drive that you want to take offline or bring online. In the tape drive table under **Mode**, the **Current** column indicates the current mode of the partition. The **New** column contains an **Online/Offline** button. The button toggles between modes.
- 3 Toggle the **Online/Offline** button to the desired mode.

---

**Note:** If you change the mode of a control path tape drive to offline, a caution dialog displays asking you to confirm the mode change. For information on control path tape drives, see [Configuring Control Paths](#) on page 67.

---

- 4 Click **Apply**.





## Chapter 7

# Encryption Key Management

---

Encryption Key Management (EKM) is a licensable feature. You must have an EKM license installed on your library in order to use the encryption key management features described in this chapter. For more information on licensing, see [Adding or Upgrading Licensable Features](#) on page 69.

The Scalar i40 and Scalar i80 libraries support Scalar Key Manager (SKM), an encryption solution using HP LTO-4 and HP LTO-5 Fibre Channel and SAS tape drives and LTO-4 and LTO-5 tape cartridges only.

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

If you purchase SKM, you will receive the software application, two servers (optional beginning with SKM 1.1), and installation and configuration instructions. This chapter describes how to configure SKM on the library. This chapter also describes all of the EKM functions available on the library.

Refer to your *Scalar Key Manager User's Guide* for information on how to manage SKM outside of the library.

This chapter covers:

- [About the EKM License](#)
- [Configuring Scalar Key Manager \(SKM\) on the Library](#)
- [EKM Path Diagnostics](#)
- [Viewing Tape Drive Encryption Settings](#)
- [Scalar Key Manager Functions Available on the Library](#)

---

## About the EKM License

If you purchase an EKM license after you purchased your library, you must install the license key on your library to enable the EKM functionality. See [Adding or Upgrading Licensable Features](#) on page 69 for instructions.

The EKM license applies to the entire library, regardless of how many slots are licensed. If you increase the number of slots in your library, your existing license applies to your new library configuration.

---

## Configuring Scalar Key Manager (SKM) on the Library

Follow these steps to configure SKM on the library.

---

### Step 1: Upgrade Firmware

---

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

---

### Step 2: Install the EKM License Key on the Library

---

If your EKM license key is not already installed on the library, install it now (see [Adding or Upgrading Licensable Features](#) on page 69).

---

### Step 3: Install SKM on a Server or Servers

---

You must use two key servers with SKM. You can purchase the two servers from Quantum or provide your own. Follow the instructions that came with your SKM system for installing SKM software on the servers.

---

**Note:** Make sure ports 80, 6000, and 6001 on the SKM servers are opened up in a bi-directional mode. If they are not, the library will not be able to communicate with the SKM servers.

---

---

### Step 4: Configure Encryption Settings and Key Server Addresses

---

Make sure to complete the above steps before proceeding.

---

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

---

- 1 Unload tape cartridges from all encryption-capable tape drives in the library.
- 2 From the Web client, select **Setup > Encryption > System Configuration** (see [Figure 31](#)).

Figure 31 Configuring Encryption Settings and Key Server Addresses

Setup Operations Tools Reports User: admin [Admin]

### Setup - Encryption System Configuration

Set up the encryption key management server access for library managed encryption.  
Host names may be entered if DNS is configured; otherwise enter IPv4 or IPv6 addresses only.

Note: These default server settings are only applicable when a partition's encryption method is set to library managed encryption, see Setup->Encryption->Partition Configuration.

Automatic EKM Path Diagnostic:  Enabled  
10 min Interval

SSL Connection:  Enabled

Primary Key Server IP Address or Host: 10.20.224.75

Primary Key Server Port Number: 6000

Secondary Key Server IP Address or Host: 10.20.224.76

Secondary Key Server Port Number: 6000

[Click here](#) to run EKM Path Diagnostics.

Cancel Apply

**3 Automatic EKM Path Diagnostics:** Enable or disable this feature and set the test interval as desired. For more information, see [Enabling Automatic EKM Path Diagnostics](#) on page 184).

**4 Secure Sockets Layer (SSL):** SSL is always enabled. The SSL port number is always 6000.

---

**Note:** While the setting is called SSL, the library actually uses Transport Layer Security (TLS), a more secure successor to SSL, to communicate with the encryption servers.

---

**5 In the Primary Key Server IP Address or Host text box,** enter either:

- The IP address of the primary key server (if DNS is not enabled), or
- The host name of the primary key server (if DNS is enabled).

**6 Port Number:** The port number is always 6000. You cannot change SKM port numbers.

**7 Enter the IP address or host name of the secondary key server into the Secondary Key Server IP Address or Host text box.**

**8 Click Apply.**

---

### Step 5: Install TLS Communication Certificates on the Library

---

Depending on when your library was manufactured, TLS certificates may already be installed. If they are not installed, you must install them. See [Installing TLS Certificates on the Library](#) on page 186 for instructions on how to verify whether they are installed, and how to install them.

---

### Step 6: Run EKM Path Diagnostics

---

Run the Manual EKM Path Diagnostics to be sure the library is connected properly to both SKM servers. See [Running Manual EKM Path Diagnostics](#) on page 183 for instructions.

---

### Step 7: Configure SKM Partitions and Generate Data Encryption Keys

---

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

Data written to encryption-supported and encryption-capable media in EKM-supported tape drives will be encrypted *unless* data was previously written to the media in a non-encrypted format. For data to be encrypted, the media must be blank or have been written to using library managed encryption at the first write operation at the beginning of tape (BOT).

Configure the partition(s) as follows:

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

A list of all your partitions displays, along with a drop-down list displaying the Encryption Method for each partition (see [Figure 32](#)).

---

**Note:** The default Encryption Method for a partition containing encryption-capable tape drives is **Allow Application Managed**. To enable SKM encryption on a partition, you must set the Encryption Method to **Enable Library Managed**. This is explained in the following steps.

---

Figure 32 Configuring  
Partition Encryption

Setup Operations Tools Reports User: admin [Admin]

### Setup - Encryption Partition Configuration

Set up the Encryption for library partitions.

Note: Encryption is supported on LTO-4 and LTO-5 media and HP LTO-4 and LTO-5 Fibre Channel and SAS tape drives. For more information refer to the online help or user's guide.  
Select "Allow Application Managed" as the encryption method to disable library managed encryption. The "Allow Application Managed" encryption selection allows your backup application to control when encryption is used. If your backup application is not configured to control encryption, data will not be encrypted.

LME Settings

Partition	Primary Host : Port	Secondary Host : Port	SSL Key Server	Encryption Method
library_a	10.20.224.76 : 6000	10.20.224.76 : 6000	<input checked="" type="checkbox"/> SKM	Allow Application Managed
library_b	10.20.224.76 : 6000	10.20.224.76 : 6000	<input checked="" type="checkbox"/> SKM	Allow Application Managed

[Click here](#) to run EKM Path Diagnostics

Cancel Apply

- 2 If you want to change the encryption method for a partition, make sure that no tape drives in that partition have cartridges loaded in them. If tape drives have cartridges loaded, you cannot change the encryption method.
- 3 Select an encryption method from the drop-down list for each partition. See [Table 6](#) on page 181 for a description of the encryption methods. (For tape drives that support encryption, the default is **Allow Application Managed**.) The encryption method applies to all encryption-capable tape drives and media in that partition.

---

**Note:** When you change the encryption method on a partition, the partition is taken offline. When the change completes, the partition comes back online automatically.

---



Table 6 Encryption Methods

Encryption Method	Description
Enable Library Managed	<b>For use with EKM.</b> Enables encryption support via a connected EKM key server for all encryption-capable tape drives and media assigned to the partition.
Allow Application Managed	<p><b>Not for use with EKM.</b> Allows an external backup application to provide encryption support to all encryption-capable tape drives and media within the partition. The library will NOT communicate with the EKM key server on this partition.</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 are connecting the library to an external EKM key server.</p> <p><b>Note:</b> If you want an external application to manage encryption, you must specifically configure the application to do so. The library will not participate in performing this type of encryption.</p>
Unsupported	<p>Means that no tape drives in the partition support encryption.</p> <p>If <b>Unsupported</b> is shown, it will be greyed out and you will not be able to change the setting.</p>

4 Click **Apply**.

**Data encryption keys are generated.** When you set the Encryption Method to **Enable Library Managed** on a partition for the first time, the library automatically triggers each SKM server to generate a set of unique data encryption keys. This may take 15 minutes to an hour or longer, depending on network performance. The library notifies you when the process is complete.

5 Wait for the process to complete before resuming library operations.

- 6 Back up both SKM servers following the instructions in the *Scalar Key Manager User's Guide*.

---

**Caution:** You must back up both SKM servers every time you generate new data encryption keys to protect against catastrophic server failure.

---

---

### Step 8: Save the Library Configuration

---

See [Saving the Library Configuration](#) on page 107 for instructions.

---

## 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.

There are two ways to run EKM Path Diagnostics:

- **Manually** — Run the Manual EKM Path Diagnostics any time you change the key server settings or library encryption settings. See [Running Manual EKM Path Diagnostics](#) on page 183 for details.
- **Automatically** — This feature runs automatically in the background and generates diagnostic tickets if there are problems. You can turn this feature off but it is recommended that you leave it on. See [Enabling Automatic EKM Path Diagnostics](#) on page 184 for details.

---

### Description

---

The EKM Path Diagnostics consists of the following tests:

- **Ping** — Verifies the Ethernet communication link between the library and the key servers.
- **Path** — Verifies that EKM services are running on the key servers.
- **Config** — Verifies that the key servers are capable of serving encryption keys.

---

## Failure Scenarios

---

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.
- **Path Test Failure** — Verify that the key server is actually running and that the IP address configured on the library is correct. Check to see if there is a network configuration issue, such as a firewall, preventing communication with the server.
- **Config Test Failure** — A database inconsistency has been detected. Contact Quantum Support.

---

## Running Manual EKM Path Diagnostics

---

- 1 Access the EKM Path Diagnostics screen in one of two ways:
  - Select **Setup > Encryption > System Configuration** or **Setup > Encryption > Partition Configuration** and click the link that says “Click here to run EKM Path Diagnostics.”
  - Enter library Diagnostics (from the Web client select **Tools > Diagnostics**) and then select **EKM > EKM Path Diagnostics**. Note that entering 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. See [Performing Library Diagnostics](#) on page 330 for more information.
- 2 Click **Apply**.
- 3 The library performs the diagnostics and displays pass/fail results on each of the tests in the Progress Window. This may take several minutes. If a test fails, try the solutions listed under [Failure Scenarios](#) on page 183.
- 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 able to be performed.

## Enabling Automatic EKM Path Diagnostics

You can enable the library to automatically perform EKM Path Diagnostics at selected intervals. During each interval, the library tests every configured key server. The default test interval is 10 minutes. The library generates a diagnostic ticket if there are problems.

Automatic EKM Path Diagnostics is enabled by default and should always be left enabled. You should not need to disable it unless Quantum Support directs you to do so.

For a list of tests performed, see [EKM Path Diagnostics](#) on page 182.

To enable Automatic EKM Path Diagnostics:

- 1 From the Web client, select **Setup > Encryption > System Configuration** (see [Figure 33](#)).
- 2 Select the **Automatic EKM Path Diagnostics** check box.
- 3 Select a test interval from the **Interval** drop-down list.

Figure 33 Enabling Automatic EKM Path Diagnostics

Setup Operations Tools Reports User: admin [Admin]

### Setup - Encryption System Configuration

Set up the encryption key management server access for library managed encryption.  
Host names may be entered if DNS is configured; otherwise enter IPv4 or IPv6 addresses only.

Note: These default server settings are only applicable when a partition's encryption method is set to library managed encryption, see Setup->Encryption->Partition Configuration.

Automatic EKM Path Diagnostic:  Enabled  
10 min Interval

SSL Connection:  Enabled

Primary Key Server IP Address or Host: 10.20.224.75

Primary Key Server Port Number: 6000

Secondary Key Server IP Address or Host: 10.20.224.76

Secondary Key Server Port Number: 6000

[Click here](#) to run EKM Path Diagnostics.

Cancel 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. For more information, see [Viewing System Information](#) on page 206.
- **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. For more information, see [Viewing the Library Configuration Report](#) on page 210.
- **Partition Encryption** — From the Web client, select **Setup > Encryption > Partition Configuration** to view and change the encryption settings of partitions. See [Step 7: Configure SKM Partitions and Generate Data Encryption Keys](#) on page 179 for more details.

## Scalar Key Manager Functions Available on the Library

Once the SKM servers are set up, most SKM functions occur automatically without user action required. SKM provides some key management capability through the library Web client.

For a complete description and instructions for using these features, see the library Web client online help or the *Scalar Key Manager User's Guide*.

These functions are:

- [Installing TLS Certificates on the Library](#)
- [Generating Data Encryption Keys](#)
- [Sharing Encrypted Tape Cartridges](#)
- [Exporting Encryption Certificates](#)

- [Importing Encryption Certificates](#)
- [Exporting Data Encryption Keys](#)
- [Importing Data Encryption Keys](#)
- [Accessing the SKM Server Logs](#)
- [Using the SKM Encryption Key Import Warning Log](#)

---

## Installing TLS Certificates on the Library

---

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

If TLS certificates are not installed, you must install them. You can install either Quantum-provided TLS certificates, or your own TLS certificates.

At any time, you may install a new set of TLS certificates to overwrite the existing set. The new TLS certificates must all be valid or the overwrite will not occur and the existing certificates will remain in place.

### Checking Whether TLS Certificates are Installed on Library

Your library may have come with TLS certificates pre-installed. You can check the Web client to see if certificates are installed (**Tools > EKM Management > Import Communication Certificates**). At the bottom of the page, a message tells you whether TLS certificates are currently installed. If certificates are installed, a table appears below the message containing information about the installed certificates. See [Figure 34](#) on page 187.

Figure 34 Checking and Installing TLS Certificates

Fill out this section if installing user-supplied TLS certificates

Fill out this section if installing Quantum-supplied TLS certificates

Tells you whether TLS certificates are currently installed on the library

Setup Operations Tools Reports User: admin [Ad

### Tools - EKM Communication Certificate Import

Import TLS communication certificate(s).

Note: Transport layer security (TLS) certificates may be uploaded by browsing to the files and selecting Apply. Either individual certificates or a Quantum certificate bundle may be uploaded and installed.

Primary Server: Available      Secondary Server: Available

Root Certificate File:  Browse...

Admin Certificate File:  Browse...

Admin Certificate Password:

Client Certificate File:  Browse...

Client Certificate Password:   Use Admin's Password

Use the Quantum Certificate Bundle:

Quantum Communication Certificate Bundle File:  Browse...

(TLS communication certificates are currently installed on the library.)

Type	Location	Serial Number	Valid Between Dates	Status	Issuer and Subject
Root	Library	AC3141FD4627D	May 1 17:45:39 2009 GMT May 1 17:45:39 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA
Client	Library	F3	May 1 19:01:53 2009 GMT May 1 19:01:53 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:QKM CN:QKM CLIENT 000081
Admin	Library	F2	May 1 19:01:52 2009 GMT May 1 19:01:52 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:akm_admin CN:QKM ADMIN 000081
Root	Primary Server	AC3141FD4627D	May 1 17:45:39 2009 GMT May 1 17:45:39 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA
Server	Primary Server	5B	May 1 19:01:08 2009 GMT May 1 19:01:08 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:QKM CN:QKM TLS 000031
Root	Secondary Server	AC3141FD4627D	May 1 17:45:39 2009 GMT May 1 17:45:39 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA
Server	Secondary Server	5B	May 1 19:01:08 2009 GMT May 1 19:01:08 2019 GMT	Valid	Issuer: C:US S:CA L:SAN JOSE O:QUANTUM OU:MFG CN:QKM CA Subject: C:US S:CA L:SAN JOSE O:QUANTUM OU:QKM CN:QKM TLS 000031

X Cancel
Apply ✓

## Installing Quantum-Supplied TLS Certificates

The Quantum-supplied certificates come on a CD which you received. The TLS certificates are bundled in a single file.

- 1 Ensure that the date on both SKM servers and the library are set to the current date. Incorrect date settings may interfere with the TLS certificates and cause the library to stop communicating with the SKM servers.
- 2 Insert the CD into the CD ROM drive of your computer. Either copy the file to a known location on your computer or use the CD as the location from which you will retrieve the file.
- 3 From the **Tools** menu, select **EKM Management > Import Communication Certificates**.

The **Tools - EKM Communication Certificate Import** screen opens (see [Figure 34](#) on page 187). At the top of the page, the primary and secondary key server status is displayed. If the status is "Not Available," it means there is no communication with the server. The most likely causes are that the server is down, not connected, or not configured correctly on the library; or that no TLS certificates are installed or the TLS certificates are invalid or expired. At the bottom of the page, a message tells you whether TLS certificates are currently installed. If certificates are installed, a table appears below the message containing information about the installed certificates.

- 4 Select the **Use the Quantum Certificate Bundle** checkbox.
- 5 Click the **Browse** button next to the Quantum Communication Certificate Bundle File field and locate the TLS certificate file.
- 6 Click **Open**.
- 7 Click **Apply**.
- 8 Verify that the TLS certificates are now installed in the library. At the bottom of the page is a statement letting you know whether the certificates are currently installed. In addition, the three rows of the table at the bottom of the screen should be filled in with the correct information.



## Installing Your Own TLS Certificates

When providing your own certificates, it is assumed you understand the concepts of PKI (Public Key Infrastructure) and can access the tools or third-party resources needed to generate or obtain certificates.

---

**Note:** You must be running SKM 1.1 or higher on your SKM servers in order to install your own TLS certificates.

---

**Note:** If you install your own TLS certificates on the SKM server, you must also install your own certificates on the library. Similarly, if you use the Quantum-provided TLS certificates on the SKM server, you must also use the Quantum provided TLS certificates on the library. Newer libraries come with Quantum-provided TLS certificates pre-installed. To verify whether TLS certificates are already installed on the library, refer to [Checking Whether TLS Certificates are Installed on Library](#) on page 186.

---

You need to provide the following certificates:

- Root certificate (also called the CA certificate, or Certificate Authority certificate)
- Client certificate
- Admin certificate

These files must be in the proper format, as follows. If any of the following requirements is not met, none of the certificates will be imported.

- The Root Certificate must be 2048 bits.
- The Root Certificate must be in PEM format.
- Admin and Client certificates must be in pkcs12 (.p12) format, with a separate certificate and private key contained in each.
- Admin and Client certificates must be 1024 bits.
- Admin and Client certificates must be signed by the Root Certificate.
- Certificates must have the Organization name (O) set in the Issuer and Subject information.
- The Admin certificate must have its Organizational Unit name (OU) set as "akm\_admin" in its Subject Information.

- The same Root certificate must be installed on the SKM servers and the library.
- All the certificates have a valid validity period, according to the library's date and time settings.

To install your own certificates:

- 1 Ensure that the date on both SKM servers and the library are set to the current date. Incorrect date settings may interfere with the TLS certificates and cause the library to stop communicating with the SKM servers.
- 2 Place the TLS certificate files in a known location on your computer.
- 3 From the **Tools** menu, select **EKM Management > Import Communication Certificates**.

The **Tools - EKM Communication Certificate Import** screen opens (see [Figure 34](#) on page 187). At the top of the page, the primary and secondary key server status is displayed. If the status is "Not Available," it means there is no communication with the server. The most likely causes are that the server is down, not connected, or not configured correctly on the library; or that no TLS certificates are installed or the TLS certificates are invalid or expired. At the bottom of the page, a message indicates whether TLS certificates are currently installed. If certificates are installed, a table appears below the message containing information about the installed certificates.

- 4 Make sure the **Use the Quantum Certificate Bundle** checkbox is deselected.
- 5 Click the **Browse** button next to the **Root Certificate File**. Locate the file and click **Open**.
- 6 Click the **Browse** button next to the **Admin Certificate File**. Locate the file and click **Open**.
- 7 Enter an Admin Certificate Password. This is the password you created when you created the Admin Certificate file. The password allows the library to read the file.
- 8 Click the **Browse** button next to the **Client Certificate File**. Locate the file and click **Open**.

- 9 Enter a Client Certificate Password. This is the password you created when you created the Client Certificate file. The password allows the library to read the file. If you want to use the same password as the Admin Certificate password, then just select the **Use Admin's Password** checkbox.
- 10 Click **Apply** to import the files onto the library.
- 11 Verify that the TLS certificates are now installed in the library. At the bottom of the page is a statement indicating whether the certificates are currently installed. In addition, the three rows of the table at the bottom of the screen should be filled in with the correct information.

---

## Generating Data Encryption Keys

---

---

**Caution:** Every time you generate new data encryption keys, you must back up both SKM servers before you begin using the keys to encrypt data. Refer to the *SKM User's Guide* for instructions.

---

Data encryption keys are generated in sets of a specified quantity (see the *Scalar Key Manager User's Guide* for more information).

The library tracks data encryption key usage and reminds you to generate more keys when needed. If you try to generate data encryption keys on an SKM server that already has sufficient unused data encryption keys, then it will not create more. You will receive a message to that effect on the library remote Web client.

---

**Note:** Each library that you connect to an SKM server requires its own set of data encryption keys. Each library only pulls data encryption keys from the set that "belongs" to it. This means that an SKM server may contain several distinct sets of data encryption keys. When the data encryption keys for one library have all been used, then more keys must be generated.

---

You can generate data encryption keys in the following ways:

- [Generating Data Encryption Keys at Initial Setup](#)
- [Generating Data Encryption Keys When 80% Depleted](#)
- [Generating Data Encryption Keys When 100% Depleted](#)
- [Manually Generating Data Encryption Keys](#)

## Generating Data Encryption Keys at Initial Setup

At initial setup, the library triggers each SKM server to generate a set of data encryption keys. The process is described in [Step 7: Configure SKM Partitions and Generate Data Encryption Keys](#) on page 179.

## Generating Data Encryption Keys When 80% Depleted

When an SKM server has used 80 percent of the data encryption keys assigned to a particular library, that library generates a diagnostic ticket to let you know. Once you receive the diagnostic ticket, you should schedule a time to manually generate more data encryption keys as described in [Manually Generating Data Encryption Keys](#) on page 192 and back up both SKM server keystores.

## Generating Data Encryption Keys When 100% Depleted

If an SKM server completely runs out of data encryption keys for a particular library, that library generates a diagnostic ticket, which states that you have run out of data encryption keys and that the library attempted to fail over to the other SKM server. If this happens, it is imperative that you manually generate a new set of data encryption keys on the depleted server immediately and then back up both SKM server keystores. See [Manually Generating Data Encryption Keys](#) on page 192.

## Manually Generating Data Encryption Keys

To manually generate data encryption keys, you need to temporarily disable library managed encryption on a partition, and then enable it again. Enabling library managed encryption on a partition triggers the library to check both SKM servers to see if new data encryption keys are needed. If so, it creates the keys.

**Note:** The key generation process takes 15 minutes to an hour, depending on network performance and quantity of keys already used. The library notifies you when the process completes. During key generation and backup, the SKM server will not be able to process any library requests for data encryption keys. You should not run any library or host-initiated operations on SKM partitions during key generation and backup.

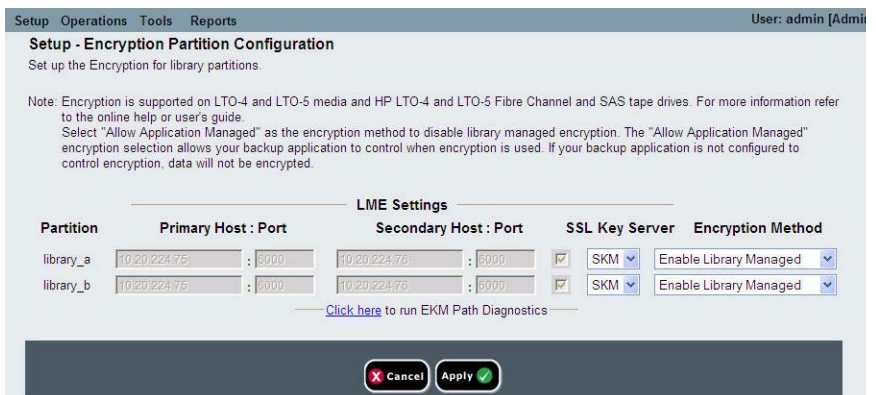
**Caution:** Avoid manually generating keys on more than five libraries simultaneously as the key generation process is resource-intensive on the server. Generating keys manually on more than five libraries at once could result in a failure to complete the key generation operation, or interfere with key retrieval operations.

If a failure does occur during key generation, wait 10 minutes, then try to start it again. The key generation process will resume from where the error was encountered.

To manually generate data encryption keys:

- 1 Make sure that both SKM servers are running and operational.
- 2 From the library's Web client, access the encryption partition configuration screen (**Setup > Encryption > Partition Configuration**). See [Figure 35](#) on page 193.

Figure 35 Accessing the Encryption Partition Configuration Screen



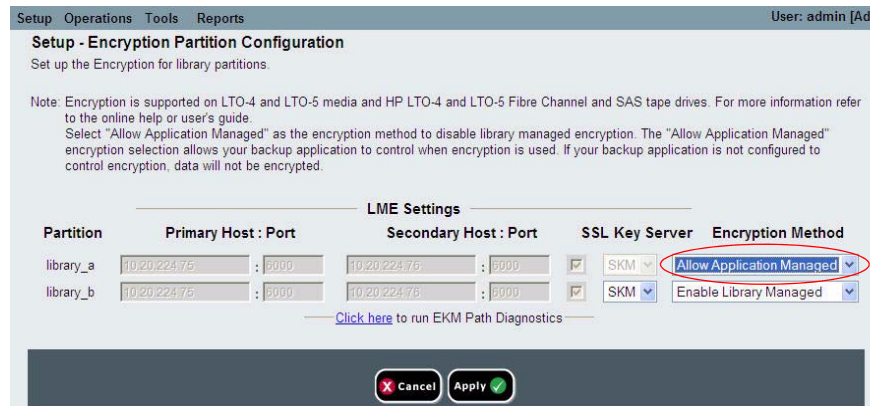
- 3 Select an SKM partition configured for library managed encryption, and temporarily disable library managed encryption by changing the Encryption Method from **Enable Library Managed** to **Allow Application Managed** (see [Figure 36](#) on page 194). *Remember which partition it is*, because you will be changing it back in a few minutes.
- 4 Click **Apply**.

---

**Caution:** When you change the partition's encryption method to **Allow Application Managed**, the data that was written to the tapes while the partition was configured for **Enable Library Managed** can no longer be read, until you change the partition back to **Enable Library Managed**. You will only be disabling for a short time, and then changing back to **Enable Library Managed** (just to trigger the key generation process) so this should have little effect, unless you forget to turn it back to **Enable Library Managed**.

---

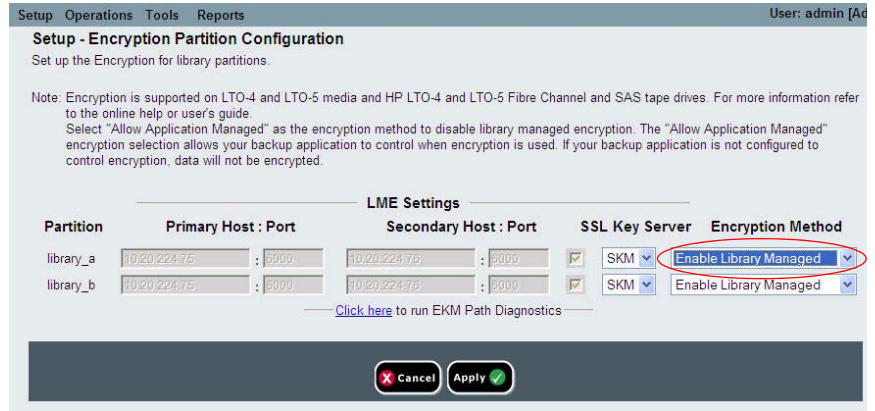
Figure 36 Changing Encryption Method to Allow Application Managed



- 5 Wait 3 minutes to allow the changes to complete.
- 6 Go back to the encryption partition configuration screen and change the Encryption Method back to **Enable Library Managed** (see [Figure 37](#)).
- 7 Click **Apply**.

**Data encryption keys are generated.** The library triggers the SKM server to generate a set of unique data encryption keys. This takes 15 minutes to an hour or longer, depending on network performance. The library notifies you when the process is complete.

Figure 37 Changing Encryption Method Back to Enable Library Managed



- 8 Wait for the process to complete before resuming library operations.
- 9 Back up both SKM server keystores. See the *Scalar Key Manager User's Guide* for instructions on backing up the keystores.

---

**Caution:** You must back up the keystores every time you generate new data encryption keys to protect against catastrophic server failure.

---

## Sharing Encrypted Tape Cartridges

If you are using SKM, you can share encrypted tapes with other companies and individuals who also use SKM for managing encryption keys.

Each SKM server provides a unique encryption key for each tape cartridge that is encrypted. To read an encrypted tape in a library that is attached to an SKM server that is different than the server that originally provided the encryption key, the encryption key from the originating (i.e., source) SKM server needs to be shared with the receiving (i.e., destination) SKM server. The key (or list of keys, if there is more than one tape), is exported from the source SKM server to a file, which is sent to the destination recipient. Each key contained in the file is encrypted using the public key of the destination SKM server. The destination SKM server provides its public key to the source SKM server as part of an Encryption Certificate, which the source SKM server uses to wrap (encrypt) the encryption keys for transport. Upon arrival, the file containing the wrapped encryption keys can only be unwrapped by the corresponding private key, which resides on the destination SKM server and is never shared.

The process is as follows:

- 1 The destination administrator exports the Encryption Certificate that belongs to the destination SKM server. The Encryption Certificate is saved as a file to a location specified by the administrator on a computer (see [Exporting Encryption Certificates](#) on page 197).
- 2 The destination administrator e-mails the Encryption Certificate file to the source administrator.
- 3 The source administrator saves the Encryption Certificate file to a location on a computer, and then imports the Encryption Certificate onto the source SKM server (see [Importing Encryption Certificates](#) on page 198).
- 4 The source administrator exports the Encryption Keys, assigning the same Encryption Certificate noted above to wrap (encrypt) the keys. The file containing the wrapped encryption keys is saved to a location on a computer specified by the source administrator. See [Exporting Data Encryption Keys](#) on page 199.
- 5 The source administrator e-mails the file containing the wrapped encryption keys to the destination administrator.
- 6 The destination administrator saves the file containing the wrapped encryption keys to a location on a computer, and then imports the keys onto the destination SKM server (see [Importing Data Encryption Keys](#) on page 201).
- 7 The destination library can now read the encrypted tapes.



For more information about the key servers and library managed encryption best practices, please refer to the *Scalar Key Manager User's Guide*.

## Exporting Encryption Certificates

To receive encryption keys from another SKM server, you must first send your native encryption certificate to that server. The public key contained in the certificate will be used to wrap (encrypt) the encryption keys to protect them during transport to you.

This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to import encryption keys.

To export an encryption certificate:

- 1 Before starting this process, read and follow the sequence of steps outlined in [Sharing Encrypted Tape Cartridges](#) on page 195.
- 2 From the **Tools** menu, select **EKM Management > Encryption Certificate > Export**. See [Figure 38](#).

Figure 38 Exporting Encryption Certificates



- 3 Click **Apply** to export your SKM server's native encryption certificate.
- 4 Click **Close** to close the Progress Window.
- 5 In the File Download dialog box that appears, click **Save**.
- 6 In the **Save As** dialog box that opens, choose a location in which to save the file, then click **Save**.

## Importing Encryption Certificates

The encryption certificate contains a public key that is used to wrap (encrypt) encryption keys prior to transporting them to another SKM server. When sharing tape cartridges, you need to import the encryption certificate of the destination SKM server.

**Note:** This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to import encryption keys.

To import encryption certificates:

- 1 Before starting this process, read and follow the sequence of steps outlined in [Sharing Encrypted Tape Cartridges](#) on page 195.
- 2 Receive the encryption certificate file from the destination SKM server administrator and save it to a known location on your computer.
- 3 From the **Tools** menu, select **EKM Management > Encryption Certificate > Import**.

Figure 39 Importing Encryption Certificates



- 4 Click **Browse** to locate the saved encryption certificate file.
- 5 Click **Open**.
- 6 Click **Apply** to import the certificate onto your SKM server.
- 7 Back up both SKM servers to protect against catastrophic server failure.

## Exporting Data Encryption Keys

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

**Note:** This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to import encryption keys.

To export encryption keys:

- 1 Before starting this process, read and follow the sequence of steps outlined in [Sharing Encrypted Tape Cartridges](#) on page 195.
- 2 From the **Tools** menu, select **EKM Management > Encryption Key > Export**.

Figure 40 Exporting  
Encryption Keys

Setup Operations Tools Reports

**Tools - SKM Encryption Key Export**

Encryption Key Export allows you to export selected encryption keys from the attached SKM server to a file so that the encryption keys can be imported into another target library.

Note: Make sure the certificate from the target library has been imported and can be selected for the encryption key export operation. Depending on the number of keys being exported, this operation could take several minutes.

Certificate Name Used For Export

Export Used

Export Current

Export Selective

- 3 Assign the encryption certificate with which you will “wrap” (encrypt) the keys by selecting it from the **Certificate Name Used For Export** drop-down list. Choose the certificate that belongs to the server to which the keys will be imported.

---

**Note:** The owner of that server should have sent you the certificate and you should have imported it (see [Sharing Encrypted Tape Cartridges](#) on page 195 and [Importing Encryption Certificates](#) on page 198). The drop-down list contains all of the encryption certificates that you have ever imported onto your SKM server (indicated by the word “imported” in the list), as well as the certificate belonging to your SKM server pair (indicated by the word “native” in the list).

---

- 4 Select which SKM encryption keys to export from the following options:
  - **Export Used** — Exports all the keys that have ever been used to encrypt tape cartridges on the library performing this export. Also exports all keys that were imported onto the key server, via a “key import” operation, from any library.
  - **Export Current** — Exports all the keys that were used to encrypt the tape cartridges that are currently in the library performing this export. This includes storage slots, I/E stations, and tape drives. If a tape cartridge is no longer in the library, the key used to encrypt it will not be exported. If a tape cartridge is missing its label, the key used to encrypt it will not be exported.
  - **Export Selective** — Exports only the key(s) associated with a string of characters that you type into the text box. Each key is associated with its encrypted tape cartridge, identified by the tape cartridge barcode. You can type in all or part of a tape cartridge barcode, and any keys that are associated with that string will be exported. This is helpful if you only want to export a single key associated with a particular tape cartridge.
- 5 Click **Apply**.

All the exported keys are saved to a single encryption key file.
- 6 A **Save As** dialog box opens allowing you to save the encryption key file to a location on your computer. Choose a location and click **Save**.

## Importing Data Encryption Keys

SKM servers provide a unique encryption key for each tape cartridge that is encrypted. In order to read tapes encrypted by a different (i.e., source) SKM server, you need to import the encryption keys used to encrypt those tapes onto your SKM server (i.e., destination).

**Note:** This function is available to administrators and only applies to SKM servers. Both SKM servers must be connected and operational in order to import encryption keys.

To import encryption keys:

- 1 Before starting this process, read and follow the sequence of steps outlined in [Sharing Encrypted Tape Cartridges](#) on page 195.
- 2 Receive the file of encryption keys from the source SKM server and save it in a known location on your computer.
- 3 From the **Tools** menu, select **EKM Management > Encryption Key > Import**.

