



HPE Storage MSL2024 G4 Tape Library User and Service Guide

Part Number: 20-STG-MSL2024G4-USG-ED2

Published: July 2026

Edition: 2

HPE Storage MSL2024 G4 Tape Library User and Service Guide

Abstract

This guide provides information on installing, configuring, upgrading, and troubleshooting the tape library. This guide is intended for system administrators and other users who need physical and functional knowledge of the tape library. This guide applies to MSL2024 G4 with product number, AK379B. Regulatory model number: LVLDC-0501, Type: 2U.

Part Number: 20-STG-MSL2024G4-USG-ED2

Published: July 2026

Edition: 2

© Copyright 2006–2026 Hewlett Packard Enterprise Development LP

Notices

The information provided here is subject to change without notice. Hewlett Packard Enterprise's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hewlett Packard Enterprise is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hewlett Packard Enterprise to possess, use, or copy the software. In accordance with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under the vendor's standard commercial license.

Links to third-party websites will take you outside of the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for the information outside the Hewlett Packard Enterprise website.

Acknowledgments

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All third-party marks are the property of their respective owners.

Table of contents

Description.....	12
Hardware overview.....	12
Front panel components.....	13
OCP LEDs.....	14
Back panel components.....	15
Controller health status indicators.....	15
Tape drive back panels.....	16
LTO-6 FC tape drive back panels.....	17
LTO-7, LTO-8, and LTO-9 FC tape drive back panel.....	17
LTO-6 SAS tape drive back panel.....	18
LTO-7, LTO-8, and LTO-9 SAS tape drive back panel.....	19
Installation.....	20
Location requirements.....	21
FC connection information.....	22
SAS connection information.....	23
Preparing the host.....	25
Unpacking the shipping container.....	26
Removing the shipping lock	27
Installing the library in a rack	29
Installing tape drives.....	32
Connecting the FC cable.....	34
Connecting the SAS cable.....	34
Powering on the library	36
Setting up the RMI.....	37
Logging into the OCP.....	38
Verifying the host connection.....	39
Understanding the user interface.....	39
Users and roles.....	40
The RMI.....	41
The OCP.....	43
OCP menu.....	44
Home screen	48
OCP buttons.....	49
Configuration.....	50

HPE Storage 1/8 Tape Autoloader and MSL Tape Libraries Encryption Kit	50
Network port requirements.....	51
Hardware-based encryption	52
KMIP-based key servers.....	52
Application-managed encryption.....	53
Configuring through RMI.....	54
Initial configuration wizard.....	54
System.....	56
Save or restore configuration.....	56
Saving configuration file.....	57
Restoring configuration file.....	57
Resetting default settings.....	57
Resetting the list of known drives.....	57
Setting time zone, date, time, and SNTP.....	58
Setting the time zone.....	58
Setting the date and time format.....	59
Setting the date and time	59
Enabling SNTP (Simple Network Time Protocol) synchronization.....	60
Media barcode compatibility check.....	60
Enabling media barcode compatibility check.....	61
Disabling media barcode compatibility check.....	61
Managing license keys.....	62
Setting RMI language.....	62
Barcode handling configuration.....	63
Configuring additional features.....	63
Network.....	63
Network management.....	64
SNMP.....	64
Adding an SNMP target.....	65
Editing an SNMP target.....	67
Deleting an SNMP target.....	68
Clearing all SNMPv3 options.....	68
Simple Mail Transfer Protocol (SMTP).....	68
Remote logging (rsyslog).....	70
Drives.....	71
Configuring the FC interface.....	75
Powering on a tape drive from the RMI.....	75
Powering off a tape drive from the RMI.....	76

Disabling Secure Mode for an LTO-6 tape drive.....	76
Mailslot.....	77
Partitions.....	77
Using the basic partition wizard.....	78
Using the expert partition wizard.....	80
Deleting a partition using the expert partition wizard.....	83
Encryption.....	83
Setting the default configuration mode for new partitions.....	84
Allowing the administrator to configure encryption with the Expert Partition Wizard...	84
Setting the encryption mode for a partition.....	85
MSL Encryption Kit configuration.....	85
Entering the key server token password when using the MSL Encryption Kit.....	86
Viewing the keys on the key server token when using the MSL Encryption Kit.....	86
Changing the key server token password when using the MSL Encryption Kit.....	86
Changing the key server token name when using the MSL Encryption Kit.....	87
Generating a new write key when using the MSL Encryption Kit.....	87
Configuring automatic key generation when using the MSL Encryption Kit.....	88
Backing up the key server token data to a file when using the MSL Encryption Kit.....	88
Restoring key server token data from a backup file when using the MSL Encryption Kit.....	89
Configuring the key server token login behavior when using the MSL Encryption Kit.....	90
Using the KMIP wizard.....	90
Configuring FIPS Support Mode.....	92
FIPS Support Mode prerequisites.....	93
User accounts.....	94
User account settings.....	94
Password rules.....	95
Allowing magazine or mailslot access by the user role.....	95
Local user accounts.....	96
Adding a local user account.....	96
Removing a local user account.....	97
Setting or modifying a user password.....	97
Changing the OCP PIN from the RMI.....	98

LDAP.....	98
Configuring LDAP servers.....	99
Configuring LDAP users.....	100
Configuring HPE Storage Command View for Tape Libraries integration.....	101
Removing the CVTL Management Station trap destination.....	103
Moving CVTL access to a new management station.....	103
Web management.....	103
Enabling secure communications.....	104
Creating a custom certificate.....	104
Backing up a custom certificate.....	105
Restoring a custom certificate.....	106
Configuring session timeout.....	106
Enabling OCP/RMI session locking.....	106
Restricting RMI log in.....	107
Secure Manager.....	107
Enabling Secure Manager.....	108
Creating an access group when using Secure Manager.....	108
Changing the name of an access group when using Secure Manager.....	109
Deleting an access group when using Secure Manager.....	110
Adding a host to an access group when using Secure Manager.....	110
Removing a host from an access group when using Secure Manager.....	111
Configuring device access when using Secure Manager.....	111
Creating a host when using Secure Manager.....	111
Changing the name of a host when using Secure Manager.....	112
Deleting a host when using Secure Manager.....	112
Configuring through OCP.....	113
Changing the OCP PIN from the OCP.....	113
Resetting the RMI administrator password.....	114
Library network overview	115
Configuring IPv4 network settings.....	115
Configuring IPv6 network settings.....	116
Configuring IPv4 networking from the OCP.....	116
Finding the IPv4 IP address obtained through DHCP.....	117
Reset to default settings.....	118
Saving the configuration settings to a USB flash drive.....	118
Restoring the configuration settings from a USB flash drive.....	119
Downloading product firmware.....	119
Resetting the RMI administrator password and OCP PIN.....	120

Maintenance.....	121
Maintenance through RMI.....	121
Library tests.....	121
Performing the system test.....	121
Performing the slot to slot test.....	122
Performing the element to element test.....	123
Performing the position test.....	124
Performing the wellness test.....	124
Performing the robotic test.....	125
Logs and traces.....	125
Viewing log files.....	125
Downloading log and trace files.....	126
Firmware upgrades.....	126
System firmware.....	126
Drive firmware.....	127
Updating library firmware from the OCP.....	127
Download support ticket.....	128
Drive support ticket.....	128
Library support ticket.....	129
System reboot.....	129
Drives.....	129
Rebooting a tape drive.....	129
Clearing drive reservations.....	130
Controlling the UID LED.....	130
Starting LTO-9 New Media Initialization Wizard.....	131
Initialization estimated times.....	132
Maintenance through OCP.....	133
Saving a support ticket	133
Saving log files.....	134
Upgrade library firmware.....	134
Saving drive support ticket.....	135
Upgrade drive firmware from a USB flash drive.....	136
Updating drive firmware from OCP.....	137
Firmware verification and configuration backup procedure.....	137
Operations.....	139
Command View TL TapeAssure.....	139
LTFS Support.....	139
Operating through RMI.....	139

Moving media.....	140
Opening a mailslot.....	141
Opening a magazine	141
Initiating a drive cleaning operation.....	142
Rescanning the cartridge inventory.....	142
Forcing a drive to eject a cartridge.....	142
Difficulty ejecting a cartridge.....	143
Operating through OCP	143
Unlocking magazines.....	144
Unlocking mailslot.....	144
Status.....	144
Viewing status information through RMI.....	145
Library status.....	145
Library information and status.....	145
Cartridge inventory.....	146
Using the partition map graphical view.....	147
Using list views.....	147
Partition map.....	148
Configuration Status screen parameters.....	149
Viewing drive status.....	150
Drive Status configuration settings.....	150
Network status.....	153
Network Status screen parameters.....	154
Command View TL status parameters.....	155
Security.....	155
Encryption status parameters.....	156
Viewing Secure Manager status.....	156
Secure Manager status parameters.....	156
Viewing status information through OCP.....	157
Viewing library information	158
Viewing drive information.....	159
Viewing network status.....	160
Viewing cartridge inventory.....	160
Working with tape cartridges and magazines.....	161
Recommended practices for labeling tape cartridges.....	161
Tape cartridges.....	163
LTO-9 Media initialization.....	164
LTO-7 Type M media for LTO-8 drives.....	164

Recommended practices for using and maintaining tape cartridges.....	165
Write-protecting data cartridges.....	165
Read and write compatibility.....	166
Supported media.....	167
Magazines.....	169
MSL2024 magazine slot numbering.....	170
Releasing the magazines manually.....	170
Opening a magazine from the OCP.....	173
Storage slots.....	173
Unlocking the mailslot (Unlock Mailslot).....	175
The mailslot cannot be opened.....	176
Upgrading and servicing the library.....	176
Possible tools needed.....	178
Secure Mode.....	178
Disabling Secure Mode for an LTO-7 or later tape drive.....	179
Installing or replacing a tape drive.....	179
Removing a drive bay cover for new drive installation.....	181
Removing a tape drive.....	181
Installing the new tape drive	182
Verifying the tape drive installation.....	184
Removing and replacing a magazine.....	185
Removing a magazine using the MSL2024 OCP	185
Releasing magazines using the RMI	186
Releasing the magazine using the manual magazine release.....	187
Replacing the power supply	189
Removing and replacing the library controller.....	191
Identifying the failed component.....	192
Saving the library configuration.....	192
Powering off the Library.....	193
Preparing to remove the controller board.....	193
Removing a library controller board.....	193
Replacing the library controller.....	194
Completing the library controller replacement.....	195
Verifying the library controller installation.....	196
Removing and replacing the chassis.....	196
Removing the tape cartridge from the tape drive.....	198
Removing the cables, magazines, and tape drive	199
Removing the power supply and library controller	200

Removing the library controller	201
Removing the chassis.....	202
Verifying the chassis replacement.....	203
Replacing the shipping lock on the old chassis.....	204
Repackaging the old chassis.....	205
Installation and replacement of the library rack kit.....	209
Removing the cartridges from tape drives.....	210
Removing the cartridges from the magazines using the OCP.....	211
Removing the cartridges from the magazines using the RMI.....	212
Removing the cartridges from the magazines using the manual release.....	213
Removing the library.....	214
Removing the old rails.....	215
Securing the rails to the rack.....	215
Installing the library.....	216
Tape drive cleaning.....	217
The auto cleaning feature.....	217
Auto cleaning configuration.....	218
Troubleshooting.....	218
The library displays errors.....	218
Fibre Channel connection problems.....	219
Detection problems after installing a SAS drive.....	219
Operation problems.....	221
Performance problems.....	228
Average file size.....	229
File storage system	229
Connection from the backup server to the disk array.....	230
Backup/archive server.....	230
Backup/archive software and method.....	230
Connection from the archive/backup host server to the library	231
Data cartridges.....	231
Tape drive read or write performance seems slow.....	231
The wellness test.....	232
Running the wellness test.....	233
Error codes.....	234
Finding library logs on the RMI.....	235
Generating a report or support ticket from L&TT.....	235
Downloading a support ticket from the library.....	236
Viewing a downloaded support ticket.....	236

Finding error code information on an L&TT support ticket or report.....	236
Error events.....	239
Warning events.....	262
Configuration change events.....	284
Informational events.....	286
Diagnosing problems with Library & Tape Tools.....	289
Electrostatic discharge.....	290
Preventing electrostatic damage.....	290
Grounding methods.....	291
Technical specifications.....	291
Physical specifications.....	292
Environmental specifications.....	292
Electrical specifications.....	293
Regulatory specifications.....	294
Regulatory compliance identification numbers.....	295
Default and restore defaults settings.....	295
Websites.....	297
Accessing the compatibility matrix.....	297
HPE Storage library websites.....	298
Support and other resources.....	298
Accessing Hewlett Packard Enterprise Support.....	298
HPE product registration.....	299
Accessing updates.....	299
Remote support.....	300
Warranty information.....	300
Regulatory information.....	301
Documentation feedback.....	301

Description

The HPE Storage MSL2024 G4 Tape Library provides compact, high-capacity, low-cost solutions for simple, unattended data backup. This unique design houses up to 12 tape cartridges for each U of height. Tape cartridges can be accessed through removable magazines and mailslots. Each magazine holds up to 12 tape cartridges.

The libraries are compatible with most operating systems. However, the libraries require either direct support from the operating system or a compatible backup application to take full advantage of their many features. To verify compatibility, see [Accessing the compatibility matrix](#).

The libraries are customer expandable with exchangeable tape drives. The libraries support Ultrium half-height tape drives. For the tape drives now available for the library, see <https://www.hpe.com/storage/tape>.

Hardware overview

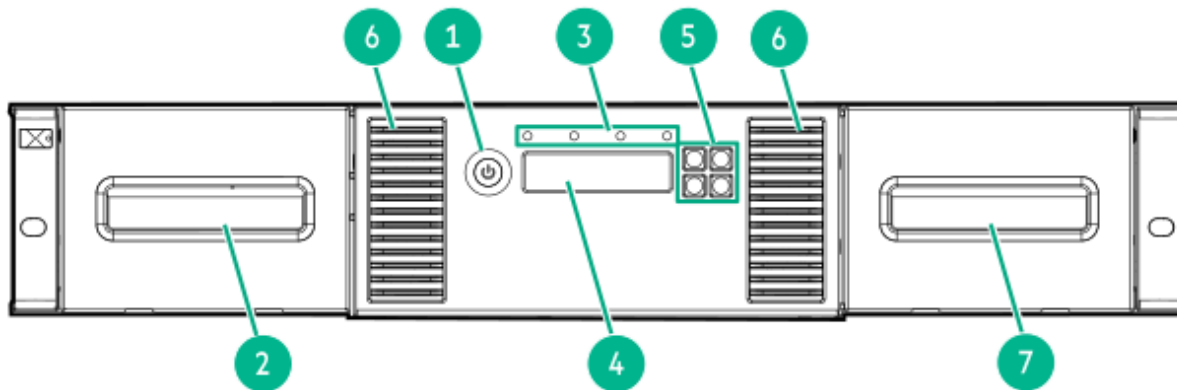
Subtopics

[**Front panel components**](#)

[**Back panel components**](#)

[**Tape drive back panels**](#)

Front panel components



Item	Description
1	Power button
2	Magazine with configurable mailslots
3	Operator Controller Panel (OCP) LEDs
4	LCD screen
5	Control keys
6	Air vents
7	Magazine

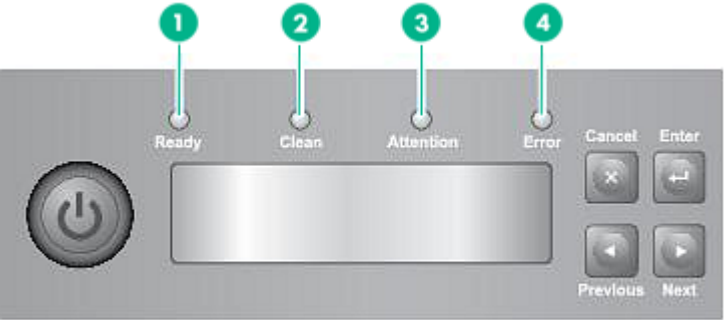
For OCP functions, see [Using the OCP](#).

Subtopics

OCP LEDs

OCP LEDs

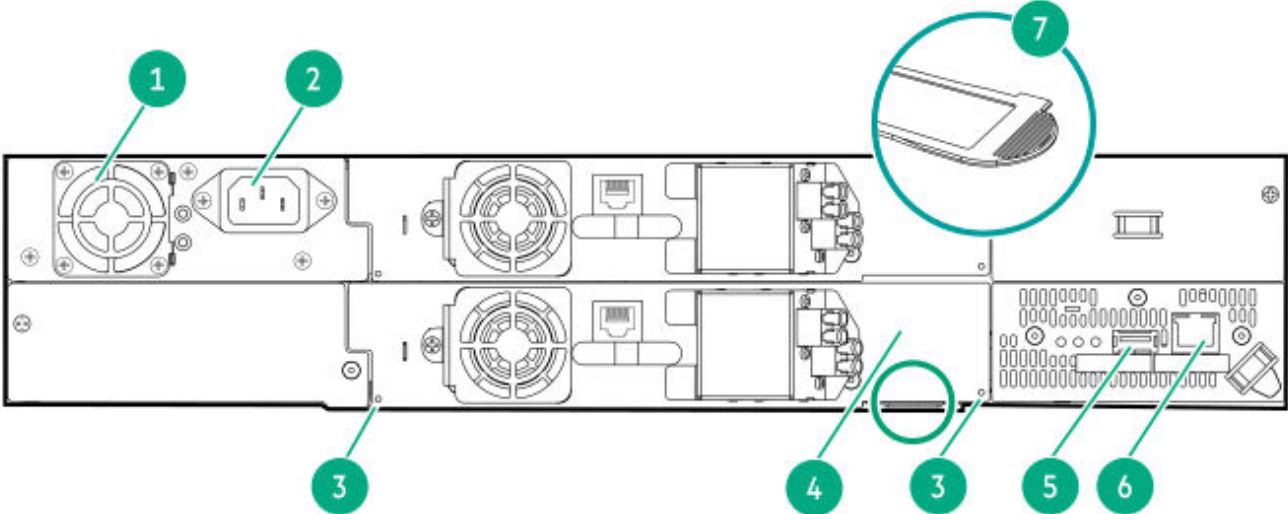
The OCP includes four LEDs that provide a summary of the library status.



11159

Item	Label	Color	Description
1	Ready	Green	Illuminated when power is on. Blinking when there is tape drive or robotics activity.
2	Clean	Amber	Illuminated when the tape drive has determined that a cleaning cartridge should be used. Cleaning is only necessary when the device directs you to do so. Extra cleaning is not necessary.
3	Attention	Amber	Illuminated if the device has detected a condition that requires attention by the operator.
4	Error	Amber	Illuminated if an unrecoverable error occurs. A corresponding error message displays on the LCD screen.

Back panel components



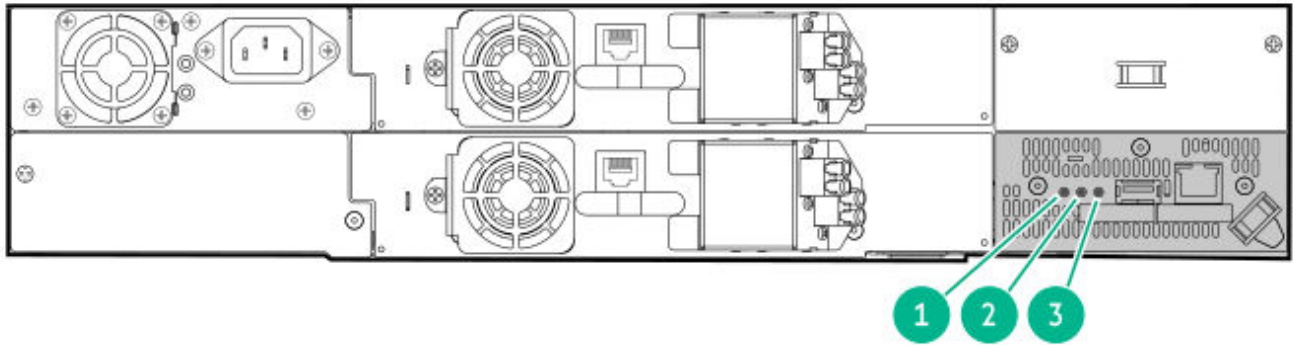
1. Fan	2. Power connector
3. Manual magazine release hole	4. Tape drive assembly
5. USB port	6. Ethernet port
7. Pull-out tab containing the serial number and other product information	

Subtopics

Controller health status indicators

Controller health status indicators

The controller health status LED indicators are located on the back panel to the right.



Item	Color	Description
1	Blue	Unit identifier (UID)
2	Amber	Error
3	Green	Controller health status LED - Pulses on and off in approximately one second cycles during normal operation. - Solid green or not illuminated (pulsing) while the library is powered on indicates th at the controller is not operating correctly. If the controller health status LED is solid green or not illuminated (pulsing), see the Operation problems topic for additional i nformation.

Tape drive back panels

Subtopics

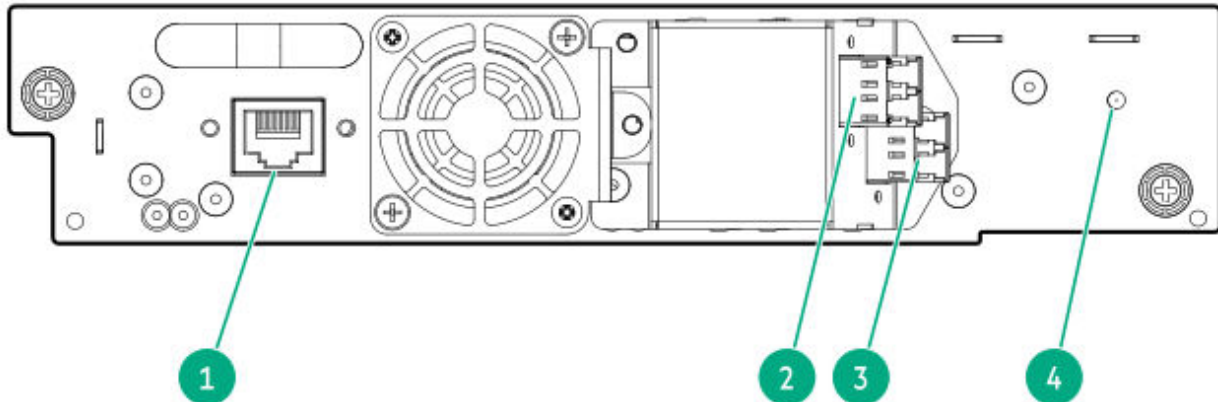
[LTO-6 FC tape drive back panels](#)

[LTO-7, LTO-8, and LTO-9 FC tape drive back panel](#)

[LTO-6 SAS tape drive back panel](#)

[LTO-7, LTO-8, and LTO-9 SAS tape drive back panel](#)

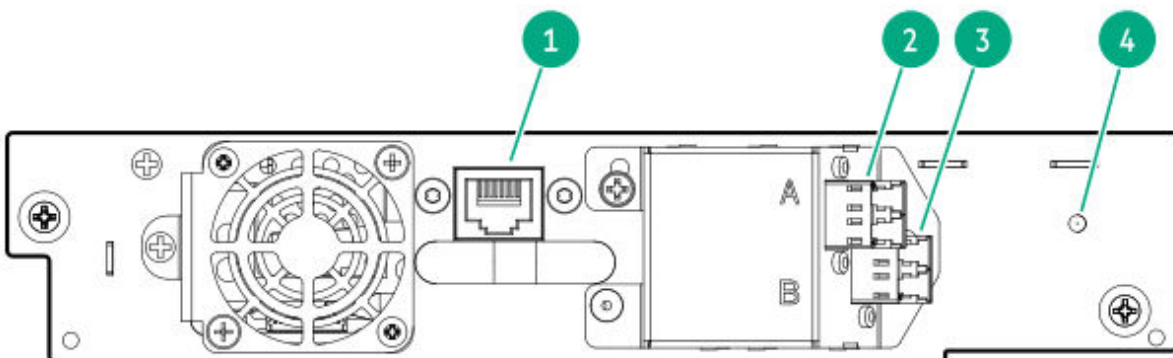
LTO-6 FC tape drive back panels



Item	Description
------	-------------

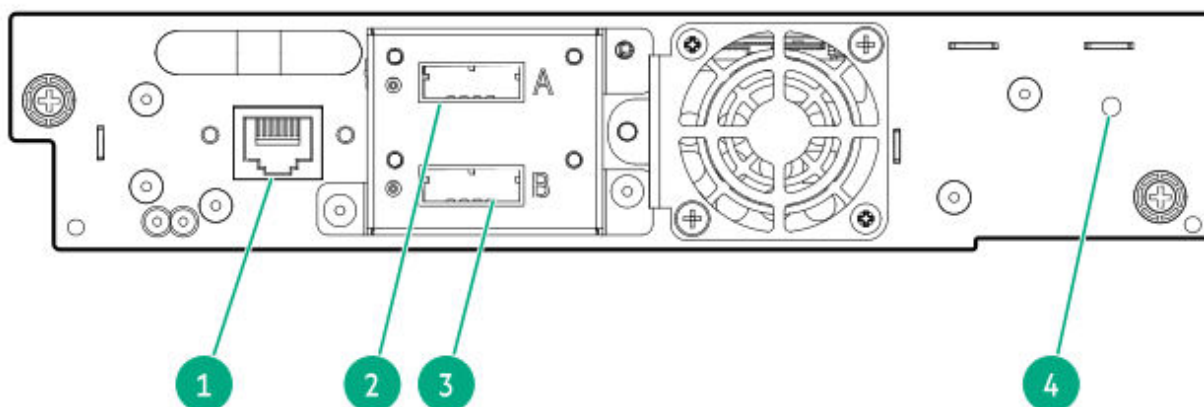
- | | |
|---|-----------------------------|
| 1 | Tape drive Ethernet port |
| 2 | FC port A |
| 3 | FC port B |
| 4 | Tape drive power LED, green |

LTO-7, LTO-8, and LTO-9 FC tape drive back panel



Item	Description
1	Tape drive Ethernet port
2	FC port A
3	FC port B
4	Tape drive power LED, green

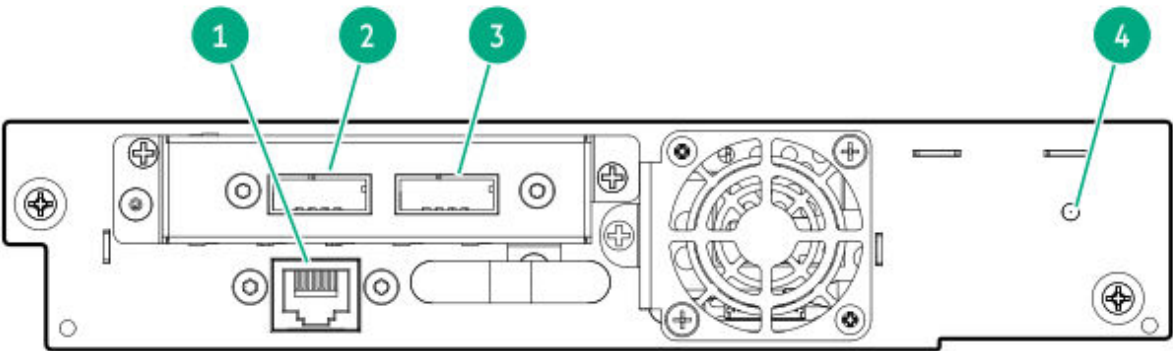
LTO-6 SAS tape drive back panel



Item	Description
1	Tape drive Ethernet port
2	SAS port A
3	SAS port B
4	Tape drive power LED, green

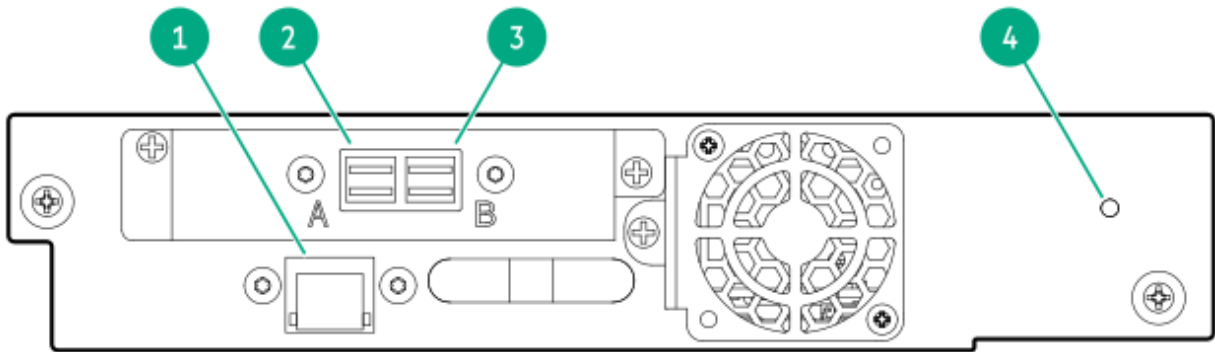
LTO-7, LTO-8, and LTO-9 SAS tape drive back panel

LTO-7 and LTO-8 SAS tape drive back panel



Item	Description
1	Tape drive Ethernet port
2	SAS port A
3	SAS port B
4	Tape drive power LED, green

LTO-9 SAS tape drive back panel



Item	Description
1	Tape drive Ethernet port
2	SAS port A

Item	Description
3	SAS port B
4	Tape drive power LED, green

Installation

Procedure

1. Plan the installation.
 - [Location requirements](#)
 - [FC configuration information](#)
 - [SAS configuration information](#)
2. [Prepare the host](#)
3. [Unpack the shipping container](#)
4. [Remove the shipping lock](#)
5. [Install the library in a rack](#)
6. [Install tape drives](#)
7. [Connect the FC cable](#)
8. [Connect the SAS cable](#)
9. [Powering on the library](#)
- .0. [Setting up RMI](#)
- .1. [Setting up OCP](#)
- .2. [Verify the connection](#)

Subtopics

[Location requirements](#)

[FC connection information](#)

[SAS connection information](#)

[Preparing the host](#)

- Unpacking the shipping container**
- Removing the shipping lock**
- Installing the library in a rack**
- Installing tape drives**
- Connecting the FC cable**
- Connecting the SAS cable**
- Powering on the library**
- Setting up the RMI**
- Logging into the OCP**
- Verifying the host connection**

Location requirements

If you plan to mount the library in a rack, select an open rack location with access to the host server and a power outlet. If possible, install the library in the middle or higher part of the rack to avoid dust from the floor and to allow easy access to the mailslot and magazines.