Figure 41 Importing Data  
Encryption Keys



- 4 Click **Browse** to locate the saved file of encryption keys.
- 5 Click **Open**.
- 6 Click **Apply** to import the keys onto your SKM server.
- 7 Back up both SKM servers following the instructions in the *Scalar Key Manager User's Guide*.

---

---

**Caution:** You must back up both SKM servers every time you import data encryption keys to protect against catastrophic server failure.

---

---

In case of an incomplete import, the library displays a message and generates a diagnostic ticket. For instructions on what to do if this happens, see [Using the SKM Encryption Key Import Warning Log](#) on page 202.

---

## Accessing the SKM Server Logs

---

The SKM server logs contain information about all activities performed by the SKM servers. You should not need to retrieve these logs unless Quantum Support directs you to do so. You can download the logs to your computer or e-mail them to a recipient. In order to e-mail the logs, the library e-mail account must be configured (see [Configuring the Library E-Mail Account](#) on page 76).

The path to open the appropriate screen is as follows:

- From the Web client, select **Tools > EKM Management > Retrieve SKM Logs**.

---

## Using the SKM Encryption Key Import Warning Log

---

This log lists the tape cartridges for which encryption keys failed the most recent encryption key import operation. If you have only partial success when importing a file of encryption keys (meaning, some keys import successfully but some keys do not), the library displays an “import warning” message and generates a diagnostic ticket that directs you to view this log to see which keys did not get imported.

For each key that failed the import, the log provides a message type that is either:

- **Error** — The key could not be imported.
- **Warning** — The key was imported, but the metadata update failed.

For each key that failed the import, the log provides one of the following message descriptions:

- **CRC Data Missing** — Error. Metadata is missing for the key. This means that the export file is corrupt. **Suggested Solution:** Export the key(s) for the listed tape cartridge(s) again, and then perform the import operation again.

- **CRC Check Failed** — Error. The CRC data does not match the key or key metadata. The export file is corrupt. **Suggested solution:** Try to import the same file again. If this fails, export the key(s) for the listed tape cartridge(s) again, and then perform the import operation again.
- **Import To Primary/Secondary Server Failed** — Error. The key import to the stated server failed (probably due to a network or other connection issue). If the key failed to import to the secondary server, it may have been imported successfully to the primary server. **Suggested solution:** Check network connections and perform the import operation again.
- **Key Metadata Update Failed (but key data was imported successfully)** — Warning. The key was imported, but the metadata update failed. You can access the key, but you cannot export it until it is actually used in an encryption operation on the library. **Suggested solution:** Use the key to read (decrypt) a tape. This marks the key as “used” and updates the metadata, which will allow you to export the key.

This log is only available if you are running SKM and have encryption key management licensed on the library (see [Adding or Upgrading Licensable Features](#) on page 69).

The log file is cleared and created new for each import operation so that it shows only the key corruptions and import failures that occurred during the latest encryption key import attempt.

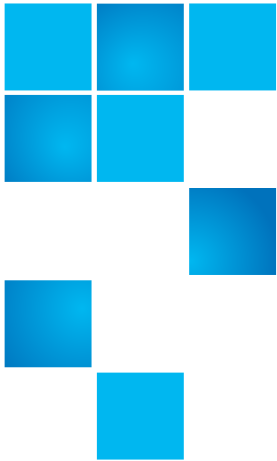
For more information about library logs, see [SKM Encryption Key Import Warning Log \(with EKM License\)](#) on page 219.

The path to open the appropriate screen is as follows:

- From the Web client, select **Reports > Log Viewer**.







## Chapter 8

# Getting Information About the Library

---

There are a number of informational screens and reports you can use to get information about the library.

This chapter covers:

- [Viewing Library Information](#)[Viewing System Information](#)
- [Viewing the Location of the Robot](#)
- [Viewing the Library Configuration Report](#)
- [Saving and E-mailing the Library Configuration Record](#)
- [Viewing the Network Settings Report](#)
- [Viewing the Logged in Users Report](#)
- [Viewing the All Slots Report](#)
- [Viewing, Saving, and E-mailing Library Logs](#)
- [Viewing Library Information on the Operator Panel](#)
- [Using Advanced Reporting Features](#)
- [Viewing the Open Source License Agreement](#)
- [Viewing the Copyright Statement](#)

---

## Viewing Library Information

The **About** screen gives you a quick glance at the following library settings:

- Library type (Scalar i40 or Scalar i80)
- Library serial number
- Copyright date
- Library firmware version

### Web Client

Select **Reports > About > Scalar i40/i80**.

---

## Viewing System Information

The System Information report contains information about the library.

On the operator panel, the report provides:

- Physical library information — serial number, system control board (SCB) revision, firmware version, board support package (BSP) version, date and time of last firmware update
- Tape drives — online/offline mode, firmware version, model, physical serial number, logical serial number
- Robot firmware versions — XY control, picker, camera

On the Web client, the report provides:

- Date & Time — Current date, time, and time zone settings.
- Physical Library — Host name, IPv4 address, serial number, firmware version of the physical library, IPv6 addresses if IPv6 support is enabled, board support package (BSP) level, and the date the firmware was last updated.

- 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, online/offline status, encryption method, encryption type, number of storage slots, number of media, and number of tape drives configured for each partition.
- Drives — Location coordinates, vendor, model, type, serial number, physical serial number (P-SN), logical serial number (L-SN), firmware level, and encryption method.

### Operator Panel

- 1 Select **Reports > About Library**.
- 2 Press **Next** to scroll through all the screens. Press **Exit** to exit at any time.

### Web Client

Select **Reports > System Information**.

---

## Viewing the Location of the Robot

You can set the operator panel to view the robot position as library operations are performed. This view is helpful in diagnosing any library problems because you can see where the robot is, whether it contains a tape, and the finger position.

If you perform an operation from the remote interface, the operator panel displays the operation as it is performed. If you perform an operation from the operator panel, once complete, you can return to the Robot View to view the completed operation status.

---

**Note:** The operator panel does not update the left side graphical display until the motion is complete (success or failed)

---

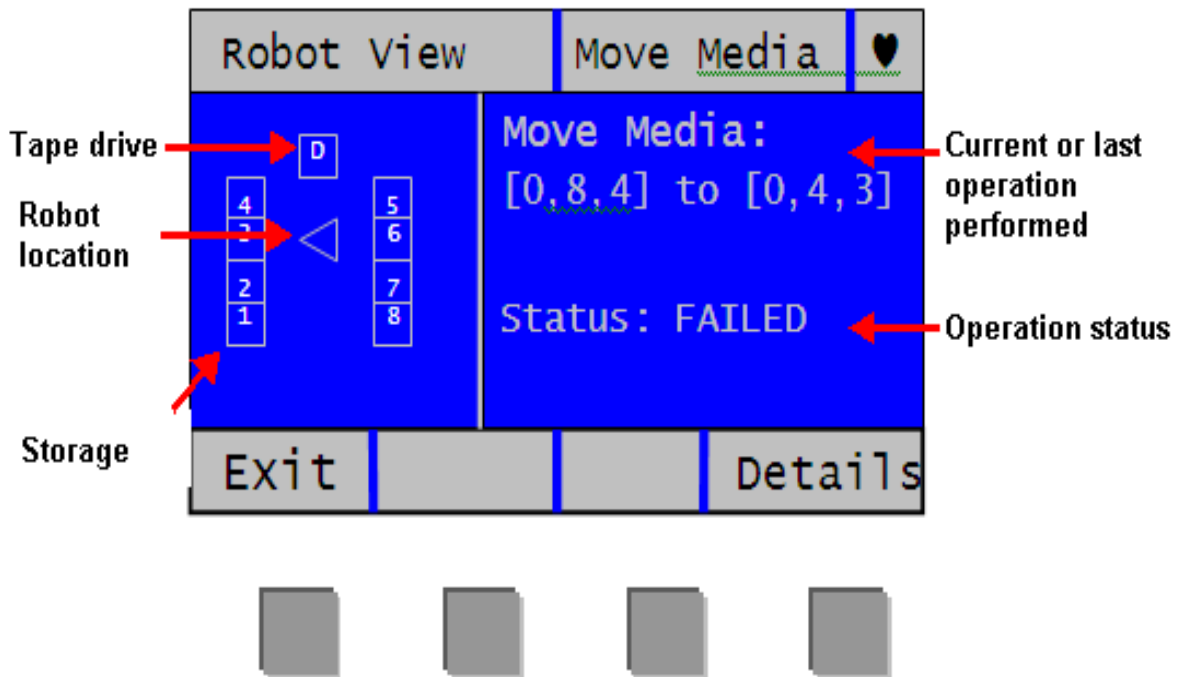
On the operator panel, do the following:

---

**Note:** If you are viewing the alternate home screen, select **Menu** to return to default home screen.

---

- 1 Select **Tools > Robotic View**.



The left graphical section depicts the top-down current location of the robot on the X axis.

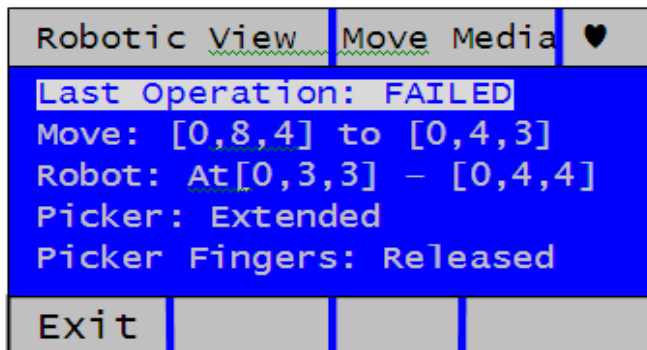
- The numbers indicate the storage column.
- The 'D' designates the tape drive column.

- The triangle represents the robot. If it is filled in, then the robot contains the media, otherwise the robot is empty. The direction the triangle points to indicates its location.

The right information section provides the following:

- Describes the current or last operation performed. If the operation performed affects a device location, the description will be numeric—for example Move Media: [1,2,5] to [1,5,1]. If the operation affects a slot location, such as unlocking a magazine, the description will be textual—for example, Unlock: Left Magazine.
- Provides the status of the operation—Active, Completed, or Failed.

2 For additional information about the status, select **Details**.



This screen provides details for the library status:

- Last Operation - Status of last completed operation—Succeeded or Failed.
- Robot - The Robot location refers to where the robot was at the end of the operation. For example, if the robot is between two slots, it will display the robot location as “Robot: At [0,1,4] - [0,1,5]”. If it is directly in front of a slot, it would then read, for example “At [0,4,4]”.
- Picker - Extended or Retracted.

- Picker Fingers - Engaged or Released.
- 3 Select **Exit** to return to the **View**.

## Viewing the Library Configuration Report

The **Library Configuration Report** is a dynamic representation of the various library resources, including tape drives, slots, partitions, and library chassis. The report shows which slots are assigned to partitions, I/E stations, configured as cleaning slots, or unassigned; whether the slot contains a tape drive; and whether a tape drive is the control path for its partition. You can view all slot location coordinates or media barcodes at the click of a button, and get detailed information about a specific resource by clicking on it.

You can view the report on the Web client.

### Web Client

- 1 Select **Reports > Library Configuration**. The Library Configuration Report displays in a new window.
- 2 Do any of the following:
  - In the Legend, click a partition name to view information about the partition.

---

**Note:** Each partition is assigned a number and color. All slots and tape drives that are assigned to a partition are represented in the library map by the partition number and color.

---

- In the library map, click a specific slot to view information about the slot.
- In the library map, click a specific tape drive to view information about the tape drive.
- In the library map, click the chassis number (0) below the tape drives to view information about the chassis.

- Click **Show Barcodes** to display the barcodes for all imported cartridges.
- 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 print the report, click the **Print** icon in the upper right of the screen.



Clicking on a resource (tape drive, slot, partition, or chassis) brings up a detailed window containing the following information:

- **Tape Drives** — The following information is provided for each installed tape drive:
  - **Fibre Channel tape drive** — interface type, tape drive type, state (ready/not ready), status (online/offline), assigned partition name, location coordinates, media barcode (if media is in slot; “No\_Label” means unreadable barcode), media type (if media is in the slot), element address, vendor, model, form factor (half height or full height), physical SN, logical SN, world wide node name (WWNN), world wide port name (WWPN), loop ID, requested topology, requested speed, actual topology, actual speed, maximum speed, tape drive firmware level, whether the tape drive is the control path for its partition, and encryption method.
  - **Serial Attached SCSI (SAS) tape drive** — interface type, tape drive type, state (ready/not ready), mode (online/offline), assigned partition name, location coordinates, media barcode (if media is in slot; “No\_Label” means unreadable barcode), media type (if media is in slot), element address, vendor, model, form factor (half height or full height), physical SN, logical SN, SAS Address, tape drive firmware level, whether the tape drive is the control path for its partition, and encryption method.
- **Slots** — The following information is provided for each slot: type, assigned partition name (storage and I/E station slots only), location coordinates, cartridge barcode (storage and I/E station slots only; “No\_Label” means unreadable barcode), 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.

- **Partitions** — The following information is provided for each partition: name, status (online/offline), emulation type, barcode policy, total number of tape drives, number of active tape drives, total media, mounted media, total slots, full slots, total I/E station slots, full (occupied) I/E station slots, and encryption method.
- **Chassis** — The following information is provided for each chassis: manufacturer, model, and serial number.

---

## 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
- License information — License keys installed and descriptions, installation date, and expiration date
- Primary Network Information — Host Name, DHCP enabled/disabled, IP address, netmask, gateway, Ethernet MAC, Ethernet link speed (Mbits/s), and Ethernet link present
- Chassis information — Manufacturer, model, serial number, and location
- Tape drive information:
  - 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, form factor, serial number, firmware version, drive type, logical serial number, interface type, World Wide (WWN), loop ID, topology, actual topology, speed, and actual speed



- 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, SAS Address, firmware level, control path status

---

**Note:** The library configuration report lists the native device identifier as reported by the tape drive. HP tape drives always report SCSI as the native device identifier, even if they are Fibre Channel or SAS. For example, if you have HP L TO-4 Fibre Channel or SAS drives, they will be listed in the report as HP LTO-4 SCSI drives.

---

- Partition information:
  - Library 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 details — Partition name, number of slots, number of tape drives, and number of cartridges

---

## 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 can only save the library configuration record from the Web client.

### Web Client

- 1 Select **Tools > Save Configuration Record**.
- 2 Save the file to a known location on your computer.

---

## 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.

---

**Note:** 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 76.

You can only e-mail the library configuration record from the Web client.

### Web Client

- 1 Select **Tools > E-mail Configuration Record**.
- 2 Type an e-mail address into the **E-mail Address** text box.
- 3 Click **Apply**.

---

## Viewing the Network Settings Report

The Network Settings report provides information on the following library settings:

- **Network** — Host name, primary DNS, and alternate DNS
- **IPv4 Settings** — DHCP enabled/disabled, IP address, gateway, and netmask
- **IPv6 Settings** (if IPv6 is enabled) — DHCP enabled/disabled, stateless configuration enabled/disabled, static configuration enabled/disabled, net prefix, gateway, and all IPv6 addresses
- **SSL** — SSL, port, and cipher
- **SMI-S** — Access (enabled/disabled) and state (enabled/disabled)
- **SNMP** — Enabled/disabled status for Access, V1, V2, V3, and encryption; algorithm; and port
- **SNMP-Traps** — IP addresses and ports

## Web Client

Select **Reports** > **Network Settings**.

---

# Viewing the Logged in Users Report

The Logged In Users report contains information about the users that are currently logged in to the library.

The report contains the following information about each user:

- **User Name** — User name of logged in user
- **Privilege** — Privilege level of the logged in user (Admin for administrator, User for user)
- **Login Date/Time** — Date and time the user logged into the library
- **Last Activity Date/Time** — Date and time when the user last logged into the library
- **Login Location** — IP address or host name of the system used to access the library
- **User Interface** — User interface used to access the system (Web Client or Operator Panel)

## Web Client

Select **Reports** > **Logged in Users**. The report displays in a new window.

---

# Viewing the All Slots Report

The All Slots report contains information on all storage, import/export (I/E) station, and tape drive slots that are currently assigned to one or more partitions.

The report contains the following information about each slot:

- **Slot Type** — I/E station, storage, cleaning, or tape drive slot.
- **Barcode** — Barcode number of the cartridge installed in the slot. No barcode number means the slot is empty. "No\_Label" means the barcode is unreadable.
- **Partition** — Partition that owns the slot (I/E station slots are shared by all partitions).
- **Location** — Location coordinates of the slot.
- **Element Address** — Element address of the slot.
- **Encryption** — The encryption state of the media in the slot. In order for the library to know the encryption state, the tape must have been placed into an encryption-capable tape drive in the library. 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.

### Web Client

Select Reports > All Slots.

## Viewing, Saving, and E-mailing Library Logs

You can view, save, and e-mail several logs containing information about the library:

- [Cleaning Log](#)
- [Diagnostic Tickets Log](#)
- Media Security Log (available only with Advanced Reporting license)
- Media Usage Log (available only with Advanced Reporting license)
- [SKM Encryption Key Import Warning Log \(with EKM License\)](#)
- [Tape Drive Log](#)

---

### Cleaning Log

---

The Cleaning Log shows all cleanings that have been performed in the library. When the log reaches its maximum size, the oldest information is replaced as new information is added.

The log 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.

### Web Client

- 1 Select **Reports > Log Viewer**.
- 2 Select **Cleaning Log** and press **Next**.

The report displays in a new window for viewing.

- 3 You can save or e-mail the report following the on-screen instructions.

---

**Note:** If you want to e-mail the log file to a recipient, type the recipient's name in the text box next to the **E-mail** button, and then click the **E-mail** button. You must have your e-mail notification configured in order to e-mail a log file. See [Configuring the Library E-Mail Account](#) on page 76 for more information.

---

## **Diagnostic Tickets Log**

The Diagnostic Tickets Log records all diagnostic tickets issued by the library.

The log provides the following information: Num (ticket number to provide a consecutive listing of tickets in the order issued; the first ticket issued is assigned number 1, the second ticket 2, and so on); State (open, unopened, closed); Priority (low, high, urgent); Created (date the ticket was first issued); Last Updated (date the ticket was last issued); Cause Code (the number assigned to the fault and which displays in the full ticket name; for example, DT031- I/E Unlock Warning has cause code 31); Description; and Details.

### **Web Client**

- 1 Select **Reports > Log Viewer**.
- 2 Select **Diagnostic Tickets Log** and press **Next**.  
The report displays in a new window for viewing.
- 3 You can save or e-mail the report following the on-screen instructions.

---

**Note:** If you want to e-mail the log file to a recipient, type the recipient's name in the text box next to the **E-mail** button, and then click the **E-mail** button. You must have your e-mail account configured in order to e-mail a log file. See [Configuring the Library E-Mail Account](#) on page 76 for more information.

---

---

### Media Security Log (with Advanced Reporting License)

---

---

**Note:** To access the Media Security log, your library must have an Advanced Reporting license. To learn more about the Advanced Reporting license, refer to [Advanced Reporting](#) on page 14.

---

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. By default, the library collects nothing and the log is empty. You can configure the library to collect information about media removal, and then view, save, and/or e-mail the log. Refer to [Working with the Media Security Log](#) on page 126.

---

### Media Usage Log (with Advanced Reporting License)

---

---

**Note:** To access the Media Usage log, your library must have an Advanced Reporting license. To learn more about the Advanced Reporting license, refer to [Advanced Reporting](#) on page 14.

---

The media usage log lists media usage information regarding capacity and read and write errors for media ever mounted in a drive., including media that are no longer in the library. Refer to [Viewing the Media Usage Log](#) on page 129.

---

### SKM Encryption Key Import Warning Log (with EKM License)

---

---

**Note:** To access the SKM Encryption Key Import Warning log, your library must have an Encryption Key Management (EKM) license. To learn more about the EKM license, refer to [Encryption Key Management](#) on page 15.

---

Lists keys that failed the most recent data key import operation. This log is only available if you are running Scalar Key Manager (SKM). For detailed information about this log, see [Using the SKM Encryption Key Import Warning Log](#) on page 202.

### Web Client

- 1 Select **Reports > Log Viewer**.
- 2 Select **SKM Encryption Key Import Warning Log** and press **Next**.
- 3 The report displays in a new window for viewing.

- 4 You can save or e-mail the report following the on-screen instructions.

---

**Note:** If you want to e-mail the log file to a recipient, type the recipient's name in the text box next to the **E-mail** button, and then click the **E-mail** button. You must have your e-mail account configured in order to e-mail a log file. See [Configuring the Library E-Mail Account](#) on page 76 for more information.

---

---

## Tape Drive Log

---

The library allows you to retrieve tape drive logs using the Web client. Tape drive log information can be used to help troubleshoot the library, the tape drive sled, and tape drive issues.

Since the log retrieval process can take up to 30 minutes, the tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

Tape drive log files 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.

### Web Client

- 1 Select **Tools > Drive Operations**.
- 2 Select **Retrieve tape drive log** and click **Next**.
- 3 If your library contains multiple tape drive interface types, select the interface type of the tape drive from which you want to retrieve logs and click **Next**.
- 4 The Retrieve Drive Log screen displays. This screen lists the available tape drives.
- 5 Select a tape drive from which you want to retrieve logs and click **Next**.

---

**Note:** If there is more than one page of tape drives, use the **Page 1 of x** arrows to view the additional tape drives.

---



---

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

---

**6 Click Apply.**

A dialog displays asking you to confirm you want to take the partition offline.

**7 Click OK.**

The Progress Window displays, displaying information on the action, elapsed time, and status of the operation.

**8 If the Progress Window displays a “completed” message, you can close the window and save the file to your computer.**

**9 If the screen displays a “failure” message, the tape drive log was not successfully retrieved. Follow the instructions listed in the Progress Window to resolve any issues that occurred during the operation. If a complete tape drive log could not be retrieved, you may still be able to access a partial log. If so, a note will appear stating, “A complete tape drive log could not be retrieved, but a partial log is available and may be saved for further analysis once the progress window is closed.”**

---

## Viewing Library Information on the Operator Panel

The operator panel provides several brief reports about the library.

---

### Viewing Partition Information

---

The operator panel provides an overview of partition information. For each partition, you can see the following information:

- Online/offline mode
- Control path tape drive location coordinates
- Number of tape drives
- Number of storage slots

- Number of I/E station slots containing a tape cartridge assigned to the partition

## Operator Panel

- 1 Select **Reports > Partitions**.
- 2 If the library contains more than one partition, use the **Up** and **Down** buttons to select a partition and press **Select**.

---

## Viewing Tape Drive Information

---

The operator panel provides an overview of tape drive information. For each installed tape drive, you can see the following information:

- Online/offline mode
- Partition to which the tape drive is assigned
- Whether the tape drive is the control path for the partition
- State (ready/active/mounted)
- WWNN (if Fibre Channel) or SAS address (if SAS)

## Operator Panel

- 1 Select **Reports > Tape Drives**.
- 2 If the library contains more than one tape drive, use the **Up** and **Down** buttons to select a tape drive and press **Select**.

---

## Viewing Network Settings

---

A short report on the operator panel displays the library's network settings: host name, IP address, and network configuration.

## Operator Panel

- 1 Select **Reports > Network Settings**.
- 2 If IPv6 is enabled, the IPv4 information is shown on the first screen. Press **Next** to see the IPv6 address information on the next two or more screens. Although the library can have unlimited IPv6 address, a maximum of three are shown in this report.

---

## Viewing the Date, Time, and Time Zone

---

The operator panel displays the current date, time and time zone configured on the library.

### Operator Panel

Select **Reports > Date/Time**.

---

## Viewing Licenses

---

The operator panel displays a list of all the licenses currently installed on the library: number of COD slots licensed, number of unlicensed slots, and whether Advanced Reporting is licensed.

### Operator Panel

Select **Reports > Licenses**.

---

# Using Advanced Reporting Features

Advanced Reporting features are only available if you have Advanced Reporting licensed on the library. See [Chapter 5, Advanced Reporting](#) for more information.

---

# Viewing the Open Source License Agreement

A number of open source packages were used to create the library firmware. You can view the open source license agreement on the Web client.

### Web Client

Select **Reports > About > Open Source Licenses**.

---

## Viewing the Copyright Statement

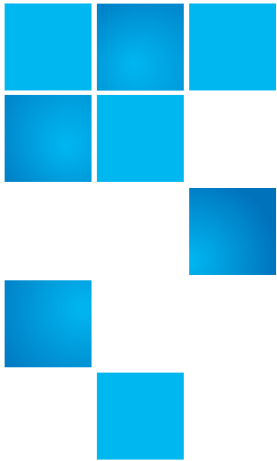
### Operator Panel

Select **Reports** > **Copyright Statement**.

### Web Client

Available in the Web client online help. To view the help, click the **Help** icon in the upper right corner of the screen.





## Chapter 9

# Installing, Removing, and Replacing Components

---

This chapter describes how to add, remove, and replace hardware components within your library.

---

**WARNING:** Two people are required to lift and install the library.

---

---

**WARNING:** Under no circumstances should a rack be moved while a library is installed.

---

This chapter covers:

- [Taking ESD Precautions](#)
- [Connecting Library Cables](#)
- [Installing the Rack Mount Kit \(Rail Kit\)](#)
- [Installing the Library In a Rack](#)
- [Removing the Library From a Rack](#)
- [Installing the Library in a Desktop Kit](#)
- [Removing the Library from a Desktop Kit](#)
- [Removing and Replacing the Front Bezel](#)
- [Replacing the Chassis](#)
- [Removing and Installing a Filler Plate](#)

- [Removing and Replacing a Magazine](#)
- [Removing and Installing a Power Supply](#)
- [Removing and Replacing the System Control Board](#)
- [Removing and Replacing a Tape Drive](#)
- [Packaging the Library for Moving or Shipping](#)
- [Replacing the Y-tray with Robot](#)

---

## Taking ESD Precautions

Some components within the Scalar i40 and Scalar i80 libraries contain static-sensitive parts. To avoid damaging these parts while performing installation procedures, always observe the following precautions:

- Use an antistatic wrist strap. If you do not have one, touch the outside of the library on the sheet metal before touching any components to discharge static from your body.
- Keep static-sensitive parts in their original shipping containers until ready for installation. Look for the ESD sticker to identify static sensitive parts.



- Avoid touching connectors and other components.

---

**Note:** Dry climates and cold-weather heating environments have lower relative humidity and are more likely to produce static electricity.

---

## Connecting Library Cables

Connect the cords and cables as follows (see [Figure 42](#) on page 228). It is recommended that you leave some slack in the cables to allow you to perform certain replacement procedures in the future.

- 1 Connect the tape drive cables from the tape drives to the host.

---

---

**Caution:** Use care when handling the fibre optic cables. Do not crimp or bend the cables. Do not exceed the bend radius specified by the manufacturer.

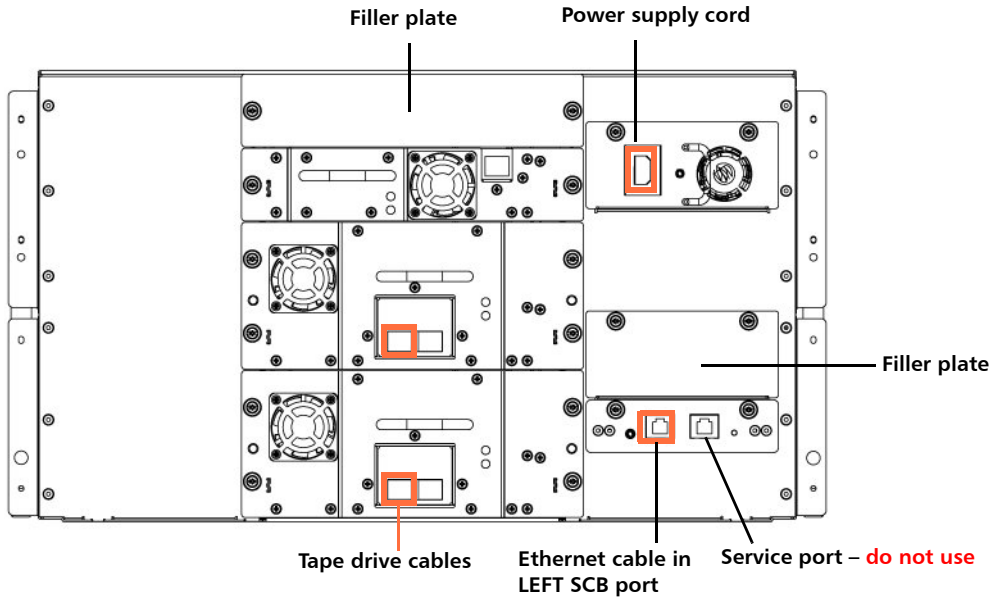
---

---

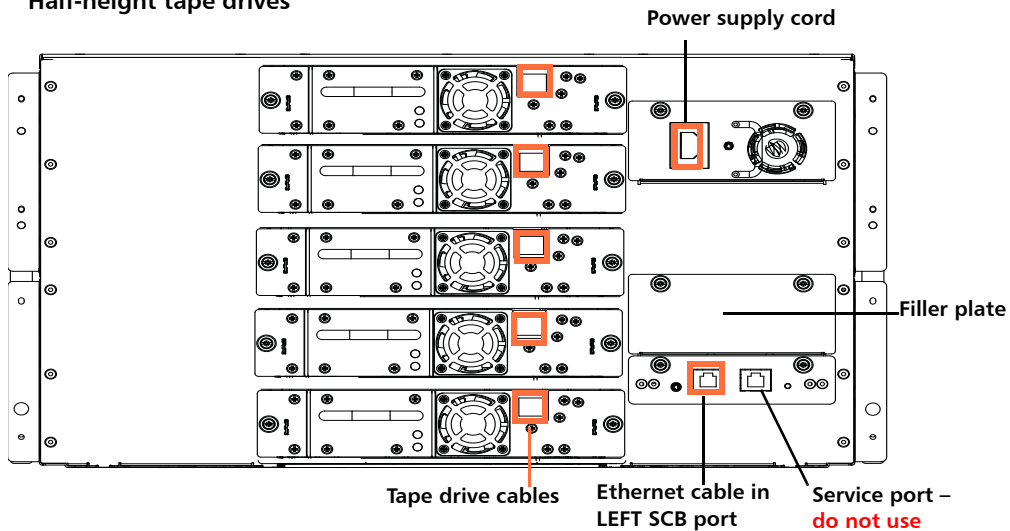
- 2 Connect an Ethernet cable (not supplied with your library) into the LEFT port on the system control board (SCB). The right SCB port is for service use only; do not use. Connect the other end of the Ethernet cable into a live Ethernet jack connected to your network.
- 3 Connect the power supply cord into the power supply connector. Plug the other end of the cord into a grounded AC outlet.

Figure 42 Connection Locations

Full-height tape drives



Half-height tape drives





## Installing the Rack Mount Kit (Rail Kit)

The instructions for installing the rails are the same for both the Scalar® i40 and the Scalar i80.

---

**WARNING:** If the rack is empty at the time of installation, do NOT install the library too high in the rack. The weight of the library may cause the rack to become “top heavy” and unstable if installed in the top of an empty rack.

---

---

**WARNING:** Do not stack objects on top of the library such as cables or other computer equipment. The additional weight could exceed the amount supported by the rack shelves.

---

---

**Caution:** Make sure the rack mounting rails are level, both left to right and front to back. If the library is not level in the rack, it will not work properly.

---

---

### Supported Rack Types

---

The Scalar i40 and Scalar i80 libraries are designed to fit in most standard 19-inch equipment cabinets, including:

- Dell, 08P157 (US-08P157910-3AU-0900), square, 2.48 - 2.72 mm thick
- SUN, 38U, NGR900R, M6
- Emcor, 10 Series, round hole
- IBM, Machine Type 9306, Model 900, square, 28.25-inch deep, 2.0-2.25 mm thick
- HP, 10K, PN 245169-001, Asm 10642U GR Metallic, square, 2.0-2.2 mm thick
- EMC CX500
- Rittal Cable Tester Rack Frame, square

Rack depth of 34 in. (86.3 cm) minimum is recommended; however, rack depths of 24 to 36 in. (60.9 to 91.4 cm) are supported.

## Space Requirements

See the following:

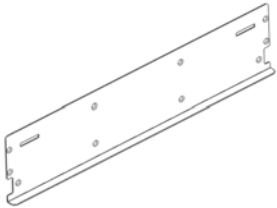
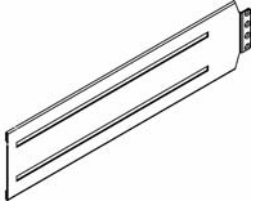
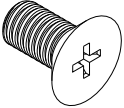
- [Physical Specifications](#) on page 341 and
- [Air Clearance Requirements](#) on page 343

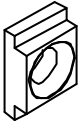
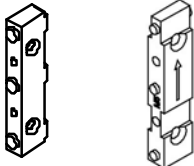
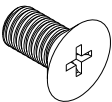

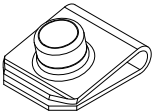
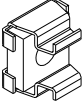
## Tools Required

- Phillips screwdriver
- Magazine lock override tool — an opened paperclip, small screwdriver, or other object (3.5 mm or less in diameter that will not break off)

## Rack Mount Kit Contents

The following items are included in the rack mount kit:

Qty	Figure	Description
2		Shelf
2		Shelf Extender
16		Phillips head screw, countersunk (M5 x 10) – for shelf assembly

Qty	Figure	Description
8		T- nut (M5) – for shelf assembly
8 total		Rail adapter – 4 each of two types are included. You need 4 for installation; choose the type appropriate for your rack (for more information, see <a href="#">Figure 45</a> on page 235)
8		Phillips head screw, countersunk (M4 x 12) – for mounting shelves to rack
8		Washer, countersunk – for mounting shelves to rack
4		Clip nut (M5 x 0.8) – for securing library in rack
4		Cage nut (M5) – to secure library to rack. Used in racks with square or round non-threaded holes.