Select an open rack location with access to the host server and a power outlet. If possible, install the library in the middle or higher part of the rack to avoid dust from the floor and to allow easy access to the mailslot and magazines.

Table 1. Location criteria

Criteria	Definition
Rack requirements	HPE G2 Enterprise Series, Enterprise Series, G2 Advanced Series, Advanced Series, Standard Series, and other HPE square-hole or round-hole racks
Rack space requirements	2U
Operating temperature	10-35° C (50-95° F) for the tape library. Some tape drives have a more limited ambient temperature range and/or have a more limited temperature range when operating at high altitudes. Verify the tape drive operating requirements before installing a tape drive. See Environmental specifications.
Power source	AC power voltage: 100-240 VAC Line frequency: 50-60 Hz Place the library near an AC outlet. The AC power cord is the main AC disconnect device for the library and must be easily accessible at all times.

Criteria	Definition
Approximate weight with two drives and no media	17 kg (37.4 lb)
Approximate weight with two drives and media	22 kg (48.4 lb)
Air quality	Place the library in an area with minimal sources of particulate contamination. Avoid areas near frequently used doors and walkways, stacks of supplies that collect dust, printers, and smoke-filled rooms. Excessive dust and debris can damage tapes and tape drives.  CAUTION Chemical contaminant levels in customer environments for Hewlett Packard Enterprise hardware products must not exceed G1 (mild) levels of Group A chemicals at any time as described in the current version of ISA-71.04-2013 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants.
Humidity	20-80 percent relative humidity noncondensing
Clearance	Back: Minimum of 15.4 cm (6 inches) Front: Minimum of 30.8 cm (12 inches) Sides: Minimum of 5.08 cm (2 inches)



TIP

Temperature and humidity specifications are more tightly controlled for tape media, tape drives, and tape library than many other products installed in the data center. Ensure that the tape media and drives reside in an area within the temperature and humidity specifications.

FC connection information

Connect the FC tape drive directly to the server with a Host Bus Adapter (HBA) or indirectly through a SAN with an FC switch.

Table 1. FC drive interface speeds

LTO generation	Supported speeds
LTO-6, LTO-7, LTO-8, LTO-9	2 Gb, 4 Gb, 8 Gb

HPE Storage MSL supported tape drives have two FC ports. Only one port can be used at a time, but both ports can be connected for path failover or with software that supports multipath. If you are using only one port, you can use either port. Path failover is a licensed library feature.

Direct connection

The host must have a 2 Gb, 4 Gb, 8 Gb, 16 Gb, or 32 Gb FC HBA. An 8 Gb or faster HBA is recommended for LTO-6 and later generation tape drives. To verify that an HBA is supported on your server and qualified for the tape drive, see [Accessing the compatibility matrix](#).

A server that has FC-attached hard drives performs best with at least two FC ports. Using the same FC port for disk and tape drive access can cause performance degradation.

SAN connection

All switches between the host and the tape drive must be of the appropriate type. A 2 Gb switch in the path might cause performance degradation when backing up highly compressible data.

Configure zoning on the FC switch so that only the backup servers can access the tape drive. For more information, see the switch documentation.

Cable requirements

An FC cable is required for each FC port that you plan to use. The tape drive has an LC-style connector. The maximum cable length is based on the tape drive and external cable type.

Drive type	Cable type	2 Gb	4 Gb	8 Gb
All	OM2	0.5 - 300 m	0.5 - 150 m	Not supported
LTO-6, LTO-7, LTO-8, LTO-9	OM3, OM4	0.5 - 500 m	0.5 - 380 m	0.5 - 150 m

SAS connection information

The server must have a SAS host bus adapter with an external connector.

Table 1. SAS drive interface speeds

LTO generation	Supported speeds
LTO-6, LTO-7, LTO-8	1.5 Gb, 3 Gb, 6 Gb
LTO-9	3 Gb, 6 Gb, 12 Gb

The library uses two Small Computer System Interface (SCSI) logical unit numbers (LUNs) and requires an HBA with multiple LUN support. Most Hewlett Packard Enterprise SAS RAID controllers support tape devices; many other SAS RAID controllers do not support tape devices. To verify the specifications of your HBA or find a list of compatible HBAs, see [Accessing the compatibility matrix](#).

**CAUTION**

- Do not connect the library to a SAS RAID controller unless the compatibility matrix shows that the controller is qualified with the library. The server might not be able to boot when the library is connected to an unsupported SAS RAID controller.
- Reliable data transfer requires high-quality cables and connections.
 - Always verify that the SAS cable is rated for the data transfer speed of the HBA and tape drive.
 - Do not use adapters or converters between the HBA and the tape drive. SAS signal rates require clean connections and a minimum number of connections between the HBA and the tape drive.
 - SAS cables described as "equalized" might not support 6 Gb/s or 12 Gb/s data rates. Do not use equalized cables with LTO-6 or later generation tape drives unless these cables are verified for 6 Gb/s or 12 Gb/s data rates.
 - For optimal performance, only use cables of the length specified as qualified for your products. If not using the HPE-supplied cable and the SAS link is operating at 6 Gb/s, the maximum SAS cable length is 6 meters. If operating at 12 Gb/s, then the maximum cable length is 4 meters.

Cable requirements

Most SAS HBA ports have four SAS channels. A tape drive uses one channel, so each HBA port can support up to four tape drives. You can use a cable with one connector on each end, but only one channel will be used. The SAS fanout cable recommended for use with the library can connect up to four SAS tape drives to a single SAS HBA port.

For proper operation, use the cable specified in the QuickSpecs, which can be found on the **Resources** page for your library on the tape product information website: <https://www.hpe.com/storage/tape>.

Connectors

The host end of the cable must have the same type of connector as the HBA external SAS port.

The LTO-9 tape drive has an HD mini-SAS connector. Earlier generation tape drives have a mini-SAS connector. The mini-SAS connector is keyed in location 4, which is the standard location for end devices. If you use a cable other than the one recommended for use with the product, verify that it is keyed in location 4.



CAUTION

Mini SAS connectors are keyed. Do not force a SAS cable mini-SAS connector into the tape drive mini-SAS port because it might be keyed differently.

Preparing the host

Procedure

- If you are not the system administrator of the host computer, check with the system administrator before powering off the computer.
- For a library with SAS drives, confirm availability or install a SAS HBA that supports multiple LUNs.
- For a library with direct-attach Fibre Channel drives, confirm availability or install an FC HBA.
- Verify that multiple LUN support is enabled on the HBA and operating system. See the host computer and HBA documentation for installation information.
- For a library with Fibre Channel drives connected through a compatible switch, verify that sufficient ports are available.
- Install the application software and compatible drivers on the host computer. See the application software manuals for installation and configuration information.
- Install the Library & Tape Tools (L&TT) diagnostic utility to see what devices are connected to the host, verify the installation, upgrade firmware, and aid in troubleshooting.

Download L&TT without charge from: <https://www.hpe.com/support/TapeTools>.

Unpacking the shipping container

Prerequisites



CAUTION

If the temperature in the room where the library will be installed varies 15°C (30°F) from the room where it was stored, allow library to acclimate to the surrounding environment for at least 12 hours before unpacking the shipping container.

Procedure

1. Clear a level work surface near where you will place the library.
2. Inspect the container for shipping damage. If you notice any damage, report it to the shipping company immediately.
3. Remove the packaging, accessories, and library from the box one layer at a time.
4. Place the library on a level work surface.



CAUTION

Do not place the library on either end or its sides as doing so might damage it.

5. Carefully remove the foam padding and then the bag from the library.
6. Save the packaging materials for moving or shipping the library in the future.
7. Verify that you received the following components:
 - a. Library
 - b. Ethernet cable
 - c. Power cord
 - d. Two rack rails with packets of rack hardware
8. Verify that you have the necessary cables.
 - a. For a library with FC drives, it is important to provide an FC cable for each FC port you plan to use. See [FC connection information](#).
 - b. For a library with SAS drives, it is important to provide a SAS cable with the correct connector for your HBA. See [SAS connection information](#).

Removing the shipping lock

About this task



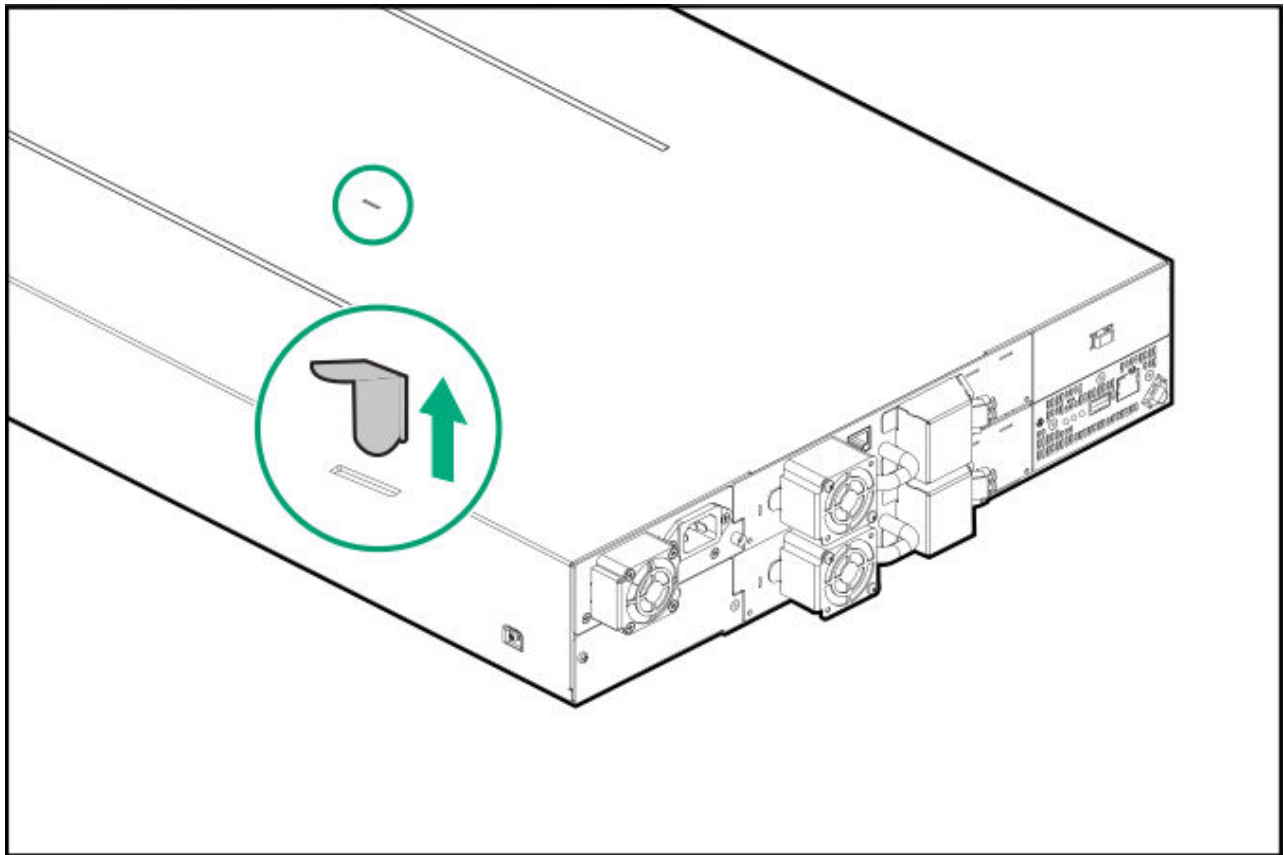
IMPORTANT

The shipping lock must be removed for the robotics to operate properly. A robot move error is displayed if the shipping lock is not removed.

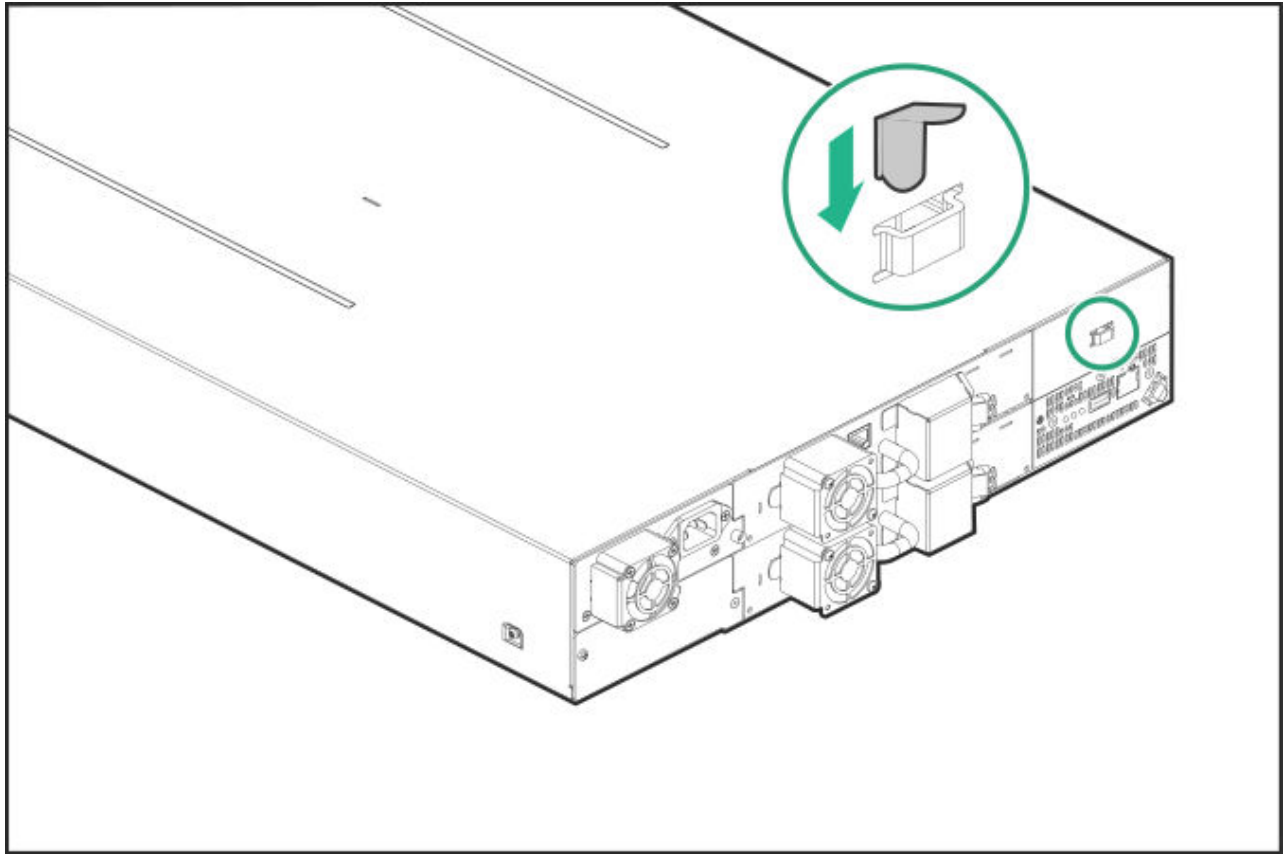
The shipping lock prevents the robotic transport mechanism from moving during shipment. Remove the shipping lock before powering on the library. The shipping lock is held in place with a piece of tape and is located in the top center of the library. After removing the shipping lock, store it on the back panel of the library for future use.

Procedure

1. Locate the tape and shipping lock at the top of the library.



2. Remove the tape, and then remove the lock.
3. Store the lock on the back panel.



Installing the library in a rack

Prerequisites

#2 and #3 Phillips screwdrivers



WARNING

To reduce the risk of personal injury or damage to equipment:

- Extend the leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install the rack stabilizer kit on the rack.
- Extend only one rack component at a time. Racks might become unstable if more than one component is extended.
- Slide/rail mounted equipment is not to be used as a shelf or a work space.
- Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed.
- Ensure that you are properly grounded when touching static sensitive components.

About this task



IMPORTANT

The library must be mounted on the enclosed rack rails. Placing the library on a surface, such as a table top or rack shelf, could result in library errors.



WARNING

The MSL2024 G4 weighs up to 17 kg (37.4 lb) without media and up to 22 kg (48.4 lb) with media (24 cartridges).

To reduce the risk of personal injury or library damage when moving the library:

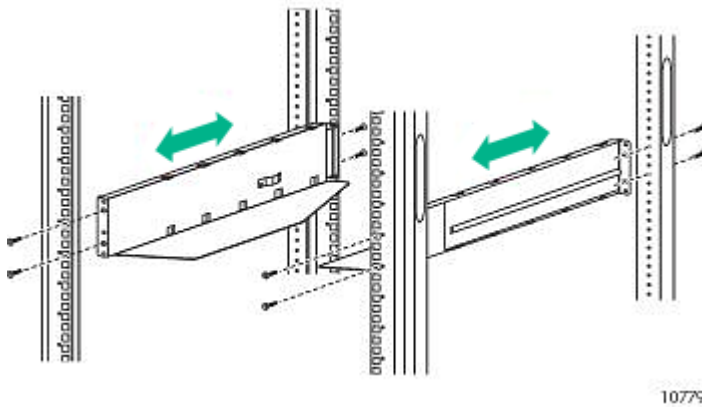
1. Observe local health and safety requirements and guidelines for manual material handling.
2. Always remove all tapes to reduce the overall weight of the library.
3. Obtain adequate assistance to lift and stabilize the library during installation or removal.

Procedure

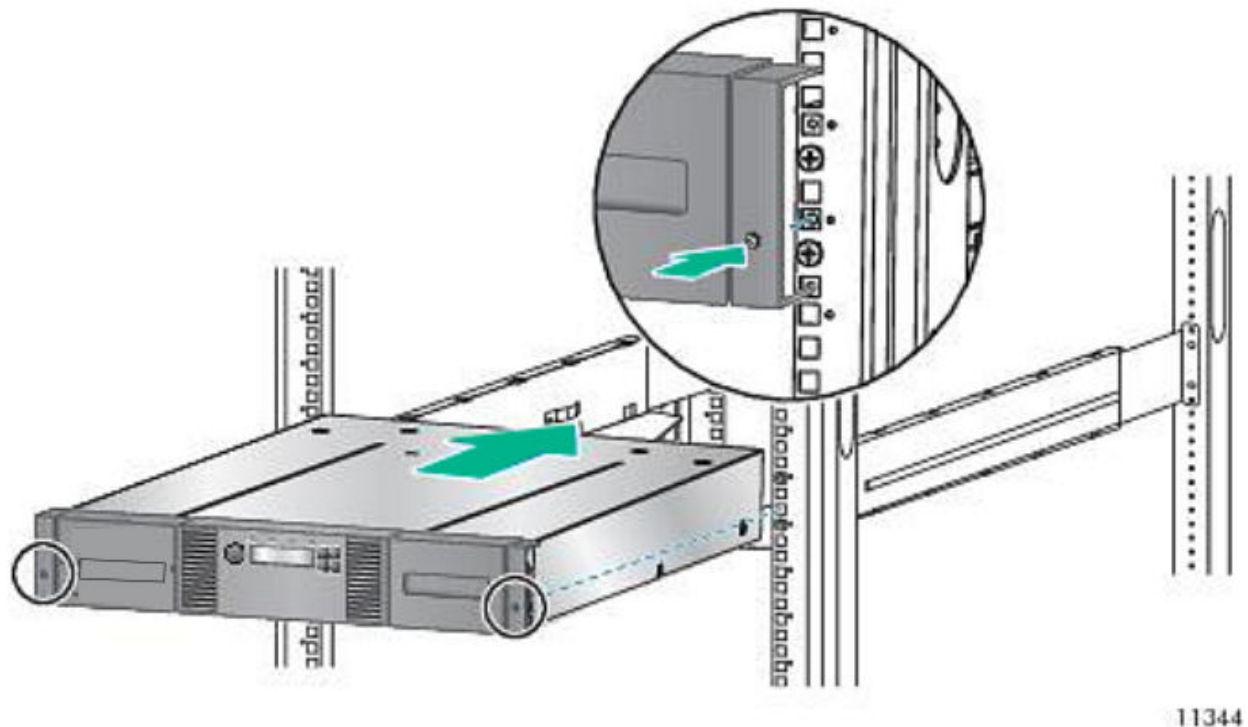
1. Select the hardware packet for your rack.

Packet label	Applicable racks
7.1 mm Round-Hole Rack	HPE supported racks with 7.1 mm round holes in the rack column
9.5 mm Square-Hole Rack	HPE supported racks with 9.5 mm square holes in the rack column

2. Install the rails.
 - a. Using the screws from the packet for your rack and a #3 Phillips screwdriver, secure the front of one rail to the front of the rack. The support platform of each rail is tapered, narrowing towards the rear.



- b. Extend the rail to the depth of the rack and secure the rail to the back of the rack.
 - c. Install the other rail.
3. Install the library in the rack.
 - a. Slide the library onto the rails.
 - b. From the front of the library, secure the front bezel to the rack. You can use either a #2 Phillips screw driver or torque driver. Place the tool through the small holes in the mounting bracket. Tighten the captive screws on each side of the library until they are seated. If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not over tighten. If using a torque driver, the recommended torque is six-inch pounds or 0.68 N m.



4. Verify that the library is contained within the 2U rack volume.

Installing tape drives

Prerequisites

#2 Phillips screwdriver

About this task



WARNING



Hazardous Moving Parts

Hazardous moving parts exist inside this product. Do not insert tools or any part of your body into the drive bay openings to avoid injury.

Only personnel with appropriate technical and product safety training (referred to as "users" in this document) may access or operate the tape library.

Read all documentation and procedures before proceeding with the tape drive installation or replacement process.

When possible, install all tape drives during the initial library installation process before the library is powered on. When installing additional tape drives after the library has been powered on, follow the instructions included with the tape drive.



TIP

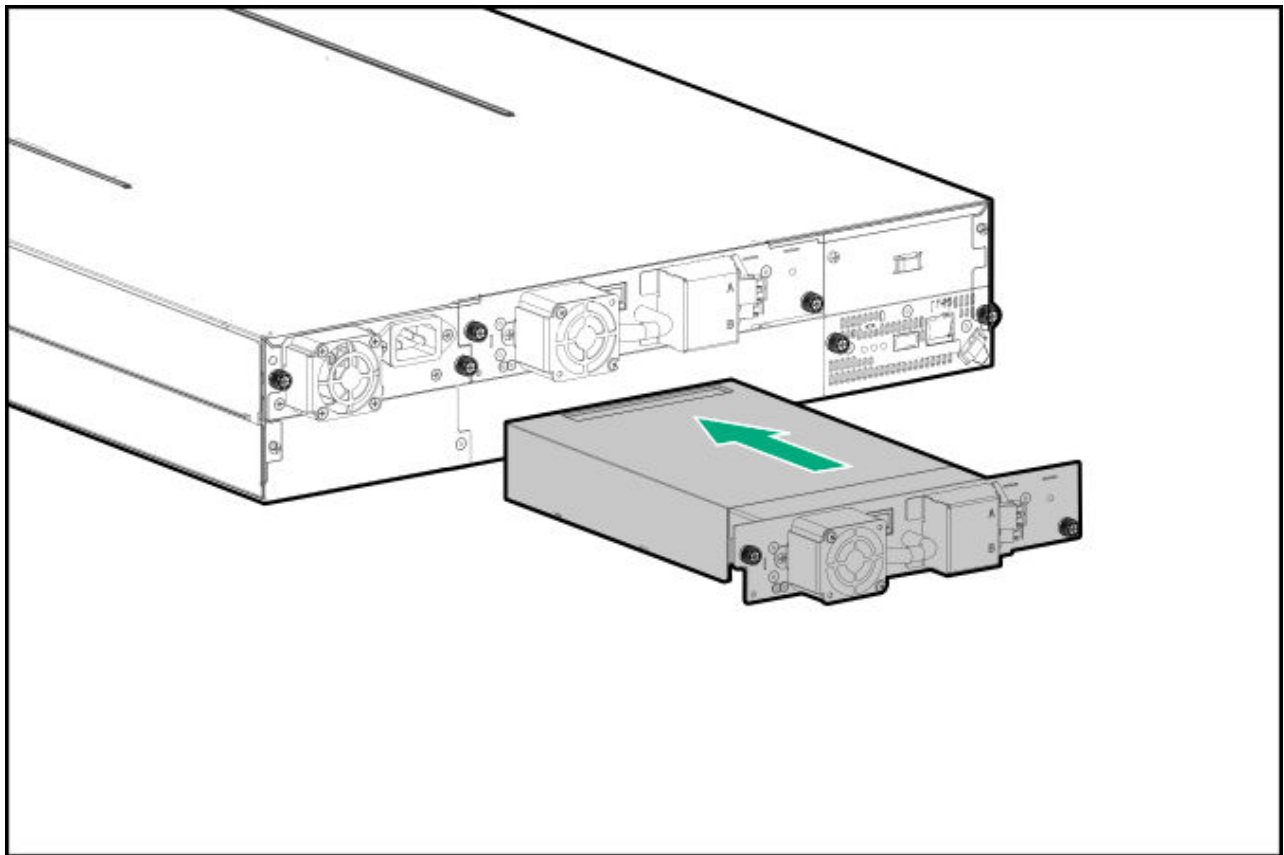
To assist in aligning the drive, only remove the drive bay covers for one drive at a time.