---

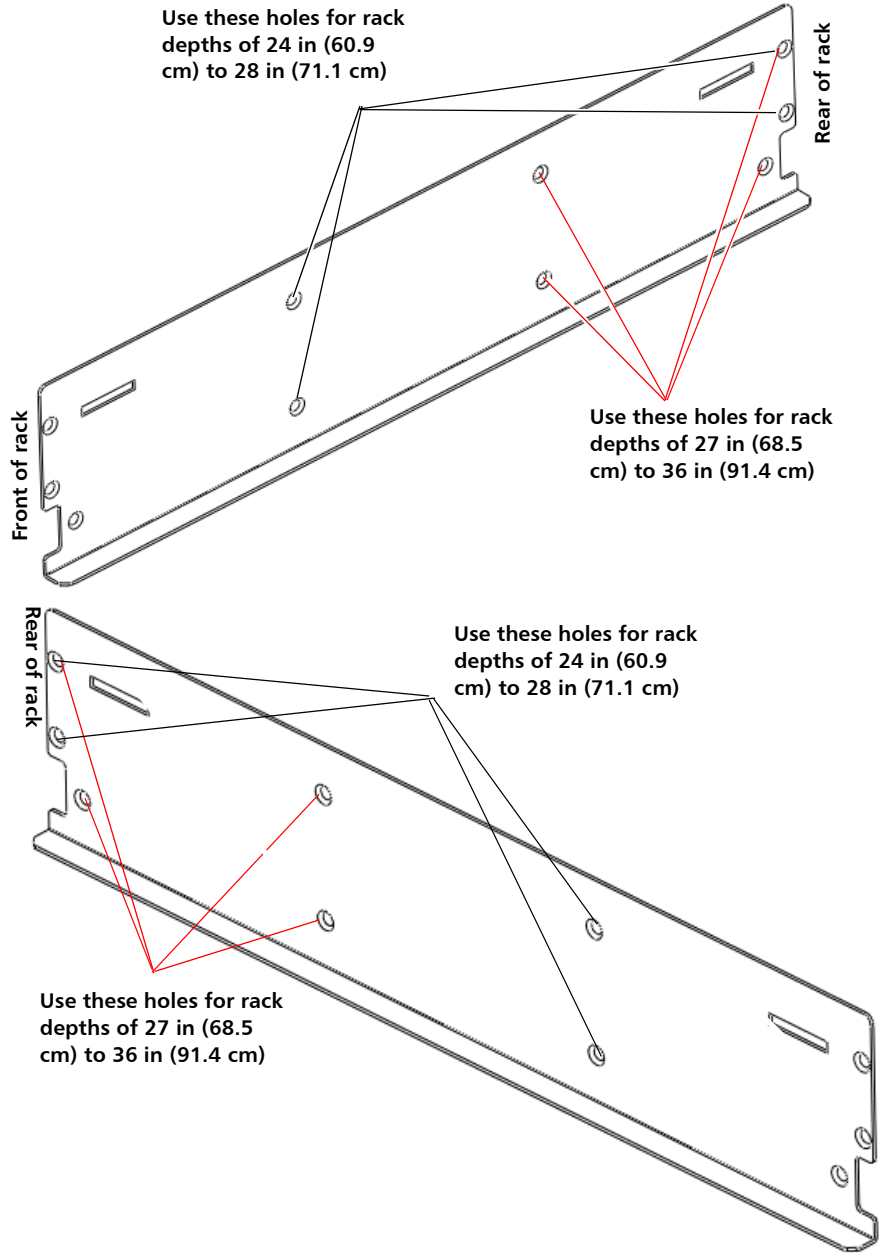
## Installing the Rack Mount Shelves

---

Before installing the rack mount shelves, you must collect the following information:

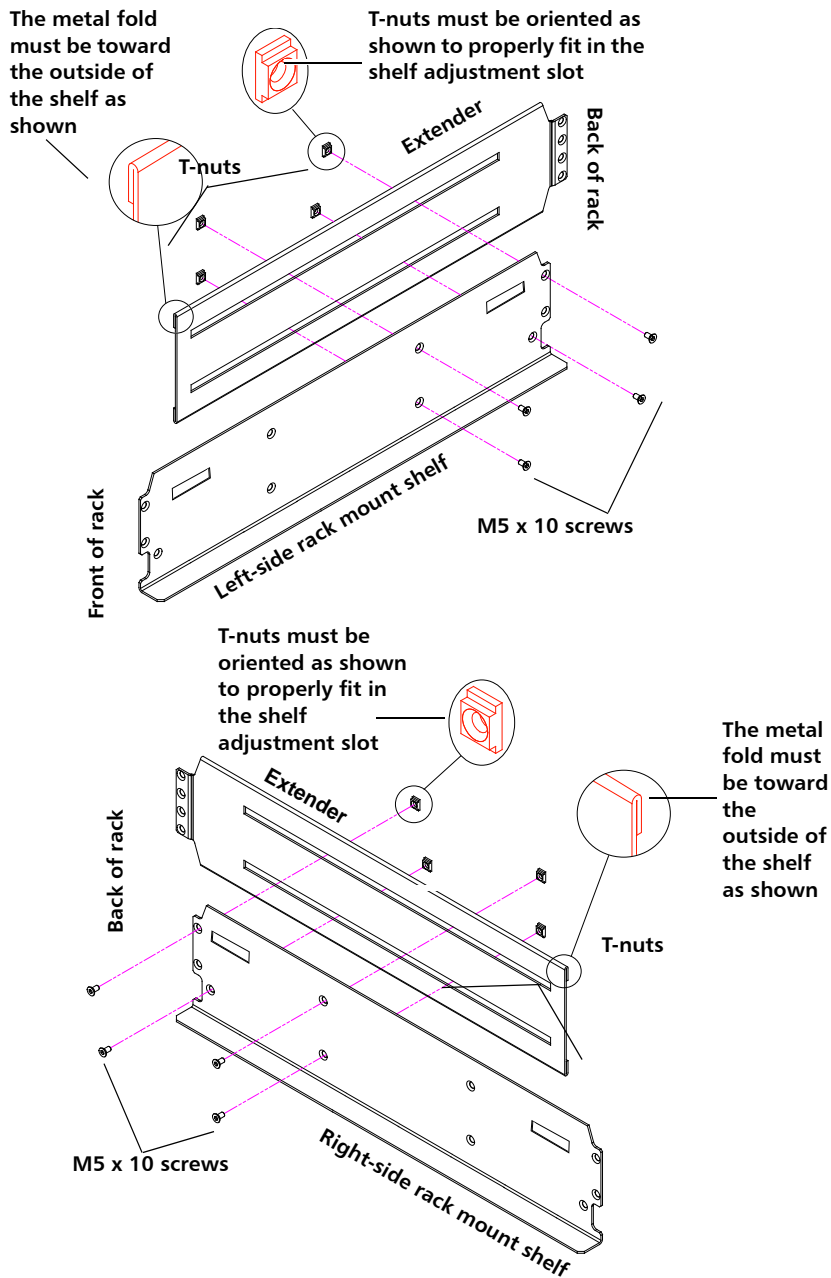
- Type of rack mount rails (square hole, through hole, or threaded hole)
  - Depth of rack
- 1 Assemble the rack mount shelves included in the accessory kit (left and right):
    - a The holes used to attach the two halves of the rack mount shelves differ depending on the depth of the rack (see [Figure 43](#) on page 233). It is recommended that you use the ones that are exposed and have the widest spacing.

Figure 43 Rack Mount Shelf  
Depth Requirements



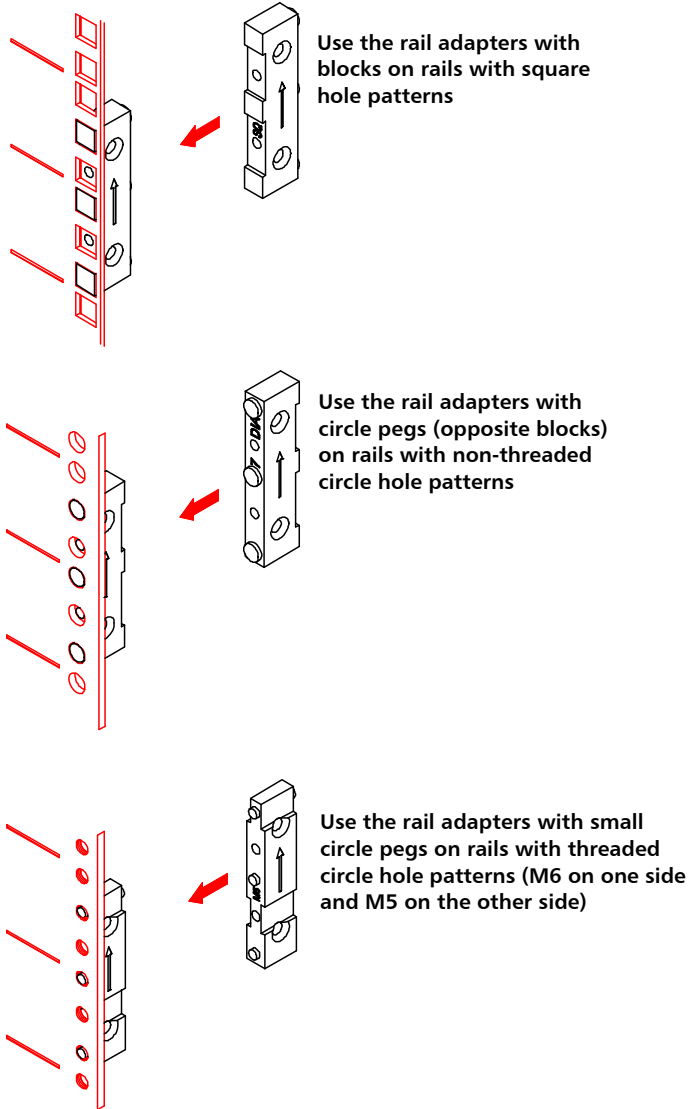
- b** Loosely attach the rack mount shelves to the extenders with 4 M5 x 10 screws and T-nuts (see [Figure 44](#)).

Figure 44 Assembling the Left and Right Rack Mount Shelves



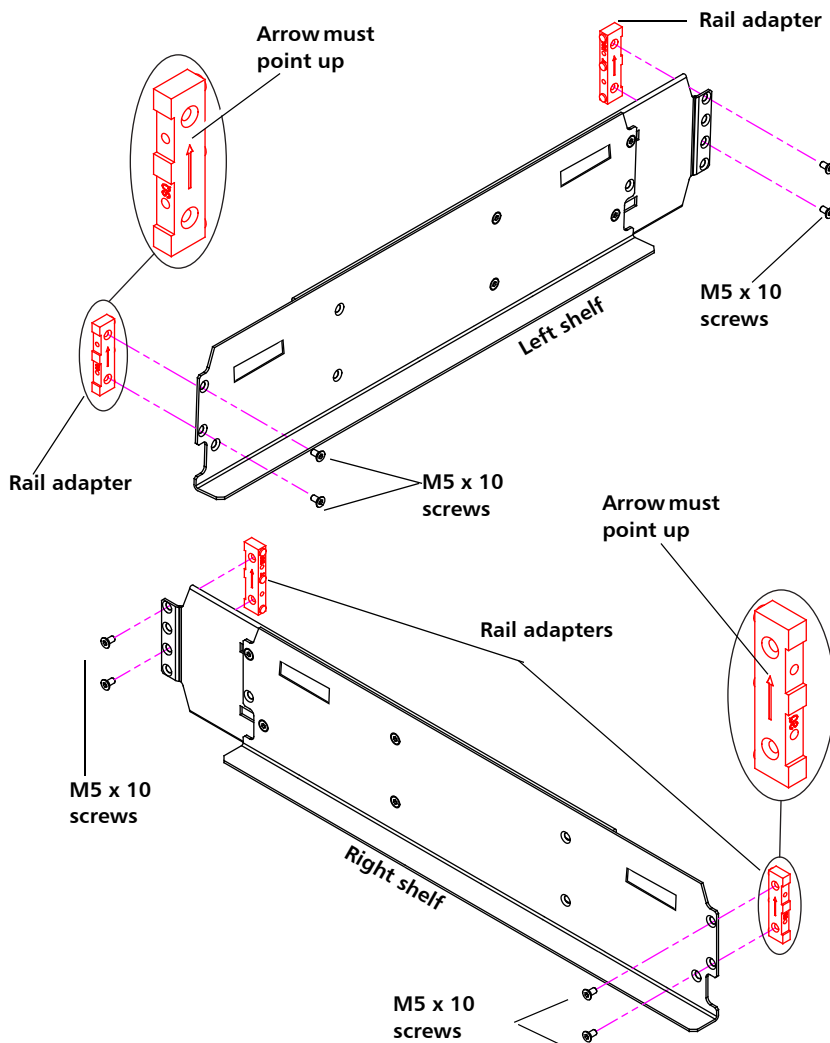
- c Determine the type of rail adapter required for your rack. Each rail adapter is marked with the specific hole type supported (see [Figure 45](#)).

Figure 45 Rail Adapter Types



- d Attach the appropriate rail adapter to the front and back of the rack mount shelves (right and left) with 2 M5 x 10 screws per adapter (see [Figure 46](#)).

Figure 46 Assembling the Left-Hand Rack Mount Shelf





2 Install the left and right rack mount shelves into the rack (the rack mount shelves adjust 24 to 36 in.) and secure with the following parts in four locations (see [Figure 47](#) on page 238):

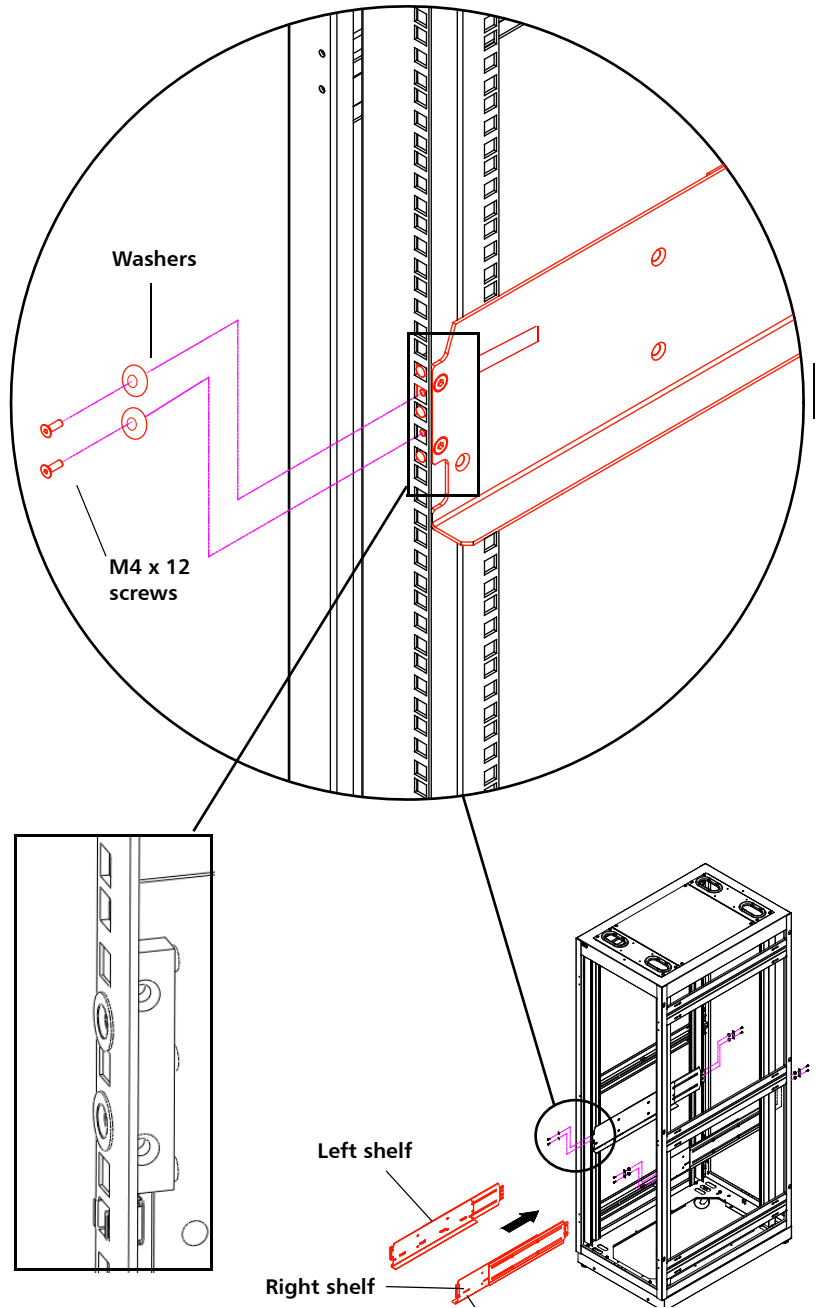
- 2 washers
- 2 M4 x 12 screws

---

**Note:** The rack mount shelves must be installed on the inside rack rails.

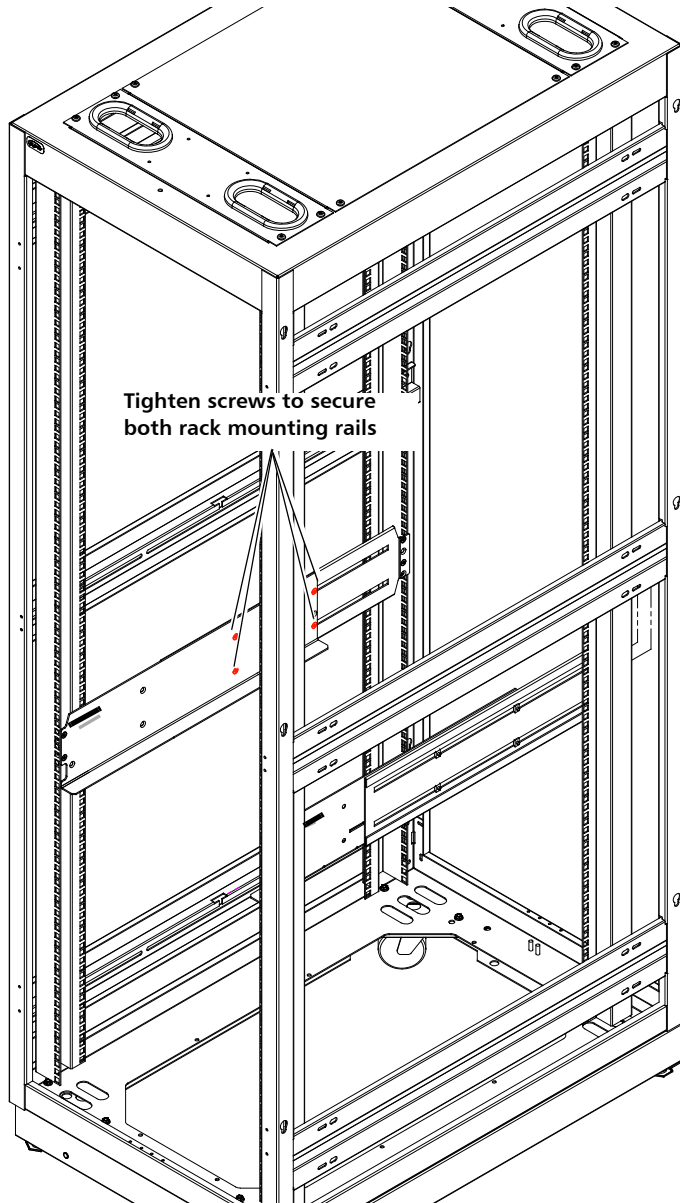
---

Figure 47 Installing the Rack Mount Shelves



- 3 Once the rack mount shelves are secured to the rack, tighten the screws securing the adjustable shelves (right and left) together (see [Figure 48](#)).

Figure 48 Tightening the Rack Mount Shelves



- 4 If the rack does not have threaded holes, install a clip nut or a cage nut in the back side of the rail, in the first empty hole below the rail adapter. This is what you will screw the library thumbscrews into to secure the library in the rack. See table below for type of nut, and [Figure 49](#) on page 241 for installation location.

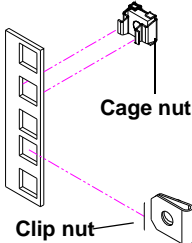
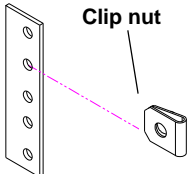
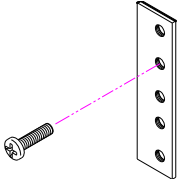
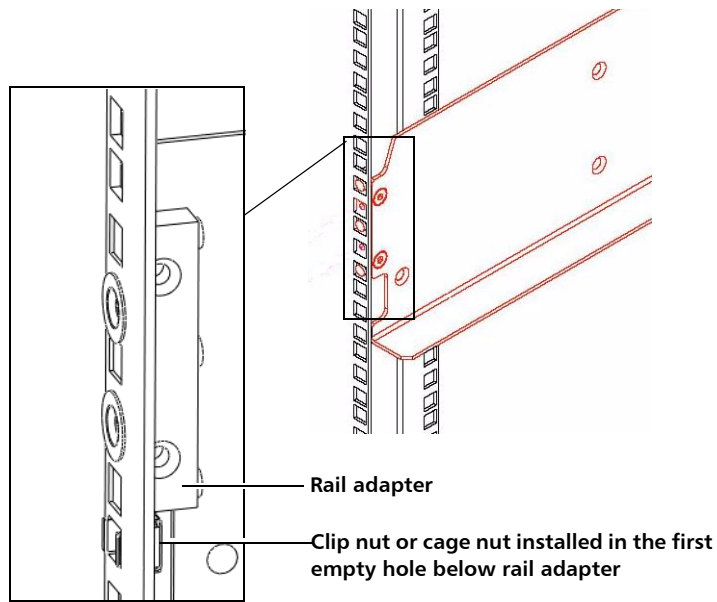
Type of Rail/Type of Nut	Description
 <p data-bbox="644 565 739 591">Cage nut</p> <p data-bbox="562 687 644 713">Clip nut</p>	<p data-bbox="869 458 1315 644">Square rack holes are the most common type of rack holes. They can accept either cage nuts which mount from the back of the rail or clip nuts which clip on from the side of the rack rail.</p>
 <p data-bbox="615 770 701 796">Clip nut</p>	<p data-bbox="869 744 1312 805">Round, unthreaded holes require clip nuts to accept mounting hardware.</p>
	<p data-bbox="869 973 1303 1065">Threaded holes require neither cage or clip nuts to accept mounting hardware.</p>

Figure 49 Location for  
Installing the Clip Nut or Cage  
Nut



## Installing the Library In a Rack

---

---

**Caution:** Make sure the rack mounting rails are level, both left to right and front to back. If the library is not level in the rack, it will not work properly.

---

---

**WARNING:** At least two people are required to lift and install the library.

---

---

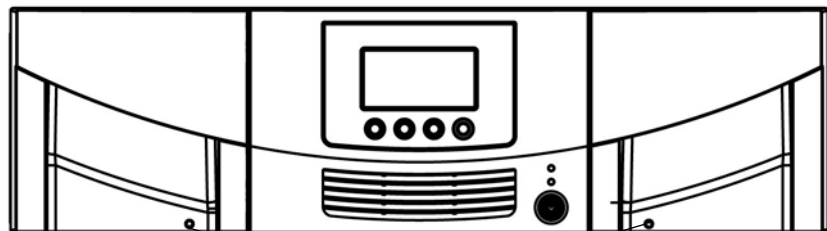
- 1 If tape drives are installed in the library, you may wish to remove them to reduce weight. To remove tape drives, unscrew the captive thumbscrews securing them to the back of the library and slide them out of the library. Set them down gently on a stable surface.

- 2 Lift the library, place it on the rack shelves, and slide it into the rack as far as it will go.
- 3 Open one of the magazines slightly to access the captive thumbscrew that is attached to the library chassis. You will use this thumbscrew to secure the library to the rack. To open the magazine, insert the magazine lock override tool into the access hole in the bottom of the magazine bezel (see [Figure 50](#) on page 242). Use the tool to depress the release latch while gently pulling outward on the magazine bezel handle.

Right-side magazines will only slide out as far as the I/E station (one column of slots). To release the right-side magazines fully:

- On the Scalar i40 and the bottom right magazine of the Scalar i80, reach under the open magazine and insert the tool directly into the access hole in the library chassis to depress the release latch, while pulling out on the magazine bezel handle.
- On the top right magazine of the Scalar i80, reach under the open magazine and press the release latch directly with your finger, while pulling out on the magazine bezel handle.

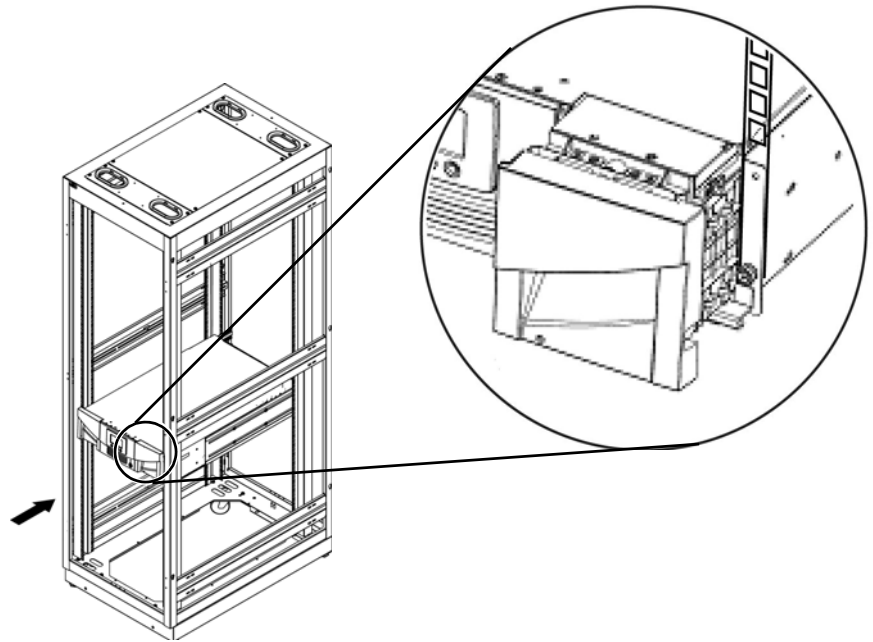
Figure 50 Magazine Release Latch Access Holes



Magazine release latch access holes

- 4 Screw the captive thumbscrew finger-tight into the rack (and through the clip nut or cage nut, if installed). See [Figure 51](#) on page 243.
- 5 Repeat [Step 3](#) and [Step 4](#) for the remaining thumbscrews.
- 6 Close all the magazines by pushing them in until they click shut.

Figure 51 Securing the Scalar i40 and Scalar i80 in the Rack



## Removing the Library From a Rack

**WARNING:** At least two people are required to lift the library and remove it from a rack.

- 1 Shut down the library by selecting **Actions > Shutdown** from the operator panel.
- 2 Turn **OFF** the library by pressing the power button on the front panel.
- 3 Disconnect the power supply cord, the Ethernet cable, and all tape drive cables from the back of the library. If you have multiple tape drives, label the cables so you can reconnect them to the correct tape drives later.

- 4 Remove all the tape drives from the library (for details, see [Removing and Replacing a Tape Drive](#) on page 286).
- 5 Remove all the magazines from the library (for details, see [Removing and Replacing a Magazine](#) on page 271).
- 6 Unscrew the captive thumbscrews in the “rack ears” that secure the library to the rack (see [Figure 51](#) on page 243).
- 7 Slide the library out of the rack. Keep the library level as you slide it out of the rack.
- 8 Place the library on a flat, stable surface.

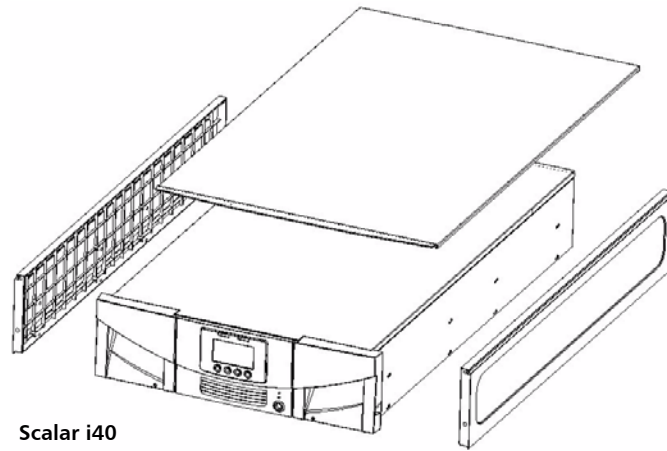
---

## Installing the Library in a Desktop Kit

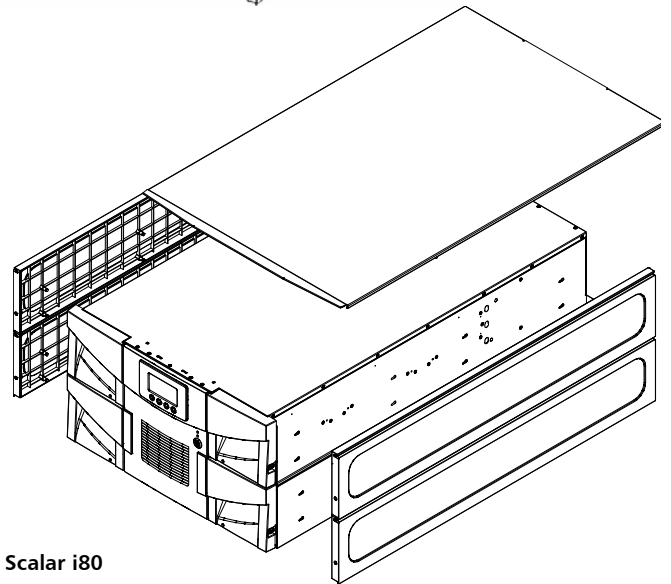
The instructions for installing the Scalar i40 and the Scalar i80 in a desktop are the same. The only difference is that the Scalar i40 has two side panels, and the Scalar i80 has four.



Figure 52 Desktop Kit,  
Scalar i40 and Scalar i80

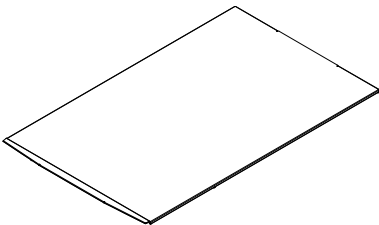
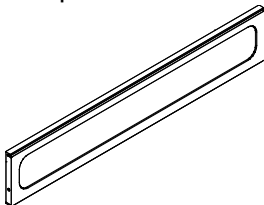




Scalar i40



Scalar i80

## Kit Contents

Item	Quantity
Top cover 	1
Side panel 	2 for the Scalar i40; 4 for the Scalar i80
Top cover screws 	2
Rubber feet 	8

## Tools Required

- Phillips screwdriver
- Magazine lock override tool — an opened paperclip, small screwdriver, or other object (3.5 mm or less in diameter that will not break off)

---

## Space Requirements

---

See the following:

- [Physical Specifications](#) on page 341 and
- [Air Clearance Requirements](#) on page 343

---

## Procedure

---

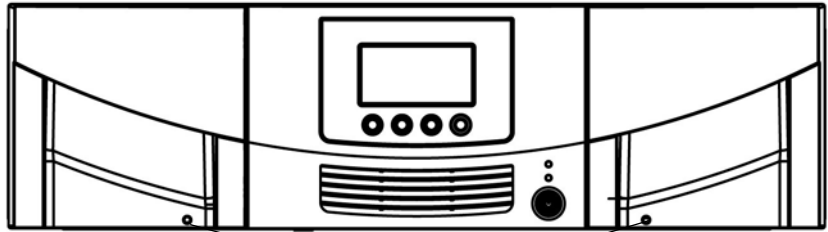
---

**WARNING:** Two people are required to safely lift the library.

---

- 1 If your library is currently installed in a rack, remove the magazines and tape drives, and then remove the library from the rack. See [Removing the Library From a Rack](#) on page 243.
- 2 Set the library on the desk or table in your chosen location.
- 3 Remove all the magazines from the library (if you have not already done so), as follows:
  - a Insert the magazine lock override tool into the access hole in the bottom of the magazine bezel (see [Figure 53](#)).
  - b Use the tool to depress the release latch while gently pulling outward on the magazine bezel handle. If the magazine is on the right side, it will only slide out as far as the I/E station. To release the magazine fully:
    - On the Scalar i40 and the bottom right magazine of the Scalar i80, reach under the open magazine and insert the tool directly into the access hole in the library chassis to depress the release latch, while pulling out on the magazine bezel handle.
    - On the top right magazine of the Scalar i80, reach under the open magazine and press the release latch directly with your finger, while pulling out on the magazine bezel handle.

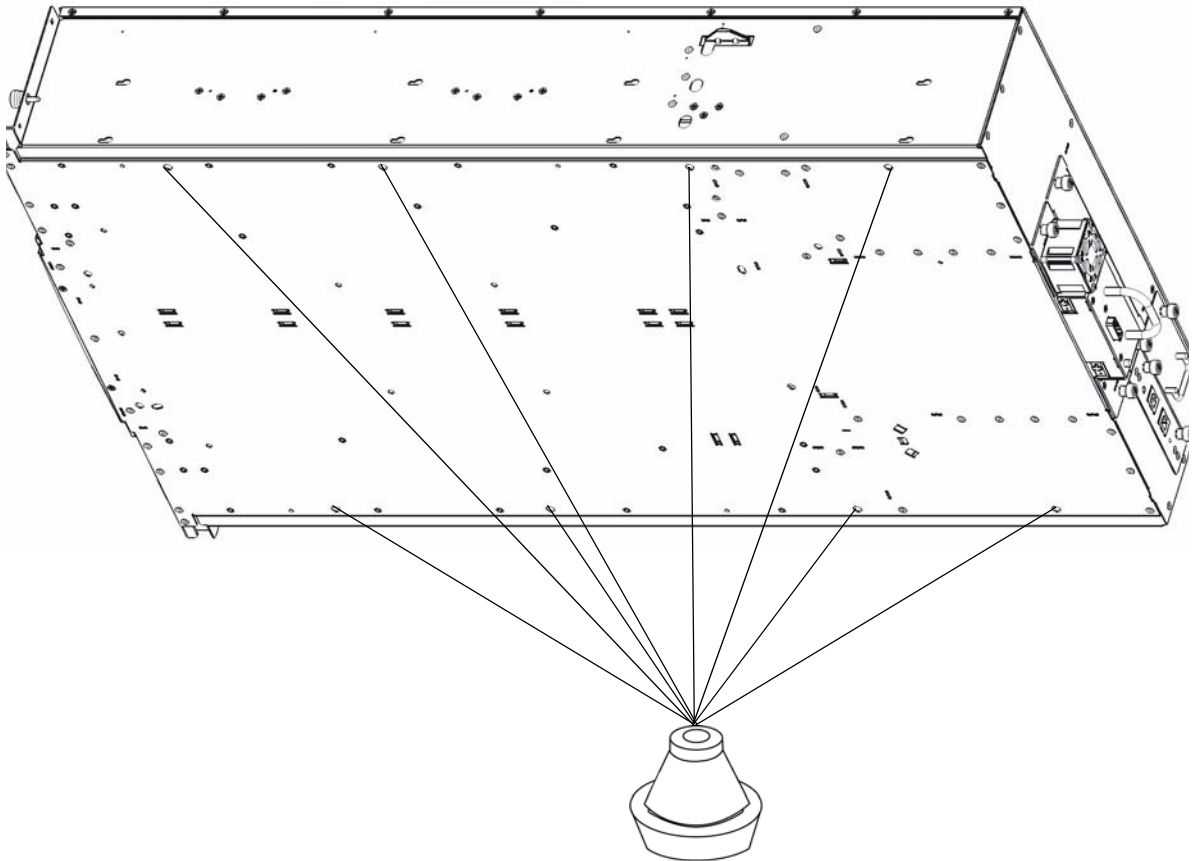
Figure 53 Magazine Release Latch Access Holes



Magazine release latch access holes

- 4 Look through the magazine slot openings to be sure the Y-tray is resting on the floor of the library. If not, reach inside and gently press down on one of the Y-tray's side metal rods until the Y-tray starts moving. It should drift down to rest on the floor of the library.
- 5 Turn the library carefully on its side (either the left or right side). Make sure the front end of the library (the "rack ear") overhangs the edge of the table so that the library lies flat.
- 6 Install the eight rubber feet on the bottom of the library, as follows:
  - a There are eight holes in the bottom of the library into which you will press the rubber feet. Four holes are located along the right edge and four along the left edge. [Figure 54](#) shows the locations of these holes.
  - b Use your fingers to press the feet into the holes. Twisting the feet as you push them may make it easier to get them in. See [Figure 54](#) on page 249.
  - c Carefully turn the library back to an upright position so that it is resting on its rubber feet.

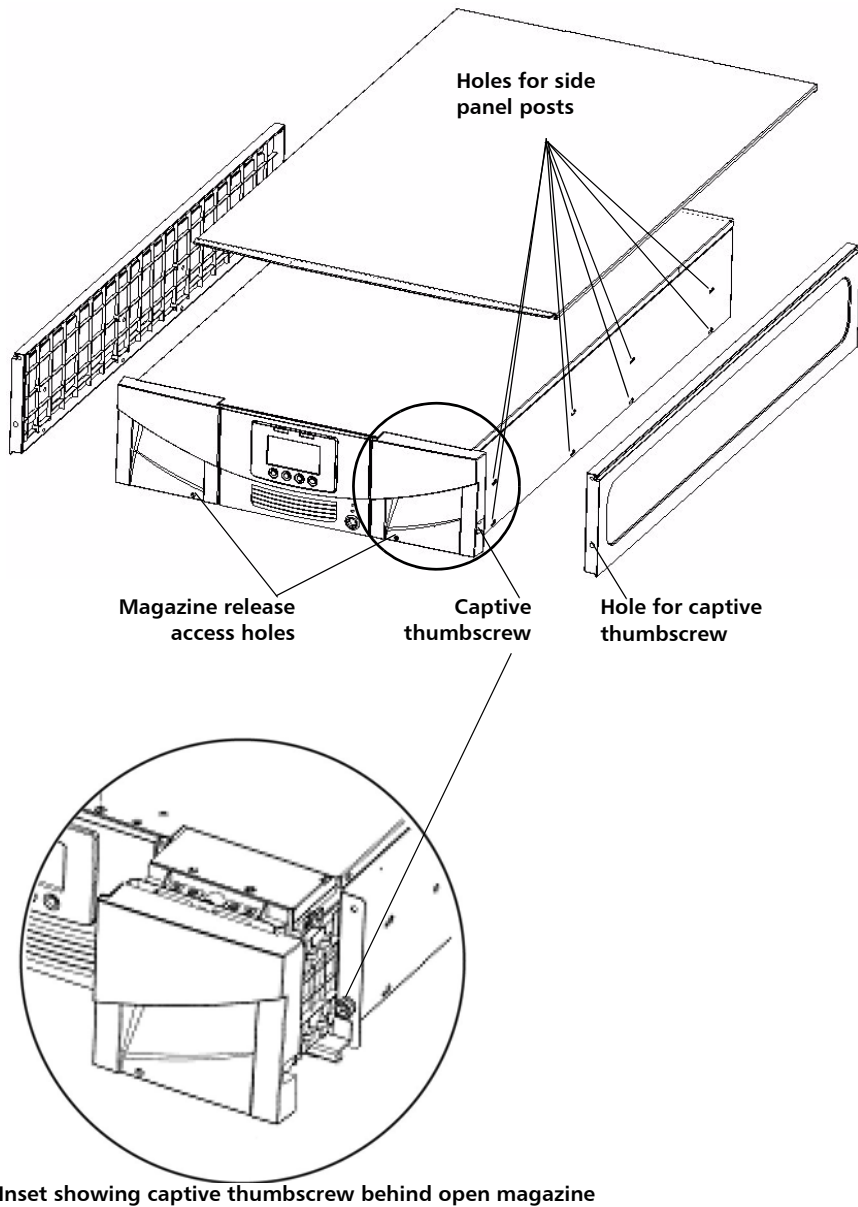
Figure 54 Location of Rubber Feet on Bottom of Library



- 7 Install the side panels one at a time (in any order) as follows (see [Figure 55](#) on page 251):
  - a Orient the side panel correctly. They are all the same but can only be installed one way. Line up the eight posts on the inside of the side panel with the holes in the side wall of the library. Line up the screw hole in the bottom front of the side panel with the captive thumbscrew behind the magazine on the library chassis.
  - b Press the side panel against the wall so that the posts go into the holes.

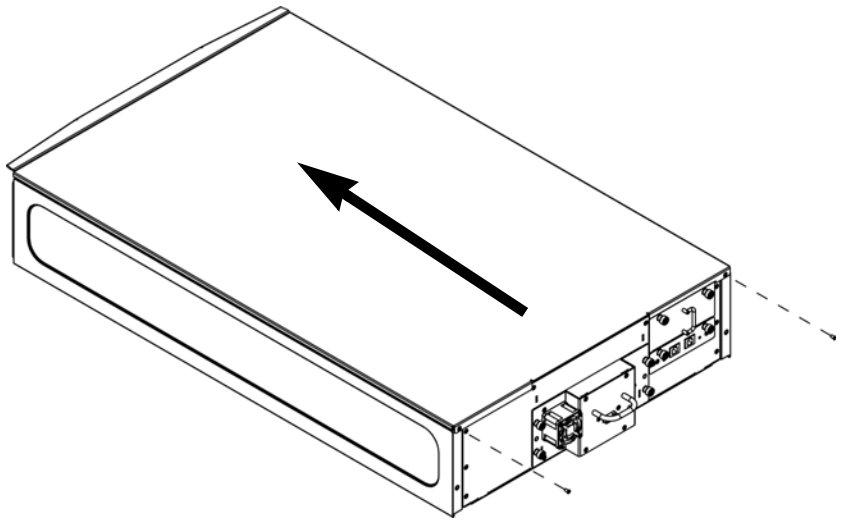
- c Slide the side panel toward the front of the library about half an inch until it stops and the posts are engaged in the holes. The side panel should be flush with the side of the library chassis.
- d Tighten the thumbscrew at the front of the library to secure the side panel to the library.

Figure 55 Installing side panels



- 8 Install the top cover as follows (see [Figure 56](#)):
  - a Slide the top cover onto the library, from back to front. The back of the top cover has two screw holes and overhangs the back of the library.
  - b Install the two top cover screws through the top cover and into the screw holes in the top of the side panels.

Figure 56 Installing Top Cover



- 9 Re-install the magazines and push them in until they close.
- 10 Re-install tape drives if you removed them previously.
- 11 Connect the tape drive cables, Ethernet cable, and power cord (see [Connecting Library Cables](#) on page 227).

## Removing the Library from a Desktop Kit

To remove the library from a desktop kit, reverse the steps in [Installing the Library in a Desktop Kit](#) on page 244.



# Removing and Replacing the Front Bezel

The procedure is similar for the Scalar<sup>®</sup> i40 and the Scalar i80. Pictures of the Scalar i40 also apply to the Scalar i80.

You may perform this procedure with library power **ON**. If you do, be careful not to accidentally press the power button and turn the library off when installing the bezel.

Read these instructions completely before beginning.

## Required Tools

- Phillips #1 screwdriver

## Bezel Replacement Kit Contents

- 1 Bezel
- 4 screws

## Bezel Replacement Procedure

- 1 Stop all library operations.
- 2 Open all the magazines in the library a few inches or remove them completely from the library.

---

**Note:** There is less chance of scratching or damaging the new bezel when you install it if you completely remove the magazines. **On the Scalar i80**, it is easier to perform this procedure with at least the bottom two magazines completely removed. You need room to maneuver your fingers on the sides of the bezel. If you remove all the magazines from a Scalar i80, label them so that you can reinstall them in the same locations later.

---

- a On the operator panel, select **Actions > Magazine**.
- b Select a magazine and press **Release**.
- c When prompted, pull open the magazine a few inches or remove the magazine completely.

- d Repeat for all magazines in the library.
- 3 Prepare to gain access to the bezel screws (see [Figure 57](#) on page 255 and [Figure 58](#) on page 256 for locations). The method depends upon how your library is installed. Follow the instructions in the table below that correspond to your library installation.

If your library is...	Follow these steps...
Installed in a rack high enough to access to the bottom bezel screws	Unscrew all the thumbscrews that secure the library to the rack (the Scalar i40 has two thumbscrews; the Scalar i80 has four). See <a href="#">Figure 58</a> on page 256.
Installed in a desktop kit	Release the desktop cover by removing two screws at rear of the desktop cover, then slide the desktop cover toward the back of the library two or three inches.
Installed very low in a rack so that you cannot access the bottom bezel screws unless you remove the library from the rack	Remove the library from the rack (see <a href="#">Removing the Library From a Rack</a> on page 243).

- 4 Slide the library one-to-two inches forward out of the rack or over the edge of the table or desk in order to access the two bottom bezel screws.

---

**WARNING:** Only slide the library out far enough out to access the two screws on the bottom of the library. The library is not secured in the rack or on the desk. Pulling it out too far could cause the library to slide out of the rack or off the desk.

---

---

**Caution:** Ensure there is enough slack in the power cords and cables connected in the rear of the library so that you do not dislodge them when you slide the library forward.

---

---

**Caution:** Do not tip the library or tilt it on its side.

---

- 5 Make sure all the magazines are pulled out a few inches (or removed) to allow you to remove and install the bezel without damaging it.
- 6 Remove and set aside the two screws securing the bezel to the bottom of the chassis (see [Figure 57](#) on page 255).
- 7 Remove and set aside the two screws securing the bezel to the top of the chassis (see [Figure 58](#) on page 256).

Figure 57 Bezel Screw  
Locations on Bottom of Library

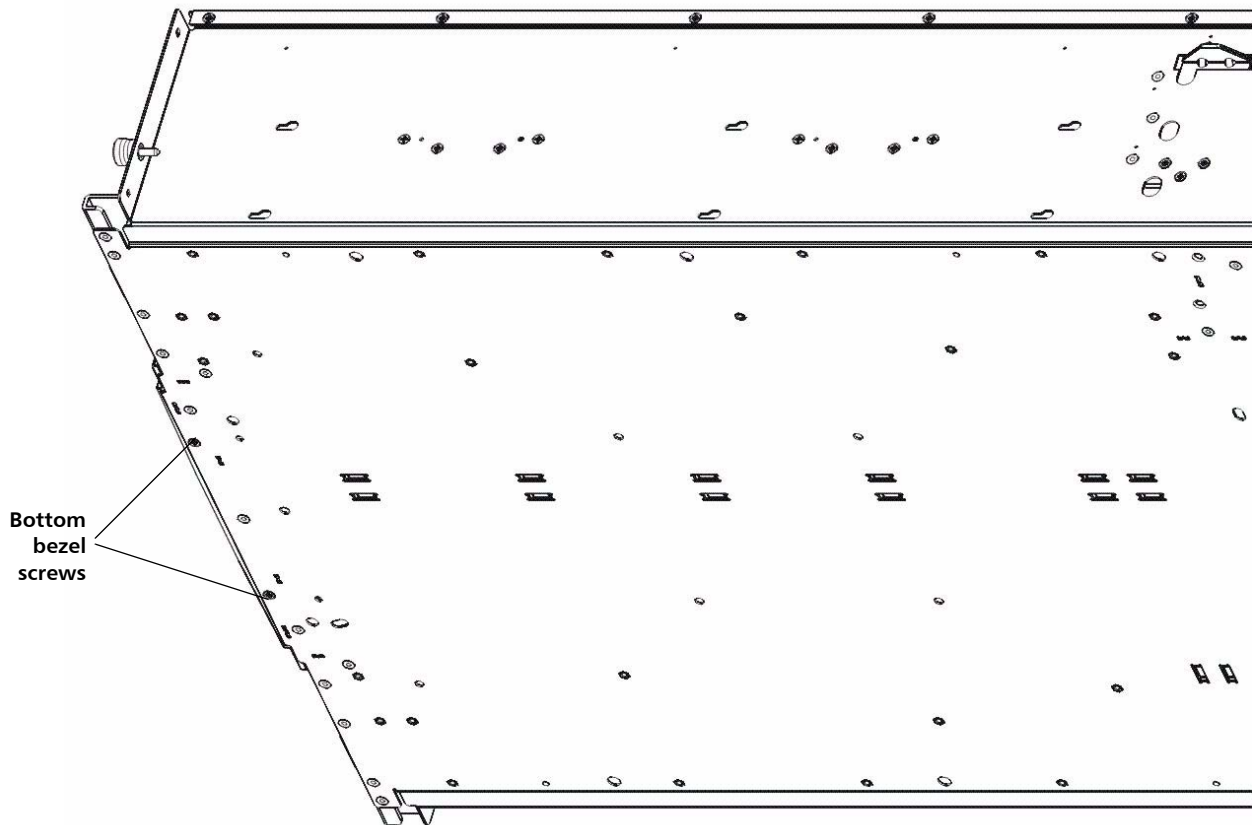
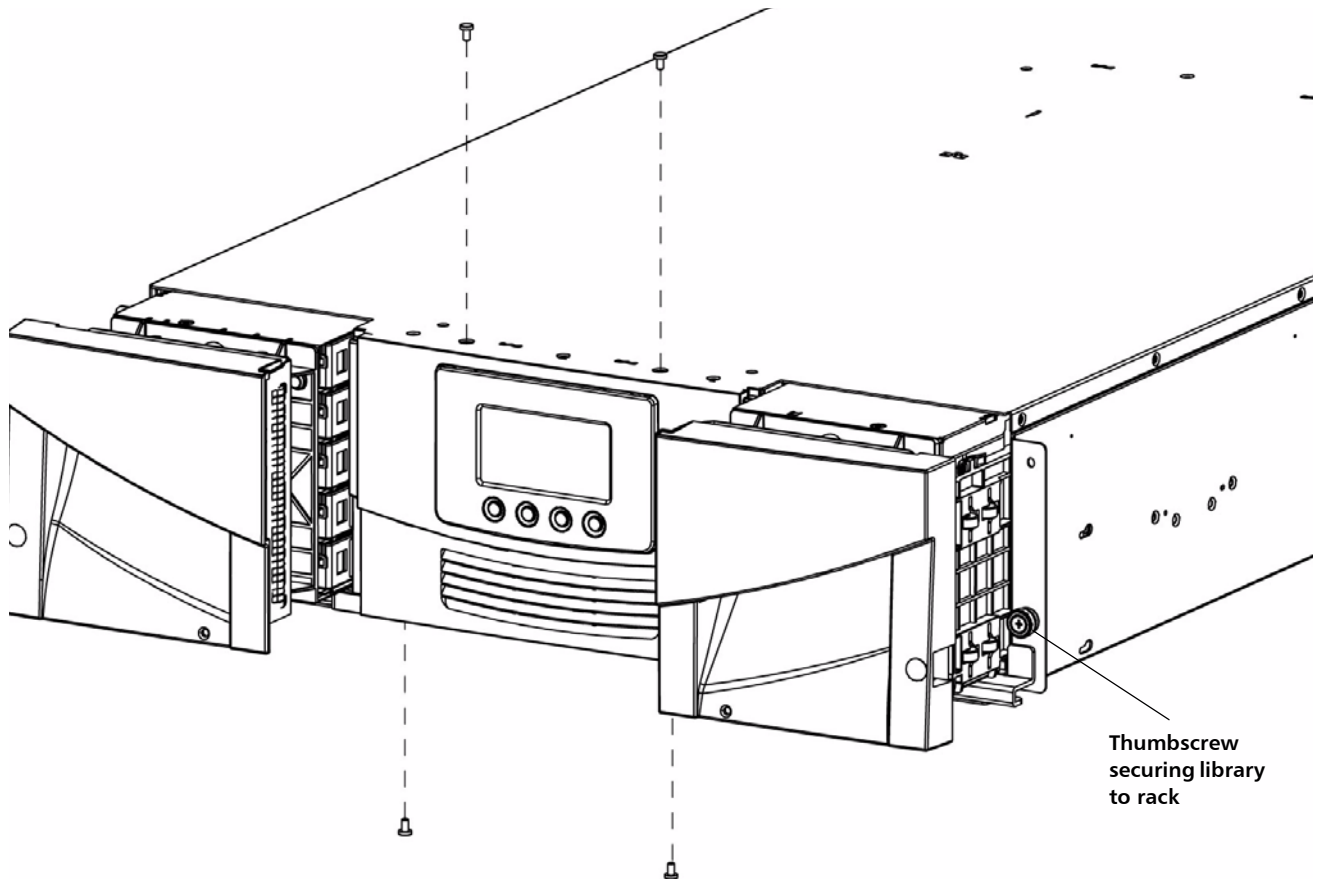


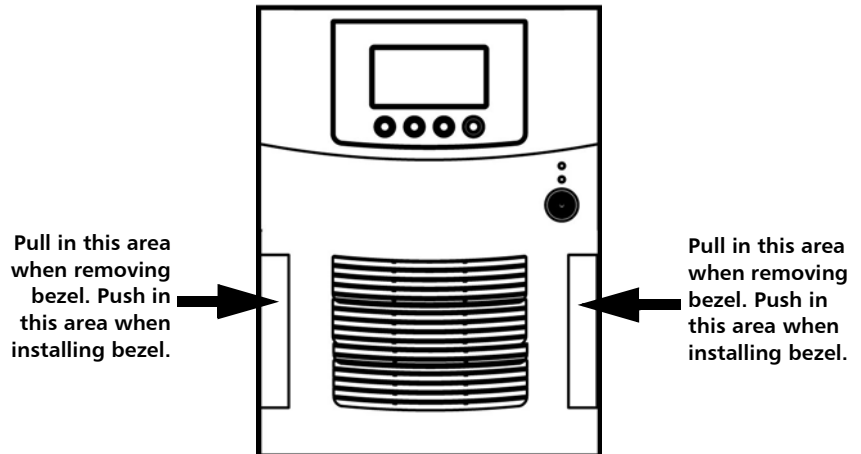
Figure 58 Bezel Screws



8 Remove the bezel as follows:

- **Scalar i40:** Grasp the bezel gently at the top and bottom and pull the bezel straight out and off of the library. Do not tip or twist the bezel as you pull it off.
- **Scalar i80:** Use your fingers to grasp the bezel near the center on both sides and pull outward to disengage the bezel (see [Figure 59](#) for location). There are plastic tabs on the inside of the bezel that help secure the bezel to the library and pulling outward from this location helps disengage them. You may need to move the bezel slightly back and forth to remove it.

Figure 59 Scalar i80 Pull/Push Locations



- 9 Install the new bezel straight onto the library. Do not tip or twist the bezel. If magazines are still in the library, be careful not to scratch or damage the bezel as you install it. Slide the top and bottom edges of the bezel to the inside of the top and bottom layers of the chassis sheet metal. **On the Scalar i80**, press in near the center on both sides of the bezel until you hear it “snap” into place (see [Figure 59](#) for locations).

---

---

**Caution:** Make sure the power button and all four operator panel control buttons appear through the holes in the bezel and are not trapped beneath the bezel.

---

---

---

---

**Caution:** Be careful not to accidentally hit the power button and turn the library off while you are installing the bezel.

---

---

- 10 Install the two top screws, then the two bottom screws.
- 11 Reinstall the library in the rack or desktop kit.
- 12 Close all the magazines.
- 13 If you turned the library off to perform this procedure, turn it **ON** now by pressing the power button on the front panel. Wait until the library initializes before resuming library operations.

- 14 If you removed the library from the rack to perform this procedure, run the Installation and Verification Test (IVT) to ensure the Y-tray, tape drives, and magazines are all functioning properly. From the operator panel, select **Tools > IVT** and follow the instructions on the screen. The IVT takes about 30 minutes. See [Running the Installation and Verification Test \(IVT\)](#) on page 325 for more information about the IVT.

---

## Replacing the Chassis

**DISCLAIMER:** Tests have been conducted on the finished product and have passed Safety Regulatory requirements at time of test.

---

**WARNING:** For field/customer replaceable sub-assemblies, all instructions pertaining to further integration and operation verification such as those in this document must be fully complied with. Do not attempt to operate the product before the product is fully assembled and self diagnostics show that the product passes, otherwise serious physical injury may occur to the user. The manufacturer(s) will not be held liable/responsible if such precautions are not adhered to.

---

---

**WARNING:** Two people are required to safely lift the library into and out of its packaging, a rack, or a desktop kit.

---

When you replace a library chassis, you will remove all the components from your existing library and install them in the new library.

---

### Required Tools

---

- Phillips #1 screwdriver
- Magazine lock override tool — an opened paperclip, small screwdriver, or other object (3.5 mm or less in diameter that will not break off)

## Procedure

When you replace a library chassis, you will remove all the components from your existing library and install them in the new library.

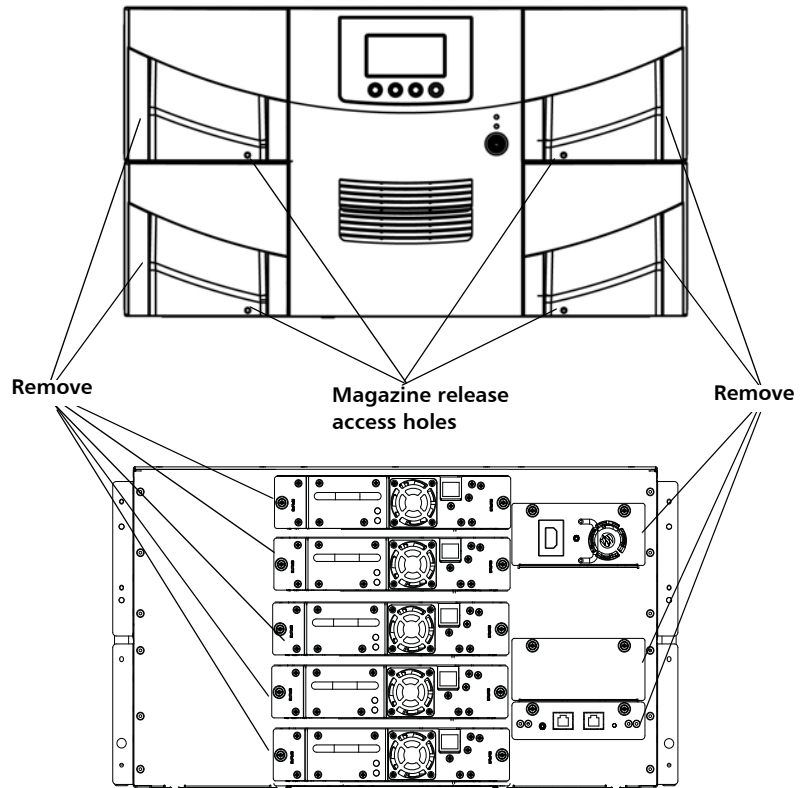
- 1 Unpack the new library chassis and place it on a flat, level surface. See the instructions in [Chapter 2, Unpacking the Library](#) for specific unpacking instructions, particularly about removing the Y-tray restraints.
- 2 Verify that the new chassis is the same type (Scalar<sup>®</sup> i40 or Scalar i80) as the unit you are replacing.
- 3 If you had license keys installed on your library, you will need to install new ones on the replacement library. Contact Quantum Support to request new license keys.
- 4 If the library you are replacing is still turned on and operational, shut down the library by selecting **Actions > Shutdown** from the operator panel.
- 5 Turn **OFF** the library by pressing the power button on the front panel.
- 6 Disconnect the power supply cord, the Ethernet cable, and all tape drive cables from the back of the library. If you have multiple tape drives, label the cables so you can reconnect them to the correct tape drives later.
- 7 Remove all of the following components from the library (see [Figure 60](#) on page 261).

Component to Remove	Instructions
Power Supplies	<hr/> <hr/> <p><b>Caution:</b> Make sure the power supply is unplugged and disconnected from live power before you remove it.</p> <hr/> <hr/> <ol style="list-style-type: none"> <li>1 Disconnect the power cord from the back of the power supply.</li> <li>2 Unscrew the captive thumbscrews.</li> <li>3 Pull outward on the power supply handle to remove it from the library.</li> </ol>
System Control Board (SCB)	<ol style="list-style-type: none"> <li>1 Loosen the two captive thumbscrews on the SCB.</li> <li>2 Grip the thumbscrews and pull outward to slide the SCB out of the library.</li> <li>3 Place the SCB on an anti-static surface or in an anti-static bag.</li> </ol>

Component to Remove	Instructions
Tape Drives	<ol style="list-style-type: none"><li>1 Label each tape drive with its location in the library slots. It is recommended that you reinstall the tape drives in the same location in the new chassis.</li><li>2 Unscrew the captive thumbscrews securing the tape drive sled to the back of the library. Half-height tape drives have two thumbscrews. Full-height tape drives have four thumbscrews.</li><li>3 Using the handle, pull the drive sled out of the library. It should slide out smoothly and easily.</li></ol>
Filler Plates	<p>Remove all filler plates (tape drive and power supply).</p> <ol style="list-style-type: none"><li>1 Unscrew the two captive thumbscrews.</li><li>2 Pull the filler plate out.</li></ol>
Magazines	<ol style="list-style-type: none"><li>1 If your library is a Scalar i80, label the magazines so you can reinstall them in the same slots.</li><li>2 Insert the magazine lock override tool into the access hole in the bottom of the magazine bezel.</li><li>3 Use the tool to depress the release latch while gently pulling outward on the magazine bezel handle. If the magazine is on the right side, it will only slide out as far as the I/E station. To release the magazine fully:<ul style="list-style-type: none"><li>• On the Scalar i40 and the bottom right magazine of the Scalar i80, reach under the open magazine and insert the tool directly into the access hole in the library chassis to depress the release latch, while pulling out on the magazine bezel handle.</li><li>• On the top right magazine of the Scalar i80, reach under the open magazine and press the release latch directly with your finger, while pulling out on the magazine bezel handle.</li></ul></li></ol>



Figure 60 Components to Remove



8 If the library is in a desktop kit or rack, remove it.

- To remove the library from a rack, unscrew the captive thumbscrews on the front of the library that secure the library to the rack, then slide the library out of the rack. Place the library on a flat, stable surface.

---

**WARNING:** Two people are required to safely lift the library out of a rack.

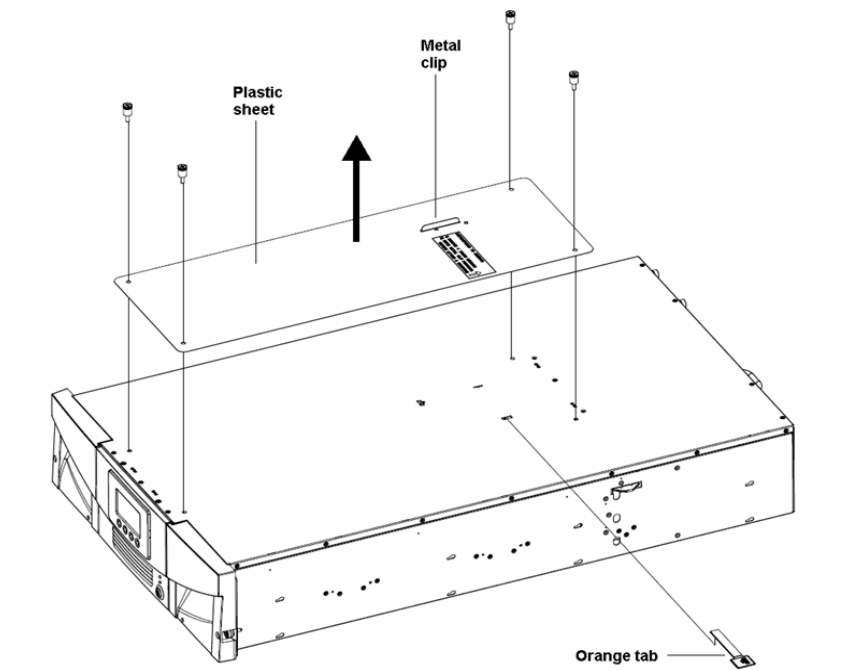
---

- To remove the library from a desktop kit, remove the two top cover screws at the rear of the top cover. Loosen the captive thumbscrews on the library chassis that are attached to the side panels of the desktop kit. Slide the side panels one-half inch toward the rear of the library to disengage the side-panel posts from the library wall, then pull the side panels off.

Do **NOT** remove the eight rubber “feet” installed on the bottom of the library (you will remove them later, in [Step c, Sub-Step c](#) on page 263, once the library is set on its side).

- 9 Remove the Y-tray restraint from the replacement chassis. The restraint consists of four (4) thumbscrews, a plastic sheet, a small metal clip, and underneath the plastic sheet, an orange restraint tab (see [Figure 61](#)) located on the top cover of the library.
  - a Unscrew and remove the four thumbscrews from the top cover. Save the thumbscrews for use in restraining the Y-tray in the chassis you are returning.
  - b Remove the plastic sheet and metal clip and discard. You will not need to use them again.

Figure 61 Removing the Y-tray Restraints



- c Remove the orange shipping restraint tab and discard. You will not need to use it again.

---

**Note:** The robot may stay at the top of the library, or it may move downward toward the floor of the library. If it moves downward, you will hear the gears turning as it moves. This is normal.

---

- 10 Restrain the Y-tray in the chassis being returned as follows (see [Figure 62](#) on page 264):
- a Look through the magazine slot openings to be sure the Y-tray is resting on the floor of the library. If not, reach inside and gently press down on one of the Y-tray's side metal rods until the Y-tray starts moving. It should drift down to rest on the floor of the library.
  - b Turn the library carefully on its side (either the left or right side). Make sure the front end of the library (the "rack ear") overhangs the edge of the table so that the library lies flat.

---

**Caution:** Do not turn the library upside down. Do not turn the library more than 90 degrees from upright.

---

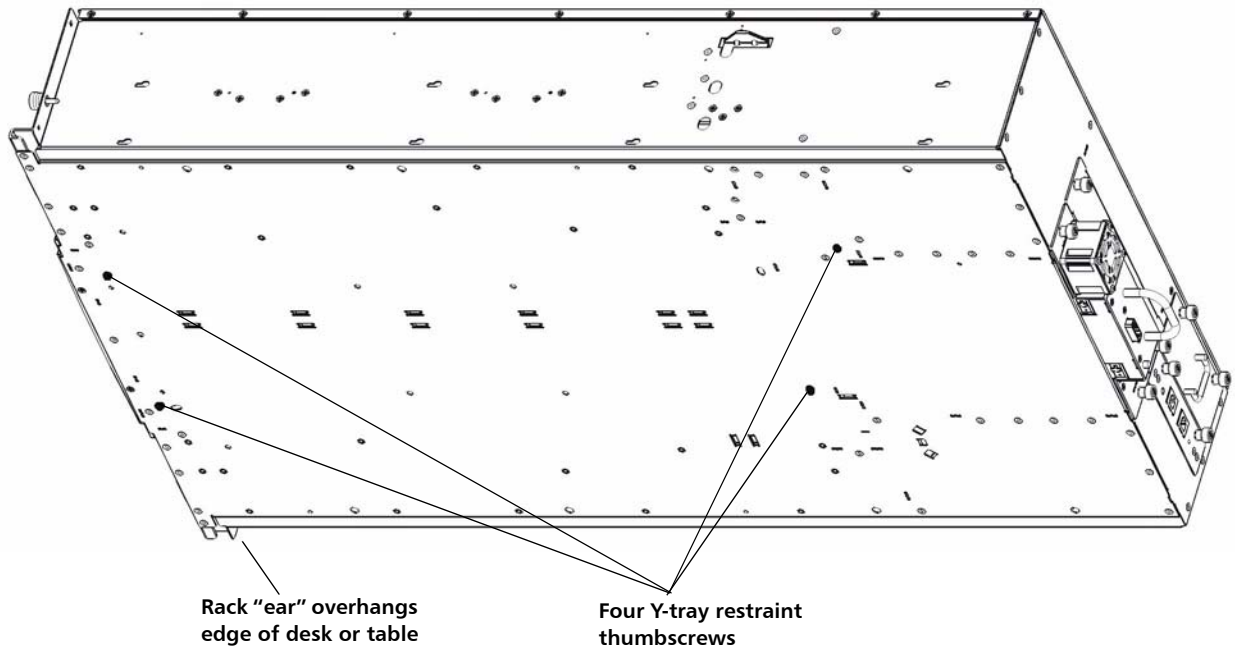
- c If your library was installed in a desktop kit, remove the eight rubber "feet" installed on the bottom of the library. You can remove them by twisting them as you pull them out. Save them to use on the replacement chassis.
- d Take the four thumbscrews you just removed from the replacement chassis and install them into the floor of the chassis you are returning in the locations shown in [Figure 73](#). They will screw through the Y-tray and secure it in place on the floor of the chassis.
- e Do NOT turn the library back to an upright position at this point. Leave it on its side until you place it in the box.

---

**Caution:** If you place the library upright with the Y-tray restraint thumbscrews installed, you could damage the chassis or the Y-tray.

---

Figure 62 Restraining the Y-tray



- 11 If desired, you may cover the holes in the replacement library top cover with stickers, which are provided in the accessory kit for this purpose. This step is optional and is intended to prevent small objects from accidentally falling into the library through the holes.
- 12 Install the new chassis in a rack or desktop kit. For instructions, see [Installing the Rack Mount Kit \(Rail Kit\)](#) on page 229 or [Installing the Library in a Desktop Kit](#) on page 244.