Procedure

1. Locate an appropriate vacant drive bay on the back of the library.

Install the first tape drive in the bottom drive bay. Install the second tape drive in the drive bay directly above the existing tape drive if available.

2. Remove the face plate covering the drive bay by removing the screws holding it in place.
3. Holding the tape drive by the handle and supporting it from the bottom, position the drive on the alignment rails. Slide the tape drive into the drive bay until it is flush with the back of the library.



4. To secure the tape drive to the chassis, use a torque driver to tighten the thumbscrews on the drive sled to 6-inch pounds or 0.68 N m.

If a torque driver is not available, use a #2 Phillips screwdriver to tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition.

If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



CAUTION

- All drive bays without tape drives installed must have drive bay covers installed.
- To prevent drive performance issues under conditions of external shock or vibration, ensure that the thumbscrews are tightened to the specified torque.

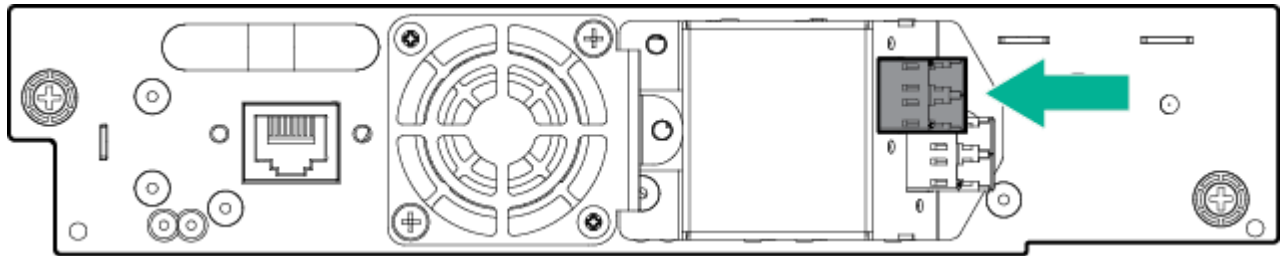
Connecting the FC cable

About this task

Using both ports on a dual-port drive requires multipath capability in the host application. For information about configuring the second port, see the application documentation.

Procedure

1. Remove the FC port caps if necessary. Attach one end of the FC cable to Port A on the tape drive.



2. Attach the other end of the FC cable to a switch or HBA.

Connecting the SAS cable

About this task



NOTE

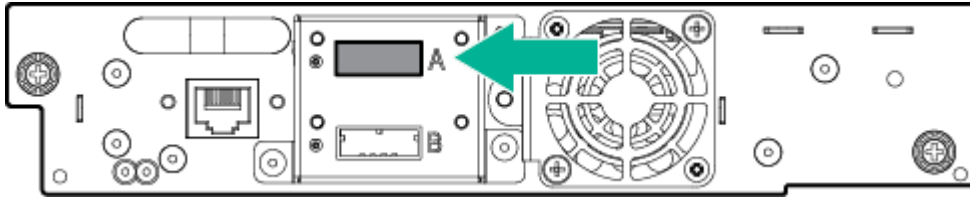
SAS signal rates require clean connections between the HBA and tape drive. Do not use adapters or converters between the HBA and the tape drive. For reliable operation, use a maximum SAS cable length of 6 meters.

Procedure

1. Determine which end of the cable to plug into the HBA.
 - a. For a cable with a single connector on each end, the end with the same type of connector as the HBA is the HBA end.
 - b. For a SAS fanout cable, the end of the cable with a single connector is the HBA end.
2. Attach the HBA end of the SAS cable to the HBA port.

3. Attach the drive end of the cable to Port A on the tape drive.

If you are using a SAS fanout cable, only attach one SAS connector to each tape drive.



NOTE

LTO-6 drive is shown in the example, other drive connectors might look different.

The unused ends of the SAS fanout cable are single-channel and not suitable for use with disk arrays. Use the other ends to connect additional tape drives, or coil and secure them to the rack to minimize stress on the connectors.



TIP

Mini-SAS connectors are keyed. Do not force a mini-SAS connector into the tape drive SAS port because the connector and port might be keyed differently.



NOTE

Each tape drive uses one channel. The cable recommended for use with the library maps each of the four channels from the HBA to one channel on the drive end.

You can plug any of the four drive connectors into any tape drive.

Powering on the library

About this task



WARNING

To reduce the risk of electric shock or damage to the equipment:

- Use an approved power cord. If you have questions about the type of power cord to use, contact your support specialist.
- Use a power cord rated for your product and for the voltage and current marked on the electrical ratings label of the product. The voltage and current rating of the cord must be greater than the voltage and current rating marked on the product.

Procedure

1. If you plan to use the RMI, use an Ethernet cable to connect the library to a working LAN connection. The library Ethernet connector is on the back of the library.
2. Attach a power cable to the power connector on each power supply on the back of the library.
3. Plug the power cables into the nearest properly grounded power outlets.
4. Power on the library by pressing the power button on the front panel.
5. To verify that the library has power, check the LCD screen.

If the library does not have power, check the power connections and your power source.

During the Power On Self-Test (POST), all four LEDs are illuminated briefly, followed by a flashing **Ready** LED. When the initialization sequence is complete, the Home screen is displayed.

If the inventory takes over five minutes, the splash screen is displayed. To see the Home screen, press any button.



NOTE

If the attention light flashes, view the event log for the event code to identify the issue. See [Error events](#) and [Warning events](#) for details and solutions.

6. Plug in the host server and all attached devices.
7. Power on any other devices you powered off earlier.

8. Power on the server.

**NOTE**

To power off the library, hold down the power button on the front panel for 5 seconds and then release it.

Setting up the RMI

About this task

Before using the RMI, you must configure the library network settings and set the INITIAL RMI administrator password with the OCP.

With the RMI, you can monitor, configure, and operate most library functions from a web browser. When possible, use the RMI as the primary library interface because it provides access to additional features, includes online help, and is easier to use. However, the RMI is not required to use the library, except to configure advanced features, such as SNMP, IPv6, encryption, and HPE TapeAssure. The only tasks that you cannot do from the RMI are: Use a USB flash drive to save configuration files and support tickets, and download firmware.

**NOTE**

- The library is shipped without an RMI administrator password. The administrator password must be set by following the OCP steps before you can use the RMI administrator functions. Once the administrator password is set, you can access the RMI by providing the administrator password on the **login** screen.
- If one person physically installs the library and a second person will configure the library, share the network settings and the INITIAL RMI administrator password created in this procedure.

Procedure

1. Log in to the OCP as administrator. (Press any key and then enter **User: “ADMINISTRATOR” PIN:0000**).
2. Verify or change network settings (**Configuration > Network**).
3. Set the INITIAL RMI password (**Configuration > Users > Reset RMI PW > Select User: “ADMINISTRATOR”**).

4. From a browser, log in to the RMI as the Administrator user. (Use the IP address and the password created in step 3).



NOTE

RMI is supported on Google Chrome, Microsoft Edge, and Mozilla Firefox browsers.

After the initial login, you will be prompted to set a new password (for password guidelines, see [Password rules](#)). Then, you will be prompted that the library has no default partition. The library will remain OFFLINE to connected hosts until a valid partition is created.

5. Create a partition using the Basic or Expert Partition Wizard (**Configuration > Partitions > Basic or Expert Wizard**).

See [Using the basic partition wizard](#) or [Using the expert partition wizard](#).

6. Complete any other configuration details required for your installation from the RMI, including **date/time** settings.

Logging into the OCP

About this task



TIP

By default, the OCP Administrator PIN is 0000. Change the administrator PIN from the OCP to protect the administrator functions on the OCP.

Procedure

1. Press any key on the OCP, then select the user to log in as at the **Select User:** prompt.
2. When prompted for the PIN, press **Next** to scroll to the first number of the PIN and press **Enter**. The number you selected is replaced with an asterisk (*), and the cursor proceeds to the next text box. Repeat this until you have entered all four numbers. After the last number has been entered, you will be logged in.
3. Press **Next**, **Prev**, **Enter**, and **Cancel** to navigate the menus and options.

Verifying the host connection

Procedure

1. Install the application software and/or drivers that are compatible with the library and tape drive.

Backup software packages might require additional software or licensing to communicate with the robotics.

For software compatibility information, see [Accessing the compatibility matrix](#).

2. Verify the connection between the library and the host:

- a. Install the Library & Tape Tools Diagnostic/Installation Check Utility onto the host computer.

This utility verifies that the library is connected and communicating with the host server. It also verifies that the device is functioning and provides diagnostic information. To verify your connections, run the **Library & Tape Tools Installation Check** from the programs menu.

L&TT is available without cost at: <https://www.hpe.com/support/TapeTools>

- b. Confirm that the host server operating system recognizes the library.

In Windows, look for tape drives and media changers in the Device Manager.

Understanding the user interface

Available user interfaces are:

- **Remote management interface (RMI):** With the RMI, you can monitor, configure, and control the library from a web browser. The RMI hosts a dedicated, protected internet site that displays a graphical representation of the library.
- **Operator control panel (OCP):** With the OCP, you can monitor, configure, and control the library from the front panel.

If using host backup software, you can perform any function provided by the backup software.

For more information about the RMI and OCP, see [The RMI](#) or [The OCP](#).

Subtopics

[Users and roles](#)

[The RMI](#)

[The OCP](#)

Users and roles

The library supports four user roles: User, Administrator, Security, and Service. The library is preconfigured with one user for each role. The administrator can add up to 80 additional library user accounts.

- **User**—The user account provides access to status information, but not configuration, maintenance or operation functions.
 - No PIN or password is required (leave the **PIN** or **Password** blank unless the user PIN or password has been set).
- **Administrator**—The administrator user has access to all functionality except for the security and service features. There are separate administrator user accounts for the OCP and RMI.
 - The administrator PIN or password is required to log in as the administrator user.
 - The administrator password is used for the RMI and administrator PIN is used for the OCP.
 - There is not a default RMI administrator password.
 - The administrator must set the INITIAL RMI administrator password from the OCP before administrator functions can be used with the RMI.
 - If the RMI administrator password is lost, reset the RMI administrator password from the OCP. After resetting the RMI administrator password from the OCP, share the new INITIAL RMI administrator password if necessary.

If the RMI administrator password and OCP administrator PIN are both lost, see [Resetting the RMI administrator password and OCP PIN](#).
- **Security**—The security user has access to all administrator functionality and can also configure security features and change the security user password.
 - The security password is required to log in as the security user.
 - The administrator user must set the security password the first time.
 - Once the security password is set, only the security user can modify it.
 - If the security password is lost, both the administrator and service passwords are required to change the security password. Changing the security user password requires assistance from Hewlett Packard Enterprise support personnel.
- **Service**—Access to the service user is by service personnel only.

- The service password is set at the factory and is only available to Hewlett Packard Enterprise support personnel.
- Both the administrator and service passwords are required for a service person to enter the service area.

The RMI

The RMI user interface is organized into the following regions:

- Top banner: Contains the home button and displays the overall status and information about the library and user.
- Left pane: Displays the library identity.
- Center pane: Provides access to operate and configure the library and to view additional status information.
- Right pane: Displays a log of recent events.

Top banner elements

-  Home icon: Returns to the main screen
- **Lib. Health:** An icon indicating the overall health status of the library
 -  - **Status OK** - All library components are fully operational, no user intervention is required.
 -  - **Status Warning** - User attention is necessary, but the library can still perform most operations. To display the event ticket log, click the icon.
 -  - **Status Error** - User intervention is required and the library is not capable of performing some operations. To display the event ticket log, click the icon.
- **Status:** The status of the library robotic assembly.
 - **Idle:** The library robotic assembly is ready to perform an action.
 - **Moving:** The library robotic assembly is moving a cartridge.
 - **Scanning:** The library robotic assembly is performing an inventory of cartridges.
 - **Offline:** The library robotic assembly has been taken offline by the library.
- Time and date: Setting the date and time to the current local time is helpful when analyzing event logs and support tickets. Service or support engineers might request the local time. The time is not updated automatically for daylight saving time.

- **User:** The user account for this session.
- **Logout:** Log out of this session.
- **?:** Access online help

Left pane elements

- Library configuration:
 - **Serial #:** The library serial number.
 - **Hostname:** The library host name.
 - **Network configuration:** The IP version (IPv4 or IPv6) and IP address.
 - **Firmware:** The library firmware version.
 - **Token:** Information about the key server token when using the encryption kit (if installed).
 - **CVTL:** Status of CVTL configuration system. This overview provides a summary of configuration and health of the library and drive.
- System Status Overview: A summary of configuration and health of the library and drive.
 - System health icon:
 -  - **Status OK** - All library components are fully operational, no user intervention is required.
 -  - **Status Warning** - User attention is necessary, but the library can still perform most operations. To display the event ticket log, click the icon.
 -  - **Status Error** - User intervention is required and the library is not capable of performing some operations. To display the event ticket log, click the icon.
 - Drive status: The number of drives installed in the library and the health of the drive.

To display drive configuration and status information, click or tap on the drive.

- A black square indicates that the drive is fully operational and that no user intervention is required.
- A yellow square indicates that user attention is necessary, but that the drive can still perform most operations.
- A red square indicates that user intervention is required or the drive is not capable of performing some operations.
- Magazine slot usage: The number of cartridge slots in use and available.
- Drive operation status: The current drive activity for the drive.

- **Write:** Drive is performing a write operation.
- **Read:** Drive is performing a read operation.
- **Idle:** Cartridge is in the drive but the drive is not performing an operation.
- **Empty:** Drive is empty.
- **Encryp:** Drive is writing encrypted data.
- **Calib:** Drive is initializing a new LTO-9 tape.

Center pane

- **Open Mailslot:** (Administrator user only) Click or tap to unlock the mailslot. Mailslots must be enabled before the slots can be used as mailslots.
- **Open Magazine:** (Administrator user only) Click or tap to unlock a magazine. Only one magazine in the library can be open at a time.
- **Configuration:** (Administrator user only) Click or tap to configure the library.
- **Maintenance:** (Administrator user only) Click or tap to access maintenance functions.
- **Operation:** (Administrator user only) Click or tap to access operation functions.
- **Status:** Click or tap to access status information.

The OCP

The OCP has a power button, navigational buttons, an LCD screen, and four LEDs. With the OCP you can monitor, configure, and operate many library functions from the library front panel. To navigate the OCP, use the navigational, enter, and cancel buttons.



NOTE

The OCP session times out and logs off after five minutes of inactivity.

To power on the library, press the power button. For more information, see [MSL2024 front panel](#). To power off the library, press the power button for five seconds and then release it.

The OCP on the front of the library includes a 2-line by 16-character green backlit liquid crystal display (LCD), four function keys, and four OCP LEDs. This panel provides everything that you need to monitor the library status and control some functions.

Subtopics

OCP menu

OCP menu

The OCP options are organized under five menus: Information/Status, Operation, Configuration, Maintenance, and Logout. You must first login to the OCP as either User, Administrator, or Service. From the factory, the OCP User user does not have an OCP PIN set. The OCP Administrator PIN is set to 0000 from the factory, but can be changed to any four-digit number. The Service user is only used by HPE service personnel.

When accessing the OCP, if a user is not already logged in, first login by pressing any key, then selecting a user at the **Select User**: prompt. Once you have entered the correct PIN for that user, you will be given access to the menus and selections available to that user level.

Select User
User
Information/Status
Library Status
Drive (x) Status
Network Status
Inventory
Magazine Left Inventory
Magazine Right Inventory
Drive Inventory
Operation
Configuration
Maintenance
Logout
Administrator
Information/Status
Library Status

Drive (x) Status
Network Status
Inventory
Magazine Left Inventory
Magazine Right Inventory
Drive Inventory
Operation
Mailslot Unlock
Magazine Unlock Left
Magazine Unlock Right
Configuration
Network
IPv4 Mode
Static
IPv4 Address
IPv4 Netmask
IPv4 Gateway
DHCP
Library
Reset to Default Settings
Save Configuration to USB Device
Restore Configuration from USB
Users
Reset RMI PIN
Configure PIN

	Disable RMI Restricted Access
Maintenance	
	Save Lib ticket to USB
	Save Lib Logs to USB
	Upgrade Lib from USB Device
	Save Drv ticket to USB Device
	Select Dump Mode Current Ticket
	Select Dump Mode Health Log
	Upgrade Lib from USB Device
Logout	
Service	
Information/Status	
	Library Status
	Drive (x) Status
	Network Status
	Inventory
	Magazine Left Inventory
	Magazine Right Inventory
	Drive Inventory
Operation	
	Mailslot Unlock
	Magazine Unlock Left

	Magazine Unlock Right
Configuration	
	Network
	IPv4 Mode
	Static
	IPv4 Address
	IPv4 Netmas k
	IPv4 Gatewa y
	DHCP
	Library
	Reset to Def ault Settings
	Reset to Man ufacturing
	Save Config t o USB Device
	Restore Conf ig from USB
	Users
	Reset RMI P W
	Configure PI N
	Disable RMI Restricted A ccess
Maintenance	
	Save Lib ticket to USB
	Save Lib Logs to USB
	Upgrade Firmware from USB Device
	Save Drv ticket to USB Device

	Select Dump Mode Current Ticket
	Select Dump Mode Health Log
	Upgrade Drive from USB Device
Logout	

The administrator user accesses all the available functionality, except for the Reset to Manufacturing option. The User has access to the Status/Information menu only.

Home screen

The OCP displays status information when no user is logged in. The OCP consists of a two-line display. The first line shows the device product name, and the second line shows the drive status. During tape movement operations, the first line displays **Moving** instead of the device product name.

- Example for drive status shown on OCP with one drive:

```
<device product name>
Drive: Empty
```

- Example for drive status shown on OCP with two drives:

```
<device product name>
D1: -E-   D2: -E-
```

Table 1. Drive status definitions

Single Drive	Dual Drive	Definition
Empty	-E-	Drive is Empty
Idle	IDLE	Drive has a tape inserted, but there is no activity
Reading	READ	Drive is reading from the tape
Writing	WRT	Drive is writing to the tape
Loading	LOAD	Drive is loading a tape
Unloading	UNLD	Drive is unloading a tape

Single Drive	Dual Drive	Definition
Cleaning	CLN	Drive is cleaning with a cleaning tape
Rewinding	REWD	Drive is rewinding a tape
Seeking	SEEK	Drive is spacing forward or backward to a specific location on tape
Erasing	ERA	Drive is erasing a tape
Calibrati	CAL	LTO-9 drive is calibrating a new LTO-9 tape (one time calibration of new, unused tape media)
Decryptin	DECR	Drive is reading and decrypting an encrypted tape
Encryptin	ENC	Drive is writing encrypted data on to a tape

OCB buttons

With the four OCB buttons, you can traverse the OCB menu structure and enter information.



10763

Button	Description
Cancel	Cancels the current menu option, returns to the previous menu level, or returns to the Home screen.
Enter	Enters the menu or selects the option displayed on the LCD screen.
Previous	Selects the previous item or value in the currently displayed menu.
Next	Selects the next item or value in the currently displayed menu.

Configuration

Prerequisites

Initial RMI password set as described in [Setting up the RMI](#).

About this task

When the library powers on the first time, it is configured with the default settings. The library must be configured before use. There must be at least one partition defined before the library and drive will be accessible by one or more connected hosts.

Procedure

1. Access the user interface.
 - **OCP:** The OCP home screen shows the drive status, press any key to access the menu.
 - **RMI:** Open a supported web browser and enter the IP address of the library in the browser address bar. Ensure that the IP address begins with https://.
2. Select **User**.
3. If required, enter the **PIN** or **Password**.
4. Select **Login**.

Subtopics

[HPE Storage 1/8 Tape Autoloader and MSL Tape Libraries Encryption Kit](#)

[Network port requirements](#)

[Hardware-based encryption](#)

[KMIP-based key servers](#)

[Application-managed encryption](#)

[Configuring through RMI](#)

[Configuring through OCP](#)

HPE Storage 1/8 Tape Autoloader and MSL Tape Libraries Encryption Kit

The encryption kit provides secure generation and storage of encryption keys. The encryption kit can be used with any HPE Storage 1/8 Tape Autoloader or MSL2024, MSL3040, and MSL6480 Tape Library with at least one LTO-4 or later generation tape drive.

The encryption kit supports your manual security policies and procedures by providing secure storage for encryption keys. Access to the key server tokens and their backup files is protected with user-specified passwords. You must create processes to protect the tokens and secure the passwords.

Before enabling the encryption kit, verify that the library is running the most current firmware to ensure compatibility between the token and library.

To use the encryption kit, insert a key server token into the USB port on the back of the library and then enable the encryption kit and configure the token from the RMI.



IMPORTANT

When encryption is enabled with the encryption kit, the library will not use encryption keys from other sources, such as a key management system or application software. Disable encryption in applications writing to the library when encryption is enabled with the encryption kit. Applications that attempt to control encryption while encryption is enabled with the encryption kit will not be able to do so, which can cause backups or other write operations to fail.

For information about configuring and using the encryption kit, see HPE Storage Tape Autoloader and MSL Tape Libraries Encryption Kit User Guide, available at <https://www.hpe.com/support/hpesc>.

Network port requirements

The MSL tape library requires several networking ports to enable network functions. The following network ports must be open in any firewalls between the tape library and hosts or appliances it communicates with.

Port	Direction	Use
22 (TCP)	Inbound	Service. The administrator can disable this port when the library is not being serviced.
80 (TCP)	Bidirectional	RMI
161 (UDP)	Bidirectional	SNMP
162-169 (UDP)	Inbound	One port in the range is required to receive SNMP traps.
427 (UDP+TCP)	Bidirectional	Service Locator Protocol (SLP)
443 (TCP)	Inbound	HTTPS secure access to the RMI
Configurable (TCP)	Outbound	KMIP communication with a key management appliance (configurable). Multicasting and ping support are also required to set up KMIP communication. The default is 5696.

Hardware-based encryption

The LTO-4 and later generation tape drives include hardware capable of encrypting data while writing data, and decrypting data when reading. Hardware encryption can be used with or without compression while maintaining the full speed and capacity of the tape drive and media.

Encryption is the process of changing data into a form that cannot be read until it is deciphered with the key used to encrypt the data. Encryption protects the data from unauthorized access and use. LTO tape drives use the 256-bit version of the industry-standard AES encrypting algorithm to protect your data.

To use this feature, you need:

- The 1/8 and MSL Encryption Kit or a KMIP-based key server or a backup application that supports hardware encryption.
- LTO-4 or later generation media; no encryption will be performed when writing LTO-3 and earlier generations of tape.

Your company policy will determine when to use encryption. For example, your company could require encryption of company confidential and financial data, but not for personal data. Company policy will also define how to generate and manage encryption keys. Backup applications that support encryption will generate a key for you or allow you to enter a key manually.

For information about using the encryption kit, see [HPE Storage 1/8 Tape Autoloader and MSL Tape Libraries Encryption Kit](#).

KMIP-based key servers

The library supports integration with encryption key management servers using the Key Management Interoperability Protocol (KMIP) standard. KMIP is an industry standard protocol for communications between a key management server and an encryption system. The KMIP technical committee of the OASIS standards body (Organization for the Advancement of Structured Information Standards) developed the KMIP specification.

The KMIP feature allows the library to obtain encryption keys from selected KMIP-compliant key managers. These keys can be used to encrypt data as it is written to tape. Up to six key servers can be configured for failover purposes.

For instructions on configuring the KMIP feature, see the HPE Storage MSL Tape Libraries Encryption Key Server Configuration Guide, available from the Hewlett Packard Enterprise Support Center at <https://www.hpe.com/support/hpesc>.

Key managers

To use the KMIP feature, the library must have access to a KMIP key manager. Hewlett Packard Enterprise only supports KMIP when used with a supported key manager, listed in the compatibility matrix. See [Accessing the compatibility matrix](#).

Operation

When the KMIP feature is enabled and properly configured, tape data will automatically be encrypted with keys delivered from the KMIP key manager. Tapes are encrypted on a key-per-tape basis.

Write, and append operations: The tape drive will request a key when data is written. The library, acting as an intermediary, can request the key manager to create a key. The library then obtains that key and delivers it to the tape drive. A name, which is associated with the media identifier, identifies the key. The key is not retained in the tape drive any longer than necessary to perform encryption operations.

Read operations: The tape drive will request a key. The library, acting as an intermediary, obtains the key identifier, requests that key from the key manager, and delivers it to the tape drive. The key is not retained in the tape drive any longer than necessary to perform decryption operations.

Licensing

The KMIP feature requires that the KMIP encryption license has been installed before the feature can be enabled and configured.

Application-managed encryption

Hardware encryption is off by default and is switched on by settings in your backup application. The backup application also generates and supplies the encryption key. Your backup application must support hardware encryption for this feature to work. For a current list of suitable backup software, see the compatibility matrix at [Accessing the compatibility matrix](#).



NOTE

The library can only obtain encryption keys from one source. Using the encryption kit will prevent application-managed encryption.

Encryption is primarily designed to protect the media once it is offline and to prevent it being accessed from another machine. The tape drive can read and append the encrypted media without being prompted for a key while the machine and application that first encrypted the tape is accessing the tape.

There are two main instances when you will need to know the key:

- If you try to import the media to another machine or another instance of the backup application.
- If you are recovering your system after a disaster.



NOTE

Encryption with keys that are generated directly from passwords or passphrases might be less secure than encryption using truly random keys. Your application will explain the available options and methods. See the application user documentation for more information.

If you are unable to supply the key when requested to do so, no one will be able to access the encrypted data, including support engineers.

This feature guarantees the security of your data, but you must carefully manage the encryption key used to generate the tape.



CAUTION

Keep a record or backup of your encryption keys and store it in a secure place separate from the computer running the backup software.

For detailed instructions about enabling encryption, see the documentation supplied with your backup application or with the encryption kit. The documentation will also highlight any default states, for example when copying tapes, that might need to be changed when using encrypted tapes.

Configuring through RMI

Subtopics

Initial configuration wizard

System

Network

Network management

Drives

Mailslot

Partitions

Encryption

User accounts

Configuring HPE Storage Command View for Tape Libraries integration

Web management

Secure Manager

Initial configuration wizard

About this task

This procedure results in a simple library configuration with RMI access, one partition, and no mailslots enabled.

Procedure

1. If the INITIAL RMI administrator password has not already been set or the default library network settings need to be modified, see [Configuring the library network](#) and [Setting the administrator password](#).
2. Log in to the RMI as an administrator user.

Use the INITIAL RMI administrator password to log in to the RMI the first time as the administrator user. The library will prompt you to set an actual RMI password (for password guidelines, see [Password rules](#)). If one person physically installs the library and a second person accesses the library using the RMI, share the INITIAL RMI administrator password as appropriate.

3. If the library has no partition, you should receive a pop-up warning when you login to the RMI stating `Library has no default partition`. Click **Basic Wizard**. If the pop-up is closed, you can also access the wizard in the RMI by clicking **Configuration** on the RMI home screen. In the right pane, click **Partitions** and then click **Basic Wizard**.
4. In the right pane, click **Partitions** and then click **Basic Wizard**.

The wizard displays the configured partitions. When the library is first powered on and before partitions are configured, this list will not have any partitions. There must be at least one partition defined before the library and drives will be accessible by one or more connected hosts.

The wizard removes any existing partitions. If you see any partitions listed, verify that they can be removed.

5. Navigate to **Information > Proceed** and then click **Next**.

The screenshot displays the 'Basic Partition Wizard' interface. On the left is a dark sidebar with the title 'Basic Partition Wizard' and a menu containing 'Information', 'Create Partition Scheme' (highlighted with a green arrow), and 'Finish Configuration'. The main content area is titled 'Create Partition Scheme' and is divided into two sections: 'Free Resources That Will Be Used by the Partition Scheme' and 'Partition Settings'.