---

**WARNING:** Two people are required to safely lift the library.

---

13 Install the components you removed from the old chassis into the new chassis.

Component to Install	Instructions
System Control Board (SCB)	<p>Install the SCB <b>before</b> you install the power supply.</p> <ol style="list-style-type: none"> <li>1 Position the SCB for installation: The board components face up. The flat part of the board faces down. The thumbscrews are on the upper side of the SCB back plate.</li> <li>2 Install the new SCB by pushing the SCB into the slot until it stops. It should slide smoothly and easily. When it reaches the end of its travel, press firmly on the back panel of the SCB to “snap” it into place.</li> <li>3 Tighten the two thumbscrews finger tight.</li> <li>4 Connect the Ethernet cable to the LEFT Ethernet port (as viewed from the back of the library; see <a href="#">Figure 63</a> on page 267).</li> </ol>
Power Supplies	<p>If your library is a Scalar i80 and you have only one power supply, install it in the top slot. If you have two power supplies, install them both.</p> <hr style="border: 1px solid red;"/> <p><b>Caution:</b> Make sure the power supply is unplugged and disconnected from live power before you install it.</p> <hr style="border: 1px solid red;"/> <ol style="list-style-type: none"> <li>1 Push the power supply straight into the slot. You may need to press firmly on the power supply sheet metal at the very end to plug in the power supply to the connector on the library. You will feel it snap into place. The power supply only goes in one way, and should slide in easily. If you cannot slide it in, you may be trying to install it upside down.</li> <li>2 Tighten the two thumbscrews finger tight.</li> <li>3 Connect the power cord to the power supply.</li> <li>4 Plug the power cord into a grounded AC outlet.</li> </ol>

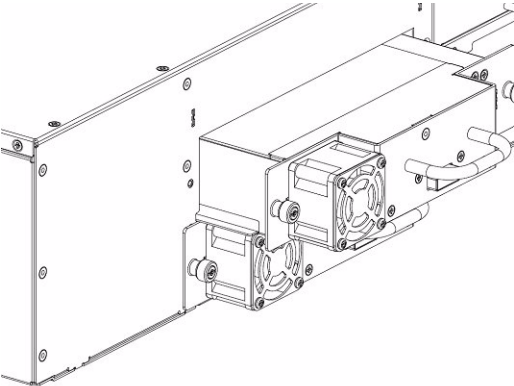
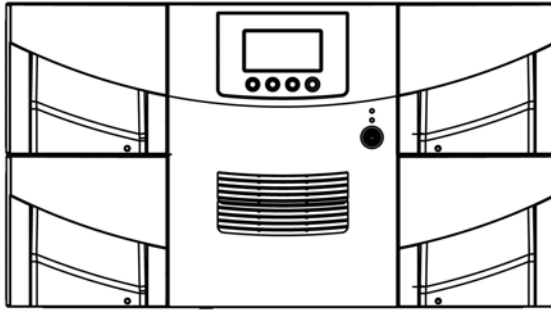
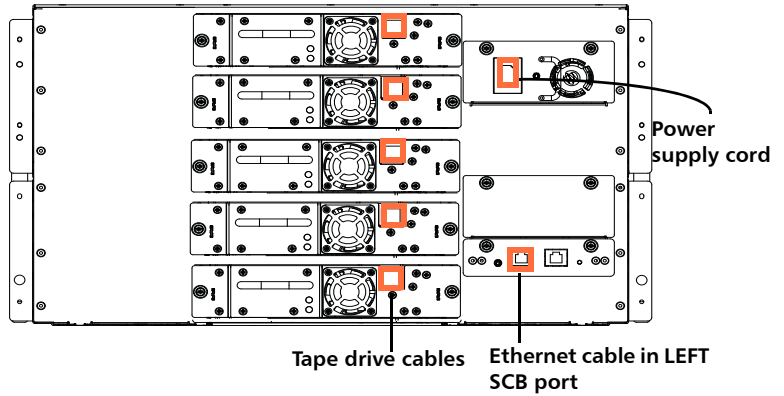
Component to Install	Instructions
Tape Drives	<p>1 Insert the tape drives into the same drive slots they were in the old chassis. The “shelf” on the bottom of the drive sled fits into the notch in the library chassis and slides on the plastic guide rails. The tape drive must be level to slide in smoothly. At the very end of the slide, you will feel a slight “click” as the tape drive sled connector connects into its mating connector in the library chassis.</p>  <p>2 Tighten the tape drive’s captive thumbscrews finger tight to secure the tape drive to the library chassis.</p> <p>3 Connect all tape drive cables as they were in the old unit. Make sure they are connected to the host or switch as they were before. For full-height Fibre Channel tape drives, the cable must go in the LEFT connector (as viewed from the back of the library; see <a href="#">Figure 63</a> on page 267).</p>
Filler Plates	<p>Make sure every empty power supply slot and tape drive slot is covered with a filler plate.</p> <p>1 Slide the filler plate into the slot.</p> <p>2 Tighten the thumbscrews.</p>
Magazine	<p>Slide each magazine into its slot and push it in all the way until it stops.</p>

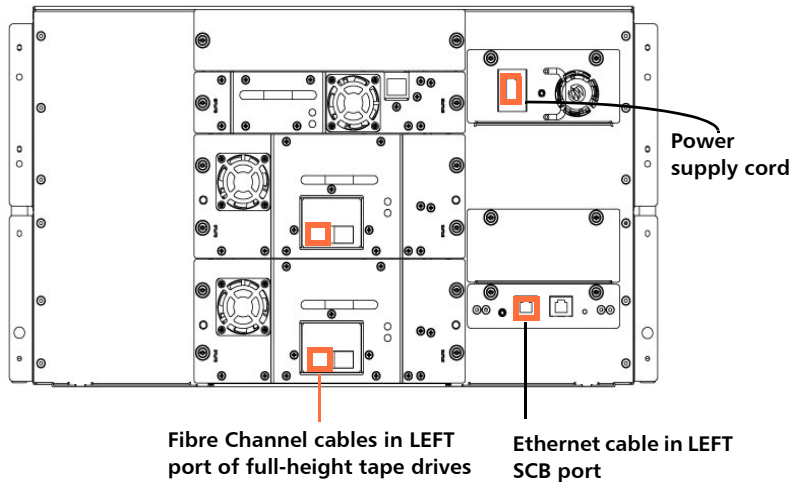
Figure 63 Reinstalled Components



Half-height tape drives



Full-height tape drives



- 14 Turn **ON** the library by pressing the power button on the front panel.
- 15 Wait for the library to initialize. This can take up to 5 to 17 minutes, depending on library size.
- 16 You will notice the library has a new diagnostic ticket (DT042) stating the library's vital product data (VPD) has changed.
- 17 Since the VPD change is caused by the intentional library chassis replacement, follow the Diagnostic Ticket resolution steps to reconfigure the host application accordingly.
- 18 If you had license keys installed on the old library, install the new license keys. From the operator panel, select **Setup > License Installation**; or from the Web client, select **Setup > License**. For further directions, see [Applying a License Key](#) on page 71.
- 19 Run the Installation and Verification Test (IVT) to ensure the Y-tray, tape drives, and magazines are all functioning properly. From the operator panel, select **Tools > IVT** and follow the instructions on the screen. The IVT takes about 30 minutes.
- 20 Save the library configuration (from the Web client, select **Tools > Save/Restore Configuration** and save the configuration to a known location).
- 21 Wrap the removed chassis in the antistatic wrapping that contained the replacement chassis. Package the removed chassis using the packaging that contained the replacement chassis. Use the enclosed RMA information to send the chassis back to Quantum.
- 22 If your library is running SKM, you must you run a special script on the SKM server after you replace the chassis. The script will correct the library serial number associations in the key server database and allow you to export used SKM encryption keys via the Web client correctly. For instructions, refer to the chapter titled "Updating the SKM Keystore After Replacing a Library Control Module" in the *Scalar Key Manager 2.0 User's Guide*.



## Removing and Installing a Filler Plate

A filler plate is required to cover every empty tape drive and power supply slot on the rear of the library, in order to maintain proper library cooling. If you remove a tape drive or power supply from the library, you must cover the opening with a filler plate.

There are two types of filler plates:

- Tape drive
- Power supply

### Removing and Installing a Tape Drive Filler Plate

The filler plate is half-height in size. If you remove a full-height tape drive, you must install two filler plates to cover the opening.

#### Removing a tape drive filler plate

- 1 Unscrew the two captive thumbscrews and pull the filler plate out.
- 2 Save the filler plate in case you need to use it again.

#### Installing a tape drive filler plate

- The tape drive filler plate has no “top” or “bottom” orientation – it can go in either way (see [Figure 64](#) on page 270).
- Slide the filler plate into the slot and tighten the thumbscrews.

### Removing and Installing a Power Supply Filler Plate

The power supply filler plate is used only on the Scalar<sup>®</sup> i80 when only one power supply is present.

#### Removing a power supply filler plate

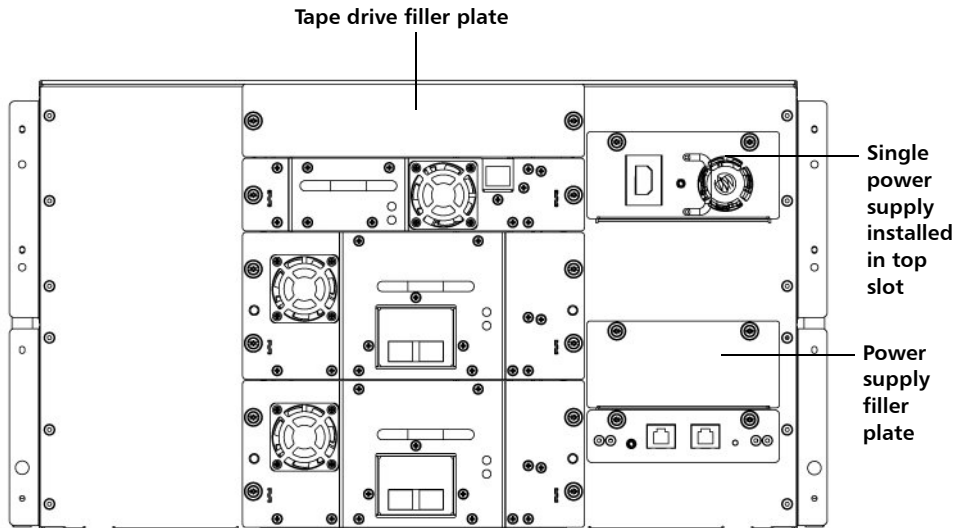
- 1 Unscrew the two captive thumbscrews.
- 2 Pull out on the thumbscrews so the filler plate is at a slight angle and the bottom of the filler plate is still attached in the slot.

- 3 Lift the filler plate up to disengage the catch at the bottom and pull the filler plate out of the slot.

### Installing a power supply filler plate:

- On the Scalar i80, if you are using only one power supply, you should install the power supply in the upper slot, and cover the lower slot with a filler plate (see [Figure 64](#) on page 270).
- 1 Hold the filler plate with the thumbscrews at the top.
  - 2 Insert the bottom edge of the filler plate into the slot, engaging the bottom edge of the filler plate into the bottom of the slot.
  - 3 Pivot the filler plate up to fit securely in the hole.
  - 4 Tighten the thumbscrews.

Figure 64 Filler Plates Installed



## Removing and Replacing a Magazine

The procedure for replacing magazines is the same on the Scalar<sup>®</sup> i40 and the Scalar i80.

---

**Note:** The library can operate with one or more magazines uninstalled. However, it will operate at reduced speed.

---

### Required Tools

- Phillips #1 screwdriver

### Magazine Replacement Kit Contents

- (1) magazine
- (1) left-side magazine bezel
- (1) right-side magazine bezel
- (4) M3 x 6 Phillips head screws
- (4) washers

### Creating a Backup Map of Cartridge Locations

When you transfer tape cartridges from the removed magazine into the replacement magazine, each cartridge needs to go in the same slot position it was in previously. One way to do this is to transfer the cartridges one by one from one magazine to the other. However, if the cartridges get mixed up or dropped, you need a backup method to know where to place your cartridges. The library configuration report provides a convenient backup “map.”

- 1 On the Web client, select **Reports > Library Configuration**.
- 2 Click the **Show Barcodes** button.

The screen displays a map of the library showing the location of each cartridge, by barcode.

- 3 Click the “print” icon in the upper right corner to print the report.



Alternatively, take a screen capture of the report and save or print it, or copy the map by hand.

---

## Removing the Magazine from the Library

---

You can perform this procedure with library power on.

- 1 From the operator panel, select **Actions > Magazine**.
- 2 Use the **Up** and **Down** buttons to select the magazine you want to remove and press **Release**.
- 3 Wait for the operator panel to display the message: “Magazine is now unlocked. Waiting for the magazine to be moved to the expected position.”
- 4 Pull out on the magazine bezel handle and remove the magazine from the library. If you do not remove the magazine within 30 seconds, the magazine locks again.

---

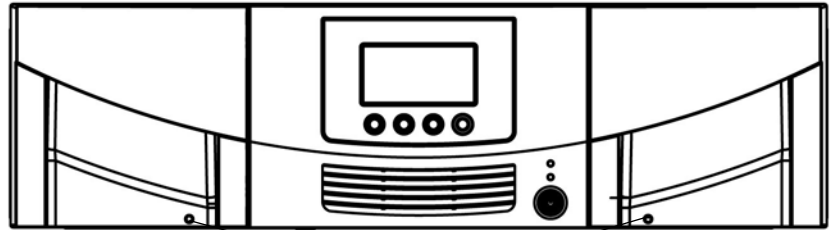
**Note:** If the library is turned off, you can release the magazine manually by inserting an opened paperclip, small screwdriver, or other object (3.5 mm or less in diameter that will not break off) into the access hole in the bottom of the magazine bezel (see [Figure 65](#)). Use the tool to depress the release latch while gently pulling outward on the magazine bezel handle.

Right-side magazines will only slide out as far as the I/E station.

To release right-side magazines fully:

- On the Scalar i40 and the bottom right magazine of the Scalar i80, reach under the open magazine and insert the tool directly into the access hole in the library chassis to depress the release latch, while pulling out on the magazine bezel handle.
  - On the top right magazine of the Scalar i80, reach under the open magazine and press the release latch directly with your finger, while pulling out on the magazine bezel handle.
-

Figure 65 Magazine Release Latch Access Holes



Magazine release latch access holes

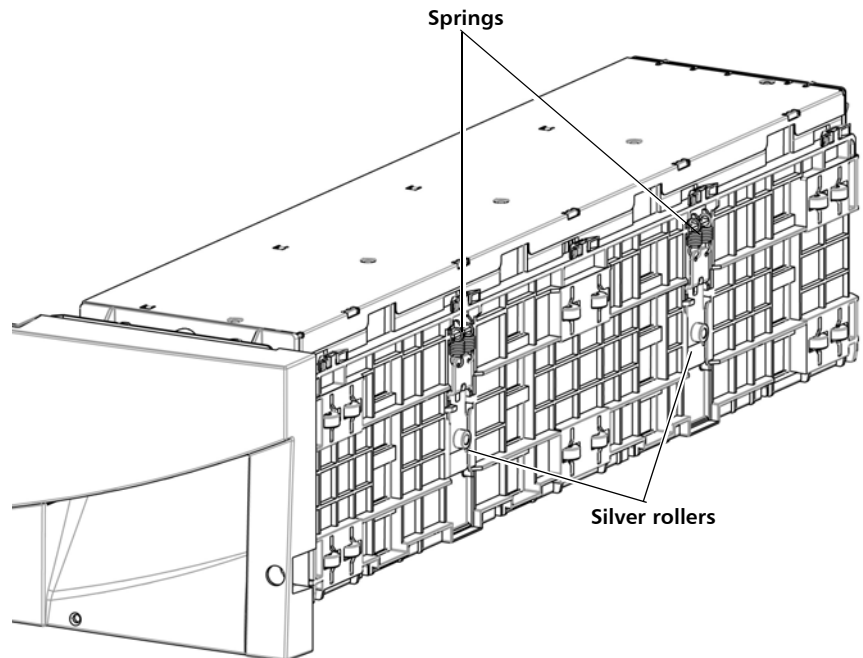
## Installing the Magazine

The replacement magazine can be used on either the left or right side of the library, depending on how it is oriented. Once it is oriented correctly, the left or right bezel can be attached.

You can perform this procedure with the library powered on.

- 1 Place the removed magazine in the orientation it would be if it were installed in the library.
- 2 Place the replacement magazine next to the removed magazine in the same orientation. Make sure they look the same from all angles.
  - The storage slots face inward.
  - On the outer wall of the magazine, the silver rollers sit below the springs (see [Figure 66](#)).

Figure 66 Proper Orientation  
(Right-Side Magazine)



- 3 Choose the correct bezel (left or right) from the magazine replacement kit.

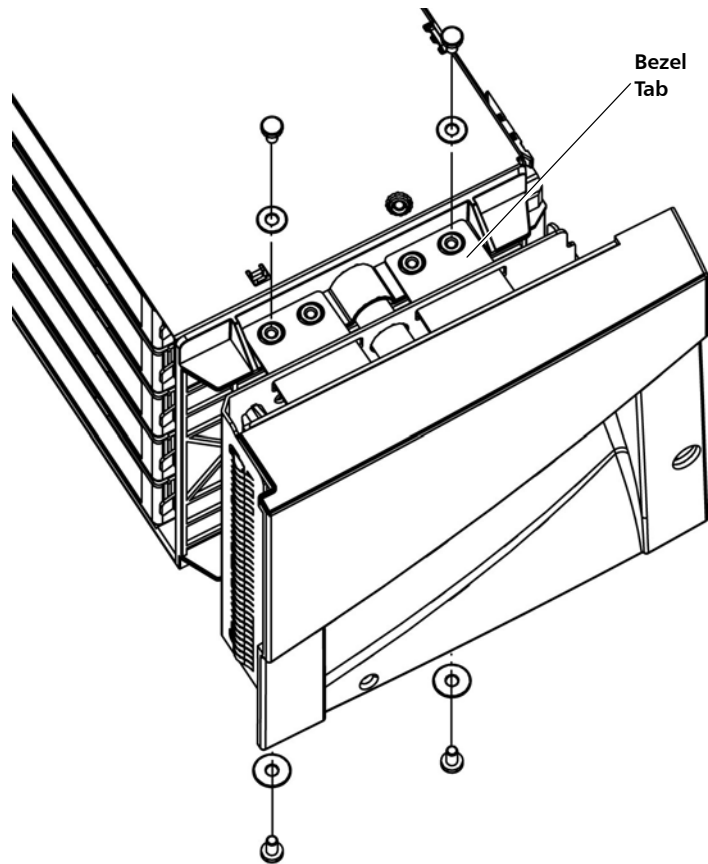
---

**Note:** If you try to install the wrong bezel, it will not fit and you will not be able to install it.

---

- 4 Push up on the top bezel tabs and fit them over the posts on the top of the magazine. Turn the magazine over and repeat on the bottom (see [Figure 67](#) on page 275).
- 5 Install the two washers and two M3 screws securing the top of the bezel to the magazine. Install them in the outer hole in each tab (see [Figure 67](#) on page 275).
- 6 Turn the magazine over and install the two washers and two M3 screws securing the bottom of the bezel to the magazine. Install them in the outer hole in each tab (see [Figure 67](#)).

Figure 67 Removing/Installing the Magazine Bezel



- 7 Remove the tape cartridges from the removed magazine and carefully install them in the exact same slots in the replacement magazine. Use the map you created if necessary.
- 8 Slide the magazine into the magazine slot all the way until it stops. The library performs an inventory on the replaced magazine.
- 9 Wait for the library to finish its inventory.
- 10 Run the magazine diagnostics test on the replaced magazine to be sure it is functioning correctly.
  - a Place a scratch tape in the top I/E station slot.
  - b If manual cartridge assignment is enabled, assign the scratch tape to the System partition.

- c From the operator panel, select **Tools > Diagnostics**.
- d Continue through the next few screens to run the magazine test on the replaced magazine.

If a problem is found during testing, you receive a diagnostic ticket. See [Running the IVT Diagnostic Subtests Individually – Robotics, Tape Drive, and Magazine Tests](#) on page 327 more information.

## Removing and Installing a Power Supply

The Scalar® i40 contains one power supply. The Scalar i80 can have up to two power supplies for redundancy purposes.

An unused power supply slot must be covered by a filler plate.

This document covers:

- [Replacing a Power Supply in a Single-Power-Supply System \(Scalar i40 and Scalar i80\)](#)
- [Adding or Replacing a Redundant Power Supply on the Scalar i80](#)

Figure 68 Single Power Supply System

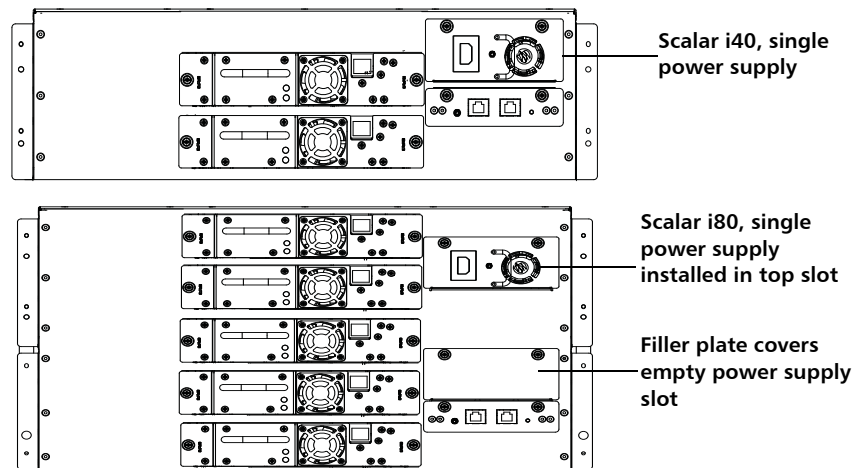
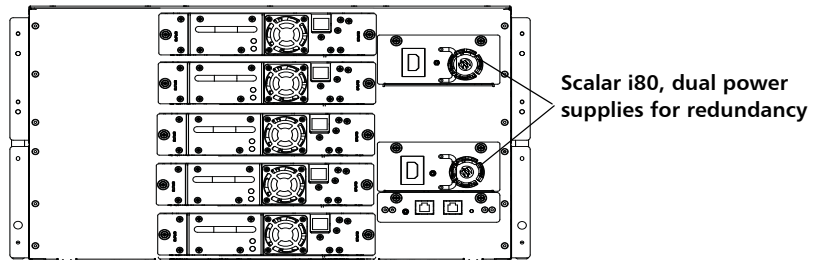




Figure 69 Redundant Power Supply System



### Replacing a Power Supply in a Single-Power-Supply System (Scalar i40 and Scalar i80)

**Note:** If you have a single power supply in a Scalar i80, it is recommended that you install it in the upper slot, to provide better temperature control (see [Figure 68](#)).

- 1 Shut down the library (from the operator panel, select **Actions > Shutdown > Shutdown Library**). Wait for the screen to prompt you to turn off library power.
- 2 Turn **OFF** library power by pressing the power button on the front panel. Wait for the operator panel screen to turn off.
- 3 Disconnect the power cord from the power supply.

---

**Caution:** Make sure you disconnect live power from the power supply before you remove or install it. Otherwise, damage to the power supply could occur.

---

- 4 Unscrew the two captive thumbscrews on the power supply.
- 5 Using the handle, slowly pull the power supply straight out of the library.
- 6 Install the new power supply by pushing it straight in to the slot. You may need to press firmly on the power supply sheet metal at the very end to plug in the power supply to the connector on the library. You will feel it snap into place.

The power supply only goes in one way, and should slide in easily. If you cannot slide it in, you may be trying to install it upside down.

- 7 Tighten the two thumbscrews finger tight.

- 8 Connect the power cord to the power supply.
- 9 Make sure the power cord is plugged in to a grounded, AC outlet.
- 10 The power supply LED should turn amber to indicate it is plugged in but the library is not turned on.
- 11 Turn **ON** library power by pressing the power button on the front panel.

The power supply LED should turn green immediately to indicate the library is turned on.

If the power supply LED is red, the power supply is not working. Contact Quantum Support.

---

### Adding or Replacing a Redundant Power Supply on the Scalar i80

---

You do not need to turn off library power to perform this procedure.

- 1 If you are adding a new power supply to a Scalar i80, remove the filler plate and start at [Step 6](#) below.
- 2 If you have two power supplies, determine which one to remove.

---

**Caution:** Make sure you remove the power supply whose LED is red or off. Do not remove the power supply whose LED is green.

---

- 3 Disconnect the power cord from the power supply you want to remove.

---

**Caution:** Make sure you disconnect live power from the power supply before you remove or install it. Otherwise, damage to the power supply could occur.

---

- 4 Unscrew the two captive thumbscrews on the power supply.
- 5 Using the handle, slowly pull the power supply straight out of the library.
- 6 Install the new power supply by pushing it straight in to the space. You may need to press firmly on the power supply sheet metal at the very end to plug in the power supply to the connector on the library. You will feel it snap into place.

The power supply only goes in one way, and should slide in easily. If you cannot slide it in, you may be trying to install it upside down.

- 7 Tighten the two thumbscrews finger tight.
- 8 Connect the power cord to the power supply.
- 9 Make sure the power cord is plugged in to a grounded, AC outlet.

The power supply LED should turn green immediately to indicate the library is turned on.

If the power supply LED is red, the power supply is not working. Contact Quantum Support.

---

## Removing and Replacing the System Control Board

These instructions explain how to remove a system control board (SCB) and replace it with a new one.

The SCB contains library firmware, tape drive firmware, all configurable settings, license keys, and SKM TLS certificates. After you replace the SCB, you must either restore a previously saved configuration, or reinstall the license keys and manually reconfigure the settings.

---

**Note:** When you replace the SCB you will permanently lose all data previously collected for logs and reports.

---

The process steps are:

- 1 [Replacing the System Control Board](#)
- 2 [Installing Library Firmware](#)
- 3 [Restoring the Library Configuration](#) *or* [Manually Reconfiguring the Library](#)

---

### Replacing the System Control Board

---

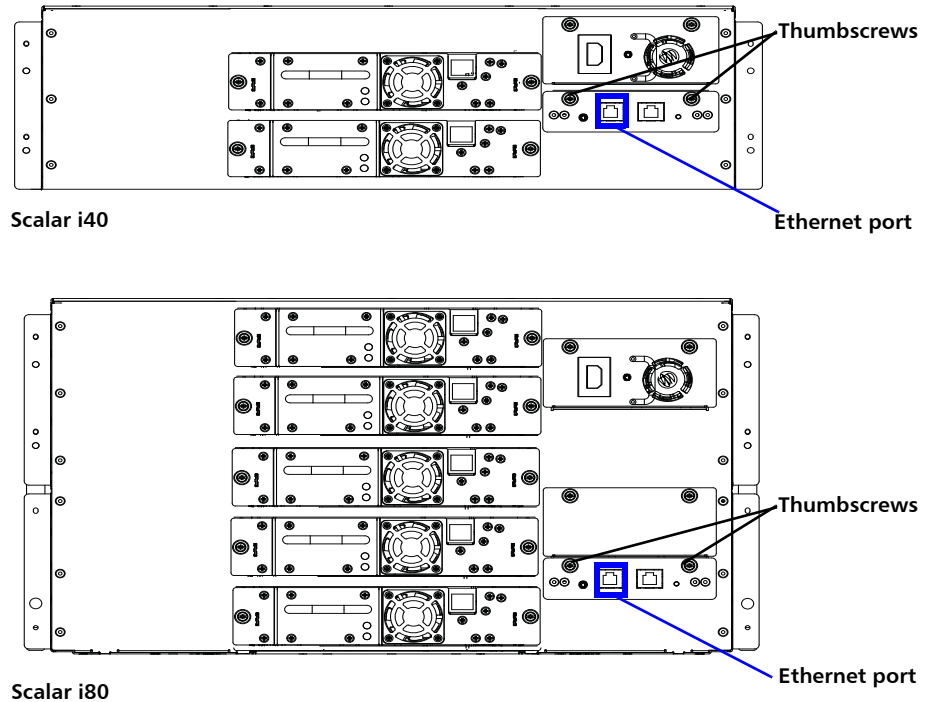
---

**Caution:** You must completely remove power from the library before removing and replacing the system control board.

---

- 1 If the library is still operational, save the library configuration. From the Web client, select **Tools > Save/Restore Configuration**. Select **Save Configuration** and click **Apply**. Save the configuration to a known location.
- 2 If the library is still operational, and you want to save log and report information for historical purposes, access the logs and reports you want using the Web client and save them to a known location.
- 3 If possible, save a library snapshot for future troubleshooting. From the Web client, select **Tools > Capture Snapshot** and follow the instructions.
- 4 If the library is still operational, shut down the library by selecting **Actions > Shutdown > Shutdown Library** from the operator panel.
- 5 When prompted, turn **OFF** the library by pressing the power button on the front panel. Wait for all the LEDs on the SCB to turn off.
- 6 Disconnect the power cords from the power supplies on the back of the library. The Scalar i40 has one power supply. The Scalar i80 may have one or two power supplies. Make sure you disconnect all power cords from the power supplies.
- 7 Remove the Ethernet cable from the SCB (see [Figure 70](#) on page 281).
- 8 Loosen the two captive thumbscrews on the SCB.
- 9 Grip the thumbscrews and pull outward to slide the SCB out of the library.
- 10 Remove the new SCB from its packaging. Wrap the old SCB in the antistatic bag that the replacement SCB was wrapped in.
- 11 Position the new SCB for installation as follows: The board components face up. The flat part of the board faces down. The thumbscrews are on the upper side of the SCB back plate (see [Figure 70](#) on page 281).
- 12 Install the new SCB by pushing the SCB into the slot until it stops. It should slide smoothly and easily. When it reaches the end of its travel, press firmly on the back panel of the SCB to “snap” it into place.
- 13 Tighten the two thumbscrews finger tight.
- 14 Connect the Ethernet cable to the LEFT Ethernet port on the SCB (as viewed from the back of the library; see [Figure 70](#) on page 281).

Figure 70 Ethernet Port Locations on the SCB



15 Continue to [Installing Library Firmware](#) on page 281.

## Installing Library Firmware

- 1 Connect the power cords to the power supplies on the back of the library. Make sure that each power supply is plugged in to a grounded, AC outlet.
- 2 Turn **ON** the library by pressing the power button on the front panel.

The LED on the SCB should illuminate green.

The green power LED on the library front panel above the power button illuminates, and the operator panel screen turns on. The library goes through a connection and initialization sequence that takes up to 60 seconds.

3 When initialization is complete, the **Library Installation** screen displays on the operator panel, displaying the text, "The library needs to have its IP Address configured." The purpose of this screen is to set the IP address so you can access the library via the Web client and download firmware. (After you have loaded firmware, you can change or reconfigure IP addresses if needed.)

4 Press **Next**.

The screen displays the text, "Current protocol: IPv4. Set protocol to IPv6?"

5 Select **Yes** or **No**.

- If you select **Yes**, the library supplies a stateless IPv6 address and displays it, along with other network settings, on two screens. Use the **Next** and **Back** buttons to view the screens. You can only change these settings via the Web client.
- If you select **No**, you are asked if you want to use DHCP.
  - If you select **Yes**, the library assigns IPv4 address and displays the information on the screen.
  - If you select **No**, use the **Up** and **Down** buttons to enter the IP address, mask, and gateway. Set the numeric value for each segment of the address, then press the **Right** button to go to the next segment. See [Navigating and Editing on the Operator Panel](#) on page 27 for more information on editing the IP address. When finished, press **Apply**.

6 Take note of the IP address.

7 Download the latest library firmware to a known location on your computer. Library firmware is available at <http://www.quantum.com>. Navigate to the appropriate firmware version and download the firmware image file.

8 Open an Internet session and enter the library IP address listed on the operator panel into the Web browser.

The Web client displays a screen instructing you to select the firmware image you want to load on the library.

9 Click **Browse** and select the firmware image you downloaded to install on the library.

- 10 Click **OK**, then click **OK** again to agree to restart the library.

The Web client displays the following message:

Decoding installation bundle...done.  
Validating bundle...good.  
Installing firmware...library will reboot when complete.

- 11 Go to the operator panel and wait until the Setup Wizard displays on the screen. The Setup Wizard screen may take up to 20 minutes to appear.
- 12 Continue as follows:
  - If you have saved a library configuration that you want to restore on the library, go to: [Restoring the Library Configuration](#) on page 283.
  - If you do NOT have a saved library configuration to restore on the library, go to: [Manually Reconfiguring the Library](#) on page 284.

---

## Restoring the Library Configuration

---

Follow the instructions in this section if you have a saved library configuration that you want to reinstall on the library.

- 1 On the operator panel, press **Cancel** to exit the Setup Wizard.
- 2 Take note of the library's IP address (on the operator panel, select **Reports > Network Settings**).
- 3 Access the Web client using the IP address and log in using the default user name and password:
  - User name: **admin**
  - Password: **password**

---

**Note:** Once you restore the configuration, all your former user names and passwords are restored.

---

- 4 Restore the configuration using the Web client as follows:
  - a Select **Tools > Save/Restore Configuration**.
  - b Select **Restore System Configuration**.
  - c Click **Browse**. Navigate to the saved configuration and click **Open**.

d Click **Apply**

e Click **OK**.

---

**Note:** Restoring the configuration does NOT restore your network settings.

---

- 5 Check the library's date, time, and time zone settings and reconfigure if necessary. From the Web client, select **Setup > Date & Time**.
- 6 If you changed the IP address from what it was originally, update host and other applications that access the library.
- 7 Save the library configuration. From the Web client, select **Tools > Save/Restore Configuration**. Select **Save Configuration** and click **Apply**. Save the configuration to a known location.
- 8 It is recommended that you run the Installation and Verification Test (IVT). From the operator panel, select **Tools > IVT** and follow the instructions. The IVT takes about 30 minutes. If any problems are detected, the library issues a diagnostic ticket.
- 9 Package the old SCB in the packaging that shipped with the new SCB and send the old SCB back to Quantum using the included return shipping label.

---

## Manually Reconfiguring the Library

---

Follow the instructions in this section if you do not have a saved library configuration.

- 1 If you had licenses installed on your library, have the license keys handy so you can install them on the library. If you no longer have them, you can obtain them at <http://www.quantum.com/licensekeys>, or from Quantum Support.
- 2 When the firmware update is complete, the Setup Wizard displays on the operator panel screen. The Setup Wizard helps you configure the date, time, IP address, IPv6 enable/disable, licenses, partitions, I/E slots, and cleaning slots.



- 3 Complete the Setup Wizard on the operator panel. If you make a mistake or do not complete all the screens, you can change the configuration later using the operator panel or Web client **Setup** menus.

---

**Note:** You cannot update the host name or time zone on the operator panel. If the displayed host name or time zone is incorrect, change it later using the Web client (see [Step 8](#) on page 285).

---

- 4 Take note of the library's IP address (on the operator panel, select **Reports > Network Settings**).
- 5 Access the Web client using the IP address and log in using the default user name and password.
  -
- 6 Optionally, install tape drive firmware for autoleveling. The library firmware contains baseline tape drive firmware for autoleveling. Verify your tape drive firmware is at the level you expect. If not:
  - a Upload the tape drive firmware you want to use. From the Web client, select **Tools > Drive Operations > Upload/remove tape drive firmware for autoleveling**.
  - b Unload all tape cartridges from the tape drives on which you want to autolevel firmware.
  - c Initiate autoleveling by doing one of the following:
    - Restart the library (from the operator panel, select **Actions > Shutdown > Restart Library**).
    - Restart all the tape drives you want to autolevel, as follows: From the Web client, select **Tools > Diagnostics**. Confirm you want to take the partitions offline. Select **Drives > Drive Tests > Drive Reset**. Select the applicable partitions and tape drives, then click **Apply**, then click **OK**.
- 7 If you changed the IP address from what it was originally, update host and other applications that access the library.
- 8 Update the library name, time zone, and any other configuration settings, if required, using the Web client **Setup** menus.

- 9 If you are connecting to a Scalar Key Manager (SKM), take note that TLS certificates will need to be loaded onto the library. See [Installing TLS Certificates on the Library](#) on page 186 for instructions.
- 10 Save the library configuration. From the Web client, select **Tools > Save/Restore Configuration**. Select **Save Configuration** and click **Apply**. Save the configuration to a known location.
- 11 To ensure the library is fully functional with the new SCB installation and configuration selections, we recommend you run the Installation and Verification Test (IVT). From the operator panel, select **Tools > IVT** and follow the instructions. The IVT takes about 30 minutes. If any problems are detected, the library issues a diagnostic ticket.
- 12 Package the old SCB in the packaging that shipped with the new SCB and send the old SCB back to Quantum using the included return shipping label.

---

## Removing and Replacing a Tape Drive

It is recommended that you remove and install tape drives with library power **ON** — it is faster and keeps non-affected tape drives and partitions active.

The tape drive always resides in a drive sled, and together they are effectively one unit. If you order a new or replacement tape drive, it will already be installed in a sled.

---

**Caution:** Do not remove the tape drive from the drive sled.

---

---

**Note:** For multiple tape drive installs in which you are changing control paths, install and verify the tape drives one at a time, rather than all at once.

---

## Preparing Partitions and Control Paths

Depending on the types of tape drives you are removing and installing, you may need to reconfigure library partitions or change the control path before you remove and replace the tape drive. There are four different types of installation, described in the table below. Follow the instructions in the table before proceeding to the remove/install procedures.

Type of Installation	Instructions
Adding a new tape drive	No special instructions.
Replacing a tape drive that is not assigned to a partition	No special instructions.
Replacing tape drive that is assigned to a partition with a tape drive that has the <b>same</b> : <ul style="list-style-type: none"> <li>• interface type (Fibre Channel or SAS), <i>and</i></li> <li>• form factor (half-height or full-height), <i>and</i></li> <li>• vendor</li> </ul>	<p>Install the replacement tape drive in the same slot as the removed tape drive.</p> <p>There are no special instructions unless the tape drive you are replacing is the control path in a partition with multiple tape drives, and you want the partition to remain online during the replacement procedure. In this case, select another tape drive as the control path. From the Web client, use the <b>Setup &gt; Control Path</b> menu path.</p>
Replacing a tape drive that is assigned to a partition with a tape drive that has a <b>different</b> : <ul style="list-style-type: none"> <li>• interface type (Fibre Channel or SAS), <i>or</i></li> <li>• form factor (half-height or full-height), <i>or</i></li> <li>• vendor</li> </ul>	<ul style="list-style-type: none"> <li>• If the partition contains only one tape drive, delete the partition before removing the tape drive and then re-create the partition once you install the replacement tape drive.</li> <li>• If the partition contains multiple tape drives and the tape drive you want to replace is <b>not</b> the control path, delete the tape drive from the partition.</li> <li>• If the partition contains multiple tape drives and the tape drive you want to replace <b>is the control path</b>, select another tape drive as the control path. Then delete the tape drive you want to replace from the partition.</li> </ul> <p>To delete tape drives from partitions, select <b>Setup &gt; Partitions</b> from the Web client.</p> <p>To modify the control path, select <b>Setup &gt; Control Path</b> from the Web client.</p>

---

## Removing a Tape Drive from the Library

---

---

**Caution:** Do not remove a tape drive that is currently performing an operation.

---

- 1 Make sure the tape drive you want to remove is empty of media. From the operator panel, select **Actions > Tape Drive > Unload**.
- 2 Take the tape drive you want to remove offline. From the operator panel, select **Actions > Tape Drive > Change Mode**. Select the tape drive and press **Modify**. Press the **Down** button to select **Offline**, then press **Apply**.
- 3 Disconnect the cable from the back of the tape drive.
- 4 Unscrew the captive thumbscrews securing the drive sled to the back of the library. Half-height tape drives have two thumbscrews. Full-height tape drives have four thumbscrews.
- 5 Using the handle, pull the drive sled out of the library. It should slide out smoothly and easily.
- 6 Wait at least 10 seconds before installing a replacement tape drive to allow the library to recognize that the tape drive has been removed.
- 7 Install a replacement tape drive following the instructions below. If any empty slots remain, install a filler plate in the empty slot.
- 8 If you are returning the tape drive to Quantum, wrap it in the antistatic bag in which the replacement tape drive is wrapped, then finish packing it in the same packaging materials from the replacement tape drive. Ship the tape drive to Quantum using the RMA materials included in the packaging.

---

## Installing a Tape Drive

---

### Tape Drive Slot Location Considerations

Tape drives can only fit in certain slots, as described below and illustrated in [Figure 71](#). Slots are numbered starting from the bottom and moving up.

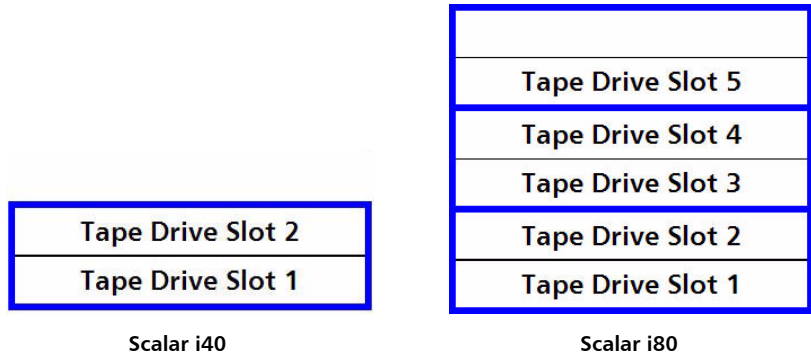
- **Scalar i40:** Half-height tape drives can be installed in slots 1 and 2. A full-height tape drive can be installed in slot 1.

- **Scalar i80:** Half-height tape drives can be installed in slots 1, 2, 3, 4, and 5. Full-height tape drives can be installed in slots 1, 3, and 5. The extra space where slot 6 would be cannot hold a half-height tape drive, but will accommodate a full-height tape drive installed in slot 5.

If possible, it is recommended to start installing the tape drives at the bottom slot and work up, without leaving spaces between.

If you are replacing an existing tape drive with a tape drive of the same interface type, form factor, and vendor, place the replacement tape drive in the same slot as the removed tape drive.

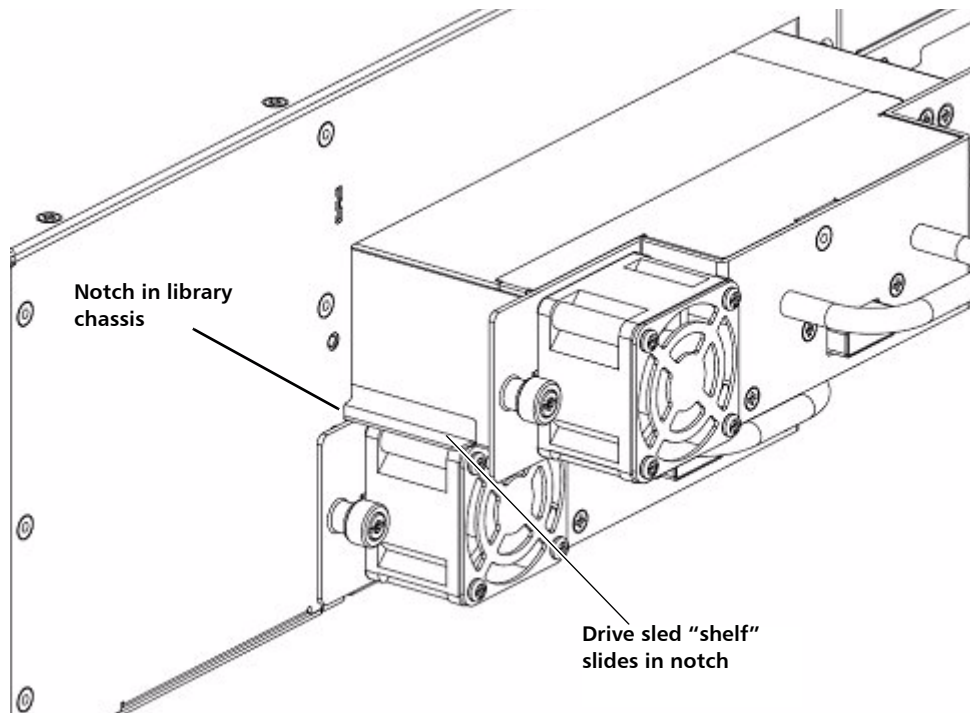
Figure 71 Acceptable Installation Locations for Full-Height Tape Drives



## Installation Procedure

- 1 If you need to remove one or more filler plates, unscrew the two thumbscrews securing the filler plate to the back of the library. Holding the thumbscrews, pull the filler plate gently out of the library. Save the filler plate in case you need to use it in the future.
- 2 Insert the tape drive into the drive slot. The “shelf” on the bottom of the drive sled fits into the notch in the library chassis and slides on the plastic guide rails (see [Figure 72](#) on page 290). The tape drive must be level to slide in smoothly. At the very end of the slide, you will feel a slight “click” as the tape drive sled connector connects into its mating connector in the library chassis.

Figure 72 Installing a Tape Drive



- 3 Tighten the tape drive's captive thumbscrews finger tight to secure the tape drive to the library chassis.

The tape drive LED illuminates red for up to 30 seconds. Then the tape drive fan starts and the LED turns amber, indicating the tape drive is offline. If this is a new installation (not a replacement), the tape drive will come online automatically.

- 4 Connect the tape drive cable from the tape drive to the host.
- 5 If the firmware on the newly installed tape drive is different from the standard configured on the library, the library will automatically autolevel the new tape drive's firmware upon installation (for more information, see [Updating and Autoleveling Tape Drive Firmware](#) on page 303).

Autoleveling takes about 7 minutes. A message displays on the operator panel indicating autoleveling is taking place.

If autoleveling is not required, the tape drive takes about 2 minutes to come ready.

- 6 If needed, add the new tape drive to an existing partition or create a new partition for it. From the Web client, select **Setup > Partitions** and complete the necessary screens.
- 7 Bring the tape drive online, if it is not online already. From the operator panel, select **Actions > Tape Drive > Change Mode**. Select the tape drive you want to bring online and press **Modify**. Use the **Up** and **Down** buttons to change the mode to **Online**, then press **Apply**.  
The tape drive LED turns green.
- 8 Verify the installation by reviewing the library configuration report on the Web client (**Reports > Library Configuration**). Make sure that the new drive is online, in the correct partition, and has the control path status that you want. You may need to refresh your Internet browser.
- 9 Verify that the host computer and backup applications can see the new tape drive configuration correctly.
- 10 If any empty slots remain, install a filler plate in the empty slot.

---

---

**Caution:** Filler plates are required to maintain proper library cooling. Do not run the library with uncovered slots.

---

---

- 11 Run the tape drive diagnostic test on the newly installed tape drive to be sure it is functioning correctly.
  - a Install a scratch tape in the top I/E station slot.
  - b If manual cartridge assignment is enabled, assign the scratch tape to the System partition.
  - c From the operator panel, select **Tools > Diagnostics**.
  - d Continue through the next few screens to run the tape drive test on the replaced tape drive.

If a problem is found during testing, you receive a diagnostic ticket. See [Running the IVT Diagnostic Subtests Individually – Robotics, Tape Drive, and Magazine Tests](#) on page 327 for more information.
- 12 Save the library configuration (see [Saving the Library Configuration](#) on page 107).

## Packaging the Library for Moving or Shipping

### Packaging Kit Contents

- Shipping carton
- Top foam
- Bottom foam
- Anti-static wrapping
- (4) M5 Thumbscrews to restrain Y-tray
- Bottom tray (Scalar i80 only)
- Pallet (Scalar i80 only)
- (2) Cardboard “corner boards” (Scalar i80 only)
- (2) Straps and buckles for securing packaging to pallet (Scalar i80 only)

### Creating a Backup Map of Cartridge Locations

You must remove all the tape cartridges before shipping the library. If you want to maintain the same partitions and magazine slot assignments in your new location as you are using currently, you will want to reinstall your tape cartridges in the same slots they are in now. The library configuration report provides a convenient “map” of your slot assignments. If you print or copy this map, you will be able to easily install your cartridges later.

1 On the Web client, select **Reports > Library Configuration**.

2 Click the **Show Barcodes** button.

The screen displays a map of the library showing the partitions and the location of each cartridge, by barcode.

3 Click the “print” icon in the upper right corner to print the report.



Alternatively, take a screen capture of the report and save or print it, or copy the map by hand.



---

## Procedure

---

- 1 As a precautionary measure, save the library configuration: From the Web client, select **Tools > Save/Restore Configuration**. Select **Save System Configuration** and click **Apply**. When prompted, save the file to a known location on your computer.
- 2 Stop all library and host operations.
- 3 Remove the magazines from the library:
  - a From the operator panel, select **Actions > Magazine**.
  - b Use the **Up** and **Down** buttons to select the magazine you want to remove and press **Release**.
  - c Wait for the operator panel to display the message: "Magazine is now unlocked. Waiting for the magazine to be moved to the expected position."
  - d Pull the magazine bezel out and remove the magazine from the library. If you do not remove the magazine within 30 seconds, the magazine locks again.
  - e Repeat for all magazines in the library.

---

**Caution:** Do not put your hands or any other objects into the magazine openings while library power is on.

---

- 4 Remove all the tape cartridges from the magazines.
- 5 Shut down the library by selecting **Actions > Shutdown** from the operator panel. Wait for the operator panel to prompt you to turn off library power.
- 6 Turn **OFF** the library by pressing the power button on the front panel. Wait for the LED on the SCB to turn off.
- 7 Disconnect the power supply cord, the Ethernet cable, and all tape drive cables from the back of the library. If you have multiple tape drives, label the cables so you can reconnect them to the correct ones later.

- 8 If the library is in a rack or desktop kit, remove it.
  - **To remove the library from a rack:**
    - a Remove all the tape drives from the library. Label tape drives so you know what order to reinstall them later. They must be reinstalled in the same slots as they were previously. Unscrew the thumbscrews and pull the tape drive handle to remove the drive from the library.
    - b Unscrew the captive thumbscrews on the front of the library that secure the library to the rack, then slide the library out of the rack. Place the library on a flat, stable surface.

---

**WARNING:** Two people are required to safely remove the library from the rack.

---

- **To remove the library from a desktop kit,** remove the two screws in the decorative top cover. Remove the decorative top cover by sliding it toward the back. Loosen the captive thumbscrews on the library chassis that are attached to the side panels of the desktop kit. Slide the side panels one inch toward the rear of the library, then pull the side panels off.
- 9 Make sure the Y-tray is sitting on the floor of the library as follows: Look inside the library through one of the magazine openings. If the Y-tray is not sitting on the floor of the library, reach inside and gently press down on one of the Y-tray's metal side rods until the Y-tray starts moving. It should drift down to rest on the floor of the library.
  - 10 Reinstall the empty magazines in the library by pushing them in until they stop.
  - 11 If you removed the tape drives earlier, reinstall them in their proper slots. Push them carefully into their slots and tighten the captive thumbscrews.
  - 12 Restrain the Y-tray as follows (see [Figure 73](#) on page 295):
    - a Turn the library carefully on its side (either the left or right side). Make sure the front end of the library (the "rack ear") overhangs the edge of the table so that the library lies flat.

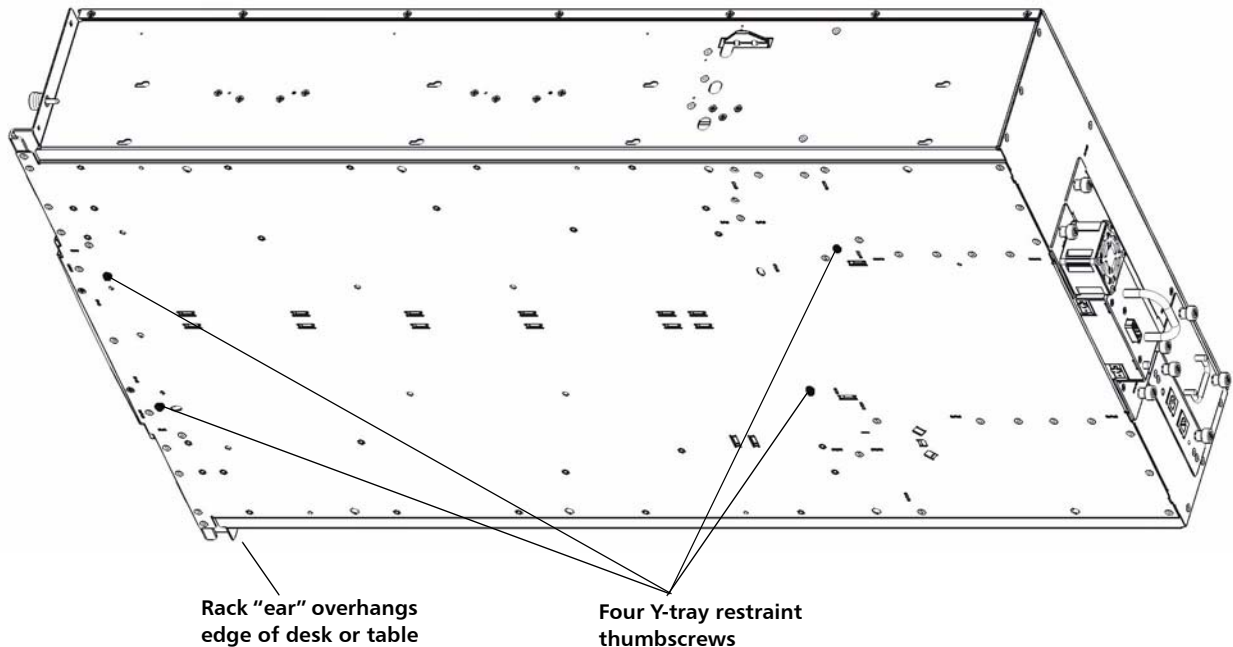
---

**Caution:** Do not turn the library upside down. Do not turn the library more than 90 degrees from upright.

---

- b Install four thumbscrews into the floor of the library in the locations shown in [Figure 73](#) on page 295. They will screw through the Y-tray and hold it in place on the floor of the library.

Figure 73 Restraining the Y-tray



- c Do NOT turn the library back to an upright position at this point. Leave it on its side until you place it in the box.

---

---

**Caution:** If you place the library upright with the Y-tray restraint thumbscrews installed, you could damage the chassis or the Y-tray.

---

---

- 13 Wrap the library in the anti-static wrapping provided in the packaging kit.

---

**WARNING:** Two people are required to safely lift the library.

---

- 14 Place the library in the packaging as shown in [Figure 74](#) and [Figure 75](#).

---

Figure 74 Scalar i40 Packaging

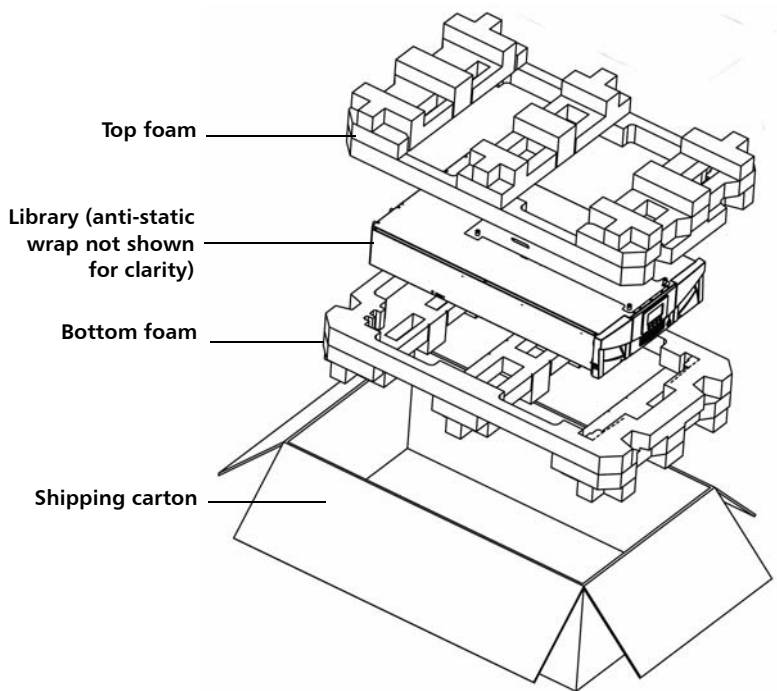
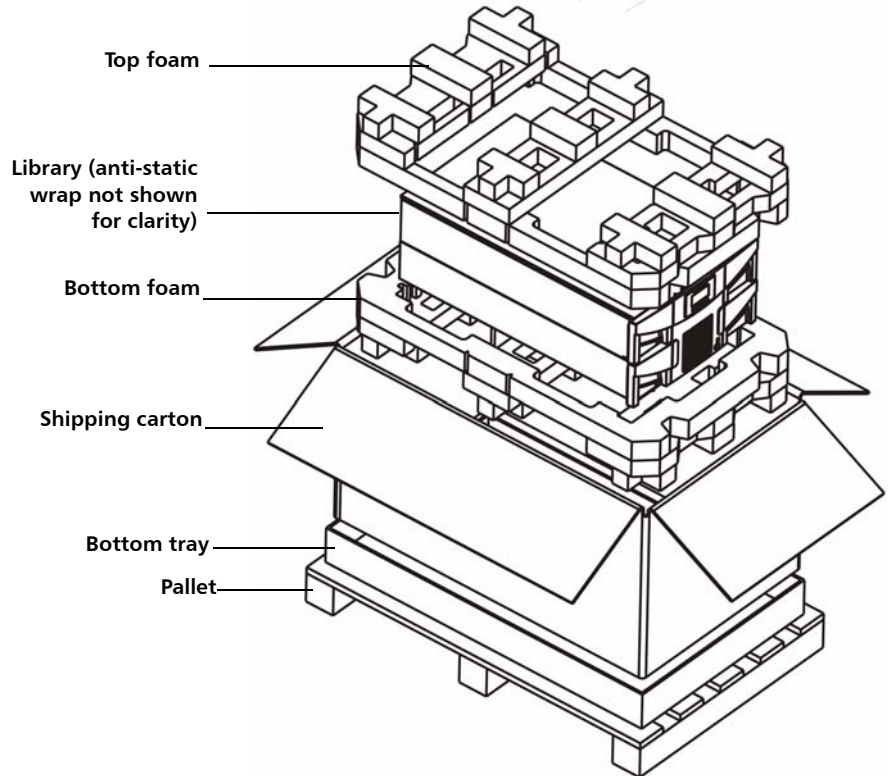


Figure 75 Scalar i80 Packaging



**Scalar i80 only:** Place two corner boards on the long edges on top of the shipping carton. Strap the box to the pallet, then wrap the entire assembly in stretch-film prior to shipping.

---

**Caution:** When unpacking the library in its new location, lift it out of the packaging and immediately place it on its side to remove the four thumbscrews securing the Y-tray to the floor of the library. Do not place it upright until you have removed the four thumbscrews, or you could damage the chassis or the Y-tray. When placing the library on its side, do not set it on the “rack ear” or the magazine handle, or you could damage them.

---

---

## Replacing the Y-tray with Robot

Y-tray with Robot replacement is a service-only procedure. If the Y-tray fails, you will need to call Quantum Support for a replacement.



## Chapter 10

# Updating Firmware

---

This chapter covers updating library and tape drive firmware, including:

- [Updating Library Firmware](#)
- [Updating and Autoleveling Tape Drive Firmware](#)
- [About Tape Drive Firmware Autoleveling](#)
- [Uploading Tape Drive Firmware Used in Autoleveling](#)
- [Deleting Tape Drive Firmware Used in Autoleveling](#)
- [Initiating Tape Drive Firmware Autoleveling](#)

---

## Updating Library Firmware

The library firmware update operation allows you to update library firmware using the Web client. With the library firmware update operation, you can upgrade firmware to a later version or downgrade firmware to an earlier version. Upgrading library firmware can take up to 30 minutes.

Before updating library firmware, it is recommended that you capture the library snapshot. The library snapshot file saves status information and trace logs for library components. This information helps technical support troubleshoot issues that might occur with the firmware upgrade. For more information, see [Capturing Snapshots of Library Information](#) on page 317.

In addition, it is recommended that you save the library configuration before upgrading the library (in case the upgrade fails) and again after the upgrade successfully completes. For more information, see [Saving the Library Configuration](#) on page 107.

When you upgrade or downgrade library firmware, the library also autolevels tape drive firmware, if needed. Autoleveling will not occur if a tape drive has a cartridge loaded in it. Make sure to unload all tape drives before updating library firmware. See [Updating and Autoleveling Tape Drive Firmware](#) on page 303.

The library automatically restarts after the firmware update 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.

---

---

**Caution:** After the update process starts, you must wait until it completes. Do not attempt to interrupt the process in any way, and do not power cycle the library. Loss of data or library operability could occur.

---

---

---

**Note:** If you downgrade library firmware to an earlier version using the firmware upgrade process, library configuration settings will be reset to the factory defaults (see [Resetting Factory Defaults](#) on page 333). You must manually reconfigure your library's settings. You can also downgrade library firmware by restoring a configuration file that contains the version of firmware to which you want to downgrade (see [Restoring the Library Configuration](#) on page 108).

After downgrading, network settings are not reset, and licenses remain—as long as the downgraded firmware version supports that licensed feature

---

You can only update firmware from the Web client.



## Web Client

- 1 Log into your library to view the latest firmware version available. Click **Tools > Update Library Firmware**.

If you are connected to the Internet, the screen displays the firmware currently loaded on your library and the latest available firmware.

Figure 76 Tools - Update Library Firmware Screen

Setup Operations Tools Drives Robotics Reports User: service [S]

### Tools - Update Library Firmware

Update your library firmware from the Quantum Support web site or browse for a specific firmware file:

Note: The library will be rebooted after the firmware file has been uploaded.  
If you downgrade library firmware to an earlier version using the firmware upgrade process, library configuration settings will be reset to the factory defaults, in such case you must manually reconfigure your library settings.

The firmware was last updated on: 04/27/2011 09:22 MDT  
Currently loaded firmware version on the library: 130G.TS016  
Latest available firmware version from the Quantum Support web site: 130G.TS017

Update library firmware with the version from the Quantum Support web site:

Update library firmware with version in this file:

**Note:** You can also view a listing of the latest version of library firmware on the following Web site:  
<http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI40/Index.aspx>  
and click the **Firmware** tab.

View your library's current firmware version by selecting **Reports > About Library** from the operator panel, or **Reports > About > Scalar i40/i80** from the Web client.

- 2 Unload tape cartridges from all tape drives installed in the library.

- 3 Capture a library snapshot (see [Capturing Snapshots of Library Information](#) on page 317).
- 4 Save the library configuration (see [Saving the Library Configuration](#) on page 107).
- 5 If the library has an internet connection, use the Web client to update the library to the latest firmware. If the library does not have an internet connection, use a Web browser to browse for a specific file.

#### Update using the Web Client

- a From the Web client, return to **Tools > Update Library Firmware**.

The Tools - Update Library Firmware screen displays.

- b Click **Read EULA** to read and click **Accept** to accept the End User License Agreement.
- c Click the check box next to **Update library firmware with the version from the Quantum Support Web site**.

---

**Note:** If a newer version is already installed on your library, you will receive a warning message.

---

- d Go to [Step 6](#).

#### Browse for a Specific File

- a Using a Web browser connected to the internet go to <http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI40/Index.aspx> and click the **Firmware** tab.
- b Download the library firmware to a known location on your computer.
- c From the Web client, return to **Tools > Update Library Firmware**.

The Tools - Update Library Firmware screen displays.

- d Click **Browse**.
- e Locate the library firmware file and click **Open**.

f Go to [Step 6](#).

6 Click **Apply**.

A confirmation dialog box displays asking you to confirm that you want to update the library firmware and reboot the library.

7 Click **OK** to continue with the library firmware update operation.

The Progress Window displays. The Progress Window contains information on the action, elapsed time, and status of the requested operation. The Progress Window closes automatically and the library shuts down and then reboots. You will need to log back into the library once it has finished rebooting. Wait for the library to completely reboot before logging back in to the library. The reboot takes several minutes.

If **Failure** appears in the Progress Window, the operation failed. The library will automatically reload the previous version of library firmware.

8 Clear the Web browser cache before logging in to the library. See your Web browser's documentation for instructions on how to clear the cache.

9 Log in to the library.

---

**Note:** If the library is still in the process of restarting, the Web browser may display an error page or message when you try to access or log in to the Web client.

---

10 Verify the library firmware installed successfully. Go to **Tools > Update Library Firmware** or view the About Scalar i40/i80 report (on the Web client) by selecting **Reports > About > Scalar i40/i80**).

11 Save the library configuration again (see [Saving the Library Configuration](#) on page 107).

## Updating and Autoleveling Tape Drive Firmware

The library firmware bundle file contains baseline tape drive firmware image that Quantum has validated. Tape drive firmware is installed at the same time as library firmware. (You can also install upgrades or patches separately, which is described in the sections below.)

In addition, the library is equipped with a tape drive autoleveling feature, that automatically updates firmware on all installed tape drives, keeping all tape drives of the same type at the same firmware level.

### About Tape Drive Firmware Autoleveling

Autoleveling occurs only at specific times:

- Tape drive firmware is verified whenever a tape drive is added, replaced, or power cycled, or when the library is rebooted. If the firmware installed on the tape drive does not match the tape drive firmware installed on the library, the tape drive firmware is autoleveled.
- Tape drive firmware is autoleveled when library firmware is updated (see [Updating Library Firmware](#) on page 299).

Details about Autoleveling include:

- The autoleveling feature is always enabled.
- The library firmware contains baseline tape drive firmware image that Quantum has validated. You cannot delete any of the baseline tape drive firmware images. You may, however, upload separate tape drive firmware images to use instead (such as a patch or upgrade provided by Quantum; see [Uploading Tape Drive Firmware Used in Autoleveling](#) on page 306). If you upload a patch, the patch will display instead of the baseline image, although the baseline image will remain, hidden. Tape drives will be autoleveled to the patch. If you delete the patch, then baseline image will reappear on the screen and the tape drives will autolevel to the baseline image (see [Deleting Tape Drive Firmware Used in Autoleveling](#) on page 308).

- If you upgrade library firmware, the baseline tape drive firmware for that version of library firmware will overwrite the existing baseline tape drive firmware images. If you did not previously upload a patch, all the tape drives will be autoleveled to the new baseline. If you previously uploaded a patch, the patch remains and tape drive firmware will remain autoleveled to the patch. You will need to delete the patch in order to have the tape drives autoleveled to the new baseline (see [Deleting Tape Drive Firmware Used in Autoleveling](#) on page 308).
- If you downgrade library firmware, the baseline tape drive firmware for that version of library firmware will overwrite the existing baseline tape drive firmware images as well as any patches you may have uploaded prior to the downgrade, and all tape drives will be autoleveled to the new baseline. If you want to continue to use the patch or a different version of tape drive firmware, you will need to upload it again. Contact Quantum Support if you need help obtaining firmware (see [Getting More Information or Help](#) on page xxvii).
- Autoleveling will not occur if a tape drive has a cartridge loaded in it. Make sure to unload tape cartridges from all tape drives before loading new firmware for autoleveling, or before upgrading library firmware.
- Autoleveling occurs after the completes its initialization. This means it is possible for a host to see the medium changer initially, but when the autoleveling starts on the drives it is likely the medium changer will disappear again. Wait until autoleveling completes before starting backup applications. (The operator panel displays a message indicating autoleveling is taking place. Wait until this message disappears before starting backup applications.)
- If you reset factory defaults, any tape drive firmware images you manually uploaded will be deleted (see [Resetting Factory Defaults](#) on page 333).

---

## Uploading Tape Drive Firmware Used in Autoleveling

---

Tape drive firmware is bundled with the library firmware and is automatically installed and autoleveled on your tape drives when you install library firmware.

In some cases, a tape drive firmware upgrade or patch may be available from Quantum Support outside of the normal library firmware release cycle. The instructions in this section explain how to install such an upgrade or patch.

You can also use these instructions to install down-rev tape drive firmware. If you wish to do this, contact Quantum Support for the firmware image files.

---

---

**Caution:** Only install tape drive firmware image files that have been tested and qualified by Quantum.

---

---

It is not necessary to delete an existing version of firmware before uploading a new version. The new version overwrites the existing version.

---

**Note:** Uploading tape drive firmware for autoleveling only uploads the firmware to the library in preparation for autoleveling. It does not initiate autoleveling or install firmware on the tape drive. To initiate autoleveling, see [Initiating Tape Drive Firmware Autoleveling](#) on page 310.

---

You can only upload tape drive firmware on the Web client.

### Web Client

- 1 Check the Quantum Web site to see if you are running the current level of firmware (go to <http://www.quantum.com/ServiceandSupport/SoftwareandDocumentationDownloads/SI40/Index.aspx> and click the **Firmware** tab).
- 2 If needed, obtain the firmware download file from Quantum Support and place it in a known location on your computer.
- 3 Verify with the release notes or Quantum Support that you are installing the correct version of tape drive firmware for your library. For support contact information, see [Getting More Information or Help](#) on page xxvii.

**4 Select Tools > Drive Operations.**

The **Tools - Drive Operations** screen displays.

**5 Select Upload/remove tape drive firmware for autoleveling and click Next.**

The **Tape Drive Firmware Autolevel** screen displays. The screen lists the vendor, type, interface type, form factor, and firmware revision number for all tape drives that the library supports, whether or not they are installed in the library.

**6 Click Upload.**

The **Upload Tape Drive Images** screen displays. The screen lists the vendor, type, form factor, and interface type of all tape drives installed in the library. You can only upload tape drive images for the listed tape drives.

**7 Click Browse.**

**8 Locate the tape drive firmware image file and click Open.**

**9 Click Apply.** The Progress Window displays. The Progress Window contains information on the action, elapsed time, and status of the requested operation. Do one of the following:

- If **Complete** appears in the Progress Window, the tape drive firmware upload completed. Check to see if a diagnostic ticket was generated for this operation. For information on diagnostic tickets, see [About Diagnostic Tickets](#) on page 312. If no diagnostic ticket(s) exists, continue to next step.
- If **Failure** appears in the Progress Window, the tape drive firmware update was not successful.

**10 To initiate autoleveling, see [Initiating Tape Drive Firmware Autoleveling](#) on page 310.**

---

## Deleting Tape Drive Firmware Used in Autoleveling

---

If you installed a tape drive firmware image to override the library's baseline image used for autoleveling, you can delete it. You cannot delete the library's baseline tape drive firmware images. For more information, see [About Tape Drive Firmware Autoleveling](#) on page 305.

---

**Note:** Deleting tape drive firmware for autoleveling only deletes the firmware and makes the library's baseline tape drive firmware available for autoleveling. It does not initiate autoleveling or install firmware on the tape drives. To initiate autoleveling, see [Initiating Tape Drive Firmware Autoleveling](#) on page 310.

---

You can only delete tape drive firmware on the Web client.

## Web Client

**1 Select Tools > Drive Operations.**

The **Tools - Drive Operations** screen displays.

**2 Select Upload/remove tape drive firmware for autoleveling and click Next.**

The **Tape Drive Firmware Autolevel** screen displays. The screen lists the vendor, type, interface type, form factor, and firmware revision number for all tape drives that the library supports, whether or not they are installed in the library.

**3 Select the tape drive firmware you want to delete.**

**4 Click Delete.**

The Progress Window displays. The Progress Window contains information on the action, elapsed time, and status of the requested operation. Do one of the following:

- If **Success** appears in the Progress Window, the tape drive firmware was successfully deleted. The library's default baseline tape drive firmware will now be used for autoleveling.
- If **Failure** appears in the Progress Window, the tape drive firmware update was not successfully deleted.

**5 To initiate autoleveling, see [Initiating Tape Drive Firmware Autoleveling](#) on page 310.**



## Initiating Tape Drive Firmware Autoleveling

Autoleveling occurs automatically at specific times (whenever a tape drive is added, replaced, or power cycled; when the library is rebooted; or when you update library firmware). If you upload or remove tape drive firmware separately from library firmware (such as a Quantum-provided upgrade or patch) and want to autolevel the tape drives immediately, follow these steps:

- 1 Unload tape cartridges from all tape drives you want to autolevel.
- 2 Stop all host commands to the tape drives you want to autolevel.
- 3 Initiate autoleveling by performing one of the following actions:
  - **Reset (power cycle) the tape drives** on which you want to install firmware. This autolevels only the tape drives you reset. If you reset all tape drives at once, each tape drive is reset sequentially, causing the autoleveling to occur one tape drive at a time. If you reset each tape drive individually, you must wait for the autolevel to occur before proceeding to the next tape drive. It takes about 7 minutes to autolevel each tape drive. For instructions, see [Resetting a Tape Drive](#) on page 331.
  - **Restart the library.** This verifies and autolevels all tape drives simultaneously. This process takes about 7 minutes for the autolevel, plus the time it normally takes the library to reboot. From the Web client, select **Operations > System Shutdown**. Select **Restart** and click **Apply**. See [Restarting the Library](#) on page 142 for more information.