Free Resources That Will Be Used by the Partition Scheme	
Slots :	21
Mailslots :	3
Drives :	2
Max. Partitions :	2

Partition Settings

Partition Count (max: 2)	1
Barcode Label Length Reported To Host	8
Barcode Label Alignment Reported To Host	Left
Auto Clean	☐
Encryption Mode	Controlled by Backup Application

At the bottom right of the main content area are four buttons: 'Back' (green), 'Next' (green), 'Finish' (grey), and 'Cancel' (green).

The wizard displays the available resources and the default partition settings:

- The library has one partition.
- Eight barcode characters are reported to the host application.
- If a barcode label has more characters than are reported to the host, the characters will be taken from the left end of the barcode label.
- Auto cleaning is not enabled.

6. To accept the default values, click **Next**.

The **Finish Configuration** screen displays the proposed allocation of library resources into partitions. If you accepted the defaults, all the tape drives and mailslots are assigned to a single partition.

7. Click **Finish**.

You can return to either partition wizard at any time to change the partition configuration.

System

Subtopics

[Save or restore configuration](#)

[Setting time zone, date, time, and SNTP](#)

[Media barcode compatibility check](#)

[Managing license keys](#)

[Setting RMI language](#)

[Barcode handling configuration](#)

[Configuring additional features](#)

Save or restore configuration

Subtopics

[Saving configuration file](#)

[Restoring configuration file](#)

[Resetting default settings](#)

[Resetting the list of known drives](#)

Saving configuration file

About this task

If the library chassis or controller must be replaced, the saved configuration database will make it easier to restore your library settings.

Procedure

1. Navigate to **RMI > Configuration > System > Save/Restore Configuration**.
2. Click **Save**.

Restoring configuration file

Procedure

1. Navigate to **RMI > Configuration > System > Save/Restore Configuration**.
2. Expand the **Restore Configuration File** section and click **Choose File**.
3. Select a configuration file that you have previously saved and click **Open**.
4. Click **Upload File & Restore**. The file will be uploaded to the library, and the system will reboot.

Resetting default settings

Procedure

1. Navigate to **RMI > Configuration > System > Save/Restore Configuration**.
2. Expand the **Reset Default Settings** section, and click **Reset**.

Resetting the list of known drives

About this task

When drives are replaced in the library, the library must update its list of known drives. With this operation, the library resets its list of known drives quickly and without requiring a reboot.

Procedure

1. Navigate to **RMI > Configuration > System > Save/Restore Configuration**.
2. Expand **Reset the List of Known Drives** area and then click **Reset**.

Results



NOTE

After the operation completes, use one of the partition wizards to verify and update the drive assignments as necessary. Other library settings are not affected by this operation.

Setting time zone, date, time, and SNTP

Subtopics

Setting the time zone

Setting the date and time format

Setting the date and time

Enabling SNTP (Simple Network Time Protocol) synchronization

Setting the time zone

Procedure

1. Navigate to **System > Date and Time Format**.
2. Click **Time Zone**.

A list of continents, countries, and regions is displayed. When an item preceded with '>' (for example, > **America**), is selected, a submenu is displayed in the next column.

3. Expand the time zone list, as necessary, until a location with the appropriate time zone is visible.
4. Select a location with the appropriate time zone.

5. Click **Submit**.

**NOTE**

There is no syslog on the library. Instead there are library logs, which when viewed or downloaded from the library, shows the timestamp on events that matches the current date or time as shown on the library.

Setting the date and time format

Procedure

1. Navigate to **System > Date and Time Format**.
2. Expand the **Date/Time Format** section.
3. Select a time format.
4. Select a date format:

For example, July 30, 2013 is displayed as:

- DD.MM.YYYY—30.07.2013
- MM/DD/YYYY—07/30/2013
- YYYY-MM-DD—2013-07-30

5. Click **Submit**.

Setting the date and time

About this task

The library will automatically adjust for daylight saving time (DST) if the selected time zone is in a location or country that observes DST clock change events.

Procedure

1. Navigate to **System > Date and Time Format**.
2. Expand the **Set Date/Time** section.

3. To set the time and date manually:
 - a. Enter the time in the configured time format.
 - b. Enter the date or select it from the calendar.
4. To synchronize the time and date with the computer running the browser, click **Now**.
5. Click **Submit**.

Enabling SNTP (Simple Network Time Protocol) synchronization

About this task

The library must have network access to an SNTP server to use this feature.

Procedure

1. Navigate to **System > Date and Time Format**.
2. Expand the **SNTP**.
3. Select the checkbox **SNTP Enabled**.
4. Enter the SNTP server address.
5. Click **Submit**.

Results

Time is synchronized with the SNTP server every eight hours.



NOTE

Time synchronization is limited to SNTP support. Secure NTP and NTS protocols are unsupported.

Media barcode compatibility check

Subtopics

[Enabling media barcode compatibility check](#)

[Disabling media barcode compatibility check](#)

Enabling media barcode compatibility check

About this task

When **Barcode Media ID Restriction** is enabled, the library will allow appropriate data cartridges to be loaded into the tape drives. The barcode media ID is the last two characters of the barcode. For example, the library will not move an LTO-9 labeled cartridge into an LTO-8 tape drive.

Procedure

1. Navigate to **Configuration > System > Media Barcode Compatibility Check**.
2. Select the checkbox by **Barcode Media ID Restriction**.
3. Click **Submit**.

Results



NOTE

Barcode labels are recommended on all cartridges in the library. For efficient operation, include the correct media ID on the label and keep the **Barcode Media ID Restriction** option enabled (the default setting).

Disabling media barcode compatibility check

About this task

When the Barcode Media ID restriction is disabled:

- The library will move any data cartridges to any tape drive. If the cartridge is incompatible with the tape drive, the library displays a message.
- The library allows a single move of an incompatible data cartridge to a tape drive. It then proactively blocks known incompatible moves that would otherwise fail.

Procedure

1. Navigate to **Configuration > System > Media Barcode Compatibility Check**.



NOTE

Barcode labels are recommended on all cartridges in the library. For efficient operation, include the correct media ID on the label and keep the **Barcode Media ID Restriction** option enabled (the default setting).

2. Clear the check box by **Barcode Media ID Restriction**.
3. Click **Submit**.

Managing license keys

About this task

License keys register licensed library functionality.

Procedure

1. Navigate to **Configuration > System > License Key Handling**.
2. In the **Add License Key** pane, enter the **License Key**.
3. Click **Add License**.

Setting RMI language

About this task

The library RMI can be displayed in English or Japanese. Use the **Language** setting to select the appropriate display language.

Procedure

1. Navigate to **Configuration > System > Language**.
2. Select either **English** or **Japanese** from the drop-down box and click **Submit**.

Barcode handling configuration

Use the Basic Partition Wizard or Expert Partition Wizard to configure barcode handling. Configurable settings include:

- The number of barcode characters reported to the host application.
- Whether to report barcode characters from the left or right end of the label.

Configuring additional features

About this task

The tape library has many features to customize it for your organization.

Procedure

1. Assign a name to the tape library through **RMI > Configuration > Network**.
2. Enable and configure SNMP network management through **RMI > Configuration > Network Management > SNMP**.

For details on configuring SNMP for use with Command View TapeAssure, see HPE Storage Command View Tape Library User Guide.

3. Set up an email event notification through **RMI > Configuration > Network Management > SMTP**.
4. To use the RMI interface in Japanese, activate the Japanese language option through **RMI > Configuration > System > Language**.

Network

About this task



NOTE

The RMI uses the standard internet ports: port 80 for HTTP or port 443 for HTTPS. The browser displaying the RMI must have firewall access to the library through at least one of these ports.

Procedure

1. Navigate to **Configuration > Network**.
2. Configure or update the **Host Name** and **Domain Name**. The RMI URL is `<Host Name>.<Domain Name>`.
3. Select the internet protocol for the library.
4. Configure the settings for the selected internet protocol.

To have the library obtain an internet address from a DHCP server, select the **DHCP** or **Static** method.
5. Click **Submit**.

Network management

- [SNMP](#)
- [SMTP](#)
- [Remote logging \(rsyslog\)](#)

Subtopics

[SNMP](#)

[Simple Mail Transfer Protocol \(SMTP\)](#)

[Remote logging \(rsyslog\)](#)

SNMP

The library supports both SNMP configuration and SNMP traps.

- **SNMP Enabled:** When selected, computers listed in the **SNMP Target IP Addresses** can manage the library. SNMP must be enabled to work with HPE Storage Command View for Tape Libraries.



NOTE

If you are using a third-party SNMP management software, click **Download MIB File** to obtain the MIB file and use with the third-party tools.

- **Community Name:** A string used to match the SNMP management station and the library. It must be set to the same name on both the management station and the library. The default community name is `public`.
- **Notification Level:** Choose to send one of the following as SNMP traps depending on the event's level of severity,
 - **Inactive:** No events
 - **Critical:** Only Critical events
 - **+Warning (Default):** Critical and Warning events
 - **+Configuration:** Critical, Warning, and Configuration events
 - **+Information:** All events
- **SNMP Targets:** List of configured SNMP targets.

Subtopics

Adding an SNMP target

Editing an SNMP target

Deleting an SNMP target

Clearing all SNMPv3 options

Adding an SNMP target

About this task

If the library is configured to use Command View TL, do not add the CVTL management station as a trap receiver using the **Configuration > Network Management** dialog. The CVTL station will be added automatically as an SNMP trap receiver during the CVTL registration process. Adding the CVTL station as a duplicate SNMP receiver could cause issues with SNMP connectivity.

Procedure

1. Navigate to **Configuration > Network Management**.
2. Click **Edit** next to a target without an IP/host name.
3. Enter the target IP address or host name.
4. Enter the port.
5. Select the SNMP version (SNMPv1, SNMPv2, or SNMPv3 unless SNMP is limited to SNMPv3 in the following configuration).

6. Enter the SNMP community string for the target.
7. If any of the targets use SNMPv3, enter the SNMPv3 configurations. These SNMPv3 configuration values require corresponding settings on an SNMPv3-enabled trap receiver.
 - a. Limit all library SNMP communication to SNMPv3: When selected, all SNMP communications must use SNMPv3.

**NOTE**

If the library is configured to use HPE Storage Command View Tape Library, confirm that the HPE Storage Command View TL version supports communication over SNMPv3. When using SNMPv3 communication between the library and HPE Storage Command View TL, the SNMPv3 settings must be identical on the library and Command View TL management station.

- b. SNMPv3 Security Levels

- **noAuthnoPriv:** Permits communication without authentication or privacy.
- **authNoPriv:** Permits communication with authentication and without privacy.
- **authPriv:** Only permits communication with authentication and privacy.

**NOTE**

Selecting SNMPv3 does not automatically disable SNMPv1 and SNMPv2.

- c. **Authentication User Name:** The user name for authentication on the SNMPv3 trap receiver.
 - d. **Authentication Password:** The authentication password is needed for security levels authNoPriv and authPriv.
 - e. **Authentication Protocol:** The supported authentication protocols are MD5 and SHA (Secure Hash Algorithm).
 - f. **Privacy/Encryption Protocol:** The supported privacy protocols are DES (Data Encryption Standard) and AES (Advanced Encryption Standard).
 - g. **Privacy/Encryption Passphrase:** The passphrase is needed for security level authPriv.
8. Click **Submit**.

Editing an SNMP target

Procedure

1. Navigate to **Configuration > Network Management**.
2. Click **Edit** for the appropriate SNMP target.
3. Enter the target IP address or host name.
4. Enter the port.
5. Select the SNMP version.



NOTE

Select SNMPv3 if SNMP is limited to SNMPv3 in the following configuration.

6. Enter the SNMP community string for the target.
7. If any of the targets use SNMPv3, enter the SNMPv3 configurations. These SNMPv3 configuration values require corresponding settings on an SNMPv3-enabled trap receiver.
 - a. **Limit all library SNMP communication to SNMPv3:** When selected, all SNMP communications must use SNMPv3.



NOTE

If the library is configured to use Command View TL, confirm that the version of Command View TL supports communication over SNMPv3. When using SNMPv3 communication between the library and Command View TL, the SNMPv3 settings must be identical on the library and Command View TL management station.

- b. SNMPv3 Security Levels:

- **noAuthnoPriv:** Permits communication without authentication or privacy.
- **authNoPriv:** Permits communication with authentication and without privacy.
- **authPriv:** Only permits communication with authentication and privacy.



NOTE

Selecting SNMPv3 does not automatically disable SNMPv1 and SNMPv2.

- c. **Authentication User Name:** The user name for authentication on the SNMPv3 trap receiver.

- d. **Authentication Password:** The authentication password is needed for security levels authNoPriv and authPriv.
 - e. **Authentication Protocol:** The supported authentication protocols are MD5 and SHA (Secure Hash Algorithm).
 - f. **Privacy/Encryption Protocol:** The supported privacy protocols are DES (Data Encryption Standard) and AES (Advanced Encryption Standard).
 - g. **Privacy/Encryption Passphrase:** The passphrase is needed for security level authPriv.
8. Click **Submit**.

Deleting an SNMP target

Procedure

1. Navigate to **Configuration > Network Management**.
2. Click **Delete** for the target to be deleted.
3. Click **Submit**.

Clearing all SNMPv3 options

Procedure

1. Navigate to **Configuration > Network Management**.
2. Click **Clear SNMPv3 Options**.
3. Click **Submit**.

Simple Mail Transfer Protocol (SMTP)

About this task

You can enable SMTP functionality and configure email notification of library events. The library must have network access to an SMTP server.

Procedure

1. Navigate to **Configuration > Network Management > SMTP**.
2. If SMTP is not enabled, click **SMTP Enabled**.

When enabled, the remaining configurations are active.

3. Configure SMTP options:

- a. **Notification Level:** The types of events for which the library should send an email:

Options	Description												
Notification Level	The types of events for which the library should send an email: <table><tr><th>Events</th><th>Description</th></tr><tr><td>Inactive</td><td>No events are sent.</td></tr><tr><td>Critical</td><td>Only critical events are sent.</td></tr><tr><td>+ Warnings</td><td>Only critical and warning events are sent.</td></tr><tr><td>+ Configuration</td><td>Only critical, warning, and configuration events are sent.</td></tr><tr><td>+ Information</td><td>All events are sent.</td></tr></table>	Events	Description	Inactive	No events are sent.	Critical	Only critical events are sent.	+ Warnings	Only critical and warning events are sent.	+ Configuration	Only critical, warning, and configuration events are sent.	+ Information	All events are sent.
Events	Description												
Inactive	No events are sent.												
Critical	Only critical events are sent.												
+ Warnings	Only critical and warning events are sent.												
+ Configuration	Only critical, warning, and configuration events are sent.												
+ Information	All events are sent.												
SMTP Server	Host name, FQDN, or IP address of the SMTP server.												
Security	The following security protocols are used to access the SMTP server: • None • SSL/TLS • STARTTLS												

Options	Description
SMTP Port	SMTP server port. The default port for the selected protocol will be selected. You can choose one of the default ports or configure a custom port.
To Email Addresses	The addresses to receive the reported events (for example, firstname.lastname@example.com).
Mailer Name	The name of the sender of the email.
E-mailer Subject	Subject line for the email message.
Email Address	Return address to use for the email message.
Authentication Required	When selected, a user name and password are required to access the SMTP server.
Username	User account for logging in to the SMTP server when authentication is required.
Password	The password is associated with the user name when authentication is required.

- Click **Submit**.

A test email is sent and all future events within the notification level configured will be sent.

Remote logging (rsyslog)

About this task

This feature allows for sending library events to a rsyslog server. The data sent only includes the ticket information generated by the library software. Low-level logs generated by Linux and other applications will not be transmitted to the remote server.



NOTE

Only non-encrypted remote logging is supported.

Procedure

- Navigate to **Configuration > Network Management > Remote Logging (rsyslog)**.

2. Select **Remote Logging Enabled**.
3. In **Notification Level**, select the level of severity of events to be sent as SNMP traps. The default is **+Warning**.
 - **Inactive**: No events are sent.
 - **Critical**: Only critical events are sent.
 - **+Warning**: Critical and warning events are sent.
 - **+Configuration**: Critical, warning, and configuration events are sent.
 - **+Information**: All events are sent.
4. In **Remote Logging Server**, enter the remote syslog server host name, FQDN, or IP address.
5. Configure the **Remote Logging Port**.

The default port for the selected protocol is selected. You can choose the default port or configure a custom port.
6. Configure the **Transport Protocol**.

TCP and UDP are supported. The default is TCP.
7. Click **Submit**.

**NOTE**

Rsyslog events are sent with the library's current date and time but without a timezone offset (treated as UTC). To correlate them with library logs, apply the timezone offset.

Drives

Procedure

1. Navigate to **Configuration > Drives > Settings**.
2. Modify any of the configurable values.

Values	Description
Drive number	The drive currently hosting the SCSI communication for the library is designated with (LUN).
Serial number	The serial number assigned to the tape drive by the library. This serial number is reported to host applications. The serial number cannot be modified. When a drive is replaced, the library reassigns the serial number and WWN from the drive that was removed to the drive that is installed. This serial number is not the serial number assigned to the drive by the manufacturer; the serial number assigned by the manufacturer is shown in Manufacturer S/N.
LTO generation	• LTO 6-Ultrium 6250 • LTO 7-Ultrium 15000 • LTO 8-Ultrium 30750 • LTO 9-Ultrium 45000
Drive form factor	• HH: half height
Drive interface	• FC: Fibre Channel • SAS: Serial Attached SCSI
Modified	When present indicates that a setting has been changed. To apply the changes, click Submit . To reset all changed fields to their previously saved values, click Undo .
Pwr	Indicates whether the drive is on or off.
Firmware	The version of firmware currently installed on the drive.
Manufacturer S/N	The serial number assigned to the drive when it was manufactured. Use this serial number when working with service.

Values

Description

Power On

Selected when the drive is powered on.



NOTE

Always power off a tape drive before removing it from the library.

Port configuration (FC only)

Drive port configuration.

Speed

The currently selected speed. The default is Automatic.

Port Type

- Automatic
- Loop: Enables selection of the Addressing Mode.
- Fabric



NOTE

When using LT O-7, LT O-8, or LTO-9 FC drives with a 32Gb or 16Gb HBA in direct attach mode, **Port Type** should typically be set to Fabric M

Values	Description
	ode. Early (Gen 5) 16Gb and 8Gb/4Gb host adapters may require the topology to be set to Loop Mode.
Addressing Mode	When Port Type is set to Loop, Addressing Mode can be set to Soft or Hard .
Loop ID / ALPA	When Addressing Mode is set to Hard, you can choose an ALPA address from the drop-down list.

3. Click **Submit**.

Subtopics

- [**Configuring the FC interface**](#)
- [**Powering on a tape drive from the RMI**](#)
- [**Powering off a tape drive from the RMI**](#)
- [**Disabling Secure Mode for an LTO-6 tape drive**](#)

Configuring the FC interface

About this task

Skip this step if you are replacing a tape drive.

Procedure

1. Log in to the RMI and enter the administrator password if requested.
2. Navigate to **Configuration > Drives**.
3. Configure the settings for your drive and connection method.

Drives connected to a SAN

Leave the FC port at the default settings of **Speed: Automatic** and **Port Type: Automatic**. With these settings, the tape drive will use the appropriate configuration.

Drives connected directly to the host

- When using LTO-7, LTO-8, and LTO-9 drives with a 32Gb or 16Gb HBA in direct-attach mode, **Port Type** should typically be set to Fabric Mode. Early (Gen5) 16Gb and 8Gb/4Gb host adapters may require the topology to be set to Loop Mode.
- For LTO-6 and earlier drives, leave the FC port at the default settings of **Port Speed: Automatic** and **Port Type: Auto Detect**. With these settings, the tape drive will use the appropriate configuration.

4. Click **Submit**.

Powering on a tape drive from the RMI

Procedure

1. Navigate to **RMI > Configuration > Drives > Settings**.
2. Select **Power On**.
3. Click **Submit**.



NOTE

Tape drives are automatically powered on when the tape library is powered on unless the drive was previously manually powered off.

Powering off a tape drive from the RMI

Procedure

1. Navigate to **RMI > Configuration > Drives > Settings**.
2. Unselect **Power On**.
3. Click **Submit**.



NOTE

Power off the tape drives before removing them from the device.

Disabling Secure Mode for an LTO-6 tape drive

About this task

To disable Secure Mode on an LTO-6 tape drive, first ensure that the tape drive is installed in the same library where Secure Mode was originally enabled. Then, you can disable Secure Mode by either powering off the tape drive itself or by powering off or rebooting the entire library.



IMPORTANT

If Secure Mode is enabled for a drive and either the drive is removed from the library without powering it off first or the library has a hard shutdown (for example, it loses power or the front panel power button is held for more than 10 seconds), the drive could still have Secure Mode enabled. To disable Secure Mode, power on the drive in the library that enabled Secure Mode and then power off the drive from the RMI or OCP.

Procedure

1. Power off the drive from **RMI > Configuration > Drives > Settings**.
2. Power off the library from the library OCP by pressing the power button on the front panel for five seconds.
3. To identify the library that enabled Secure Mode, install the tape drive in any 1/8 G3 Autoloader, MSL2024 G4, MSL3040, or MSL6480 tape library with 4.70 or later firmware. The serial number of

the library that enabled Secure Mode is shown in the **RMI > Status > Drive Status** for the drive in the common name (CN) field.

Mailslot

About this task

The **Configuration > Mailslot** screen shows whether the mailslot is enabled or disabled.

Procedure

- To change whether a mailslot is enabled or disabled, click the **Enable** or **Disable** for the mailslot and then click **Submit**.

Slots that have not been designated as mailslots are available as storage slots.

- To change the length of time that a mailslot or magazine remains unlocked, select the duration and then click **Submit**.

Partitions

The library has a flexible partitioning scheme with a few key constraints:

- Each partition must have at least one tape drive which will host the library LUN for the partition.
- Mailslots must be enabled before they can be allocated to a partition.

A partition does not need to have a mailslot. If a partition does not have a mailslot, the magazine must be accessed to import or export cartridges. Opening a magazine takes the library offline.

Wizards guide you through the partition configuration process. The wizards are only accessible from the RMI.

- **Basic Partition Wizard**—You specify the number of partitions and the wizard removes the current partition configuration and assigns the drives and storage slots as evenly as possible to the partitions.

Use the Basic Partition Wizard to configure the number of barcode characters to report to the host application and whether to report them from the left or right end of the label for an library with a single partition.

- **Expert Partition Wizard**—Use the Expert Partition Wizard to adjust resource assignments for existing partitions or partitions created with the Basic Partition Wizard.

Subtopics

[Using the basic partition wizard](#)

[Using the expert partition wizard](#)

[Deleting a partition using the expert partition wizard](#)

Using the basic partition wizard

About this task



NOTE

- The library will go offline while partitions are being configured. Ensure that all host operations are idle before running a partition wizard.
- If you want to enable or disable the mailslot, **Cancel** out of the wizard and update the mailslot configuration before configuring partitioning.

Procedure

1. From the **Configuration > Partitions**, select **Basic Wizard** to start the wizard.

The **Information** lists any current partitions, which the wizard will delete.

2. Click **Proceed** and then click **Next**.

The **Create Partition Scheme** displays the number of slots, mailslots, tape drives, and maximum available partitions for the library.

3. Select the number of partitions.
4. Select the number of barcode characters reported to the host application. This option provides interchange compatibility with libraries with more limited barcode reading capabilities. The minimum length is 6, the maximum length is 16, and the default is 8.



NOTE

The industry standard length for LTO barcode labels is eight characters. Barcode labels longer than eight characters might scan incorrectly, particularly if they are not high-quality labels.

5. Select whether to report barcode characters from the left or right end of the barcode label to the host application. This choice applies when reporting fewer than the maximum number of characters. For example, when reporting only six characters of the barcode label `12345678`, if alignment is left, the library will report `123456`. If the alignment is right, the library will report `345678`. The default is left.
6. To enable the auto cleaning feature, select **Auto Clean**. When enabled, the library automatically initiates a cleaning operation when media is unloaded from a drive that requires cleaning. This behavior replaces the creation of a warning event when a drive requires cleaning. LTO-7 and later generation tape drives might request to clean more frequently than earlier generation tape drives. For reliable operation, enable Auto Clean for each partition with an LTO-7 or later generation tape drive and ensure that the partition has a valid cleaning cartridge.

When initiating a cleaning operation, the library will use an unexpired cleaning cartridge from the same partition as the tape drive. If the partition does not contain an unexpired cleaning cartridge, the library will use an unexpired cleaning cartridge from an unpartitioned area of the library. When enabling auto cleaning, ensure that each partition has an unexpired cleaning cartridge or place at least one unexpired cleaning cartridge in an area that is not assigned to a partition.



NOTE

The cleaning cartridge label must begin with the letters “CLN” for the library to recognize it as a cleaning cartridge.

The same LTO Ultrium cleaning cartridges are used for all LTO tape drives. The library does not limit movement of a cleaning cartridge based on the LTO generation in the barcode media identifier. It allows cleaning cartridges to be moved to any generation tape drive. All Hewlett Packard Enterprise labels for cleaning cartridges end with “L1” media identifier characters.

7. Click **Next**.
8. The **Finish Configuration** displays the proposed allocation of library resources into partitions.
 - a. To update the configuration, click **Back**.
 - b. To have the wizard configure the partition as shown, click **Finish**.

After the wizard reconfigures the partition, the library will come on line automatically.

- c. To exit the wizard, click **Cancel** or **Exit**.



TIP

You can use the expert partition wizard to adjust the allocation of resources after creating the partitions with the basic partition wizard.

Using the expert partition wizard

About this task



NOTE

- The library will go offline while partitions are being configured. Ensure that all host operations are idle before running a partition wizard.
- If you want to enable or disable the mailslot, **Cancel** out of the wizard and update the mailslot configuration before configuring partitioning.

Procedure

1. From the **Configuration > Partitions**, select **Expert Wizard** to start the wizard.

This lists the current partitions, if any, and the free resources. Use the wizard to configure one partition at a time.

2. Select a partition.
 - a. To add a partition, click **Add** and then click **Next**.



NOTE

The **Add** button will only be active if there are available resources, such as tape drives, storage slots, or mailslot slots. If there are no available resources, either edit a partition and release resources from it or remove a partition that contains extra resources.

- b. To reconfigure a partition, click **Edit** and then click **Next**.
3. Enter a name for the partition.

4. Select the number of barcode characters reported to the host application.

This option provides interchange compatibility with libraries with more limited barcode reading capabilities. The minimum length is 6, the maximum length is 16, and the default is 8.

**NOTE**

The industry standard length for LTO barcode labels is eight characters. Barcode labels longer than eight characters might scan incorrectly, particularly if they are not high-quality labels.

5. Select whether to report the barcode characters from the left or right end of the barcode label to the host application when reporting fewer than the maximum number of characters.

For example, when reporting only six characters of the barcode label 12345678 if alignment is left (the default), the library will report 123456. If the alignment is right, the library will report 345678.

6. To enable the auto cleaning feature, select **Auto Clean**. When this feature is activated, the library will automatically perform a cleaning operation whenever media is unloaded from a drive that requires cleaning, rather than simply generating a warning event. LTO-7 and newer generation tape drives may request cleaning more frequently than earlier models. For reliable operation, enable Auto Clean for each partition with an LTO-7 or newer tape drive, and ensure that each partition has a valid cleaning cartridge available.

When initiating a cleaning operation, the library will use an unexpired cleaning cartridge from the same partition as the tape drive. If the partition does not contain an unexpired cleaning cartridge, the library will use an unexpired cleaning cartridge from an unpartitioned area of the library. When enabling auto cleaning, ensure that each partition has an unexpired cleaning cartridge or place at least one unexpired cleaning cartridge in an area that is not assigned to a partition.

**NOTE**

The cleaning cartridge label must begin with the letters “CLN” for the library to recognize it as a cleaning cartridge.

The same LTO Ultrium cleaning cartridges are used for all LTO tape drives. The library does not limit movement of a cleaning cartridge based on the LTO generation in the barcode media identifier. It allows cleaning cartridges to be moved to any generation tape drive. All Hewlett Packard Enterprise labels for cleaning cartridges end with “L1” media identifier characters.

7. If only one host will be accessing each LTO-7 or later generation drive in the partition, select **LTO-7+ Multi-initiator SCSI Conflict Detection**.

**TIP**

Only enable this setting if you are sure that only one host will access each drive. Do not enable this feature if your use model or SAN setup requires multiple hosts sending commands to any drive in the partition.

LTO-7 and newer generation tape drives track which hosts (SCSI initiators) are sending commands to the drive. When **LTO7+ Multi-initiator SCSI Conflict Detection** is activated for a partition, the library monitors the initiator lists for all the LTO-7 and newer generation drives in that partition. If the library detects more than a single host WWNN (World Wide Unique Number) for a drive, the library generates an LTO-7+ Multi-initiator SCSI Conflict Detection warning event. The event lists all the host WWNNs for the given tape drive. So the administrator can disable access for any host that must be stopped from sending drive commands.

The **LTO-7+ Multi-initiator SCSI Conflict Detection** setting only appears if one or more LTO-7 or later generation drives are detected in the library.

8. Click **Next**.
9. In the **Assign Storage Slots**, use the >> and << buttons to assign slots to the new partition and then click **Next**.
10. In the **Assign Mailslots**, use the >> and << buttons to assign mailslots to the new partition and then click **Next**.

Importing or exporting cartridges in a partition without an assigned mailslot will require magazine access, which will take the library offline.

1. In the **Assign Drives** screen, use the >> and << buttons to assign drives to the new partition and then click **Next**.
2. In the **Select Control Path Drive**, select the **Active Control Path Drive** and click **Next**.
3. Verify the partition configuration and then click **Finish**.
4. After the wizard reconfigures the partition, the library will come on line automatically.

Deleting a partition using the expert partition wizard

Procedure

1. Select the partition.
2. Click **Remove**.
3. Click **Next**.
4. Verify that you want to remove the partition and then click **Finish**.

After the wizard removes the partition, the library will come on line automatically.



NOTE

With no partition defined on the library, a connected host will only be able to communicate with the tape drive, and will not have access to the robotic assembly.

Encryption

The library supports the following methods of encryption.

- USB - MSL Encryption Kit
- KMIP Wizard
- LTO FIPS Support Mode



NOTE

- The library goes offline when the encryption configuration is changed.
- Only a security user can modify the encryption configuration.

Subtopics

Setting the default configuration mode for new partitions

Allowing the administrator to configure encryption with the Expert Partition Wizard

Setting the encryption mode for a partition

MSL Encryption Kit configuration

Using the KMIP wizard

Configuring FIPS Support Mode

Setting the default configuration mode for new partitions

Prerequisites

Logged in to the RMI as a security user.

Procedure

1. Navigate to **RMI > Configuration > Encryption**.
2. Under **Set Default Encryption Mode for new Partitions**, select a mode.
3. Click **Apply to all existing partitions** to update the settings for all existing partitions.
4. Click **Submit**.

Allowing the administrator to configure encryption with the Expert Partition Wizard

Prerequisites

Logged in to the RMI as a security user.

About this task

By default, the security user must configure encryption. With this setting, the library administrator users can configure encryption with Expert Partition Wizard.

Procedure

1. Navigate to **Configuration > Encryption**.
2. Select **Allow Administrator encryption configuration during Expert Partition Wizard**.
3. Click **Submit**.

Setting the encryption mode for a partition

Prerequisites

Logged in to the RMI as a security user.

Procedure

1. Navigate to **Configuration > Encryption**.
2. In the **Set Encryption Mode per Partition** section, select an encryption mode for one or more partitions.

To disable library-managed encryption, set the encryption mode to **Controlled by Backup Application**. When encryption is disabled for a partition, encrypted media in that partition cannot be read until the same encryption method is enabled.

3. Click **Submit**.

MSL Encryption Kit configuration

The **Configuration > Encryption > USB—MSL Encryption Kit** displays information about the key server token and provides access to enter the key server token password and configure a new key server token. Access to this screen is only available to the security user.

For additional information on using the encryption kit, see the HPE Storage MSL Encryption Kit User Guide on the Hewlett Packard Enterprise Support website: <https://www.hpe.com/support/hpesc>. The terms “token PIN” and “token password” are used interchangeably in the encryption kit documentation.

Subtopics

Entering the key server token password when using the MSL Encryption Kit

Viewing the keys on the key server token when using the MSL Encryption Kit

Changing the key server token password when using the MSL Encryption Kit

Changing the key server token name when using the MSL Encryption Kit

Generating a new write key when using the MSL Encryption Kit

Configuring automatic key generation when using the MSL Encryption Kit

Backing up the key server token data to a file when using the MSL Encryption Kit

Restoring key server token data from a backup file when using the MSL Encryption Kit

Configuring the key server token login behavior when using the MSL Encryption Kit

Entering the key server token password when using the MSL Encryption Kit

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Verify that the correct key server token is available.

If the token is not visible, see [Viewing the keys on the key server token when using the MSL Encryption Kit](#).

3. Enter the **Token Password** and then click **Submit**.

Viewing the keys on the key server token when using the MSL Encryption Kit

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. If the **Keys on the Key Server Token** area is not visible, click **Gather Key Information**.
3. Expand **Keys on the Key Server Token** area to see the keys on the key server token.

Changing the key server token password when using the MSL Encryption Kit

About this task



CAUTION

The key server token password protects the encryption keys. If you lose the key server token password, you will not be able to restore data from your encrypted data cartridges using that key server token. Neither you nor a service engineer can recover a lost key server token password. Keep a copy of the key server token password in a safe place.

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand the **Password Management** section.
3. Enter the current and new key server token passwords.
4. The key server token password must consist of at least 8 characters and no more than 16 characters, and it must contain at least one lower case letter, one upper case letter, and no less than two digits.
5. Click **Submit**.

Changing the key server token name when using the MSL Encryption Kit

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand **Password Management** section.
3. Enter the new key server token name. The name can have up to 126 characters.



TIP

Using a descriptive name, including the dates when the keys on the key server token were used, could be helpful if your log of data cartridges written with keys on the key server token is lost.

4. Click **Submit**.

Generating a new write key when using the MSL Encryption Kit

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand the **Key Management** section.
3. Click **Apply**.

Configuring automatic key generation when using the MSL Encryption Kit

About this task

When you enable automatic key generation, the library will automatically request the key server token to generate a new key periodically, according to the policy you configure. Be aware that automatically generated keys are not backed up unless you do so manually. To ensure you have more than one copy of a new key, schedule automatic key generation for a time when you can back up the key before any data cartridges are written using it.

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand **Key Management** section.
3. Check the **Enable** box in the automatic key generation policy section.
4. Set the policy for the new key generation frequency, and the date and time this will occur.
5. Click **Submit** to apply your selections.

Results



NOTE

A key is not generated when the library time is advanced past a time when a new key would have been generated. If you advance the library time, check the automatic key generation policy to see whether a new key is needed, and if so, manually generate it.

One new key is generated if the library is powered off at a time when a new key would have been automatically generated. To prevent a new key from being generated, disable automatic key generation before powering off the library.

Backing up the key server token data to a file when using the MSL Encryption Kit

About this task

As a best practice, back up the key server token data to a file each time an encryption key is added.

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand **Key Management** section.
3. Enter a password for the backup file.

The password must be at least eight characters and no longer than 16 characters. The password must contain at least one lower case letter, one upper case letter, and at least two digits.

4. If you are creating a backup file to seed a new key server token, enter the number of keys to include in the backup.

The library will back up the highest-numbered keys, which are normally the most recent.



NOTE

You must create a full backup before you can select the number of keys to backup in a partial backup.

5. Click **Save**.

Restoring key server token data from a backup file when using the MSL Encryption Kit

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand **Key Management** section.
3. Enter the key server token restore password.

This password is the password that was created when the key server token backup file was created. It is not usually the key server token password.

4. Click **Choose File** and browse to the location of the key server token backup file on the local computer.
5. Click **Restore**.

Configuring the key server token login behavior when using the MSL Encryption Kit

About this task

By default, the security user must provide the key server token password each time the library is powered on or booted. When the **Keep Token Logged In Across Reboots** option is enabled, the key server token password is only required after the library has been powered off or encounters a hard shutdown. The password is not required after a reboot.

Procedure

1. Navigate to **Configuration > Encryption > USB—MSL Encryption Kit**.
2. Expand **Keep Token Logged In Across Reboots** section.
3. Check the box next to **Keep Token Logged In Across Reboots**.
4. Click **Submit**.

Using the KMIP wizard

Prerequisites

- The library configuration is complete, including defining all library partitions.
- The KMIP server is available on the network and has been configured for use with this library.
- The KMIP license has been added from the **ConfigurationSystemLicense Key Handling** screen.
- The security user is logged in to the RMI.

About this task

With the Key Management Interoperability Protocol (KMIP) Wizard, you can configure use of KMIP key management servers with the library.

For additional information about configuring KMIP servers for use with the library, see the KMIP server documentation.

Procedure

1. Navigate to **Configuration > KMIP Wizard** in the **Encryption** menu to start the wizard.

The **Wizard Information** screen displays information about the wizard.
2. Click **Next** when the library configuration is complete and the KMIP server is available on the network.

The **Certificate Authority Information** screen displays prerequisites for using the KMIP certificate.

3. Click **Next** when the prerequisites are met.

The **Certificate Authority Certificate Entry** screen displays instructions for obtaining the certificate for the KMIP server.

4. Follow the instructions to copy the certificate from the management console. Paste the certificate into the wizard and then click **Next**.
5. The **Library Certificate Information** screen displays information about the next wizard steps. Click **Next**.
6. The **KMIP Client Configuration** screen appears, providing options for two types of server authentication.
 - a. If your KMIP server uses a client username and password for authentication, enter the username and password that were specified on the KMIP management console for the library.
 - b. If your KMIP server uses only certificate-based authentication, select **Enable KMIP Certificate-only Authentication**. Select this option only if your KMIP server requires it and you do not have a client user name and password.
7. Click **Next**. The **Certificate Generation** screen displays the current library certificate, if one exists.
8. Do one of the following:
 - a. To use the current certificate, select **Keep Current Certificate** and then click **Next**.
 - b. To generate a new certificate, select **Generate New Certificate**. The wizard will generate and display a new library certificate. Click **Select Certificate** to copy the new certificate text and then click **Next**.
9. If you selected **Generate New Certificate**, the **Sign Library Certificate** screen displays the new certificate for the library. Sign the new library certificate with the certificate authority as a client certificate, paste the new KMIP certificate in the box, and then click **Next**.
10. In the **KMIP Server Configuration** screen, enter the IP address or fully qualified host name and port number for up to ten KMIP servers. To verify access to the KMIP servers, click **Connectivity Check**.
11. The **Setup Summary** screen displays the settings that were collected by the wizard. Verify that the settings are correct and that there are no errors in the **Done** column. If you need to modify any settings or fix any issues, either click **Back** to reach the applicable screen or **Cancel** out of the wizard to fix the issues and return later.
12. If the settings are correct and there are no errors, click **Finish**.

Configuring FIPS Support Mode

About this task



IMPORTANT

Once an LTO-6 drive is configured for Secure Mode, this mode can only be disabled when the drive is installed in the same library that enabled Secure Mode. LTO-6 tape drives should not be moved between libraries when they have Secure Mode enabled. If an LTO-6 drive that still has Secure Mode enabled is placed in another library that has FIPS Support Mode Enabled, the drive will not be allowed to read or write encrypted data.

Procedure

1. Log in to the RMI as a security user.
2. Navigate to **Configuration > Encryption > FIPS Support Mode** and click **Start FIPS Wizard**.
3. Read the information screen and then click **Next**.

The **Partition FIPS Support Mode Status** lists all partitions. The **FIPS Support Mode** box is selected if FIPS Support Mode is enabled for a partition.

4. If a partition is not ready for FIPS Support Mode, its line will have a gray background and a note explaining the issues. If you want to enable FIPS Support Mode for a partition that is not ready, click **Cancel** to exit the wizard, and then correct the issues.
 - Verify that all tape drives in the partition are LTO-6 or later generation.
 - Verify that all LTO-6 tape drives in the partition are running firmware that supports Secure Mode.
 - Verify that all LTO-7 and later generation tape drives in the partition are running Secure Mode firmware.
 - Verify that library-managed encryption is configured and enabled for the partition.
5. Select the **FIPS Support Mode** box for all partitions that should have FIPS Support Mode enabled, and unselect the **FIPS Support Mode** box for any partitions that should NOT have FIPS Support Mode

enabled. (If a partition already has FIPS Support Mode enabled and you want it to continue to have FIPS Support Mode enabled, leave the box selected.)



NOTE

If an LTO-7 or later generation drive has firmware that does NOT support Secure Mode and the partition is configured with FIPS Support Mode enabled, the drive ports will be offline.

If an LTO-7 or later generation drive has firmware that supports Secure Mode and the partition is configured with FIPS Support Mode disabled, the drive ports will be left configured and all keys will be sent to the drive wrapped. The library will issue warning events.

For a current list of products that are FIPS 140-2 validated, see the NIST FIPS 140-2 Crypto Module Validation List. If FIPS 140-2 validation is required, verify the validation status before purchasing the product.

6. Click **Next**.

The **Finish** lists each partition that will have a configuration change and whether FIPS Support Mode will be enabled or disabled.

7. To complete the FIPS Support Mode configuration, click **Finish**.

The wizard updates the screen as it configures each partition.

8. Click **Exit** when the wizard is finished.

Subtopics

FIPS Support Mode prerequisites

FIPS Support Mode prerequisites

The Federal Information Processing Standards (FIPS) are standards that are developed and released by the United States federal government for use in computer systems by nonmilitary government agencies and contractors. FIPS 140-2 covers standards for secure data encryption.

With FIPS Support Mode, the tape drives in a library partition operate in a mode that is compliant with FIPS 140-2 requirements. Full compliance requires that the drives are running FIPS 140-2 compliant firmware. When the LTO FIPS Support Mode wizard configures a partition for FIPS Support Mode, the library enables Secure Mode for all the drives in that partition. FIPS Support Mode only works with library-managed encryption (such as KMIP or the MSL Encryption Kit); it does not work with application-managed encryption.

- All partitions must be defined.
- All drives in the partition must be LTO-6 or later generation and running a firmware version that supports Secure Mode.
 1. For LTO-6 drives: All drive firmware that supports Secure Mode can be used with or without Secure Mode enabled. If necessary, upgrade the drive firmware to a version that supports Secure Mode.
 - FC—253W or later
 - SAS—354W or later
 2. For LTO-7 and later generation drives: LTO-7 and later generation tape drives have separate firmware images that enable or disable Secure Mode when the firmware image is loaded onto the drive. If necessary, download and install the Secure Mode firmware image.

For a current list of products that are FIPS 140-2 Validated, see the NIST FIPS 140-2 Crypto Module Validation List. If FIPS 140-2 Validation is required, verify the validation status before purchasing the product.

User accounts

- [User account settings](#)
- [Local user accounts](#)
- [LDAP](#)

Subtopics

[User account settings](#)

[Local user accounts](#)

[LDAP](#)

User account settings

Subtopics

[Password rules](#)

[Allowing magazine or mailslot access by the user role](#)

Password rules

Prerequisites

Network Time Protocol (NTP) must be enabled before using two-factor authentication to ensure accurate time on the library.

Procedure

1. On the RMI, navigate to **Configuration > User Accounts > User Account Settings** page.
2. Configure the password rules to meet your security requirements.
 - Minimum number of characters - default is 8
 - Minimum number of upper case alphabetic characters (A-Z) - default is 0
 - Minimum number of lower case alphabetic characters (a-z) - default is 0
 - Minimum number of numeric characters (0-9) - default is 0
 - Minimum number of special characters (!@#\$%^&*O_+=[]\|;:"<>?,./) - default is 0
 - Maximum number of identical consecutive characters - default is Unlimited
 - Maximum number of failed logins before password is locked - default is 10
 - Maximum number of days before password must be changed - default is Unlimited
 - Minimum number of days before password can be changed - default is unlimited
 - Number of password changes before an old password can be used again - default is 3
 - Maximum number of failed TOTP attempts before login is locked - default is 10
3. Click **Submit**.

Allowing magazine or mailslot access by the user role

About this task

By default, only the administrator and security users are allowed to open the mailslots or magazines. The administrator and security users can enable the “user” user account access to the magazines or mailslots.

Procedure

1. Navigate to **Configuration > User Accounts > User Account** .

2. Expand the Allow Magazine or Mailslot Access by the **"User role"** section.
 - a. Select the checkbox next to **Allow magazine access by the "User role"**: to enable magazine access.
 - b. Select the checkbox next to **Allow mailslot access by the "User role"** to enable mailslot access.
3. Click **Submit**.

Local user accounts

Subtopics

Adding a local user account

Removing a local user account

Setting or modifying a user password

Changing the OCP PIN from the RMI

Adding a local user account

About this task

The administrator can add a maximum of 80 local users to the library.

Procedure

1. Navigate to **Configuration > User Accounts > Local User Accounts**.
2. Click **Add User**.
3. Enter the user account details.
 - **Name** - a series of characters and numbers with a minimum length of 1 and maximum length of 32. Allowed characters are a-z, A-Z, and 0-9.
 - **Role** - User, administrator, and security.
 - **Password** - Enter the password, and verify the password.

- **Two-factor authentication** - Check the box to enable two-factor authentication for new users.



NOTE

Only users who have two-factor authentication enabled can activate two-factor authentication for other users. If enabled, the new user is prompted to set up two-factor authentication with their authenticator at first login.

4. Click **Add**.

Removing a local user account

Procedure

1. Navigate to **Configuration > User Accounts > Local User Accounts**.
2. In the **Local Users** section, click **Delete** next to the user name.
3. Click **Yes**.



NOTE

The default accounts (administrator, security, and user) cannot be deleted.

Setting or modifying a user password

Prerequisites

Network Time Protocol (NTP) must be enabled before using two-factor authentication to ensure accurate time on the library.

Procedure

1. Navigate to **Configuration > User Accounts > Local User Accounts**.
2. Click **Edit** next to the user name.

To filter the user list, enter one or more characters in the filter box and then click **Filter By Name**. For example, the sub-string "tr" will return both "administrator" and "Tristan".

3. Enter the user password in both password fields.

4. Verify if **Two-Factor Authentication** is enabled.

**NOTE**

Only users who have two-factor authentication enabled can activate two-factor authentication for other users.

5. Click **Modify**.
6. If two-factor authentication is enabled for the current user, you will be prompted to set up an authenticator application. Use your authenticator application to scan the provided QR code, or to provide a custom seed to use for authentication. Once the seed is added to your authentication application, use the generated code as the passcode and press **OK**.

Changing the OCP PIN from the RMI

Procedure

1. Navigate to **Configuration > User Accounts > Local User Accounts**.
2. In the **Modify OCP PINs** section, click **Modify OCP PINs**.
3. Select the user in the **Name** field.

Only the administrator and user users can log in from the OCP.

4. Enter a new PIN in the **PIN** and **Verify PIN** fields.

The PIN number must contain exactly four digits. For example, **1234**.

5. Click **Modify**.

LDAP

Subtopics

[Configuring LDAP servers](#)

[Configuring LDAP users](#)

Configuring LDAP servers

Procedure

1. Navigate to **Configuration > User Accounts > LDAP**.
2. If not already listed, add your LDAP servers.
 - a. In the **LDAP Servers** area, enter your LDAP server's IP address or domain name, and then click **Add Server**.

The RMI displays the **Add Server** dialog box.

- b. Enter the required LDAP configuration information in the **Primary Server** section.

See your LDAP server documentation or local LDAP administrator for the preferred values for the various LDAP configuration settings, such as the port number and distinguished names.

- **Host:** IP address for the LDAP server.
- **Port:** The default is 389 if **Use SSL** is not checked. If **Use SSL** is checked, set to 636. Use port 3268 if adding users from the Global Catalog.
- **User CN** (Common Name): The LDAP user with permission to connect to the LDAP server and perform user queries. Many environments use the format "Surname, Name" or the email address for a group of library administrators.
- **User DN** (Distinguished Name): The DN of the User CN configured to authenticate with the LDAP server. If copying the DN from the LDAP server, make sure to remove the CN from the beginning if present.
- **Password:** LDAP password of the User CN. This might be the User CN's Windows password or an environment-specific password.
- **Use SSL:** If SSL is required, select **Use SSL** and then paste the appropriate CA certificate.
- Enter the **Secondary/Backup Server** host address and port number.
- Enter the **Distinguished Names** parameters.

Base DN: The LDAP parameters needed to identify the LDAP domain. User queries will be performed as a recursive tree search against this Base DN. For example:

```
DC=Examplegroup, DC=local
```

- Enter the Attribute Mapping parameters.

Username/LDAP Server Name: The LDAP name for the specified user account. For example: `sAMAccountName`.

- c. Click **Test Connection** to verify the configuration.
 - d. When the library successfully connects to the LDAP server, click **OK**.
3. In the **LDAP User** area, click **Add User**. Adding groups is not supported.
- The RMI displays the **Add User** dialog.
 - Click **Query LDAP Servers** to see a list of available users. There is a return limit of 1000 by default. Entering part of the name of the user will filter the list.
 - Select the username and then assign the user a role (User, Administrator, or Security). Click **OK**.

Configuring LDAP users

By default, the library has three predefined user accounts: user, administrator, and security. When LDAP servers and users are configured, the RMI and OCP login screens show the LDAP users along with the predefined users.

Each LDAP user is assigned to a role based on the predefined user accounts. This role determines the access level for the LDAP user.

- Verify that the passwords for the predefined administrator and security user accounts are set.
- Using LDAP does not disable the predefined user accounts. For library security, ensure that the passwords for the predefined administrator and security user accounts are always set.
- Setting the administrator password is required for any user with administrator or security roles to log in from the RMI.
- Setting the default security password is required for any user with security roles to log in from the RMI.
- Changing the default security password is required for any user with security roles to log in from the RMI.

If the security password is set or reset to `security`, neither the security user nor any LDAP users with the security role will be able to log in to the RMI.

- Collect the LDAP server configuration settings. LDAP server configuration is dependent on the company IT environment and security model. See your IT administrator for the settings for your environment. Before adding an LDAP user, you will need to know:
 - IP address and port for the primary and backup LDAP servers.
 - Common Name for the library administrator.
 - Base Distinguished Name and Domain.

- Distinguished Name for the library administrator. These are the parameters needed to search for potential library users in the LDAP server. For example, `OU=Internal,OU=Users,OU=RW,DC=libgroup,DC=local`.
- Attribute Mapping, Username. For most Windows Active Directory environments, the **Username** field under **Attribute Mapping** should be set to `sAMAccountName`. Other LDAP servers may be mapped differently.
- If SSL is required for the LDAP server. This field is likely required for newer versions of LDAP servers.
- Check for the Global Catalog role on a domain controller by navigating through **Server Manager > Tools > Active Directory Sites and Services**. Expand the Sites container until you find the domain controller. Expand the domain controller to show **NTDS Settings**, then right click and select **Properties**. The Global Catalog option is on the **Properties**.
- The ports can be changed on the LDAP server so verify that the correct ports are used in the configuration.

Configuring HPE Storage Command View for Tape Libraries integration

About this task

For more information, see HPE Storage Command View for Tape Libraries User Guide, available from the Hewlett Packard Enterprise website at <https://www.hpe.com/support/cvttl>.



NOTE

The CVTL management station should only be configured using **Configuration > Command View TL**. Do not add the CVTL management station as an SNMP target using **Configuration > Network Management > SNMP**.

Procedure

1. Verify that SNMP is enabled.
2. Navigate to **Configuration > Command View TL Configuration**.
3. Configure the library information.
 - **Name:** The name of the library to display in CVTL.
 -

-
- **Serial Number:** The serial number of the library. This field cannot be modified.
- **Management URL:** The URL of the management station, including port. For example, https://192.0.2.24:8099.



NOTE

The Management URL can be entered manually, or the Command View Management Station will automatically register its URL with the library when the library is added to the Management Station.

4. Verify product information.

- **Name:** Displays the product name. This field cannot be modified.
- **Version:** library firmware version. This field cannot be modified.

5. Configure the contact information.

- **Name:** Name of the person to contact about management of the library.
- **Phone:** Phone number of the contact person.
- **Email:** E-mail address of the contact person.

6. Configure Library REST Interface Enablement.

- **Enable Library REST Interface:** Select to allow Command View TL and other applications using the REST interface to communicate with the library over the SSH protocol. Enabling and the REST interface does not enable full SSH access for the console or other uses.
- **Library REST Interface User Name:** The user name that the library uses to communicate with Command View TL and all other applications using the REST Interface. This user name is created in Command View TL and is always **cvtl**.
- **Library REST Interface Password:** This password must be the same as the REST password configured for this library on the Command View TL management station. The same password is used for all applications using the REST Interface to access this library.

7. Click **Submit**.

Subtopics

Removing the CVTL Management Station trap destination

Moving CVTL access to a new management station

Removing the CVTL Management Station trap destination

Procedure

1. On the CVTL Management Station, delete the library being moved or removed from the CVTL Management Station.
2. Navigate to **RMI > Configuration > Command View TL**.
3. Ensure that the **Management URL** is blank. If it is not blank, clear it out, and then click **Submit**.

Moving CVTL access to a new management station

About this task

Only one CVTL Management Station can be set up at a time with MSL tape libraries. Before moving the CVTL access to another Management Station or disabling CVTL, the library must be removed from the current Management Station. The CVTL Management Station sets up SNMP communication with the library.

Procedure

1. Removing the CVTL Management Station trap destination.
2. Add the library to a new CVTL management station. For instructions, see Configuring Command View for Tape Libraries integration.

Web management

Subtopics

Enabling secure communications

Configuring session timeout

Enabling OCP/RMI session locking

Restricting RMI log in

Enabling secure communications

About this task

Enable or disable secure access to the RMI using Secure Socket Layer (SSL). The default is disabled.

Procedure

1. Navigate to **RMI > Configuration > Web Management**.
2. In the **Secure Communications** section, select **SSL (Secure Socket Layer)** to require all connections to the RMI to use HTTPS.
3. Click **Submit**.

Subtopics

[Creating a custom certificate](#)

[Backing up a custom certificate](#)

[Restoring a custom certificate](#)

Creating a custom certificate

About this task

Use the Add Signed Certificate Wizard to add a self-signed certificate to the library for use with SSL/TLS connections. The certificate will be used by the library for https connections to the RMI and connections to Command View TL.

The certificate will also be used on the client side of the connection and will need to be applied to each server or computer where the web browser will be used to access the RMI.

The wizard generates a certificate and then you will need a Certificate Authority to sign the certificate.

Procedure

1. Before starting the wizard, prepare your Certificate Authority to sign the certificate. You will paste the certificate generated by the wizard into a field in the Certificate Authority for signing.
2. To start the wizard click **Start Certificate Wizard** from the **Configuration > Web Management**.
3. Read the **Information** screen and then click **Next**.
4. In the **Certificate Signing Request**, create the certificate.
 - a. Enter the information about the device and organization.
 - b. Click **Generate CSR**.

The wizard displays the certificate in the lower pane.

- c. Click **Select CSR**.
- d. Use a web browser copy command, such as **Ctrl-c** to copy the certificate generated by the wizard that is now in your computer copy buffer.
5. Paste the certificate into the appropriate field in your Certificate Authority and then have the Certificate Authority sign the certificate.
6. In the wizard **Certificate Signing Request**, click **Next**.
7. In the **Signed Certificate**, paste the signed certificate into the **Signed Certificate** pane and then click **Next**.
8. On the wizard **Finish** page, click the **Finish** button to complete the wizard, apply the changes, and reload the page.
9. To verify that the certificate is being used, open an https connection to the library from a server or computer where the server-side certificate has been imported.