The operator panel displays a message indicating autoleveling is taking place. If the install or autolevel fails, you receive a diagnostic ticket.

- 4 Wait until autoleveling is complete before resuming host commands. To make sure autoleveling is complete, check the system information report to see if the tape drive firmware is installed on all intended tape drives. From the Web client, select **Reports > System Information**.

Chapter 10: Updating Firmware  
Updating and Autoleveling Tape Drive Firmware



## Chapter 11

# Troubleshooting

---

The Scalar i40 and Scalar i80 libraries include advanced system monitoring and alerting mechanisms that inform you of library status and issues. The library provides you with status information about various library subsystems and components. It also notifies you of issues it detects and guides you through diagnosing and correcting issues before problems interfere with backups.

This chapter covers:

- [About Diagnostic Tickets](#)
- [Capturing Snapshots of Library Information](#)
- [Troubleshooting Library “Not Ready” Messages](#)
- [Retrieving Tape Drive Logs](#)
- [Interpreting LEDs](#)
- [Running the Installation and Verification Test \(IVT\)](#)
- [Running the IVT Diagnostic Subtests Individually – Robotics, Tape Drive, and Magazine Tests](#)
- [Running the Random Move Test](#)
- [Performing Library Diagnostics](#)
- [Resetting Factory Defaults](#)

## About Diagnostic Tickets

The 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 diagnostic ticket that identifies the component that is likely causing the problem. If the problem is not severe, the library continues to provide full functionality to all unaffected partitions.

The tickets are assigned one of three priority levels:

- **Urgent** — The highest level of priority. A ticket with urgent priority 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 highly unreliable. This level of priority is conveying a critical issue.
- **High** — The middle level of priority. A ticket with high priority indicates that a condition exists within the library that impacts system performance, redundancy, or just 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. This level of priority is conveying a warning message.
- **Low** — The lowest level of priority. A ticket with low priority indicates that an abnormal condition existed within the library that warrants investigation and correction but the nature of the condition may have little or no effect on operations. This level of priority is conveying an informational message.

The library has a number of visual cues to alert you that one or more diagnostic tickets exist:

- The library's ticket indicator LED turns on to indicate that at least one ticket exists (see [Front Panel LEDs](#) on page 321).
- The operator panel displays a health status icon (see [Health status](#) on page 26 for description).
- The Web client displays a subsystem status icon (see [Subsystem Status](#) on page 32).

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 Quantum Support. Only qualified service technicians can service FRUs.

---

## Viewing, Closing, and Resolving Diagnostic Tickets

---

The initial status of all diagnostic tickets is Unopened. Once you select the **Resolve** button, the ticket status changes to Opened. When you close 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.

You can view and close diagnostic tickets on both the operator panel and the Web client, but only the Web client provides a complete description of the event and guides you through a series of steps to resolve the issue. It is recommended that you use the Web client to view and resolve all your diagnostic tickets.

You can close all tickets at once but this is not recommended. It is recommended that each diagnostic ticket be viewed, analyzed, and closed individually.

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 diagnostic ticket, you must wait 3 minutes before you can continue resolving the diagnostic ticket.

If you do not close a diagnostic ticket and the issue recurs, the only thing that gets updated in the ticket is the date and time the issue recurred (listed under **Last Occurrence** on the Web client and **Updated** on the operator panel). Ticket details are not updated because the original issue is often the root cause. If the location of the error in the library changed since the ticket was first issued, the ticket details will continue to reflect the original error location.

---

**Note:** A diagnostic ticket can have a status of Canceled. As discussed below in [Closing Diagnostic Tickets Automatically](#) on page 316, after a reboot or power request, the system may elect to close a ticket. This cancelled state does not indicate that a problem has been corrected. The system would re-open the ticket if the issue is encountered again.

---

## Operator Panel

- 1 Select **Reports > Diagnostic Tickets**.
- 2 Select **Library, Tape Drives, or Media** to view tickets related to the selected subsystem. Only the subsystems that contain tickets are listed.
- 3 You can also close all tickets at once by selecting **Close ALL**.

---

**Caution:** Be careful when choosing **Close ALL**. This closes all diagnostic tickets even if they are not resolved. It is recommended that each diagnostic ticket be viewed, analyzed, and closed individually.

---

- 4 Press **Select**.  
All of the tickets posted for the selected subsystem are displayed.
- 5 Scroll through the tickets and select the one you want to view. Press **View**.  
Basic details about the ticket are displayed, such as ticket ID number, short description, priority, and when the ticket was created and updated.
- 6 You can either press **Close** to close the ticket, or press **Exit** to exit without closing the ticket.

## Web Client

- 1 You can view all diagnostic tickets by selecting **Tools > All Diagnostic Tickets**. Alternatively, you can view library, tape drive, and media tickets separately via the Home Page Subsystem Status buttons (see [Subsystem Status](#) on page 32).

Whichever method you choose, the tickets are displayed 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 diagnostic ticket. Ticket details are not updated when a ticket recurs.

---

- 2 Identify the diagnostic ticket you want to resolve.

---

**Note:** You can use the **Go to Diagnostic Ticket** text box at the bottom of the screen to locate a specific ticket number. In addition, if there is more than one page of tickets, use the **Page 1 of x** arrows to view the additional tickets.

---

- 3 To view more details about the ticket, including the location coordinates of resources that may be involved, click the **Details** button.
- 4 To resolve the ticket, click the **Resolve** button. A series of screens guides you through steps to resolve the issue on your own. If the situation cannot be resolved, you are instructed to contact technical support. When you have finished reading all of the Resolution screens, do one of the following:
  - To close the ticket now, click **Close**. The **Tools - All Diagnostic Tickets** window displays, with the ticket no longer in the list.
  - To leave the ticket open for future troubleshooting, click **Exit**. The ticket remains on the list.

- 5 You can also close all tickets at once by clicking the **Close All Tickets** button.

---

**Caution:** Be careful when pressing the **Close All Tickets** button. This closes all diagnostic tickets even if they are not resolved. It is recommended that each diagnostic ticket be viewed, analyzed, and closed individually.

---

---

**Note:** To display all closed tickets, select the **Include Closed Tickets** check box at the bottom of the screen. The **Tools - All Diagnostic Tickets** screen refreshes, with the **Resolve** button unavailable for all closed diagnostic tickets.

---

## Closing Diagnostic Tickets Automatically

When you reboot the library, all currently open diagnostic tickets are closed automatically. If any errors occur during the reboot, the library issues new tickets.

Automatic ticket closure occurs only 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.

### Disabling or Enabling this Feature

Automatic ticket closure is enabled by default. You can enable or disable this feature from the operator panel.

- 1 Select **Setup > System Settings**.
- 2 Press **Modify**.
- 3 Press **Up** to change setting as desired,
- 4 Press **Apply**.

### Viewing Closed Diagnostic Tickets

You can view closed diagnostic tickets from the Web client.

- 1 Select **Tools > All Diagnostic Tickets**.
- 2 Click the **Include Closed Tickets** check box.



---

**Note:** Tickets that were auto-closed are designated as “Canceled.”

---

## Capturing Snapshots of Library Information

Technical support personnel may ask you to capture a snapshot of the library 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 the Web client. You can also download the Capture Snapshot file to a computer, however, you cannot print Capture Snapshot files directly from the Web client.

Depending on the library configuration and your connection speed, saving the 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 76.

You can set up the library to automatically capture and attach a snapshot to specific diagnostic ticket e-mail notifications (see [Configuring the Library E-Mail Account](#) on page 76). 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. You can only capture a snapshot via the Web client.

## Web Client

- 1 Select **Tools** > **Capture Snapshot**.
- 2 Select whether to download the file or e-mail it to a recipient, and click **Apply**.

---

# Troubleshooting Library “Not Ready” Messages

---

## “Not Ready” Messages on the Operator Panel

---

If a “not ready” message displays on the operator panel at startup, it means the robot cannot move. The library may display a message stating that it did not initialize. Try the following steps to resolve the issue:

- If the “not ready” message occurs upon initial installation (first time out of the box or after a chassis replacement), make sure you removed the Y-tray restraint as described in [Chapter 2, Unpacking the Library](#).
- Press the **Tickets** button on the operator panel to view any diagnostic tickets that occurred as a result of the error.
- Log in to the Web client using the IP address that is displayed on the operator panel screen to view ticket details and resolution steps that may help resolve the issue.

If none of the above steps works, contact Quantum Support.

---

## “Not Ready” Messages on the Web Client

---

The Web client includes 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.) For more information on Web client user interface elements, see [Web Client Layout and Functions](#) on page 29.

Library “not ready” messages continue to display in the header until the issue has been resolved, and the robot has completed its calibration.

If the library displays a “not ready” message, you may be able to tell from the message how to remedy the situation. If not, the library generates a diagnostic ticket whenever the library encounters a problem. The diagnostic ticket may provide information that can help you troubleshoot the problem. For more information, see [About Diagnostic Tickets](#) on page 312. The library “not ready” messages include the following, with possible solutions listed:

Message	Resolution
Library is not ready	The library is initializing and becoming ready. Wait for the library to finish initialization.
Library is becoming ready	Wait for the library to finish initialization.
Library is not initialized	Most likely a problem with the robot. Try the following: <ul style="list-style-type: none"> <li>• Check the diagnostic ticket and follow the resolution steps listed (see <a href="#">About Diagnostic Tickets</a> on page 312).</li> <li>• Power cycle the library to clear the error. If that fails, contact Quantum Support.</li> </ul>
Library needs manual attention	Most likely a problem with the robot or other component. Try the following: <ul style="list-style-type: none"> <li>• Check the diagnostic ticket and follow the resolution steps listed (see <a href="#">About Diagnostic Tickets</a> on page 312).</li> <li>• Power cycle the library to clear the error. If that fails, contact Quantum Support.</li> </ul>

**Note:** You may not see the “not ready” message in the Web client until the browser refreshes. Similarly, even if the problem has been resolved, the “not ready” message will not disappear from the Web client until the browser refreshes.

---

## Retrieving Tape Drive Logs

The library allows you to retrieve tape drive logs using the Web client. Tape drive log information can be used to help troubleshoot the library, the tape drive sled, and tape drive issues.

Since the log retrieval process can take up to 30 minutes, the tape drive and associated partition are automatically taken offline during the operation and brought back online when the operation completes. You will be asked to confirm that you want to take the tape drive and partition offline.

Tape drive log files 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 only retrieve tape drive logs via the Web client.

### Web Client

- 1 Select **Tools > Drive Operations**.
- 2 Select Retrieve Tape Drive Log.
- 3 Click **Apply**.
- 4 When the **Success** message displays, complete the next screens to save the log file to your computer.

---

## Interpreting LEDs

LEDs provide a visual indication about the status of certain library components. LEDs can sometimes communicate that a problem exists when diagnostic tickets cannot.

The following components of the library have LEDs:

- Front panel
- System control board (SCB)

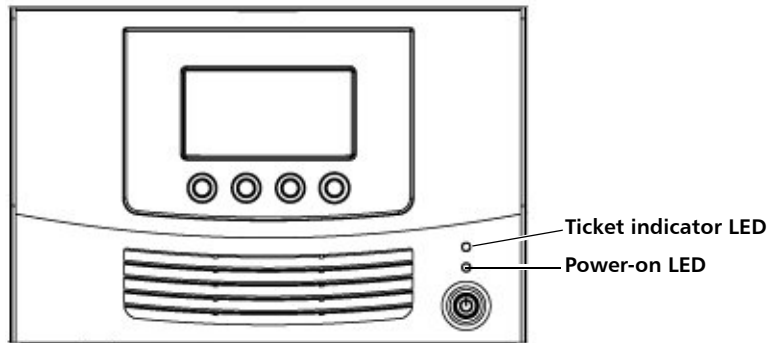
- Tape drives
- Power supplies

## Front Panel LEDs

There are two LEDs on the front panel, above the power button. They function as follows:

LED Location	Color	Indicates
Power-on LED (closest to power button)	Green	Library power is <b>ON</b> .
Ticket indicator LED. (farthest from power button)	Amber	The LED is illuminated when at least one open or unopened diagnostic ticket exists.

Figure 77 Front Panel LEDs

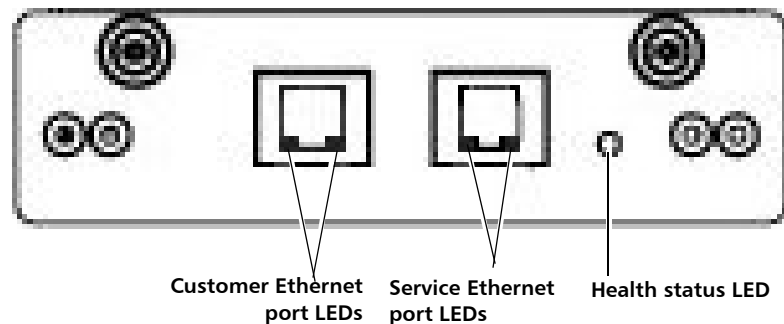


## System Control Board LEDs

The SCB has one health status LED. In addition, each Ethernet port contains two LEDs, a green “activity indicator” and an amber “link indicator.” The Ethernet port closest to the center of the library is for customer use. The Ethernet port farthest from the center of the library is for service use only.

LED	Color	Indicates
SCB Health Status LED	Green	Healthy and operational.
	Red	Failure. Replacement required.
Ethernet Port Green LED (Activity Indicator)	Green	This LED illuminates when actual “traffic” is being sent over the Ethernet cable. The LED may be blinking or on solid; it blinks more rapidly the more traffic is being sent over the connection. When the LED is lit, communications are in process and when the LED is off no communication is occurring.
Ethernet Port Amber LED (Link Indicator)	Amber	This LED illuminates solidly when a “link” is established, and will be off when no “link” is present. “Link” means an Ethernet cable is connected and the other end of the cable is also connected to another powered-up and operational Ethernet device.

Figure 78 System Control Board LEDs



## Tape Drive/Sled LEDs

The library supports SAS and Fibre Channel tape drives. The drive sled LEDs for each are described below.

### SAS

SAS Tape Drive Sleds have one LED that indicates the following:

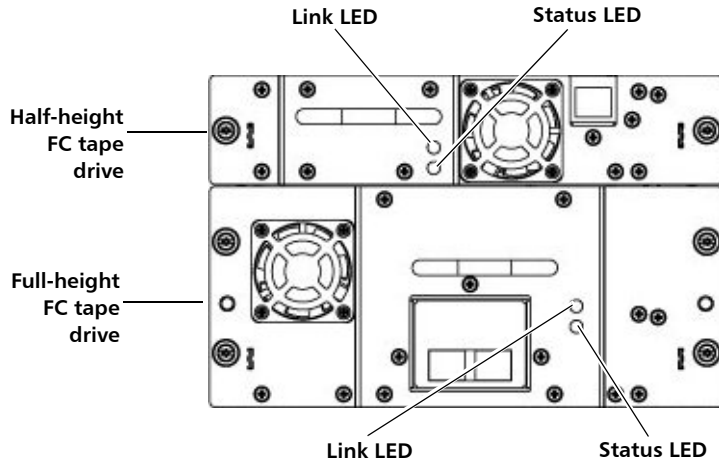
Color	Indicates
Green	Healthy and operational.
Amber	Tape drive is offline.
Red	Failure. Replacement required.

### Fibre Channel

Fibre Channel tape drive sleds have two LEDs on their rear panel, indicated on the drive sled as STATUS and LINK (see [Figure 79](#)).

LED	Color	Indicates
Status	Green	Healthy and operational.
	Amber	Tape drive is offline.
	Red	Failure. Replacement required.
Link	Green	On solid — Fibre Channel link is present Flashing — Fibre Channel link is present and communications are in process
	Off	No Fibre Channel link is currently present.

Figure 79 Fibre Channel Tape  
Drive LEDs



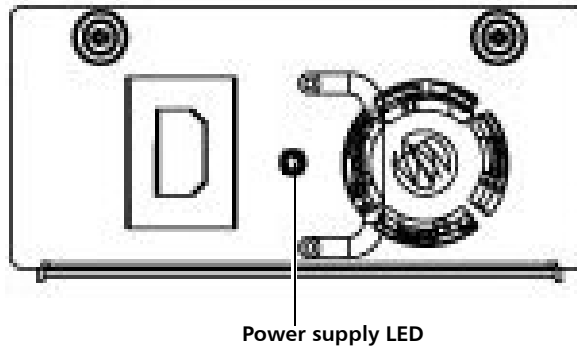
## Power Supply LED

Diagnostic tickets typically report all problems related to power supplies. You can also observe the power supply LED to see if the power supply is functioning appropriately (see [Figure 80](#)). The power supply LED indicates the following:

LED Color	Indicates
Green	AC power is present and the library front panel power switch is turned <b>ON</b> .
Amber	AC power is present but the library front panel switch is turned <b>OFF</b> .
Red	Power supply failure.
Off	No power. Ensure the power supply is correctly plugged into a wall outlet.



Figure 80 Power Supply LED



## Running the Installation and Verification Test (IVT)

The Installation and Verification Test (IVT) is used to evaluate a newly installed library or one that has been moved. The test calibrates the robot to the library, verifies that the robot is functioning properly, and verifies that the magazines and tape drives are installed correctly and reachable by the robot. The test also verifies that barcode labels can be read by the robot scanning operation.

You should run the full IVT upon installation of a new library, and at any other time you remove, replace, or service components that require you to move the library into or out of a rack or desktop kit. You must run the robotics test after a Y-tray replacement.

The full IVT consists of three subtests. You may run the subtests separately (see [Performing Library Diagnostics](#) on page 330). The full IVT takes up to 30 minutes to complete.

- **Robotics Test** — A series of tests that evaluates the basic functionality of the robotics assembly, including picker travel, Y-carriage assembly travel, barcode scanning, calibration sensors, and several moves of a scratch tape. It also calibrates the robot to the library. The test takes up to 11 minutes to complete.

- **Tape Drive Test** — For each installed tape drive, the robot moves a scratch tape into the tape drive, inventories the scratch tape, and moves the scratch tape out of the tape drive. The test takes 1–2 minutes per tape drive.
- **Magazine Test** — Moves a scratch tape through all storage slots in the library. These tests verify the robotics can reach all the slots in the magazine for both get and put operations. The test takes up to 5 minutes per magazine.

Details about running the IVT include:

- Running the IVT takes partitions offline and logs all users off of the Web client.
- The operator panel displays progress of all three subtests. Before a test begins, its progress is “Scheduled.” When a test begins, its progress changes to “Running.” Once a test completes, its progress changes to either “Passed” or “Failed.”
- You can stop the IVT by pressing the **Stop** button. The progress of the currently running test changes to “Stopping.” Once stopped, the current test and all other scheduled tests display “Stopped.”
- You can only perform the IVT from the operator panel.

### Prerequisites for Running IVT

Certain prerequisites must be met in order to run the IVT. Prior to running the IVT, the library checks to make sure all the prerequisites are met. If any is not, the operator panel displays a message telling you how to resolve the issue. Prerequisites include:

- All diagnostic tickets must be closed.
- I/E station slots must be allocated (minimum of five).
- All magazines must be installed in the library (two in the Scalar i40; four in the Scalar i80).
- At least one tape drive must be installed in the library.
- All installed tape drives must be in the ready state. (You can check the Web client **Setup > Drive Settings** for listing of which drives are in the ready state.)

- A scratch tape must be in the top I/E station slot. The scratch tape must be assigned to the System partition. The scratch tape must be compatible with all unloaded tape drives installed in the library. For a list of supported media, see [Supported Media](#) on page 347.

## Operator Panel

- 1 Make sure the prerequisites listed in [Prerequisites for Running IVT](#) on page 326 are met.

- 2 Select **Tools > IVT**.

A message displays, telling you that partitions will be turned offline and all Web client users will be logged out.

- 3 Press **Yes** to set partitions offline, log users off the Web client, and continue with the test.

The library conducts a series of prerequisite checks to be sure everything is in order. Each prerequisite is listed as the library checks it. If something is not set up correctly to run the IVT, the operator panel displays a message letting you know how to fix it. Once you fix the issue, again select **Tools > IVT**. If all is in order, the test begins.

- 4 When the test completes, if any of the three subtests fails, check the library diagnostic tickets to help determine and resolve the problem.

---

# Running the IVT Diagnostic Subtests Individually – Robotics, Tape Drive, and Magazine Tests

If you do not need to run the full IVT, you can run the robotics, tape drive, or magazine test separately to check an individual component. You should do this when you remove, replace, or service a component that does not require you to remove the library into or out of a rack or desktop kit.

For a description of the diagnostic subtests, see [Running the Installation and Verification Test \(IVT\)](#) on page 325.

Details about running the diagnostic subtests include:

- Running a diagnostic takes partitions offline and logs all users off of the Web client.
- The operator panel displays progress of the diagnostic. When a test begins, its progress displays as “Running.” Once a test completes, its progress changes to either “Passed” or “Failed.”
- Once a diagnostic test starts, you cannot stop it. You must let it run to completion.
- **For the tape drive and magazine diagnostics**, you may choose just one device to test, or you can choose to test all. The magazine diagnostic tests all the slots in the selected magazine(s).
- You can only perform the subtests from the operator panel.

### Prerequisites for Running Diagnostic Subtests

Certain prerequisites must be met in order to run the diagnostics. Prior to running a diagnostic, the library checks to make sure all the prerequisites are met. If any is not, the operator panel displays a message telling you how to resolve the issue. Prerequisites include:

- All diagnostic tickets must be closed.
- I/E station slots must be allocated (minimum of five).
- All magazines must be installed in the library (two in the Scalar i40; four in the Scalar i80).
- A scratch tape must be in the top I/E station slot. The scratch tape must be assigned to the System partition. The scratch tape must be compatible with all unloaded tape drives installed in the library. For a list of supported media, see [Supported Media](#) on page 347.
- **For the tape drive diagnostics only**, at least one tape drive must be installed in the library. All installed tape drives must be in the ready state. (You can check the Web client **Setup > Drive Settings** for listing of which drives are in the ready state.)

## Operator Panel

- 1 Make sure the prerequisites listed in [Prerequisites for Running Diagnostic Subtests](#) on page 328 are met.
- 2 Select **Tools > Diagnostics**.
- 3 Select **Robotics Test, Tape Drive Test, or Magazine Test** and press **Select**.
- 4 For the tape drive or magazine test, select which tape drive or magazine you want to test, or select **ALL**, then press **Select**.
- 5 Press **Yes** to set partitions offline, log users off the Web client, and continue with the test.

The library conducts a series of prerequisite checks to be sure everything is in order. Each prerequisite is listed as the library checks it. If something is not set up correctly, the operator panel displays a message letting you know how to fix it. Once you fix the issue, start over from [Step 1](#). If all is in order, the test begins.

- 6 Once complete, if the test fails, check the library diagnostic tickets to help determine and resolve the problem.

---

## Running the Random Move Test

The random move test is a demonstration that consists of moving a scratch tape into random slots around the library. Partitions are set offline and the test runs continuously until you stop it. You can only run this test from the operator panel.

## Operator Panel

- 1 Install a scratch tape in the top I/E station slot.
- 2 Assign the scratch tape to the System partition.
- 3 Select **Tools > Random Move Test**.
- 4 Press **Run**.
- 5 Press **Yes** to set partitions offline, log users off the Web client, and continue with the test.

- 6 When you are ready to stop the test, press **Stop**.
- 7 When the operator panel displays the message that the test has stopped, press **OK**.

## Performing Library Diagnostics

The Diagnostics menu on the Web client contains tests you can run to determine if tape drives and robotics, are working as they should.

Notes about Diagnostics include:

- 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.
- 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 Web client users with the same or lower privileges (the operator panel user is not logged out, but any attempted operation using partitions will fail). Users will be unable to log in to the Web client and will get an error message stating that Diagnostics is in progress.
- You can only enter Diagnostics from the Web client.

### Web Client

- 1 Select **Tools > Diagnostics**.

A confirmation dialog displays, alerting you that all other users will be logged out and library partitions will be taken offline.

- 2 Click **OK**.

You are now in a page that looks much like the regular Home page, but with different choices in the menu bars. Also, you will notice that all your partitions are offline.

- 3 Select the test you want to run from the menus. Your choices include:
  - Tape Drive Reset (see [Resetting a Tape Drive](#) on page 331 for more information)
  - Robotics Get/Put Test (see [Robotics Get/Put Test](#) on page 332 for more information)
- 4 To exit Diagnostics, select **Exit**.

---

## Resetting a Tape Drive

---

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).

The reset may take several minutes. 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.

You may perform a tape drive reset from either the operator panel or the Web client. If you use the Web client, you must enter Diagnostics, which logs out all users of the same or lower privilege level (see [Performing Library Diagnostics](#) on page 330).

### Operator Panel

- 1 Select **Actions > Tape Drive > Reset**.
- 2 If more than one tape drive is installed in the library, select the tape drive you want to reset and press **Reset**, or select **ALL**.
- 3 Once the operation completes, the operator panel displays a message stating that the operation completed, and there will be diagnostic tickets if it failed.
- 4 Press **OK**.
- 5 Check to see if the library generated diagnostic tickets.

## Web Client

- 1 Enter Diagnostics (**Tools > Diagnostics**, then click **OK** to take partitions offline and log out all other users of the same or lower privileges).
- 2 Select **Drives > Drive Tests > Drive Reset**.
- 3 If the tape drives are assigned to more than one partition, select the partition in which the tape drive(s) you want to reset are located. Select **Unassigned** if the tape drive(s) you want to reset are not assigned to a partition. Click **Next**.
- 4 Select the tape drive(s) you want to reset.
- 5 Click **Apply**.
- 6 The test runs. When complete, a “success” or “failure” message displays.

---

## Robotics 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.

You can only perform this test from the Web client, by entering Diagnostics (see [Performing Library Diagnostics](#) on page 330).

## Web Client

- 1 Install a scratch tape in the top I/E station slot.
- 2 If manual cartridge assignment is enabled, assign the scratch tape to the System partition.
- 3 Enter Diagnostics (**Tools > Diagnostics**, then click **OK** to take partitions offline and log out all other users of the same or lower privileges).
- 4 Select **Robotics > Robotics Get/Put Test**.
- 5 Click **Apply**.
- 6 The test runs. When complete, a “success” or “failure” message displays.



# Resetting Factory Defaults

Resetting factory defaults restores the library's default configuration (see [Default Configuration](#) on page 40).

## Resetting factory defaults clears:

- Most of the library's configurable items, such as partitions, user accounts, import/export (I/E) station slots, cleaning slots.
- All diagnostic tickets and log information.
- Any tape drive firmware images uploaded manually.

## Resetting factory defaults does NOT clear:

Date and time, network configuration, or license key settings, nor does it change the library firmware version.

You may want to reset factory defaults if you are completely reinstalling or reconfiguring the library.

If you downgrade your library's firmware version to an earlier released version, library configuration settings will be reset to the factory defaults for the newly installed firmware.

If you upgrade firmware, your library configuration settings remain as you have set them.

## Web Client

On the Web client, this feature is only available to service users using the service login and password.

## Operator Panel

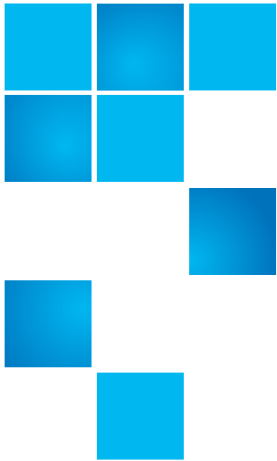
On the operator panel, if logins are disabled (default), this operation is available to all users. If logins are enabled, this operation is only available to service users using the service login and password.

### 1 Select **Tools > Reset Factory Defaults**.

A message displays stating that configuration data will be cleared and library rebooted.

### 2 Press **Yes** to continue.





## Chapter 12

# Working With Cartridges and Barcodes

---

This chapter describes how to work with cartridges and barcodes. When working with tape cartridges, certain considerations should be taken into account. For example, all tape cartridges in the library must have a barcode label. In addition, when loading your library, you should be aware of whether or not your cartridges are write-protected.

This section discusses these types of items in general terms. See [Supported Media](#) on page 347 for information on what type of tape cartridges are supported for each drive type.

This chapter covers:

- [Handling Tape Cartridges Properly](#)
- [Write-Protecting Tape Cartridges](#)
- [Supported Barcode Formats](#)
- [Barcode Label Requirements](#)
- [Installing Barcode Labels](#)

## Handling Tape 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.
- Store cartridges in a vertical orientation, not horizontally. Vertical orientation is particularly important for long-term or archival storage.
- 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).
- If cartridges have been exposed to temperatures outside the range specified above, stabilize the cartridges at normal operating room temperature for the same amount of time they were exposed to extreme temperatures or 24 hours, whichever is less. Temperatures above 125°F (52°C) can cause permanent damage.
- Do not place cartridges near sources of electromagnetic energy or strong magnetic fields, such as computer monitors, electric motors, speakers, or x-ray equipment. Exposure to electromagnetic energy or magnetic fields can destroy data and the embedded servo code written on the media by the cartridge manufacturer, rendering the cartridges unusable.
- Place barcode labels only in the designated slots on the cartridges.

- If you ship cartridges, ship them in their original packaging or something stronger.
- Do not insert damaged cartridges into tape drives.
- Do not touch the tape or tape leader.

---

---

**Caution:** Do not degauss cartridges that you intend to reuse.

---

---

## Write-Protecting Tape Cartridges

All tape cartridges have a write-protect (write-inhibit) switch to prevent accidental erasure or overwriting of data. Before loading a tape cartridge into the library, make sure that the write-protect switch is positioned correctly (either on or off).

Slide the red or orange write-protect switch to the right so that the padlock shows in the closed position. The switch is located on the left side of the cartridge front.

## Barcode Label Requirements

Cartridges must have an external barcode label that is machine readable. Quantum-supplied barcode labels provide the best results. Barcode labels from other sources can be used, but they must meet the following requirements:

- ANSI MH10.8M-1983 Standard.
- Type font: Code 39 (3 of 9).
- Characters: only uppercase letters A to Z and/or numeric values 0 to 9.

- Number of digits: 5 to 15 (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:  $\pm 57$  mm.
- Length of the rest zones: 5.25 mm  $\pm$  0.25 mm.
- No black marks should be present in the intermediate spaces or rest zones.
- No white areas should be present on the bars.

## Supported Barcode Formats

Quantum supplies industry standard LTO barcode labels with a length of 6 + 2 corresponding to the Standard Six and Plus Six formats listed below. For advanced uses, your Quantum library supports label lengths of up to 15 characters allowing you to create custom labels. Refer to [Barcode Label Requirements](#) on page 337 for label details.

The library supports the following tape cartridge barcode formats.

- **Standard Six** — Six character barcode number with or without a one or two-character media ID; for example, “XXXXXX” or “XXXXXXL4”. Only the six character barcode is reported to the host.
- **Plus Six** — Six character barcode number followed by a media ID; for example, “XXXXXXL3”. Six character barcode and media ID are reported to the host.

- **Extended** — Five to 15 characters total, including a barcode number and optional media ID. All characters are reported to the host, regardless of having a media ID or not. If a media ID is included, the label must have a five to 13 character barcode followed by a media ID; for example, “XXXXXL2” or “XXXXXXXXXXXXXXXXL2”. If a media ID is not included, the label must have a five to 15 character barcode; for example, “XXXXX” or “XXXXXXXXXXXXXXXXXX”.
- **Media ID Last** — Five to 13 character barcode number followed by media ID; for example, “XXXXXXXXXXXXXXXXL4”. The media ID is reported to the host last.
- **Media ID First** — Five to 13 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”.
- **Standard (default)** — Five to 15 characters total, including a barcode number and optional media ID. The media ID is not reported to the host. If a media ID is included, the label must have a five to 13 character barcode followed by a media ID; for example, “XXXXXL3” or “XXXXXXXXXXXXXXXXL3”. If a media ID is not included, the label must have a five to 15 character barcode; for example, “XXXXX” or “XXXXXXXXXXXXXXXXXX”.

## 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 81](#) on page 340).

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.

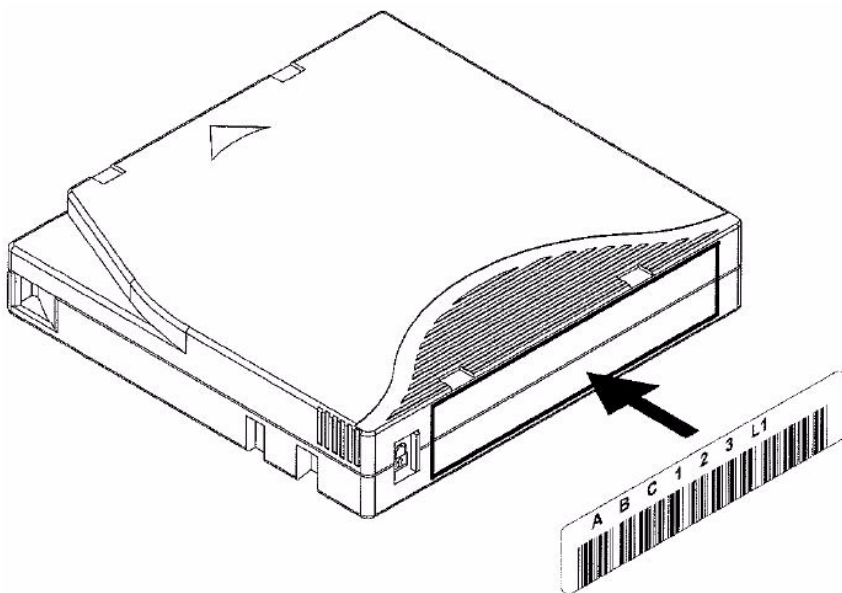
The cartridge cannot have any stickers or labels attached to the top or bottom because if the labels come loose, they can get caught in the tape drives or become unreadable by the scanner.

---

**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 81 Barcode Label Orientation





# Appendix A

## Specifications

### Physical Specifications

Table 7 Base Library

	Scalar i40	Scalar i80
<b>Height</b>	5.2 in. (132 mm)	10.4 in. (264 mm)
<b>Width</b> (excluding "rack ears")	17.5 in. (445 mm)	17.5 (445 mm)
<b>Depth</b> (from library front bezel to back of library; excluding drive sleds)*	31.2 in. (793 mm)	31.2 in. (793 mm)
<b>Weight</b> (one power supply, no tape drives, and no tape cartridges installed)	34.9 lbs. (15.8kg)	52.4 lbs. (23.8 kg)
<b>Weight</b> (one power supply, two tape drives, and no tape cartridges installed)	With 2 half-height SAS tape drives: 44.2 lbs. (20 kg)	With 2 full-height SAS tape drives: 65.7 lbs. (29.8 kg)

\* Depths listed above exclude drive sleds. Drive sleds will add up to 50 mm to the overall length of the library depending on tape drive type (half-height, full-height, Fibre Channel, SAS). Additionally, when planning space requirements, take into account installed cables (particularly fibre-optic cable radius on Fibre Channel tape drives).