IMPORTANT

If the server-side signed certificate is not imported correctly, the library will revert to the built-in certificate.

The built-in certificate has an expiration date of September 7, 2047. You can view the expiration date by navigating to the RMI page on the library and viewing the certificate details.

Backing up a custom certificate

Procedure

1. Navigate to **RMI > Configuration > Web Management**.
2. In the **Backup Custom Certificate** section, click **Backup Custom Certificate**.
3. Follow the instructions on the screen to save the custom certificate to a folder accessible from the computer running the RMI.

Restoring a custom certificate

Procedure

1. Navigate to **RMI > Configuration > Web Management**.
2. In the **Restore Custom Certification** section, click **Choose file** and then select the custom certificate file from the local computer and click **Restore Custom Certificate**.

Configuring session timeout

Procedure

1. Navigate to **Configuration > Web Management**. Expand the **Session Timeout** section.
2. Select one of the available settings from the drop-down menu.
The default is 30 minutes.
3. Click **Submit**

Enabling OCP/RMI session locking

About this task

The library only supports one OCP or RMI user session at a time. By default, when a user logs in to the RMI or OCP, the existing user session closes.

When **OCP/RMI Session Locking** is enabled, a new session will not end the current session and the new user will not be able to log in.



NOTE

When this setting is enabled, always log out of the RMI or OCP when finished with a session. Otherwise, no new sessions will be allowed until the current session times out.

Procedure

1. Navigate to **Configuration > Web Management**.
2. Check the box **OCP/RMI Session Locking**.

3. Click **Submit**.

Restricting RMI log in

About this task

Restricting RMI access for the administrator and security users can be used in high secure environments where policies require all configuration changes to occur from the physical library front panel. Many settings cannot be configured from the OCP.

The user and service users will still be able to log in with the RMI. To remove all RMI access, unplug the Ethernet cable from the library controller.

Procedure

1. Navigate to **Configuration > Web Management**.
2. Check the box **Restricted Remote Management Interface (RMI) Login**.
3. Click **Submit**.

Secure Manager

Secure Manager allows you to group hosts and drives into access control groups managed by the library, without requiring changes to the SAN layout. Secure Manager is a licensed feature and can only be enabled after the license has been added to the library.

SAS drives are not supported by Secure Manager. The Secure Manager RMI screens display SAS hosts and SAS drives with gray text. The only Secure Manager function that you can perform on the items is to change the name of a SAS host.



NOTE

Secure Manager alters the drive device access method programmed into the tape drives to prevent access by unauthorized hosts on the SAN. With Secure Manager enabled, only hosts that are included in the access control group for a tape drive can see the drive. Before moving a tape drive to an library that is not using Secure Manager, reset the tape drive access method to the default open state by disabling Secure Manager.

Subtopics

Enabling Secure Manager

Creating an access group when using Secure Manager

Changing the name of an access group when using Secure Manager

Deleting an access group when using Secure Manager

Adding a host to an access group when using Secure Manager

Removing a host from an access group when using Secure Manager

Configuring device access when using Secure Manager

Creating a host when using Secure Manager

Changing the name of a host when using Secure Manager

Deleting a host when using Secure Manager

Enabling Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Select **Secure Manager Enabled**.
3. Click **Finish**.



NOTE

When Secure Manager is first enabled, you cannot see the library or the Secure Manager-supported tape drive installed in the library from the host computers until Secure Manager is configured and the library and drive are made visible to the hosts. The host computers will always see drives that are not supported by Secure Manager.

After Secure Manager is enabled, configure the hosts and drives into access groups with the wizards in the **Secure Manager Configuration** area.

Creating an access group when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager** screen.
2. Click **Edit** next to **Access Group Configuration and Host(s) selection**, read the information on the **Welcome** screen, and then click **Next**.

3. In the **Select Action to Perform** screen, click **Create New Host Access Group**, and then click **Next**.
4. In the **Access Group Name** screen, enter the **Group Name**, and then click **Next**.

The library discovers and displays the attached host WWPNs. The SAN switch interface that is being used can also be referenced to see the WWPN-to-port association to help determine which servers are attached.

**NOTE**

A host WWPN can only be in one Access Group. An library and drive device can be in multiple Access Groups.

5. In the **Access Group Hosts**, select the hosts for the group.

If no hosts are listed, check the following:

- Are all available hosts already assigned to other access groups?

Each host can only be assigned to one group. If necessary, click **Back** twice and then remove the host from another access group.

- Is the host configured in the same zone controlled by the FC switch?

Secure Manager creates access groups as a refinement of zones configured by the FC switch. If you are using FC switch zoning, the host and library must already be in the same zone.

- Is the host physically connected to the SAN?

If not, connect the host to the SAN or create a host in the wizard to be connected into the SAN later.

6. Click **Finish**.

Changing the name of an access group when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Access Group Configuration and Host(s) selection**, and then click **Next**.
3. Select the group from the list of **Existing Groups**, click **Change Access Group Name**, and then click **Next**.
4. Enter the new group name and then click **Finish**.

Deleting an access group when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Access Group Configuration and Host(s) selection** and then click **Next**.
3. Select the group from the list of **Existing Groups**, click **Delete Host Access Group**, and then click **Finish**.

Adding a host to an access group when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Access Group Configuration and Host(s) selection** and then click **Next**.
3. Select the group from the list of **Existing Groups**, click **Add Host to Group**, and then click **Next**.
4. Select one or more available hosts to add to the group and then click **Finish**.

If no hosts are listed, check the following:

- Are all available hosts already assigned to other access groups?

Each host can only be assigned to one group. If necessary, click **Back** twice and then remove the host from another access group.

- Is the host configured in the same zone controlled by the FC switch?

Secure Manager creates access groups as a refinement of zones configured by the FC switch. If you are using FC switch zoning, the host and library must already be in the same zone.

- Is the host not physically connected to into the SAN?

If not, connect the host to the SAN or create a host in the wizard to be connected to the SAN later.

Removing a host from an access group when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Access Group Configuration and Host(s) selection** and then click **Next**.
3. Select the group from the list of **Existing Groups**, click **Remove Host from Group**, and then click **Next**.
4. Select one or more hosts to remove from the group and then click **Finish**.

Configuring device access when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Device Access Configuration**.
3. Select one of the groups and then click **Next**.
4. Expand the partition entries and select the ports that you would like accessible with this group.



NOTE

When an LTO-7 or later generation drive is configured as the control path drive for a partition, the drive must also be configured for data access. At least one FC port on the drive must be added to the access group.

5. After configuring each partition, click **Finish**.

Creating a host when using Secure Manager

About this task



IMPORTANT

Once the host is added to the SAN, verify that the WWPN of the host matches the WWPN value that was preconfigured.

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Host Configuration**.
3. Click **Create Host**, and then click **Next**.
4. Enter a name for the host for use with Secure Manager and the WWPN, and then click **Finish**.



NOTE

- The wizard does not verify that the host exists or is accessible.
- Using Modify Host to give a discovered host WWPN a more recognizable name can simplify future configuration changes in a large SAN.

5. Click **Submit**.

Changing the name of a host when using Secure Manager

Procedure

1. Navigate to **Secure Manager > Secure Manager**.
2. Click **Edit** next to **Host Configuration**.
3. Select a host from the list of **Current Hosts**, click **Modify Host**, and then click **Next**.
4. Enter a name for the host for use with Secure Manager, and then click **Finish**.
5. Click **Submit**.

Deleting a host when using Secure Manager

Procedure

1. Navigate to **Configuration > Secure Manager**.
2. Click **Edit** next to **Host Configuration**.

3. Select a host from the list of **Current Hosts**, click **Delete Host**, and then click **Finish**.
4. Verify that you want to delete the host.
5. Click **Submit**.

**NOTE**

Deleted hosts will be added if they are rediscovered and added to an access control group.

Configuring through OCP

Procedure

1. Login to the OCP as administrator, then press **Previous** or **Next** until the screen displays **Configuration**.
2. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays your selected function.
4. Press **Enter** to select.

Subtopics

Changing the OCP PIN from the OCP

Resetting the RMI administrator password

Library network overview

Configuring IPv4 networking from the OCP

Finding the IPv4 IP address obtained through DHCP

Reset to default settings

Saving the configuration settings to a USB flash drive

Restoring the configuration settings from a USB flash drive

Downloading product firmware

Resetting the RMI administrator password and OCP PIN

Changing the OCP PIN from the OCP

Procedure

1. After logging in using the OCP, navigate to **Configuration > Users > Configure PIN**.

2. Select the user whose PIN you want to change.
3. Enter a new PIN in the **Enter PIN** and **Verify PIN** fields. The pin number must have exactly four digits. For example, "1234".
4. Select **Yes** when asked to change the PIN.

Resetting the RMI administrator password

About this task

The library has two administrator users: the OCP administrator and the RMI administrator. The OCP administrator requires a PIN to access the OCP functions. The RMI administrator requires a password to access the RMI functions. These administrator users are separate, and the OCP PIN and RMI password are independent of each other. Having two administrator users allows for recovery because the OCP administrator can reset the RMI administrator password and the RMI administrator can reset the OCP administrator PIN.

- If the OCP PIN is known, use this procedure to reset the RMI administrator password.
- If both the RMI administrator password and the OCP administrator PIN are lost or forgotten, see [Resetting the RMI administrator password and OCP PIN](#).

Procedure

1. Log in to the OCP as an administrator using the OCP administrator PIN.
2. Select **Configuration > Users > Reset RMI PW**.
3. Select user **RMI administrator**.
4. Enter a PIN to be used as the INITIAL RMI administrator password.
5. Repeat the PIN.
6. Read the onscreen directions and then select **Submit**.
7. On the **Update PIN** message, click **Yes**.
8. Use the INITIAL RMI administrator password to log in to the RMI for the first time as the administrator user.

The library prompts you to set an RMI administrator password. If one person physically installs the library and a second person accesses the library using the RMI, share the INITIAL RMI administrator password as appropriate.

Library network overview

Configuring the network enables you to monitor, configure, and control most library functions from the RMI. By default, the library will request an IP address from a DHCP server. Optionally, you can configure the library to use a static IP address. Once logged into the RMI, you can administer further network changes through the RMI.



NOTE

Most IPv4 network configurations are also available through the OCP.

The library supports IPv4 and IPv6 Internet Protocols. By default, the library is configured to use IPv4, the most common current version. You can enable IPv6 or both Internet Protocols from the RMI, and then continue configuring IPv6 settings from the RMI.

The IPv4 address obtained from a DHCP server is displayed in the **OCP > Information/Status > Network Status** screen.

If your organization requires a static IPv4 address, you can configure those features from within **OCP > Configuration > Network IPv4 Mode > Static** screen.

If you require IPv6, you must configure IPv6 from the RMI after setting the administrator password.

Subtopics

[Configuring IPv4 network settings](#)

[Configuring IPv6 network settings](#)

Configuring IPv4 network settings

About this task

The library can automatically obtain an IP address from a DHCP server when the device is powered on. The library also supports user-specified fixed addresses.

Procedure

1. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Configuration**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Network**. Press **Enter** to select.
3. The screen displays **IPv4 Mode**. Press Previous or Next to select either DHCP or Static addressing. Press **Enter** to select.

4. If **Static** is enabled, the screen displays **IP Address**. The second line displays the current IP address.
5. To change the IP address, press **Enter**. The screen displays the **IPv4 Address** with the first number flashing. Press **Previous** or **Next** to change the flashing number to the correct value.
6. Press **Enter** to select the next number, until all numbers have been set.
7. The screen displays **IPv4 Netmask** with the first number flashing.
8. Press **Previous** or **Next** to change the flashing number to the correct value. Press **Enter** to select the next number.
9. Repeat Step 9 until all numbers have been set.
10. The screen displays the **IPv4 Gateway** with the first number flashing.
11. Press **Previous** or **Next** to change the flashing number to the correct value. Press **Enter** to select the next number.
12. Repeat Step 11 until all numbers have been set. The screen displays **Change Config?** Press **Yes**.

Configuring IPv6 network settings

Procedure

1. From the Home screen, press **Previous** or **Next** until the screen displays **Configuration**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Configure Network Settings**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **IPv6 Networking**. Press **Enter** to select.
4. The screen displays **IPv6 Network Addressing Disabled**. To change the setting, press **Enter**.
5. Press **Next** until the screen displays the desired setting. Press **Enter** to accept the new setting.
6. Configure IPv6 networking from the RMI.

Configuring IPv4 networking from the OCP

About this task

If IPv4 networking is enabled, you can continue configuring the IPv4 network settings from the OCP.

Procedure

1. Log in to the Operator Control Panel (OCP) as administrator (**press any key > Select User: “ADMINISTRATOR”PIN:0000**).
2. From the **Home** screen, press **Next** until the display shows **Configuration**. Press **Enter**.
3. Press **Next** until the display shows **Network**. Press **Enter**.
4. Press **Next** until the display shows **IPv4**. Press **Enter**.
5. Press **Next** until the display shows **DHCP (IPv4) Enabled**. To change the setting, press **Enter**. Press **Next** until the screen displays the desired setting. Press **Enter** to accept the new setting.
6. If DHCP is disabled, press **Next** to display the **IP address**. To change the IP address, press **Enter**. Set the new IP address with the **Next**, **Prev**, and **Enter** keys.
7. Press **Next** to display the subnet mask. To change the subnet mask, press **Enter**. Set the new subnet mask with the **Next**, **Prev**, and **Enter** keys.
8. Press **Next** to display the gateway address. To change the gateway address, press **Enter**. Set the new subnet address with the **Next**, **Prev**, and **Enter** keys.

Finding the IPv4 IP address obtained through DHCP

Procedure

1. Log in to the OCP as administrator (**press any key > Select User: “ADMINISTRATOR” PIN:0000**).
2. From the Home screen, press **Next** until the display shows **Status/Information**. Press **Enter**.
3. Press **Next** until the display shows **Network Status**. Press **Enter**.

The display shows **IPv4 Network Enabled**. Press **Enter**.
4. Press **Next** until the display shows the IP address.
5. Press **Cancel** until the display shows the home screen.

Reset to default settings

About this task

The library can reset most of the configurations to the factory defaults, while retaining the settings necessary to use the RMI. The library will perform an inventory after the defaults are restored.

- SCSI addresses: The SCSI ID for the bottom drive is 4; the SCSI ID for the top drive is 5. The library will no longer recall a drive that has been removed.
- Master drive: reset to Drive 1 or the lowest numbered existing drive

The following settings are not reset:

- Administrator password
- Network settings (network is always enabled)

Procedure

1. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Configuration**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Library**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Reset to Default Settings**. Press **Enter** to select.

Saving the configuration settings to a USB flash drive

About this task

This feature is useful when installing multiple devices. Either save the configuration before configuring the network or ensure that only one device with the same network configuration is on the network at a time.



NOTE

You can also save the configuration settings to a file from the RMI.

Procedure

1. Insert the USB flash drive in the USB port on the back of the library.
2. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Configuration**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Library**. Press **Enter** to select.

4. Press **Previous** or **Next** until the screen displays **Save Config to USB Device**. Press **Enter** to save.
5. When the save operation is completed, remove the USB flash drive from the USB port.

Restoring the configuration settings from a USB flash drive

Procedure

1. Insert the USB flash drive in the USB port on the back of the library.
2. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Configuration**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Library**. Press **Enter** to select.
4. Press **Previous** or **Next** until the screen displays **Restore Config from USB**. Press **Enter**.
5. Press **Previous** or **Next** until the screen displays the filename of the device configuration file on the USB drive. Press **Enter** to select the configuration file.
6. When the restore operation is completed, remove the USB flash drive from the USB port.

Downloading product firmware

Procedure

1. Product firmware can be found on the HPE Support Center at: <https://www.hpe.com/support/hpesc>.



IMPORTANT

Certain updates accessed through the Hewlett Packard Enterprise Support Center may require valid product entitlements. Make sure that your HPE Passport account is configured with the necessary entitlements. To review and manage your entitlements, as well as link your contracts and warranties to your profile, see <https://www.hpe.com/support/AccessToSupportMaterials>.

2. Browse or search for the necessary firmware.
3. Download the firmware.

To upgrade the library or drive firmware from the OCP, first copy the firmware image onto a USB flash drive formatted with FAT-32. Insert the USB drive into the library's USB port, then follow the prompts on the OCP to update the firmware.

Resetting the RMI administrator password and OCP PIN

Prerequisites

You can see the library OCP while you contact Hewlett Packard Enterprise support. The temporary administrator password is generated based on the current date and time shown on the OCP.

About this task

If you have the OCP PIN, see [Resetting the RMI administrator password](#).

If both the RMI administrator password and the OCP administrator PIN are lost or forgotten, use the following procedure,

Procedure

1. Obtain a temporary administrator password from Hewlett Packard Enterprise support.

Hewlett Packard Enterprise support will request the current date and time shown on the OCP login screen.
2. From the library OCP, select **Lost PIN**.
3. Enter the temporary administrator password.
4. When prompted, enter a new temporary RMI PIN.
5. Use a browser to access the library RMI and log in using the temporary administrator RMI PIN.
6. When prompted, enter a new RMI administrator password and then repeat the password. For password guidelines, see [Password rules](#).
7. Set a new OCP administrator PIN.
 - a. Navigate to **RMI > Configuration > User Accounts**.
 - b. Select **Modify OCP PINs** and then set a new OCP administrator PIN.

Maintenance

Subtopics

[Maintenance through RMI](#)

[Maintenance through OCP](#)

Maintenance through RMI

Subtopics

[Library tests](#)

[Logs and traces](#)

[Firmware upgrades](#)

[Download support ticket](#)

[System reboot](#)

[Drives](#)

[Controlling the UID LED](#)

[Starting LTO-9 New Media Initialization Wizard](#)

Library tests

Subtopics

[Performing the system test](#)

[Performing the slot to slot test](#)

[Performing the element to element test](#)

[Performing the position test](#)

[Performing the wellness test](#)

[Performing the robotic test](#)

Performing the system test

Prerequisites

- The library must contain at least one compatible cartridge for the tape drive in the library.
- The tape drives must be empty before starting the test.

To remove a tape from a tape drive, use the backup application or **Move Media** command from the RMI.

About this task

The system test exercises overall library functionality by moving cartridges within the library.

- During each cycle, the library moves a cartridge from a full slot to an empty slot and then returns it to its original slot. You can select the number of cycles for the test. If the test is canceled, the library will return the cartridge to its original slot.
- The library will not move cleaning cartridges during the test.
- The test operates over the whole library and does not consider partition configuration.
- During the test, the library is offline.

Procedure

1. Navigate to **Maintenance > Library Tests > System Test**.
2. Select the number of test cycles.
3. Select the media handling option:
 - **Seating:** The cartridge is loaded into the tape drive but is not threaded onto the take-up reel. Choose this option for a faster test.
 - **Threading:** The cartridge is loaded into the tape drive and threaded in the drive. Choose this option for a complete test of the tape drive mechanical operation.
4. Click **Start Test**.

Performing the slot to slot test

Prerequisites

- The library must have at least one cartridge, which can be in any slot.
- The library must have at least one empty slot.

About this task

The slot-to-slot test randomly exchanges cartridges between slots to verify that the library is operating correctly. At the end of the test, the cartridges are NOT returned to their original slots. If a data cartridge is moved to an incompatible drive, the drive will reject the cartridge, as designed.

Procedure

1. Navigate to **Maintenance > library Tests > Slot to Slot Test**.
2. Select the number of cycles.
3. Click **Start Test**.

Performing the element to element test

Prerequisites

- The test requires at least one cartridge in the library.

If moving a cartridge to or from a tape drive, the cartridge must be compatible with the generation of the tape drive.

- One of the selected element locations must be empty and one of the selected element locations must be full.

About this task

The element to element test moves a selected cartridge to a selected slot or tape drive, and then returns it to the original slot. You can select the number of times to move the selected cartridge to the destination location and back.

The element to element test is intended to show that the library is operating correctly. To diagnose problems with the robotic assembly or verify that it has been correctly replaced, use the robotic test.

Procedure

1. Navigate to **Maintenance > library Tests > Element to Element Test**.
2. Select a cartridge from the **Source Elements** list.
3. To select from a subset of the cartridges:
 - a. Click **Filter On**.
 - b. Enter characters in the search box, and then click **Search**.

The **Source Elements** list is updated only to include cartridges with a barcode label including the search characters.

4. Select a location from the **Destination Elements** list.
5. Select the number of cycles.

6. Click **Start Test**.

Performing the position test

About this task

The position test moves the robotic between two element addresses for the specified number of cycles. The test does not move cartridges.

Procedure

1. Navigate to **Maintenance > Library Tests > Position Test**.
2. Select the source and destination element addresses and number of cycles.
3. Click **Start**.

Performing the wellness test

Prerequisites

- At least one drive must be empty.
- At least one cartridge that is compatible with the empty drive must be in a magazine slot or mailslot.

If moving a cartridge to or from a tape drive, the cartridge must be compatible with the generation of the tape drive.

- One of the selected element locations must be empty and one of the selected element locations must be full.
- All backup operations are stopped.

The test takes the library offline to hosts for the duration of the test.

About this task

The wellness test exercises basic library functionality. At the end of the test, cartridges will be in different storage slots.

Procedure

1. Navigate to **Maintenance > Library Tests > Wellness Test**.

2. Click **Start Test**.

Performing the robotic test

About this task

The robotic test performs a full inventory and exercises all robotic assembly movements and sensors.

Procedure

1. Navigate to **Maintenance > Library Tests > Robotic Test**.
2. Click **Start Test**.

Logs and traces

Subtopics

Viewing log files

Downloading log and trace files

Viewing log files

Procedure

1. Navigate to the **Maintenance > Logs and Traces > View Logs**.
2. Select one of the logs.
 - a. **Event Ticket Log**: Records library error and warning events
 - b. **Information Log**: Records library information events
 - c. **Configuration Log**: Records configuration changes
 - d. **Show All**: Displays events from all the above logs
3. Check the box next to **Include closed tickets** to display events that have been marked as closed.

The log entries are displayed in order of most recent to oldest. The log entries contain a date and time code, event code, severity, component identifier, and event details.

Downloading log and trace files

About this task



NOTE

When possible, download support tickets instead of log and trace files. Support tickets have complete information about library events and are more useful for support engineers.

Procedure

1. Navigate to **RMI > Maintenance > Logs and Traces > Download Logs and Traces**.
2. Click **Save**.

Firmware upgrades

The firmware version installed on the library is displayed in the library status area on the home page.

Subtopics

System firmware

Drive firmware

Updating library firmware from the OCP

System firmware

Procedure

1. Download the firmware file to the system running the browser that is logged into the RMI.
2. Navigate to **RMI > Maintenance > Firmware Upgrades > System Firmware**.
3. Click **Choose File** and select the firmware file from the local computer.

4. Once the firmware file is selected, click the **Upload** button to start the upgrade process.
5. Once the firmware file is uploaded, the RMI will be briefly disconnected while the library updates and reboots. Do not log back into the RMI until the login page displays the new firmware version.

Drive firmware

Procedure

1. Navigate to **RMI > Maintenance > Firmware Upgrades > Drive Firmware**.
2. Select the tape drive.
3. Click **Choose File**, and then select the firmware file from the local computer.
4. Click **Submit**.

Results

To see the current firmware version installed on the drives, navigate to **Status > Drive Status**.

Updating library firmware from the OCP

Procedure

1. Copy the firmware file to a USB flash drive.
2. The library only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.
3. Insert the USB thumb drive into the USB port on the back of the library.
4. In the OCP, navigate to **Maintenance > Upgrade Lib from USB device**.
5. Select the firmware file.
6. Click **Start Upgrade**.

Download support ticket

Subtopics

[Drive support ticket](#)

[Library support ticket](#)

Drive support ticket

Procedure

1. Navigate to **Maintenance > Download Support Ticket**.
2. Expand the drive support ticket list, if necessary, by clicking the down arrow on the left side of the screen. The drive list displays:
 - **Drive** — The drive number. Drives are numbered, starting with number one at the bottom of the library. Each drive above is given the next higher number as you move up the library.
 - **Type** — The drive type, form factor (half height or full height), and interface type
 - **Firmware** — The current drive firmware version
 - **Serial** — The drive serial number
 - **Partition** — The logical library associated with the tape drive
3. Select the drive.
4. Select the ticket to download.
 - **Current Ticket** — Pulls and saves a new support ticket from the drive. The Current Ticket contains detailed drive logs and is useful when working on an issue with a service engineer.
 - **Last Unload Ticket** (LTO-6 and earlier) — Saves the ticket that was pulled automatically after the last cartridge was unloaded from the drive.
 - **Health Log** (LTO-7 and later) — Pulls and saves a new support ticket with less information than the Current Ticket. The Health Log is faster to download when you only need basic drive health information.
5. Click **Save**.

Library support ticket

Procedure

1. Navigate to **Maintenance > Download Support Ticket**.
2. Expand the **Library Support Ticket** area, if necessary, by clicking the down arrow on the left side of the screen.
3. Click **Save**.

System reboot

Procedure

1. Navigate to **Maintenance > System Reboot**.
2. Click **Reboot**.

Drives

Subtopics

Rebooting a tape drive

Clearing drive reservations

Rebooting a tape drive

Procedure

1. Navigate to **Maintenance > Drives > Drive**.
2. Select the drive to be rebooted.
3. Click **Submit**.

Clearing drive reservations

Prerequisites

- A host is able to connect to a drive or library.
- Commands are rejected with a `reservation conflict` error or a generic I/O error.

About this task

Hosts can reserve drive access or library access for exclusive use by a specific host port. If a connection is lost due to a host crash, link break, or other failure while a host has a reservation, access to that device from other hosts can be blocked.

Procedure

1. Navigate to **Maintenance > Drives > Clear Drive Reservation**.
2. Select the drive for reservation clearing.
3. Click **Submit**.

Controlling the UID LED

About this task

The UID LED is a blue LED on the controller. The UID LED is useful for identifying the library in a data center. The user controls the UID LED.

Procedure

1. Navigate to **Maintenance > UID LED Control**.
2. To change the LED status, select the controller, and click **Switch LEDs On** or **Switch LEDs Off** button.

Starting LTO-9 New Media Initialization Wizard

About this task



IMPORTANT

- This procedure is for new media only and not meant for media that have been initialized.
- The library will be offline to hosts while the LTO-9 New Media Initialization Wizard is running.
- Media Initialization can take up to two hours per tape to complete.

Procedure

1. Navigate to **Maintenance > LTO-9 New Media Initialization Wizard**.
2. Click **Start LTO-9 New Media Initialization Wizard**.
3. Click **Next** on the **Information**.
4. Select one or more cartridges that you want to initialize and click the right arrow. If all the cartridges need to be initialized, click **Select All**, then click the right arrow.

This will place the cartridges in the section to the right, titled **Selected Cartridges**.

5. Click **Next**.
6. Select the drive to be used for initializing the media and click the right arrow. If all the drives are to be used, click **Select All**, then click the right arrow. This will place the drives in the section to the right titled **Selected Drives**.
7. Click **Next**.
8. Click **Finish** to complete the wizard and begin the media initialization process on the selected tapes. The wizard screen will show the progress as the process completes. If you click **Exit**, you will leave the wizard,

but the process will continue and updates will be displayed on the **Maintenance > LTO-9 New Media Initialization Wizard** page.



NOTE

If needed, it is possible to end the media initialization process. It should be noted, however, that once a tape is loaded into a drive, that media will complete its initialization, which could take up to two hours. Once the loaded media completes initialization, the wizard will end and not process any remaining media that was selected.

Subtopics

Initialization estimated times

Initialization estimated times

All new LTO-9 tapes require an industry-wide standard initialization process the first time that they are loaded into an LTO-9 drive. It is a one-time process per tape, and is required on all new LTO-9 media from all vendors. For a new library with all new tapes, the time required to run the initialization wizard for eight tapes with a single LTO-9 drive could take up to 16 hours.



NOTE

- The LTO-9 initialization wizard is one method for initializing new media on the MSL2024 G4 library. The wizard helps users initialize a batch of new media with one operation, rather than initializing all the tapes in an entire library at once. Another option is to let each piece of media automatically initialize upon the first load into a drive. Most ISV software is designed to allow for this media initialization time as it is an industry-wide standard. This will add that initialization time (up to two hours) to the backup window the first time a new, unused tape cartridge is loaded to a drive by the application. This spreads out the time required to initialize many new tapes by performing the initialization as needed on each tape rather than all at once.
- The two-hour per tape initialization time is an absolute worst-case scenario; the actual time is often much less.

Maintenance through OCP

1. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Maintenance**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays your selected function. Press **Enter** to select.

Subtopics

Saving a support ticket

Saving log files

Upgrade library firmware

Saving drive support ticket

Upgrade drive firmware from a USB flash drive

Updating drive firmware from OCP

Firmware verification and configuration backup procedure

Saving a support ticket

About this task

A support ticket contains information that can help a system administrator or support engineer diagnose library problems.

Use this option to download a support ticket to a USB flash drive. Downloading the support ticket to a USB flash drive lets you view the ticket on a computer that is not connected to the library.

You can view the support ticket with the Library & Tape Tools.

Procedure

1. Insert the USB flash drive in the USB port on the back of the library.
2. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Maintenance**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Save Lib Ticket to USB Device**. Press **Enter** to select.
4. Once the ticket has been saved, the display will read **Save Successful**. Press any button to return to the menu.
5. Remove the USB flash drive from the USB port.

Saving log files

About this task

Library logs contain information that can help a system administrator or support engineer diagnose library problems.

Use this option to download the log file to a USB flash drive. Downloading the log file to a USB flash drive lets you view the logs on a computer that is not connected to the library.

Procedure

1. Insert the USB flash drive in the USB port on the back of the library.
2. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Maintenance**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Save Lib Logs to USB Device**. Press **Enter** to select.
4. Once the logs have been saved, the display will read **Save Successful**. Press any button to return to the menu.
5. Remove the USB flash drive from the USB port.

Upgrade library firmware

About this task

The library allows two types of firmware to be upgraded — one for the tape drive and the other for the library itself.

You can upgrade both types of firmware from a USB flash drive using the OCP.

Procedure

1. Download current library firmware from <https://www.hpe.com/support/storage>.

2. Copy the firmware onto the USB flash drive.

**TIP**

The display will only show the first 16 characters of the file name. If the USB drive has multiple firmware files, ensure that you can distinguish the files from the first 16 characters in their file names.

3. Insert the USB flash drive in the USB port on the back of the library.
4. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Maintenance**. Press Enter to select.
5. Press **Previous** or **Next** until the screen displays **Upgrade Lib from USB Device**. Press Enter to select.
6. Press **Previous** or **Next** until the screen displays the filename of the library firmware file on the USB drive. Press **Enter** to select the firmware file.
7. Press **Enter** when the display shows **Are you Sure? Yes**.
8. Once the firmware file has been updated, the library will reboot.
9. Remove the USB flash drive from the USB port.

Saving drive support ticket

About this task

A support ticket contains information that can help a system administrator or support engineer diagnose drive problems.

Use this option to download a support ticket to a USB flash drive. Downloading the support ticket to a USB flash drive lets you view the ticket on a computer that is not connected to the library.

You can view the support ticket with the Library & Tape Tools.

Procedure

1. Insert the USB flash drive in the USB port on the back of the library.
2. Login to the OCP as Administrator, then press Previous or Next until the screen displays Maintenance. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Save Drv Ticket to USB Device**. Press Enter to select.
4. Press **Enter** when the display shows Select Drive Drive 1.

5. Press **Previous** or **Next** to select either **Current Ticket** or **Health Log** when the display reads **Select Dump Mode**. Press **Enter**.

**NOTE**

The current ticket will contain more information, and is more useful for troubleshooting drive issues.

6. Press **Enter** when the display shows **Are you Sure? Yes**.
7. Once the ticket has been saved, the display will read **Save Successful**. Press any button to return to the menu.
8. Remove the USB flash drive from the USB port.

Upgrade drive firmware from a USB flash drive

About this task

The library allows two types of firmware to be upgraded — one for the tape drive and the other for the library itself.

You can upgrade both types of firmware from a USB flash drive using the OCP.

Procedure

1. Download current drive firmware from the <https://www.hpe.com/support/storage>.
2. Copy the firmware onto the USB flash drive.

**TIP**

The display will only show the first 16 characters of the file name. If the USB drive has multiple firmware files, ensure that you can distinguish the files from the first 16 characters in their file names.

3. Insert the USB flash drive in the USB port on the back of the library.
4. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays Maintenance. Press **Enter** to select.
5. Press **Previous** or **Next** until the screen displays **Upgrade Drive from USB Device**. Press **Enter** to select.
6. Press **Enter** when the display shows **Select Drive Drive 1**.

7. Press **Previous** or **Next** until the screen displays the filename of the drive firmware file on the USB drive. Press Enter to select the firmware file.
8. Press **Enter** when the display shows **Are you Sure? Yes**.
9. Once the firmware file has been updated, the drive will reset and the Ready light on the library will be on.
10. Remove the USB flash drive from the USB port.

Updating drive firmware from OCP

Procedure

1. Copy the firmware file to a USB flash drive.
2. The library only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.
3. Insert the USB thumb drive into the USB port on the back of the library.
4. Navigate to **OCP > Maintenance > Upgrade Drive from USB device**.
5. Select the firmware file.
6. Click **Start Upgrade**.

Firmware verification and configuration backup procedure

Procedure

1. Verify that the library and drives have the latest firmware version:
 - The library firmware version is displayed on the RMI login page and in the top-left corner of the RMI screen after logging in.
 - The drive firmware version is shown at **RMI > Status > Drive Status**.
2. Log in to the OCP.
 - a. Press **Next** until the display reads information or status, then press **Enter**.
 - b. Press **Next** until the display reads library status, then press **Enter**.

- c. Press **Next** until the display shows firmware version; note the installed firmware version.
 - d. Press **Cancel** to return.
3. Check the drive firmware version:
 - a. Press **Next** until the display reads drive 1 status, then press **Enter**.
 - b. Press **Next** until the display shows the drive firmware version; note the value.
 - c. For additional drives, repeat this step for each one.
4. Check the current available firmware version, see [Accessing the compatibility matrix](#).
5. If required, update the library firmware through:
 - **OCP > Maintenance > Upgrade Lib from USB device**, or
 - **RMI > Maintenance > Firmware Upgrades > System Firmware**.
6. If required, update the drive firmware through:
 - **OCP > Maintenance > Upgrade drive from USB device**, or
 - **RMI > Maintenance > Firmware Upgrades > Drive Firmware**.
7. After configuring the library, back up the configuration:
 - Save to a USB flash drive through **OCP > Configuration > Save Config to USB Device**, or
 - Save to a file on your computer through **RMI > Configuration > System > Save/Restore Configuration**.

**NOTE**

Maintaining a backup helps when recovering from configuration errors or during servicing.

8. If needed, set the security user password through **RMI > Configuration > User Accounts**.

**NOTE**

The account is only necessary for accessing hardware encryption settings.

Operations

Subtopics

Command View TL TapeAssure

LTFS Support

Operating through RMI

Operating through OCP

Command View TL TapeAssure

HPE Command View TL (CVTL) software provides a browser-based GUI for remote management and monitoring of most Hewlett Packard Enterprise libraries. With Command View TL, you can view and analyze the performance and health of supported tape drives and media in multiple devices at the same time. In addition, TapeAssure displays more extensive drive and media health information than is visible in the RMI.

Command View TL software is installed on a management station. For best performance, locate the management station in the same physical location and on the same IP subnet as the library. Command View TL software is available for download from the Hewlett Packard Enterprise website at <https://www.hpe.com/support/cvttl>.

For information on installing and using Command View TL, see the HPE Storage Command View TL User Guide, available from the Hewlett Packard Enterprise Support Center at: <https://www.hpe.com/support/hpesc>.

Command View TL support is included in all library firmware that supports LTO-5 and later generation tape drives. To find and download the most up-to-date firmware version, visit the Hewlett Packard Enterprise support website at <https://www.hpe.com/support/hpesc>.

LTFS Support

The HPE StoreOpen Software application for Microsoft Windows simplifies use of the Linear Tape File System (LTFS) functionality. LTFS makes tape self-describing, file-based, and easy-to-use. The application extends LTFS functionality, presenting the library and its tape cartridges as a collection of folders. This extension results in easy data access and management. For more information about LTFS capabilities, see <https://www.hpe.com/storage/StoreOpen>.

Operating through RMI

Subtopics

Moving media

Opening a mailslot

Opening a magazine

Initiating a drive cleaning operation

Rescanning the cartridge inventory

Forcing a drive to eject a cartridge

Moving media

Procedure

1. Navigate to **Operation > Move Media**.

2. Select the cartridge from **Source Elements**.

Available source elements are tape drives, enabled mailslots, and storage slots that contain a data cartridge.

Slots are listed in numerical order. Each slot is numbered as **m . s**, where **m** is the module number and **s** is the slot within the module.



NOTE

The library is configured with a single module. As a result, all storage slots are designated using the format **1 . s**, where **s** indicates the slot number.

3. To see a subset of the cartridges in the library, click **Barcode Filter On**, enter some or all the barcode label characters in the search area and click **Search**.

The **Source Elements** list updates to display only the cartridges with labels that include the characters in the search box.

4. To perform a different search or display all the available cartridges, click **Barcode Filter Off**.

5. Select the destination location from **Destination Elements**.

Available destination elements are tape drives, enabled mailslots, and storage slots that do not contain a data cartridge.

6. Click **Submit**.

Opening a mailslot

Procedure

1. Navigate to **Operation > Open Magazine**.
2. Click **Open** for the mailslot.

The library will release the lock. A message will be displayed on the OCP that the mailslot is unlocked.

Opening a magazine

About this task



WARNING: Hazardous Moving Parts

Hazardous moving parts exist inside this product. Do not insert tools or any part of your body into the magazine openings to avoid injury.

Only personnel with appropriate technical and product safety training (referred to as "users" in this document) may access or operate the tape library.

Read all documentation and procedures before installing or operating the magazine extension.

- Opening a magazine will take the library off line.
- The magazines will relock after 30 seconds.
- If a host application set the Prevent Media Removal (PMR) setting for the library, the library displays **Removal Prevented** instead of the **Open** button. If you must open the magazine manually, have the application release the PMR setting for the magazine.

Procedure

1. Navigate to **Operation > Open Magazine**.
2. Click **Open** for the magazine.

The library will release the lock. The OCP will display a magazine unlocked message.

Initiating a drive cleaning operation

Procedure

1. Navigate to **Operation > Clean Drive**.
2. Select a cleaning cartridge from the **Source Elements** list. The library uses the barcode label to identify cleaning cartridges.
3. If no cleaning cartridges are available, load one into a mailslot or magazine slot.
4. Select the tape drive to be cleaned from the **Destination Elements** list.
5. Tape drives currently containing a cartridge are not listed. To clean an unlisted tape drive, move the cartridge out of the drive.
6. Click **Submit**.

Rescanning the cartridge inventory

Procedure

1. Navigate to **Operation > Rescan Inventory**.
2. Click **Rescan**.

Library status will change to Scanning. Other operations will be unavailable until the scan is complete. A progress indicator will display in the top banner during a full library inventory.

Forcing a drive to eject a cartridge

About this task

The force drive media eject operation attempts to force the tape drive to eject the cartridge and place it into an open slot.

Before performing this operation, attempt to eject the data cartridge using the backup software or using the library, move the media operation through the RMI. While a drive is being force ejected, a window indicating the process is ongoing should appear. No operations will be available until the force eject completes.

Procedure

1. Navigate to **Operation > Force Drive Media Eject**.

2. Select the drive in the **Source Elements** list.
3. Select the destination in the **Destination Elements** list.
4. Click **Submit**.

Subtopics

Difficulty ejecting a cartridge

Difficulty ejecting a cartridge

Symptom

A drive has difficulty ejecting a cartridge.

Cause

This problem is usually caused by bad or damaged media.

Action

Remove the cartridge from the media pool,

Operating through OCP

1. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Operation**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays your selected function. Press **Enter** to select.

Subtopics

Unlocking magazines

Unlocking mailslot

Unlocking magazines

Procedure

1. Login to the OCP as Administrator, then press **Previous** or **Next** on the OCP until the screen displays **Operation**.
2. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays either **Magazine Unlock Left** or **Magazine Unlock Right**.
4. Press **Enter** to select the desired magazine to unlock.
5. The display reads **Magazine unlocked for 30s**.
6. Pull the released magazine out of the library.
7. The library cannot perform any other operation until the magazine is replaced. After exchanging tapes in a magazine, slide the magazine completely into the library. The magazine locks into place once it is correctly installed and the device inventories the magazine. The Ready LED blinks while the device inventories the magazine and then stops when the operation is complete.

Unlocking mailslot

Procedure

1. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays Operation. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays Mailslot Unlock. Press **Enter**.
3. The display reads **Mailslot unlocked for 30s**.
4. Pull the left magazine handle to open the mailslot and remove or insert media as desired. Slide the mailslot closed and the mailslot will lock into place and the library will inventory the mailslot. The Ready LED blinks while the device inventories the mailslot and then stops when the operation is complete.

Status

Subtopics

Viewing status information through RMI

This section describes the various tasks available from the **Status** menu on the RMI Home screen.

Subtopics

- [Library status](#)
- [Cartridge inventory](#)
- [Partition map](#)
- [Viewing drive status](#)
- [Network status](#)
- [Command View TL status parameters](#)
- [Security](#)

Library status

Procedure

1. See summary information and status in the top banner and left side bar.
2. For additional library configuration and status information, navigate to **Status > Library Status**.

Subtopics

- [Library information and status](#)

Library information and status

Parameters	Library information
Vendor	Vendor ID of the SCSI Inquiry string
Product ID	Product ID of the SCSI Inquiry string
Serial Number	library serial number

Parameters	Library information
Base Firmware Revision	
Base Controller Revision	
Robotic Hardware Revision	
Robotic Firmware Revision	Version of the currently installed robotic assembly firmware. The robotic assembly firmware is bundled and installed with the library firmware.
Barcode Reader Hardware Revision	
Barcode Reader Firmware Revision	Version of the currently installed barcode reader firmware. The barcode reader firmware is bundled and installed with the library firmware.
Library status	Idle: The library robotic is ready to perform an action . Moving: The library robotic is moving a cartridge. Scanning: The library robotic is performing an inventory of cartridges. Offline: The library robotic has been taken off line by the library.
Total Power On Time	Total time that the library has been powered on since it was manufactured.
Cartridge in Transport	When applicable, displays the barcode label of the cartridge currently in the robotic assembly.
Odometer	Robotic assembly move count.
Left Magazine Status	The lock status of the left magazine.
Right Magazine Status	The lock status of the left magazine.
Mailslot Status	The lock status of the mailslot.
Shipping Lock	The shipping lock status.

Cartridge inventory

Procedure

In the **Status > Cartridge Inventory > Graphical View**, you can see a graphical representation of the cartridges in each magazine. Elements containing media are designated with a barcode label. Hover over a cartridge to see information about that cartridge.

Subtopics

Using the partition map graphical view

Using list views

Using the partition map graphical view

Procedure

1. Navigate to **Status > Partition Map > Graphical View**.

This screen displays a graphical representation of the cartridges in the storage slots, mailslots, and tape drives.

2. The partition number is shown for each element.
3. Hover over an element for status and configuration information about the partition or drive.

Using list views

About this task

The inventory lists display each of the elements, such as slots and tape drives, with information about the cartridge stored in the element.

Procedure

1. Navigate to one of the list views.
 - To see the elements organized by module, navigate to **Status > Cartridge Inventory > List View**.
 - To see the elements organized by logical library or partition, navigate **Status > Partition Map > List View**.
2. In the inventory list, you could see:

- **Slot #**—The slot number in the form `<module>.<slot>`, where `module` is the module number and `slot` is the slot number.



NOTE

The library is configured with a single module. As a result, all storage slots are designated using the format `1.s`, where `s` indicates the slot number.

- **Barcode**—Barcode label
 - **Full**—**X** if a cartridge is using the element.
 - **Gen**—LTO generation of the cartridge
 - **Partition**—The partition number
3. To filter the list based on barcode label, enter characters in the filter box and then click **Search**.
 - a. Click **Filter On**.

The search box is displayed.
 - b. Enter characters into the search box and then click **Search**.

The characters can be anywhere in the barcode label. The search characters are not case sensitive. There are no wildcards.
 4. To disable filtering, click **Filter Off**.
 5. To limit the list to tape drives, click **Drives**.
 6. To limit the list to cartridges, click **Cartridges**.

Partition map

About this task



NOTE

The configurations listed in this screen can be modified using the Expert Partition Wizard. See [Using the expert partition wizard](#).

Procedure

Navigate to **Status > Partition Map > Configuration Status**.

The library displays the current configuration settings for the partition.

Subtopics

Configuration Status screen parameters

Configuration Status screen parameters

Settings	Description
Partition Number	The partition number assigned by the library.
Partition Name	The partition name assigned with one of the partition wizards.
Partition S/N	The partition serial number assigned by the library.
Number of Drives	The number of tape drives configured for the partition. Expand the section to see information about each drive, including the drive number, LTO generation, interface, and serial number.
Number of Slots	The number of storage slots assigned to the partition.
Number of Mailslots	The number of mailslots assigned to the partition.
Barcode Label Length Rep. to Host	The number of barcode characters reported to the host application.
Barcode Label Alignment Rep. to Host	The end of the barcode label reported to the host application when reporting fewer than the maximum number of characters. For example, when reporting only six characters of the barcode label <code>12345678</code> , if alignment is left (the default), the library will report <code>123456</code> . If the alignment is right, the library will report <code>345678</code> .
Auto Clean	Indicates whether library-managed cleaning is enabled or disabled.
Key Manager Type	The type of encryption key manager configured for use with the partition.
FIPS Support Mode	Indicates whether FIPS support mode is enabled or disabled.
Active Control Path Drive	The tape drive that hosts the LUN for the partition.

Settings	Description
LTO-7+ Multi-initiator SCSI Conflict Detection	Indicates whether LTO-7+ Multi-Initiator SCSI Conflict Detection is enabled or disabled.

Viewing drive status

Procedure

In the **Status > Drive Status** screen, you can see the configuration and status of the drive installed in the library.

Subtopics

Drive Status configuration settings

Drive Status configuration settings

Settings	Description
Drive number	Drives are numbered, starting with number one at the bottom of the library. Each drive above is given the next higher number as you move up the library. The drive currently hosting the SCSI communication for the library is designated with (LUN) .
Serial number	The serial number assigned to the tape drive by the library. This serial number is reported to host applications.
LTO generation	- LTO 6—Ultrium 6250 - LTO 7—Ultrium 15000 - LTO 8—Ultrium 30750 - LTO 9—Ultrium 45000
Drive form factor	HH—Half height FH—Full height

Settings	Description
Drive interface	• FC—Fibre Channel • SAS—Serial Attached SCSI
Status icon	•  - Status OK - All library components are fully operational, no user intervention is required. •  - Status Warning - User attention is necessary, but the library can still perform most operations. To display the event ticket log, click the icon. •  - Status Error - User intervention is required and the library is not capable of performing some operations. To display the event ticket log, click the icon.
Drive status	• Write—The drive is performing a write operation. • Read—The drive is performing a read operation. • Idle—A cartridge is in the drive but the drive is not performing an operation. • Empty—The drive is empty. • Encrypt—The drive is writing encrypted data.
Power on status	Indicates whether the drive is powered on or off.
Firmware	The version of firmware currently installed on the drive.
Power	On or Off.
Vendor	The Vendor ID of the SCSI Inquiry string.
Personality	A service engineer might request this information.
Manufacturer S/N	The serial number assigned to the drive when it was manufactured. Use this serial number when working with service.
WWNN	Worldwide unique number for the drive. The library assigns WWNNs to the drive bays. If a tape drive is replaced, the WWNN is reassigned to the replacement drive.
Temperature	Internal temperature reported by the drive. The normal temperature range varies depending on the type

Settings

Description

of tape drive. If the temperature gets too high or too low, the drive will report an error to warn you of possible issues.



NOTE

The temperature reported here is not the temperature of the tape path inside the drive, nor is it the temperature of the room or environment where the drive is located.

Partition	Partition to which the drive is assigned.
Encryption	Indicates the type of encryption the drive is configured for.
Cartridge	Information about the cartridge, if any, currently in the drive.
IP Address	Network address assigned to the Ethernet port of the tape drive. The drive ethernet port is not used when installed in the library.
Media Removal	Whether the media can be removed from the drive or not. Many host applications prevent media removal while accessing the cartridge in the tape drive.
Data Compression	Indicates whether the drive is using data compression.
Cooling Fan Status	When the drive cooling fan is operating correctly, the status will be Active.
Product ID	The product ID portion of the SCSI inquiry string.
Firmware Type	For LTO-7 and later drives, indicates whether Normal or Secure Mode firmware is loaded on the drive.
Manufacturer S/N	The serial number assigned to the drive when it was manufactured. Use this serial number when working with service.
WWNN	Worldwide unique number for the drive. The library assigns WWNNs to the drive bays. When a tape drive is replaced, the WWNN is reassigned to the replacement drive. This applies to FC only.
Partition	Partition to which the drive is assigned.
Cartridge	Information about the cartridge, if any, currently in the drive.
Media Removal	Whether the media can be removed from the drive or not. Many host applications prevent media removal while accessing the cartridge in the tape drive.

Settings	Description
Data Compression	Indicates whether the drive is using data compression.
Fibre Channel Fabric Log-in Name	(LTO-6 only)
Port configuration	Drive port status. • WWPN—Displays the worldwide port name, a unique identifier for each interface. • Speed—Displays the current interface speed. • Port Type ◦ Automatic (FC only) ◦ Loop—Enables selection of the Addressing Mode. ◦ Fabric (N/F). • Interface—The status of the port connection. • N-Port ID—Logical port identifier for the FC drive port (FC only). • Fibre Channel Fabric Log-in Name (LTO-6 only) (FC only).

Network status

Procedure

In the **Status > Network** screen, you can see the status of the library network.

Subtopics

Network Status screen parameters

Network Status screen parameters

Settings	Description
Host Name	library host name
Domain Name	library Domain Name
Protocol	IPV4 and/or IPv6
MAC Address	A unique identifier for the library controller network interface
Link Status	Enabled or disabled
Link Speed	Speed of the Ethernet connection to the library
Duplex	Enabled or disabled

Table 1. IPv4 settings

Settings	Description
DHCP	When enabled, the library requests an IP address from a DHCP server each time the library is powered on.
Address	IP address in use by the library. If DHCP is enabled, this address is obtained from the DHCP server. When DHCP is not enabled, the address was configured.
Netmask	The network mask of the library controller used when DHCP is not enabled.
Gateway	The gateway used when DHCP is not enabled.
DNS 1	Address of the first DNS server.
DNS 2	Address of a secondary DNS server (if applicable).

Table 2. IPv6 settings

Settings	Description
Stateless Addressing	When enabled, the library will generate an address for itself based on the routing information obtained from a router advertisement and the MAC address. The library can manage up to five global addresses at the same time, which can be assigned from different routers.
Static Addressing	When enabled, the library will use a statically configured address.

Settings	Description
Static Assigned Address	The IPv6 address when Static Addressing Enabled is on.

Command View TL status parameters

Library information

- **Name**— library name displayed in Command View TL
- **Serial Number**— library serial number reported to Command View TL.
- **Management URL**—Management station URL, including port. For example: https://192.0.2.24:8099.

Product information

- **Name**—Product name reported to Command View TL.
- **Version**— library firmware version reported to Command View TL.

Contact information

- **Name**—Name of the person to contact about management of the library
- **Phone**—Phone number of the contact person
- **Email**—E-mail address of the contact person

Security

Procedure

Navigate to **Status > Security** to see the status of any key servers configured for use with the library, as well as the encryption status of the tape drive and partition.

Subtopics

[Encryption status parameters](#)

[Viewing Secure Manager status](#)

Encryption status parameters

- **USB—MSL Encryption Kit**—Status of the key server token.
- **ESKM**—Status of the connection to the ESKM server.
- **KMIP**—Status of the connection to the KMIP server.
- **Key Server Token Status**—Identity of the key server token, if any, present in the USB port
- **Partition Encryption Status**—Configured encryption method for the partition.
- **Drive Encryption Status**—Whether each drive is configured to encrypt data with the key server configured for the drive's partition.
- **FIPS Support Mode Status**— Displays the FIPS Support Mode for each partition and its associated drives.

Viewing Secure Manager status

Navigate to **Status > Secure Manager** to see the currently defined Secure Manager access groups.

Subtopics

Secure Manager status parameters

Secure Manager status parameters

Hosts

- **Name**—Host name used with Secure Manager. The name is defined when the host is created in Secure Manager and can be modified.
- **WWPN**—World Wide Port Number. The WWPN is defined when the host is created in Secure Manager. To modify the WWPN, remove and then recreate the host.

Drives

- **Drive number**—The drive number assigned by the library. Drives are numbered, starting with number one at the bottom of the library. Each drive above is given the next higher number as you move up the library.

- LTO generation
 - **LTO6**—Ultrium 6250
 - **LTO7**—Ultrium 15000
 - **LTO8**—Ultrium 30750
 - **LTO9**—Ultrium 45000
- Form factor
 - **HH**—Half height
 - **FH**—Full height
- Drive interface
 - **FC**—Fibre Channel
 - **SAS**—Serial Attached SCSI
- **Serial#**—The serial number assigned to the tape drive by the library.
- **Partition**— library partition to which the drive is assigned.
- Available ports—Displays the available ports on the drive.
- **WWPN_A, WWPN_B**—The worldwide port name, a unique identifier for each FC interface. (FC only)
- **Secure Mode**—Indicates whether the drive is running in Secure Mode.

Partition Library LUN Device

- **Name**—The partition name assigned with one of the partition wizards.
- **Serial#**—The serial number of the drive port hosting the LUN, or SCSI communication interface, for the partition.

Viewing status information through OCP

1. Login to the OCP as Administrator or User, then press **Previous** or **Next** until the screen displays **Information/Status**.
2. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays your selected function.

4. Press **Enter** to select.

Subtopics

Viewing library information

Viewing drive information

Viewing network status

Viewing cartridge inventory

Viewing library information

Procedure

1. Login to the OCP as Administrator or User, then press **Previous** or **Next** until the screen displays **Information/Status**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Library Status**. Press **Enter** to select.
3. By using **Previous** or **Next**, you can select from the following information screens:
 - Library Status
 - Moves
 - Power On Time
 - Max Temperature
 - Slots and Mailslots
 - Slots Empty
 - Serial Number
 - Firmware Version
 - Vendor ID
 - Product ID
 - Library Name

Viewing drive information

Procedure

1. Login to the OCP as Administrator or User, then press **Previous** or **Next** until the screen displays **Information/Status**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Drive 1 Status** or **Drive 2 Information**. Press **Enter** to select.
3. By using **Previous** or **Next**, you can select from the following information screens:
 - Powered
 - Activity
 - Load Status
 - Temperature
 - Enabled
 - LUN Master
 - Port A Connected
 - Port A Speed
 - Port A Type
 - Port A ID
 - Port B Connected
 - Port B Speed
 - Port B Type
 - Port B ID
 - Firmware Version
 - Vendor ID
 - Product ID
 - LTO Generation
 - Interface Type
 - Serial Number

Viewing network status

Procedure

1. Login to the OCP as Administrator or User, then press **Previous** or **Next** until the screen displays **Information/Status**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Network Status**. Press **Enter** to select.
3. Press **Previous** or **Next** to access the following information:
 - Protocol
 - DHCP Enabled
 - IPv4 Address
 - IPv4 Netmask
 - IPv4 Gateway
 - MAC Address

Viewing cartridge inventory

About this task

This option provides information on which slots have cartridges and which are empty. The second line on the screen displays one of:

- Full (tapes without barcode labels)
- Barcode identification from the tape
- Empty

The library has the following inventory locations:

- Left magazine
- Right magazine
- Drive 1
- Drive 2 (if two drives are present)

Each location provides tape status information:

- For example, the screen might display **Slot 1 AESO32L9**, where AESO32L9 is the barcode label on the tape, or it might display **Full** or **Empty**.