Table 8 Library Installed in a  
Desktop Kit

	Scalar i40	Scalar i80
<b>Height</b> (with desktop "feet" installed)	5.3 in. (135.6 mm)	10.6 in. (268.8 mm)
<b>Width</b>	18.9 in. (480 mm)	18.9 in. (480 mm)
<b>Depth</b> (from library front bezel to back of library; excludes drive sleds)*	31.2 in. (793 mm)	31.2 in. (793 mm)

\* Depths listed above exclude drive sleds. Drive sleds will add up to 50 mm to the overall length of the library depending on tape drive type (half-height, full-height, Fibre Channel, SAS). Additionally, when planning space requirements, take into account installed cables (particularly fibre-optic cable radius on Fibre Channel tape drives).

## Capacity

	Scalar i40	Scalar i80
<b>Form Factor</b>	3U	6U
<b>Maximum number of tape drives</b>	1 full-height or 2 half-height tape drives	3 full-height or 5 half-height tape drives
<b>Number of magazines</b>	2 magazines (20 slots each)	4 magazines (20 slots each)
<b>Number of cartridge slots</b>	Base unit: 25 Fully licensed: 40	Base unit: 50 Fully licensed: 80
<b>Maximum native capacity</b>	25 slots: 20 TB 40 slots: 32 TB	50 slots: 40 TB 80 slots: 64 TB
<b>Number of I/E station slots</b>	0 or 5	0, 5, or 10

## Environmental Specifications

The environmental specifications of the library are listed below.

**Note:** Temperature ranges apply to product inlet temperatures, not necessarily to ambient room temperatures. Airflow restrictions or other heat-generating equipment within the rack enclosure may cause a rise over ambient room temperatures.

	<b>Operating</b>	<b>Non-Operating</b>	<b>Shipping and Storage</b>
<b>Altitude</b>	–500 to 10,000 ft (–152 to 3,048 m)	–500 to 10,000 ft (–152 to 3,048 m)	–500 to 10,000 ft (–152 to 3,048 m)
<b>Temperature</b>	50° to 95° F (10° to 35° C)	50° to 113° F (10° to 45° C)	–40° to 140° F (–40° to 60° C)
<b>Relative Humidity</b>	20 to 80%, non-condensing	10 to 90%, non-condensing	0 to 95%, non-condensing

## Air Clearance Requirements

There must be at least 4 in. (10 cm) of open space in front of and behind the library for proper air flow

## Library Power Specifications

	Scalar i40	Scalar i80
<b>Line voltage</b>	100 – 240 VAC	100 – 240 VAC*
<b>Line frequency</b>	50 – 60 Hz	50 – 60 Hz*
<b>Rated AC Input Current</b>	100 Volt – 2.8 Amps 240 Volt – 1.4 Amps	100 Volt – 5.0 Amps 240 Volt – 2.5 Amps
<b>Typical Power Consumption</b>	100 watts	200 watts

\* A Scalar i80 library with dual power supplies will have these requirement on both AC inputs to the library but will load share the current draw equally between each supply and from each AC connection.

## Power Consumption and Heat Output

Typical library power consumption (watts/hour) and heat output (BTU/hour) are listed below. The values listed below are average (not peak or maximum) values.

Component	Typical Power Consumption (Watts/Hour)	Typical Heat Output (BTU/Hour)
Scalar i40 library minimum configuration: no tape drives installed; random robot movement	18	61
Scalar i40 library maximum configuration: two (2) tape drives*, writing	70	239
Scalar i80 library minimum configuration: no tape drives installed; one power supply, random robot movement	18	61
Scalar i80 library maximum configuration: five (5) tape drives*, writing, two power supplies	159	544
HP LTO-4 tape drive*, writing, one power supply, no robot movement	24	82
HP LTO-5 tape drive*, writing, one power supply, no robot movement	27	92
Second power supply, Scalar i80	7	24

\* The difference in power consumption and heat output between full-height and half height tape drives, and between Fibre Channel and SAS tape drives, is negligible.

## Communication Interfaces

Library Control	Logical Unit Number (LUN)
Connectivity	Native drive interface (FC, SAS)
Library Management	Operator panel Web client SNMP protocol SMI-S protocol

## Supported Tape Drives

Vendor	Media Generation	Interface Type	Speed	Connector
HP	LTO-4	Fibre Channel	4 Gb/s	LC
		SAS	3 Gb/s	SFF-8088
HP	LTO-5	Fibre Channel	8 Gb/s	LC
		SAS	6 Gb/s	SFF-8088

## Supported Media

Cartridge Type	Access
LTO-5	Read/write in LTO-5 tape drives; supports WORM functionality
LTO-4	Read/write in LTO-4 and LTO-5 tape drives; supports WORM functionality
LTO-3	Read/write in LTO-4 tape drives; read-only in LTO-5 tape drives; supports WORM functionality
LTO-2	Read-only in LTO-4 tape drives

## Supported Internet Browsers

The Internet browser software is not supplied with the Scalar i40 and Scalar i80 systems; you must obtain and install it independently. The Scalar i40 and Scalar i80 systems support the following Internet browsers:

---

**Note:** For correct operation of the software, disable any pop-up blockers.

---

### Microsoft® Windows®

- Internet Explorer® (IE) 6.0, 7.0, and 8.0
- Mozilla® Firefox® 1.0.6 or later

### Linux®

- Firefox 1.0.6 or later

### Solaris™

- Firefox 1.0.6 or later

---

## Supported Operating Systems

The Scalar i40 and Scalar i80 systems support the following operating systems:

- Microsoft® Windows® Enterprise Server
- Sun™ Solaris™
- HP-UX®
- IBM® AIX®
- Red Hat® Enterprise Linux®





## Appendix B

# Tape Alert Flag Descriptions

Tape Alert is an open industry standard that flags errors and provides possible solutions for storage devices and their media. This section provides information about Tape Alert flags issued by tape drives, including the identifying number, severity, recommended message, and probable cause. [Table 9](#) explains the severity codes, and [Table 10](#) lists all the existing Tape Alert flags and their descriptions.

Support for specific Tape Alert flags may vary based on tape drive type and firmware revision. Not all tape drives support every Tape Alert. Consult your tape drive SCSI manual for more information.

For more information on Tape Alert, see <http://www.t10.org/index.html> for INCITS *SCSI Stream Commands - 3 (SSC-3)*.

Table 9 Tape Alert Flag Severity Codes

I	<b>Informational.</b>
W	<b>Warning</b> — The system may not be operating optimally. Continued operation without corrective action may cause a failure or raise critical Tape Alert flags.
C	<b>Critical</b> — Either a failure has already occurred or a failure is imminent. Corrective action is required.

Table 10 Tape Drive Tape Alert 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: <ol style="list-style-type: none"> <li>1 Copy any data you require from this tape.</li> <li>2 Do not use this tape again.</li> <li>3 Restart the operation with a different tape.</li> </ol>	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: <ol style="list-style-type: none"> <li>1 Use a good tape to test the drive.</li> <li>2 If the problem persists, call the tape drive supplier help line.</li> </ol>	The drive can no longer write data to the tape.

No.	Flag	Severity	Recommended Application Client Message	Probable Cause
7	Media life	W	The tape cartridge has reached the end of its calculated useful life: 1 Copy any data you need to another tape. 2 Discard the old tape.	The media has exceeded its specified life.
8	Not data grade	W	The tape cartridge is not data-grade. Any data you write to the tape is at risk. Replace the cartridge with a data-grade tape.	The drive has not been able to read the MRS* stripes.
9	Write protect	C	You are trying to write to a write-protected cartridge. Remove the write-protection or use another tape.	Write command is attempted to a write-protected tape.
10	Media removal prevented	I	You cannot eject the cartridge because the tape drive is in use. Wait until the operation is complete before ejecting the cartridge.	Manual or software unload attempted when prevent media removal on.
11	Cleaning media	I	The tape in the drive is a cleaning cartridge.	Cleaning cartridge loaded into drive.
12	Unsupported format	I	You have tried to load a cartridge of a type which is not supported by this drive.	Attempted load of unsupported tape format.
13	Recoverable mechanical cartridge failure	C	The operation has failed because the tape in the drive has experienced a mechanical failure: 1 Discard the old tape. 2 Restart the operation with a different tape.	Tape snapped/cut or other cartridge mechanical failure in the drive where medium can be demounted.

Appendix B: Tape Alert Flag Descriptions

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"> <li>1 Do not attempt to extract the tape cartridge.</li> <li>2 Call the tape drive supplier help line.</li> </ol>	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"> <li>1 Use another tape cartridge for your next backup.</li> <li>2 Store this tape cartridge in a safe place in case you need to restore data from it.</li> </ol>	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"> <li>1 If the operation has stopped, eject the tape and clean the drive.</li> <li>2 If the operation has not stopped, wait for it to finish and then clean the drive.</li> </ol> <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"> <li>1 Wait for the current operation to finish.</li> <li>2 Then use a cleaning cartridge.</li> </ol> <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"> <li>1 Discard the worn-out cleaning cartridge.</li> <li>2 Wait for the current operation to finish.</li> <li>3 Then use a new cleaning cartridge.</li> </ol>	The cleaning cartridge 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"> <li>1 Do not use this cleaning cartridge in this drive.</li> <li>2 Wait for the current operation to finish.</li> <li>3 Then use a valid cleaning cartridge.</li> </ol>	Invalid cleaning cartridge type used.

Appendix B: Tape Alert Flag Descriptions

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"> <li>1 Eject the tape or magazine.</li> <li>2 Reset the drive.</li> <li>3 Restart the operation.</li> </ol>	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"> <li>1 Turn the tape drive off and then on again.</li> <li>2 Restart the operation.</li> <li>3 If the problem persists, call the tape drive supplier help line.</li> </ol>	The drive has a hardware fault that is not read/write related or requires a power cycle to recover.
32	Primary interface	W	<p>The tape drive has a problem with the host interface:</p> <ol style="list-style-type: none"> <li>1 Check the cables and cable connections.</li> <li>2 Restart the operation.</li> </ol>	The drive has identified an interface fault.
33	Eject media	C	<p>The operation has failed:</p> <ol style="list-style-type: none"> <li>1 Eject the tape or magazine.</li> <li>2 Insert the tape or magazine again.</li> <li>3 Restart the operation.</li> </ol>	Error recovery action.
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>	Microcode update failed.
35	Drive humidity	W	<p>Environmental conditions inside the tape drive are outside the specified humidity range.</p>	Drive humidity limits exceeded.
36	Drive temperature	W	<p>Environmental conditions inside the tape drive are outside the specified temperature range.</p>	Cooling problem.
37	Drive voltage	W	<p>The voltage supply to the tape drive is outside the specified range.</p>	Drive voltage limits exceeded.
38	Predictive failure	C	<p>A hardware failure of the tape drive is predicted. Call the tape drive supplier help line.</p>	Predictive failure of drive hardware.

Appendix B: Tape Alert Flag Descriptions

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.



No.	Flag	Severity	Recommended Application Client Message	Probable Cause
54	No start of data	C	<p>The start of data could not be found on the tape:</p> <ol style="list-style-type: none"> <li>1 Check that you are using the correct format tape.</li> <li>2 Discard the tape or return the tape to your supplier.</li> </ol>	Tape damaged, bulk erased, or incorrect format.
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"> <li>1 Remove the cartridge, inspect it as specified in the product manual, and retry the operation.</li> <li>2 If the problem persists, call the tape drive supplier help line.</li> </ol>	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"> <li>1 Do not attempt to extract the tape cartridge.</li> <li>2 Call the tape driver supplier help line.</li> </ol>	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"> <li>1 Check the power to the automation system.</li> <li>2 Check the cables and cable connections.</li> <li>3 Call the supplier help line if problem persists.</li> </ol>	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.

Appendix B: Tape Alert Flag Descriptions

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"> <li>1 If a WORM medium was used inadvertently, replace it with a normal data medium.</li> <li>2 If a WORM medium was used intentionally:               <ol style="list-style-type: none"> <li>a) Check that the software application is compatible with the WORM medium format you are using.</li> <li>b) Check that the medium is bar-coded correctly for WORM.</li> </ol> </li> </ol>	The application software does not recognize the medium as WORM.
61 – 64	Reserved			

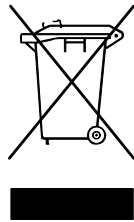
\* Media Recognition System (MRS) is a method where pre-defined stripes are placed at the beginning of the media to identify the media. The MRS stripes are read to determine if the media is of data-grade. Data-grade media should be used in SCSI streaming devices since it is of the required quality and consistency to be used to store data (i.e., audio/video grade media should not be used).



## Appendix C

# Disposal of Electrical and Electronic Equipment

---



This symbol on the product or on its packaging indicates that this product should not be disposed of with your other waste. Instead, it should be handed over to a designated collection point for the recycling of electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner

that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please visit our website at: <http://qcare.quantum.com> or contact your local government authority, your household waste disposal service or the business from which you purchased the product.



含汞電池  
減少使用  
務必回收





# Glossary

---

---

## Numerals

**1U, 2U, 3U, etc.** Racks manufactured for mounting computer hardware often define vertical space as “units.” The components that are mounted in the racks are defined by how many units of rack space they require. For example, the height of a unit in a rack is 1.75 inches. If a component is 5.25 inches in thickness, the component is said to be a 3U component.

---

## A

**Arbitrated loop** A Fibre Channel configuration that attaches multiple communicating ports in a loop. Two or more ports can interconnect, but only two ports can communicate simultaneously.

**Arbitration** The submission of a request to gain access to an arbitrated loop by a device, so that it can transmit data in the loop.

---

## B

**Barcode** A printed array of varied rectangular bars and spaces that can be scanned and read for object identification.

**Bus** A transmission channel through which electrical signals are carried from one device to another device.

---

C

- Cartridge** A container that is a protective housing for storage media, such as cartridges for tapes or optical disks.
- Cleaning tape / cleaning cartridge** A tape used to clean recording heads and reading heads on a tape drive.
- Cleaning slot** The physical home where a cleaning tape or cartridge resides.
- COD (Capacity on Demand)** A library feature that allows users to have a large physical library, but only be licensed to use a subset of its total capacity. Users pay only for what they are currently using. License upgrades enable more capacity without causing a system interruption.
- Connectivity** The method by which hardware devices or software communicate with other hardware or software.
- Control path** The connection between a partition and host application. The control path connection is made through a designated tape drive. Only one tape drive can be selected as the control path per partition.
- Controller** The PCB or system that translates computer data and commands into a form suitable for use by the storage disks.
- CRU (Customer Replaceable Unit)** The smallest hardware component that can be replaced at a customer installation by a customer.

---

D

- Default** A value or setting that is selected by the hardware or software unless specified otherwise by the user.
- DHCP (Dynamic Host Configuration Protocol)** A protocol for assigning dynamic IP addresses to devices on a network. DHCP supports a mix of static and dynamic IP addresses.
- Diagnostic ticket** A ticket that alerts service personnel and customers of an issue with the library. Diagnostic tickets identify which library components are most likely causing the issue. When possible, a diagnostic ticket provides instructions for resolving the issue.
- Directory** A file that contains a list of other files. *Directory* is short for *directory file*.

**Drivers** Software programs that enable a computer to communicate with hard drives, CD ROM drives, printers, and other peripherals. Drivers are stored on a hard disk and loaded into memory at boot up.

---

**E**

**Element ID - Logical** An address used by a library to locate and track library component. The address is specified in programming logic rather than on the physical location of a component within a library. When a logical library is used, the logical element ID masks the physical element ID.

**Element ID - Physical** An address used by a library to locate and track library component. The address is based on the physical location of a component within a library. Applications expect to see resources at specific IDs.

**Ethernet** A type of local area network designed to transport data at rates up to 100 million bits per second. Other software, such as TCP/IP runs on top of Ethernet to provide high-level networking services to applications.

**Event** A condition that matches a numbered, predefined set of circumstances.

**Event log** A list of all predefined events logged by library and software management tools.

---

**F**

**FC (Fibre Channel)** A high speed data transfer architecture. Using optical fibre to connect devices, Fibre Channel communications are serial communications that occur at full duplex and achieve data transfer rates of 200 MBps.

**FC-AL (Fibre Channel Arbitrated Loop)** A form of Fibre Channel network in which up to 126 nodes are connected in a loop topology. See also *Arbitrated loop*.

**FC-AL Device** A device that employs Fibre Channel-Arbitrated Loop and consists of one or more NL\_Ports.

**Fiber** A thin filament of glass. An optical waveguide consisting of a core and a cladding which is capable of carrying information in the form of light. Fiber is also a general term used to cover all

physical media types supported by Fibre Channel, such as optical fiber, twisted pair, and coaxial cable.

**Firewall** A set of security tools designed to separate an internal network from the public Internet in order to keep unauthorized users out of a restricted network. Firewalls are the primary line of security defense for businesses.

**FL\_Port** Fabric Loop Port. An F\_Port that is capable of supporting an attached Fibre Channel Arbitrated Loop. An FL\_Port on a loop will have the AL\_PA hex'00' giving the fabric the highest priority access to the loop. N\_Ports or NL\_Ports can attach to it in an Arbitrated Loop topology and are capable of communicating with FC-AL protocol.

**FRU (Field Replaceable Unit)** The smallest hardware component that can be replaced at a customer installation by a certified field service representative.

---

## G

**GUI (Graphical User Interface)** A computer environment that provides a visual view of a system by incorporating windows, icons, menus, and a pointing device. Also referred to as a Windows, Icons, Mouse, and Pointers (WIMP) interface.

---

## H

**HDD (High Density Drive)** A drive that contains increased storage capacity of bits and/or tracks per square inch.

**Home position** Accessor axes positioned at 0 vertical and 0 horizontal, that serve as the point of reference for the position of other library components. Home position is used as a basis for calibration.

**Host** In general, a host is a computer or program that contains data and provides services to other computers or devices. In Fibre Channel terms, a host is a computer that initiates contact with storage devices.

**Hot swappable** The ability to replace a defective component while the system continues to function normally.

**HTTP (Hypertext Transfer Protocol)** The communication rules by which a Web browser (client) and a server delivering Web pages exchange information.



- 
- I**
- I/E** Import/Export. The movement of data or hardware in and out of processing and storage systems.
- I/E slot** A bin that contains a single piece of media in the station.
- I/E station** A door on the front of the library that contains tape magazines, into which cartridges to be imported are placed manually or cartridges to be exported are placed by the picker.
- Interoperability** The capability of two or more hardware devices or two or more software routines to work together.
- IP (Internet Protocol)** A protocol that specifies the formats of packets and addresses. Addresses are formulated as four groups of 2 or 3 digit numbers separated by periods, such as 255.255.255.255.
- 
- K**
- Kernel** The heart of the UNIX operating system. The kernel is the part of the operating system that allocates resources and controls processes. The design strategy has been to keep the kernel as small as possible and to put the rest of the UNIX functionality into separately compiled and executed programs.
- 
- L**
- L\_Port** Loop Port. It only has the capability to communicate over FC-AL hubs and through FL\_Ports.
- LED (Light Emitting Diode)** The mode of data transmission for multimode cables with short wave optical transceivers. Single-mode cables, by comparison, use high powered, long wave lasers.
- Library** A large-scale tape device with robotics that can house multiple tape drives and a significant amount of tape cartridges.
- Library Control Module** See *Control module*.
- License key** An absolute value that can only increase a licensed feature. For example, a license key can be applied to the library to enable unlicensed slots.
- Logical library** See *Partition*.
- Loop** With this Fibre Channel option, the port operates with attached loop-capable devices. If a point-to-point device is attached, the appliance is not able to communicate with it.

**Loop ID** A unique 7-bit value from 0 to 126 that represents the 127 valid AL\_PAs (physical addresses) on a loop.

**LTO (Linear Tape Open)** A family of magnetic tape media that are “open” in the sense of not being owned by a single proprietor. LTO comes in two formats, Accelis and Ultrium. Accelis is the fast access implementation, while Ultrium is the high capacity implementation.

**LUN (Logical Unit Number)** A unique identifier used on a SCSI bus to distinguish between devices that share the same bus. A LUN can be an end user, a file, or an application. In storage technology, a single large storage device might be divided into smaller pieces, either to make the vast storage space more manageable or because the storage space is dedicated to different servers, drives, or applications. When the storage space is divided into smaller parts, each part is configured with its own SCSI unique identifier, or LUN.

---

## M

**Magazine** A container for removable media storage used in tape libraries.

**Media** A material that stores data, such as tapes in cartridges or optical disks.

**Media ID** A barcode number attached to a specific piece of media.

**Media type** A format/size of media, for example, LTO.

**Medium** See *Media*.

**Mixed media** The ability of a library to simultaneously support multiple types of storage media.

---

## N

**N\_Port** Node Port. It only has the capability to communicate through an F-Port. It is a port on a computer, disk drive, and so on, through which the device does its Fibre Channel communication as a direct fabric-attached port for use with the point-to-point or fabric topology. It is identified by a world wide name.

**NL\_Port** Node Loop Port. It has the capability to communicate over both FC-AL hubs and through F\_Ports.

---

**O** **Online** A status for a component that indicates it is active and available for use.

**OS (Operating System)** A control program for a computer that allocates computer resources, schedules tasks, and provides the user with a way to access the resources.

---

**P** **Partition** An abstraction of an underlying physical library that may present a different personality, capacity, or both to a host. It is a representation of real physical elements, combined to create a grouping that is different from the physical library. Also a logical portion of the physical library that is viewed by the host as if it is a complete library. Partitions present the appearance of multiple, separate libraries for purposes of file management, access by multiple users, or dedication to one or more host application.

**Pathname** A list of directories separated by slashes (/) and ending with the name of a directory or nondirectory file. A pathname is used to trace a path through the file structure to locate or identify a file.

**Picker** The robotic hand that handles cartridges.

**Point to Point** A Fibre Channel topology that consists of a dedicated connection between two devices: a sending device and a receiving device.

---

**R** **Rack Mount** An industry standard communication and computer equipment rack cabinet.

---

**S** **SAN (Storage Area Network)** A dedicated network that connects storage devices and servers in a pool, providing consolidated storage and storage management. Storage interconnects between many initiators and target devices. The SAN allows for sharing resources (target devices) among multiple servers (initiators).

**SCSI (Small Computer System Interface)** A set of standards for a high-speed, parallel interface that connects processing devices

to peripheral devices, such as storage subsystems. The acronym is pronounced "scuzzy."

**Server** A powerful, centralized computer (or program) designed to provide information to clients (smaller computers or programs) upon request.

**Setup wizard** A tool for initially configuring the library. It appears the first time the user starts the library. However, it can be used to modify configurable items anytime after the initial configuration.

**Sled** The hardware that houses tape drives in the library.

**SMI-S (Storage Management Initiative Specification)** An industry standard SMI-S application programming interface (API) developed by SNIA that facilitates the management of multi-vendor devices in a storage area networks (SANs) environment.

**Snapshot** A rapid, point-in-time image of a volume created initially on the same disk as the original by duplicating metadata rather than copying the full data set. Snapshots are often used to protect against data corruption (viruses, etc.) or to create test or pre-production environments. Snapshots are also often used as a first step for creating non-disruptive point-in-time backups, and for copying datasets to a second disk to create a full duplicate copy of the volume. Snapshots are created on disk, and in the same format as the original data. Snapshots are also referred to as point-in-time copies and as shadow copies.

**SNMP (Simple Network Management Protocol)** The protocol governing network management and the monitoring of network devices and their functions. Similar in function to SAM, except SNMP governs LAN, whereas SAM governs SAN.

**SSL (Secure Sockets Layer)** A protocol that provides encrypted communications on the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP and is layered above the connection protocol TCP/IP.

**Storage device** An appliance containing data that can be accessed, added to, changed, or deleted by the user. The storage media types include tapes and optical disks. A storage device can be a single disk drive, or constitute thousands of tapes in a large tape library.

**Storage slot** The physical home where a data cartridge resides.

**Subsystem status** A feature that provides predictive alerts, warning of any loss of connectivity or device failure using local or remote alerts. Subsystem status allows administrators to correct faults before they affect backup or other data transfer operations.

---

**T**

**Tape drive** A device that spins disks and tapes while it reads and writes data in storage.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** The communications protocol used by the Internet. It runs on top of Ethernet to provide high-level networking services to applications.

**Topology** The logical and/or physical arrangement of stations on a network.

**Trap** An SNMP alert that is sent when predefined conditions are met. For example, an error trap tests for an error condition and provides a recovery routine.

---

**U**

**User ID** An alphanumeric value that the password database associates with a login name. Also, UID.

**UTC (Coordinated Universal Time)** The world-wide standard for time, commonly considered to be the equivalent of "Greenwich Mean Time" and "Zulu time." For all of these time standards, zero (0) hours is midnight in Greenwich England, which lies on the zero longitudinal meridian. The sequence of the letters in the acronym is a compromise between the English and French terms (*Temps Universel Coordonné*).

---

**W**

**WORM (Write Once, Read Many)** A common type of data storage medium, in which data can be read and reread, but not altered, after it has been recorded.

**WWNN (World Wide Node Name)** A unique number assigned by a recognized naming authority. The world wide name is integral to Fibre Channel operations.

**WWPN (World Wide Port Name)** The WWPN is a 64-bit, hard-coded address for each port on an FC-connected device. It is used to identify available SAN devices at end points.

---

**X**

**X-axis, X-position** The horizontal position of the library's robotic arm.

---

**Y**

**Y-axis, Y-position** The vertical position of the library's robotic arm.



# Index

---

---

## A

- aborting an operation 27
- About Library 206
- administrator privileges 81
- advanced reporting 14, 223
- all slots report 215
- authentication traps 46
- authorization code 69
- AutoClean 164
- autoleveling 304
- automatic EKM path diagnostics 184

---

## B

- back button, browser 28
- barcode
  - label requirements 337
  - labels, installing 339
  - scanner 3
  - supported formats 55, 338
- bezel, library, replacing 253
- browser back button 28

- browsers, supported 347
- bulk loading cartridges 155
- buttons
  - back, browser 28
  - navigation 3
  - navigation/selection 26
  - operator panel 27
  - power 3

---

## C

- cabling the library 227
- canceling an operation 27
- Capacity on Demand 13
- cartridges, see tape cartridges 336
- certificates, see encryption certificates
- chassis, removing and replacing 258
- cleaning cartridges
  - exporting 167
  - importing 165
  - valid 164
- cleaning log 217
- cleaning slots, configuring 61

- cleaning tape drives 163
  - automatic 164
  - manually 169
- COD, see Capacity on Demand 13
- community string 47
- configuration
  - default 40
  - record 212
  - report 210
  - restoring 108
  - saving 107
- contact information
  - customer 78
  - Quantum xxvi
- control path 67
- copyright 224
- customer contact information 78

---

## D

- data encryption keys
  - depletion of 192
  - exporting 196, 199
  - generating 181, 191, 195
    - at initial setup 192
    - manually 193

- when 100% depleted 192
- when 80% depleted 192
- importing 196, 201
- date, setting 49
- daylight saving time, setting 51
- default administrator account 80
- default configuration 40
- default gateway 43
- default password 81, 136
- default user name 81, 136
- defaults, resetting factory 333
- desktop kit
  - installing library in 244
  - removing library from 252
- DHCP 42
- diagnostic tickets
  - about 312
  - log 218
  - viewing, closing, and resolving 312, 313
- diagnostics 330
  - EKM path 179, 182
  - resetting a tape drive 331
  - robotics get/put 332
- disabling library managed encryption 194
- disposal information 359
- DNS addresses 43
- downgrading library firmware 108
- dust 17

---

## E

- EKM
  - about 175
  - license 15
  - path diagnostics 179
    - about 182
    - automatic 184
    - manual 183
- e-mail account, library 76

- e-mail notifications
  - about 72
  - creating 73
  - deleting 75
  - modifying 74
  - send snapshot 77
- emergency power-off procedure 144
- encryption certificates
  - exporting 196, 197
  - importing 196, 198
- encryption key management, see EKM
- encryption keys, see data encryption keys
- encryption, see EKM and SKM
- ESD precautions 226
- exiting an operation 27
- exporting
  - cleaning cartridges 167
  - data encryption keys 196, 199
  - encryption certificates 196, 197
  - tape cartridges 158
- external management applications 44

---

## F

- factory defaults, resetting 333
- fast scrolling 27
- filler plate
  - power supply, removing and installing 269
  - tape drive, removing and installing 269
- firmware
  - library, downgrading 108
  - library, updating 299
  - tape drive, autoleveling 304
  - tape drive, updating 304
- front panel 2

---

## G

- gateway 43
- generating data encryption keys 181, 191, 195
- get/put test 332

---

## H

- health status icons 26
- home page 30, 31
- host name 41

---

## I

- I/E station
  - opening 145
  - unlocking 145
- I/E station slots, configuring 63
- I/E station, unlocking more than one 146
- ICMP 104
- importing
  - cleaning cartridges 165
  - data encryption keys 196, 201
  - encryption certificates 196, 198
  - tape cartridges 152
  - tape cartridges, unassigned 153
- installation and verification test 325
- Internet browsers, supported 347
- internet control message protocol 104
- IP address
  - configuring 42
  - IPv4 42
  - IPv6 42
  - library 137
- IVT 325



---

**K**

- Kerberos 94
- Kerberos service keytab file 96
- key, public 196
- keys, see data encryption keys

---

**L**

- LDAP
  - accounts 88
  - configuring 90
  - server guidelines 89
- LEDs 320
  - front panel 321
  - power supply 324
  - power-on 3
  - system control board 322
  - tape drive/sled 323
  - ticket indicator 3
- library configuration
  - record 212
  - report 210
  - saving 107
- library managed encryption
  - disabling 194
- library name 41
- library not ready messages 318
- licensable features 69
- license key certificate 69
- license keys
  - about 69
  - applying 71
  - chassis replacement and 69
  - obtaining 70
  - SCB replacement and 70
  - viewing 70
- licenses
  - encryption key management (EKM) 15
  - report 223
  - viewing 70

- loading tape drives 160
- local user accounts
  - about 79
  - creating 82
  - deleting 84
  - modifying 83
- location coordinates
  - slot 5
  - tape drive 9
- logged in user's report 215
- logging off 138
  - automatically 138
- logging on
  - first time 136
  - Kerberos enabled 138
  - LDAP enabled 138
  - operator panel 137
  - simultaneous 136
  - Web client 137
- logical serial number addressing 99
- logs
  - cleaning 217
  - diagnostic tickets 218
  - SKM encryption key import
    - warning log 202, 219
  - SKM server 202
  - tape drive 220, 320

---

**M**

- magazines
  - description 4
  - releasing 148
  - removing and replacing 271
  - test 327
- manual cartridge assignment 100
- manual EKM path diagnostics 183
- mask, subnet 43
- media barcode formats 55
- menu trees 33
- MIB, SNMP 47
- move test 329

- moving tape cartridges 156
- moving the library 292

---

**N**

- navigation buttons 3
- network interface 103
- network prefix 43
- network settings
  - changing 40
  - configuring 40
  - report 214, 222
- network time protocol 49
- NTP 49

---

**O**

- online/offline
  - library 145
  - partitions 59
  - tape drives 172
- open source license agreement 223
- opening the I/E station 145
- operator panel
  - buttons 27
  - changing home screen view 109
  - description 2
  - functions 24
  - layout 22
  - passwords 84
  - power save 101

---

**P**

- packaging the library 292
- partitions
  - about 51
  - access 59
  - automatic creation 53

- deleting 57
- description 12
- manual creation 54
- modifying 56
- reports 221
- taking online/offline 59
- viewing 58
- passwords, operator panel
  - creating 84
  - disabling 87
  - misplaced 88
  - modifying 87
  - resetting 88
- passwords, Web client
  - creating 82
  - default 81, 136
  - misplaced 137
  - modifying 83
- path diagnostics, EKM 179, 182
  - automatic 184
  - manual 183
- popup blockers 28
- power button 3
- power save 101
- power supply
  - description 8
  - removing and installing 276
- power-off, emergency 144
- power-on LED 3
- privilege levels 81
- public key 196

---

## R

- rack
  - installing library in 241
  - removing library from 243
- rack mount kit, installing 229
- rail kit, see rack mount kit 229
- random move test 329
- registering the library 109

- releasing magazines 148
- remote access, enabling/disabling 105
- remote authentication 88
- remote service login 105
- removing power 139, 144
- reports
  - about 206
  - advanced reporting 223
  - all slots 215
  - date/time 223
  - library configuration 210
  - licenses 223
  - logged in users 215
  - network settings 214, 222
  - operator panel 221
  - partition 221
  - system information 206
  - tape drives 222
- resetting factory defaults 333
- resetting tape drive 331
- restart 139, 142
- restoring the library configuration 108
- restraint, robot 19
- robot 3
  - get/put test 332
  - releasing 19
  - restraint 19
  - test 327
- running out of keys 192

---

## S

- saving the library configuration 107
- Scalar Key Manager, see SKM
- scanner, barcode 3
- SCB, see system control board 8
- scrolling, fast 27
- secure socket layer, enabling/disabling 106

- security settings 103
- service port 78
- session timeout 97
- setup wizard 39
- sharing encrypted tapes 195
- shipping the library 292
- shut down 139, 140
- SKM
  - about 175
  - configuring 176
  - encryption key import warning log 202, 219
  - installing on servers 177
  - logs 202, 219
  - partition configuration 179
  - server configuration 177
  - server log 202
  - TLS certificates 179
- slots, location coordinates 5
- SMI-S, enabling/disabling 101
- SNMP
  - authentication traps 46
  - community string 47
  - configuring 44
  - enabling/disabling 101
  - MIB, downloading 47
  - versions 46
- specifications 341
- SSH services, enabling/disabling 104
- SSL, enabling/disabling 106
- subnet mask 43
- subsystem status 32
- system control board
  - description 8
  - removing and replacing 279
- system information report 206
- system settings 98
- system summary 31

---

**T**

Tape Alerts 349

tape cartridges

- bulk loading 155
- exporting 158
- importing 152
- map, creating 271
- moving 156
- proper handling 336
- storing 336
- unassigned 153
- write protecting 337

tape drives

- autoleveling 304
- cleaning, about 163
- cleaning, automatically 164
- cleaning, manual 169
- description 9
- loading 160
- location coordinates 9
- log 220
- online/offline 172
- parameters, configuring 65
- removing and replacing 286
- reports 222
- resetting 331
- test 327
- unloading 161

TCP 45

test LDAP 94

tests

- installation and verification (IVT) 325
- magazine 327
- random move 329
- robotics 327
- robotics get/put 332
- tape drive 327

ticket indicator LED 3

time zone, setting 50

time, setting 49

timeout 97

TLS certificates

- installing 179
- Quantum-supplied 188
- user-supplied 189

traps 46

troubleshooting 311

turning off 139, 143

---

**U**

UDP 45

unassigned tape cartridges, importing 153

unload assist 98

unloading tape drives 161

unlocking the I/E station 145

unpacking the library 17

updating library firmware 299

user name, default 81, 136

user privileges 81

---

**W**

Web client

- description 28
- display 31
- home page 30, 31

WORM 13

write protecting cartridges 337