NOTE

If the mailslot is enabled, the storage slot count is reduced.

Procedure

To view the tape inventory:

1. Login to the OCP as Administrator or User, then press **Previous** or **Next** until the screen displays **Information/Status**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Inventory**. Press **Enter** to select.
3. Use **Previous** or **Next** to select from the following inventory locations:
 - Mailslot
 - Left magazine
 - Magazine Inventory Right
 - Drive 1
 - Drive 2 (if two drives are present)

Working with tape cartridges and magazines

Subtopics

Recommended practices for labeling tape cartridges

Tape cartridges

Magazines

Storage slots

Recommended practices for labeling tape cartridges

The library contains a barcode reader that reads the tape labels and stores the inventory data in memory. The device then provides the inventory information to the host application, OCP, and RMI. A barcode

label on each tape cartridge enables the barcode reader to identify the cartridge quickly, which speeds up inventory time. Make using barcode labels on your tape cartridges a practice.



TIP

The barcode scanner scans each tape or the back of the storage slot until it reads the barcode label for the cartridge or storage slot. If no label is found, it determines that the slot is empty. The barcode scanner can identify a properly labeled cartridge on the first scan. It can identify an empty slot on the second scan. It will try several more scans and then tap on the cartridge before determining that an unlabeled cartridge is in the slot, which takes about four times as long as identifying a properly labeled cartridge.

The inventory time for larger libraries filled with unlabeled cartridges can be long. Even if you do not need the barcode information, use barcode labels to speed up inventory time.

A proper code label includes the Media ID in the last two characters of the barcode. LTO-3 and earlier generation tape drives prevent later generation media from being loaded into the drive. If an LTO-4 or later tape drive is installed in the library or is in the removed state, the library will not load an unlabeled cartridge into an LTO-3 or earlier generation tape drive.

Though not recommended, checking **Ignore Barcode Media ID** in the **RMI > Configuration > System** will keep the library from interpreting the barcode Media IDs.

The host software might track the following information through the associated barcode:

- Date of format or initialization
- Tape cartridge media pool
- Data residing on the tape
- Age of the backup
- Errors encountered while using the tape (to determine if the tape is faulty)



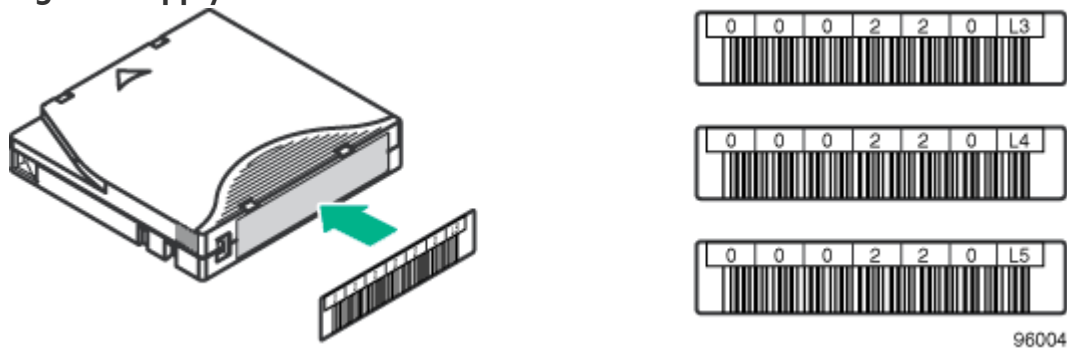
IMPORTANT

Misusing and misunderstanding barcode technology can result in backup and restore failures. To ensure that your barcode labels meet Hewlett Packard Enterprise quality standards, always purchase them from an approved supplier. Do not print barcode labels yourself. To purchase barcode labels, see the Hewlett Packard Enterprise Storage Media website at <https://www.hpe.com/storage/storagemedia>. Search for **Barcode and RFID** to find the document titled: Barcode and RFID labels for HPE Storage tape automation.

Apply a high-quality preprinted barcode label to each tape cartridge.

LTO tape cartridges have a recessed area on the face of the cartridge next to the write-protect switch. Use this area for attaching the adhesive-backed barcode label. Only apply labels as shown:

Figure 1. Apply the label within the recessed area



IMPORTANT

Only apply the barcode label as shown, with the alphanumeric portion facing the hub side of the tape cartridge. Never apply multiple labels onto a cartridge because extra labels can cause the cartridge to jam in a tape drive.

Tape cartridges

Use the data and cleaning tape cartridges designed for your tape drives.

WORM data cartridges

The LTO-3 and later tape drives support both rewritable and WORM data cartridges. Write-Once, Read-Many (WORM) data cartridges provide an enhanced level of data security against accidental or malicious alteration of data on the tape cartridge. The WORM data cartridge can be appended to maximize the full capacity of the tape cartridge. Data cannot be erased or overwritten on the WORM data cartridge. WORM data cartridges have a two-tone cartridge color for easy identification.

To see whether your backup or archive software application supports WORM cartridges, see the Storage Media website at <https://www.hpe.com/storage/storagemedia>.

Subtopics

[LTO-9 Media initialization](#)

[LTO-7 Type M media for LTO-8 drives](#)

[Recommended practices for using and maintaining tape cartridges](#)

[Write-protecting data cartridges](#)

[Read and write compatibility](#)

[Supported media](#)

LTO-9 Media initialization

Media initialization is used in LTO-9 technology to optimize data placement on each LTO-9 cartridge. Each new LTO-9 cartridge requires this one-time initialization prior to starting read/write operations. This is only required for the first use of a new LTO-9 cartridge, subsequent loads do not require additional initialization. The initialization process varies in time depending on the environmental conditions of the tape and drive. Most initializations will complete within an hour; however, in some cases it can take up to two hours.

To help you complete this one-time initialization of new LTO-9 media in tape libraries, Hewlett Packard Enterprise has added a feature to all MSL tape libraries and the 1/8 Autoloader. This new feature, the LTO-9 New Media Initialization Wizard, guides you through an automated process to load a selection of uninitialized media into LTO-9 tape drives to quickly complete the initialization process.

LTO-7 Type M media for LTO-8 drives

The library supports LTO-7 cartridges initialized as Type M media in LTO-8 tape drives. See the library firmware release notes for specific library firmware versions that support LTO-7 Type M media.

Important notes for LTO-7 Type M media:

- When a new, unused LTO-7 cartridge has an 'M8' barcode label applied, it can be initialized as LTO-7 Type M media.



NOTE

The unused tape needs to be loaded and formatted or labeled before it shows as type M media.

- Once an LTO-7 cartridge has been initialized to LTO-7 Type M media, the format is irreversible. Do not place an 'M8' barcode on an LTO-7 cartridge that has been previously used in an LTO-7 drive. A used LTO-7 cartridge cannot be initialized as LTO-7 Type M media, even in an LTO-8 drive.
- LTO-7 Type M media provides up to 9 TB native capacity, instead of the 6 TB specified for LTO-7. As such, LTO-7 Type M media can provide up to 22.5 TB with 2.5:1 compression (depending on the data being compressed.)
- LTO-7 Type M media support regular LTO features, including encryption, LTFS, and compression. LTO-7 Type M media does not support WORM cartridges.
- LTO-7 Type M media are only compatible with LTO-8 tape drives. They are not compatible with any other generation of LTO tape drives.

For more information about LTO-7 Type M media, see <https://www.hpe.com/storage/storagemedia>.

Recommended practices for using and maintaining tape cartridges



CAUTION

Do not degauss LTO data cartridges! These data cartridges are prerecorded with a magnetic servo signal. This signal is required to use the cartridge with the tape drive. Keep magnetically charged objects away from the cartridge.

- Use only the data cartridges designated for your device.
- Clean the tape drive when the **Clean** drive LED is illuminated.



CAUTION

Use only Ultrium Universal Cleaning Cartridges (UCC).

- Do not drop a cartridge. Excessive shock can damage the internal contents of the cartridge or the cartridge case itself, making the cartridge unusable.
- Do not expose data cartridges to direct sunlight or sources of heat, including portable heaters and heating ducts.
- The operating temperature range for data cartridges varies by tape drive generation. For details, see [Environmental specifications](#).
- If the data cartridge has been exposed to temperatures outside the specified ranges, stabilize the cartridge at room temperature for the same length of time it was exposed to extreme temperatures or 24 hours, whichever is less.
- Do not place data 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. The cartridge is unusable without the embedded servo code.
- Place identification labels only in the designated area on the cartridge.

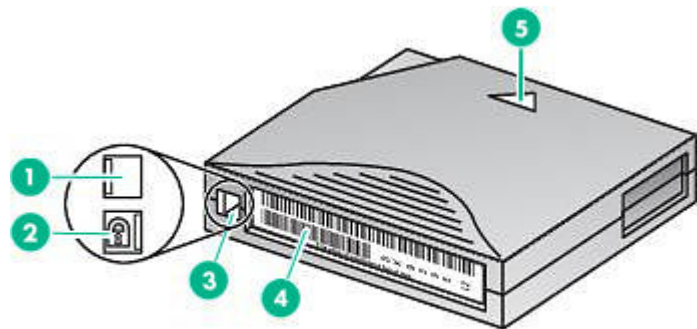
Write-protecting data cartridges

About this task

All rewritable data cartridges have a write-protect switch to prevent accidental erasure or overwriting of data. Before loading a cartridge into the device, ensure that the write-protect switch on the front of the cartridge is in the desired position.

Procedure

- Slide the switch to the **right** to write-protect the cartridge. An indicator, such as a red mark or small padlock, is visible showing that the cartridge is write-protected.



10454

Item	Description
1	Write-enabled
2	Write-protected
3	Write-protect switch
4	Barcode label
5	Insertion arrow

- Slide the switch to the **left** to allow the library to write data to the cartridge.

Read and write compatibility

Hewlett Packard Enterprise Ultrium data cartridges are fully supported and compatible with all Ultrium tape products. Because Hewlett Packard Enterprise Ultrium media is Ultrium logo compliant, it can be used with any other tape drive that bears the Ultrium logo.

	LTO-6 drive	LTO-7 drive	LTO-8 drive	LTO-9 drive
LTO-4 media — unencrypted	Read only	Incompatible	Incompatible	Incompatible
LTO-4 media — encrypted	Read only with encryption key	Incompatible	Incompatible	Incompatible

	LTO-6 drive	LTO-7 drive	LTO-8 drive	LTO-9 drive
LTO-5 media — unencrypted	Read/Write	Read only	Incompatible	Incompatible
LTO-5 media — encrypted	Read/Write with encryption key	Read only with encryption key	Incompatible	Incompatible
LTO-6 media — unencrypted	Read/Write	Read/Write	Incompatible	Incompatible
LTO-6 media — encrypted	Read/Write with encryption key	Read/Write with encryption key	Incompatible	Incompatible
LTO-7 media — unencrypted	Incompatible	Read/Write	Read/Write	Incompatible
LTO-7 media — encrypted	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Incompatible
LTO-7 Type M media — unencrypted	Incompatible	Incompatible	Read/Write	Incompatible
LTO-7 Type M media — encrypted	Incompatible	Incompatible	Read/Write with encryption key	Incompatible
LTO-8 media — unencrypted	Incompatible	Incompatible	Read/Write	Read/Write
LTO-8 media — encrypted	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key
LTO-9 media — unencrypted	Incompatible	Incompatible	Incompatible	Read/Write
LTO-9 media — encrypted	Incompatible	Incompatible	Incompatible	Read/Write with encryption key



NOTE

On LTO-7 and later tape drives, during the initial load of a new tape cartridge, the drive must be able to write to the media. Since LTO-7 drives are capable of reading LTO-5 tapes but cannot write to them, they cannot be the first drive to initially load a brand new LTO-5 tape cartridge. An LTO-5 tape must be written to with an LTO-5 or LTO-6 drive prior to being loaded and read in an LTO-7 drive.

Supported media

Use Hewlett Packard Enterprise storage media to prolong the life of the library and tape drives. To learn more about, or to purchase media, see: <https://www.hpe.com/us/en/storage/storage-media.html>

Cleaning cartridge for all supported tape drives

Cartridge type	Part number
HPE Ultrium universal cleaning cartridge (50 cleans), orange	C7978A

LTO-6 data cartridges

Cartridge type	Part number
HPE LTO-6 Ultrium 6.25 TB MP RW Data Tape, purple	C7976A
HPE LTO-6 Ultrium 6.25 TB BaFe RW Data Tape, purple	C7976B
HPE LTO-6 Ultrium 6.25 TB MP WORM Data Tape, two-tone (purple and gray)	C7976W
HPE LTO-6 Ultrium 6.25 TB BaFe WORM Data Tape, two-tone (purple and gray)	C7976BW

LTO-7 data cartridges

Cartridge type	Part number
HPE LTO-7 Ultrium 15 TB RW Data Tape, blue	C7977A
HPE LTO-7 Ultrium 15 TB WORM Data Tape, two-tone (blue and gray)	C7977W

LTO-7 Type M media for LTO-8 drives

Cartridge type	Part number
HPE LTO-7 Ultrium Type M 22.5 TB RW Custom Labeled Data Cartridges (20 pack)	Q2078ML
HPE LTO-7 Ultrium Type M 22.5 TB RW Non-Custom Labeled Data Cartridges (20 pack)	Q2078MN

LTO-8 data cartridges

Cartridge type	Part number
HPE LTO-8 Ultrium 30 TB RW Data Tape, green	Q2078A
HPE LTO-8 Ultrium 30 TB WORM Data Tape, two-tone (green and gray)	Q2078W

LTO-9 data cartridges

Cartridge type	Part number
HPE LTO-9 Ultrium 45TB RW Data Tape, blue	Q2079A
HPE LTO-9 Ultrium 45 TB WORM Data Tape, two-tone (blue and gray)	Q2079W

Magazines

The library has removable magazines. Magazine access is password protected. For safety reasons, the robotic motion is stopped when a magazine is removed.

The magazines can be released using the OCP, the RMI, or by a manual release. When possible, release the magazine using the OCP or RMI.



IMPORTANT

Only use the manual process if the magazine cannot be released using the OCP or the RMI, and the library no longer has power.

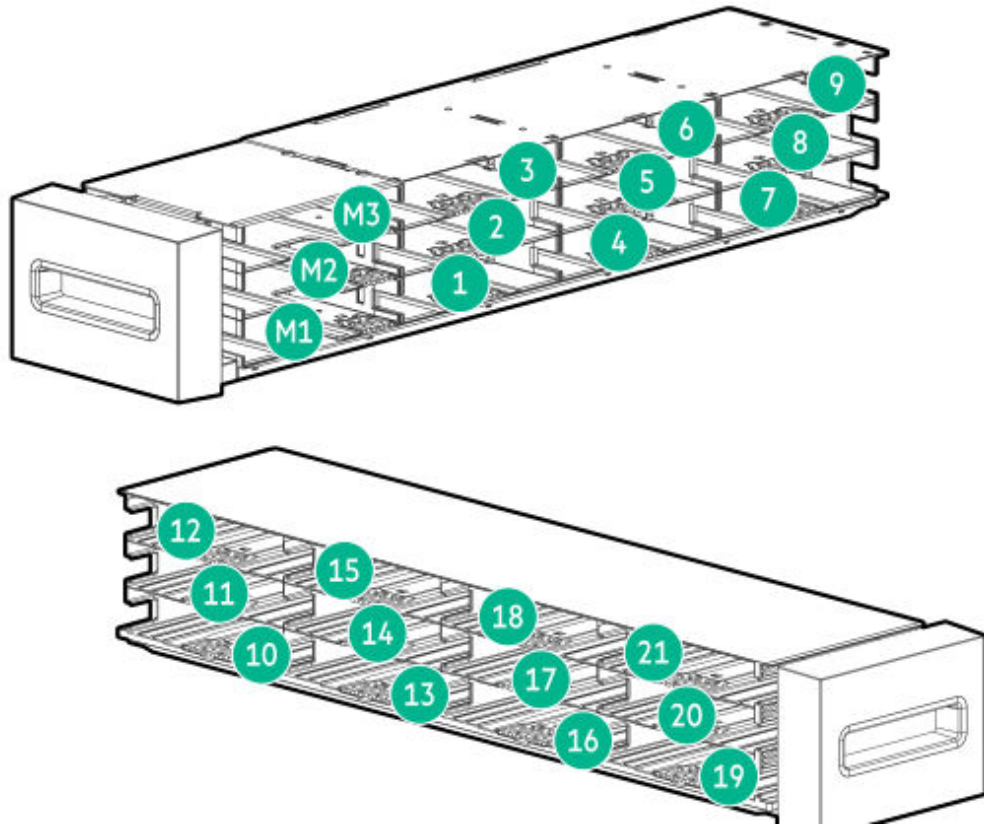
Subtopics

[MSL2024 magazine slot numbering](#)

[Releasing the magazines manually](#)

[Opening a magazine from the OCP](#)

MSL2024 magazine slot numbering



When the mailslot is disabled, the mailslot (M1) becomes Slot 1 and all other slots are renumbered accordingly.

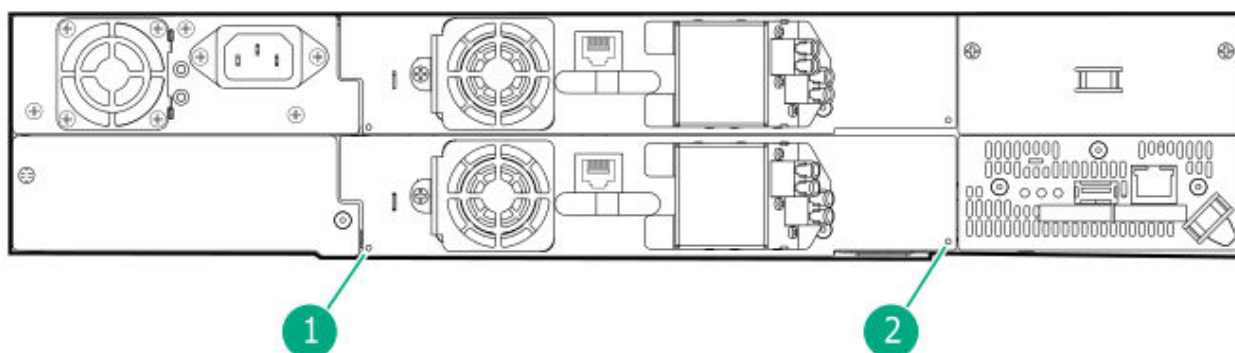
Releasing the magazines manually

About this task

Only use this manual process if the magazine cannot be released using the OCP or RMI, and the device no longer has power.

Procedure

1. If the library is powered on, return all cartridges to the magazines with the RMI **Operation > Move Media**.
2. Unplug the power cord from the library.
3. From the back of the library, find the access holes for the right and left magazines.



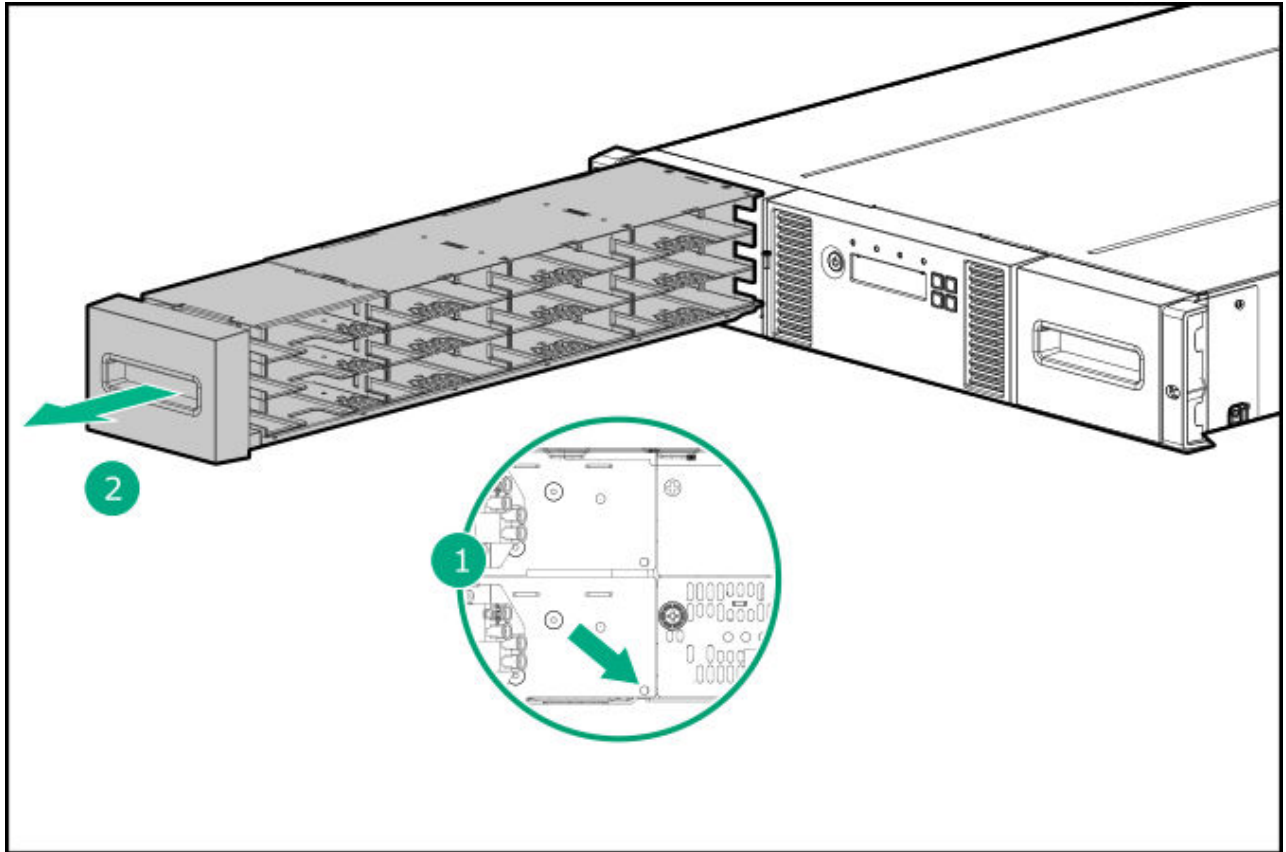
Item	Description
------	-------------

1	Right magazine release access hole
---	------------------------------------

2	Left magazine release access hole
---	-----------------------------------

The magazine release is a small latch.

4. Insert the end of a small metal pin or straightened paper clip into the appropriate magazine access hole at the back of the library about 1.5 cm (0.6 inch), while another person grasps the magazines on that side and pulls them out of the front of the library.



Item	Description
------	-------------

- | | |
|---|--|
| 1 | Push a paper clip into the access hole. |
| 2 | Pull the magazine out of the front of the library. |



IMPORTANT

Do not force the pin once you encounter resistance. Doing so can damage the device.

5. Repeat step 3 for the other magazine if necessary.
6. If other tapes are still in the library, for example loose on the robotic or loose on the bottom of the library, attempt to remove them through the magazine openings. If it is unable to remove the magazines, power cycle the library and attempt removal again.

Opening a magazine from the OCP

About this task



WARNING: Hazardous Moving Parts

Hazardous moving parts exist inside this product. Do not insert tools or any part of your body into the magazine openings to avoid injury.

Only personnel with appropriate technical and product safety training (referred to as "users" in this document) may access or operate the tape library.

Read all documentation and procedures before installing or operating the magazine extension.

Procedure

1. Navigate to **Operation > Magazine Unlock Left** or **Magazine Unlock Right**.
2. The library will release the lock. A message will be displayed on the OCP indicating the magazine is unlocked.
3. Pull the magazine out of the library.



NOTE

The magazine will relock after 30 seconds.

4. Insert the magazine into the magazine slot.

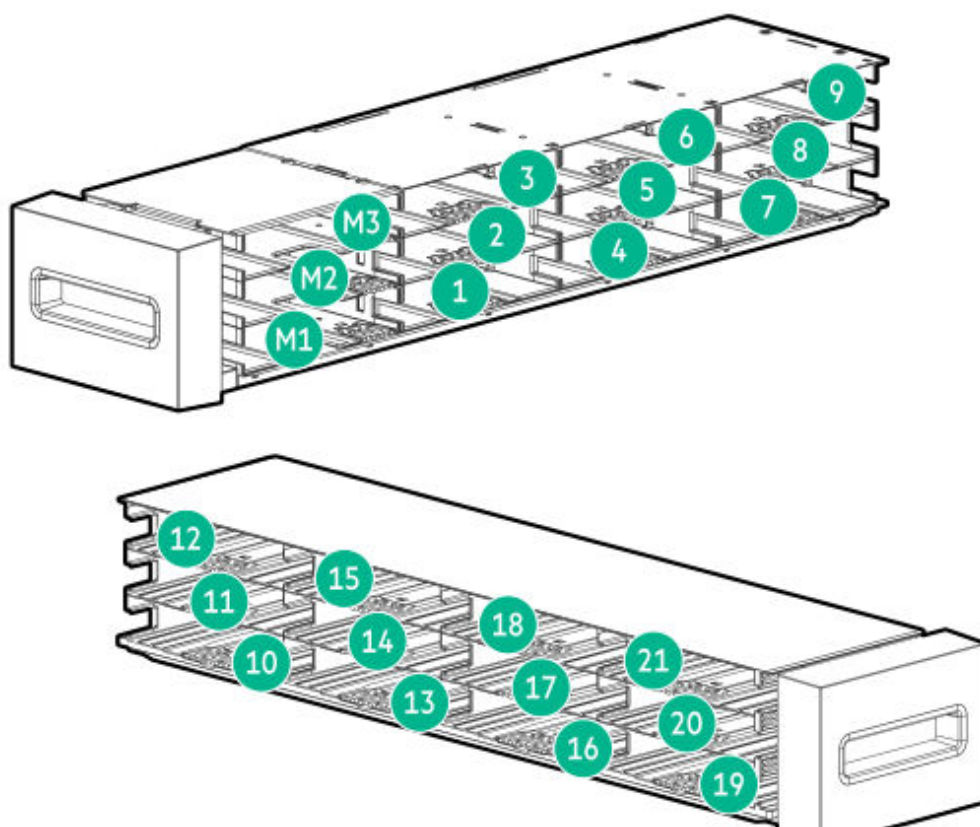
When reinstalling the magazine, ensure that the guides of the magazine correctly engaged.

Storage slots

Each library has two magazines of storage slots that can be removed from the front of the library. Each magazine has 12 storage slots for tape cartridges.

The following illustration shows the slot numbers for all the slots in the magazines.

The mailslots are in the magazine on the left. When enabled, the mailslots take the place of storage slots 1-3, and the remaining slots are renumbered as shown below.



Left magazine, front to back:

M3	3	6	9
M2	2	5	8
M1	1	4	7

Right Magazine back to front:

12	15	18	21
11	14	17	20
10	13	16	19

Subtopics

Unlocking the mailslot (Unlock Mailslot)

The mailslot cannot be opened

Unlocking the mailslot (Unlock Mailslot)

About this task

The mailslot in the left magazine is used only with host system software that supports this feature. The mailslot feature allows you to insert or remove tapes without removing the entire magazine. The benefit of using a mailslot is that the device will not inventory the rest of the slots in the magazine so the device can return to service sooner. The mailslot is in the left magazine.

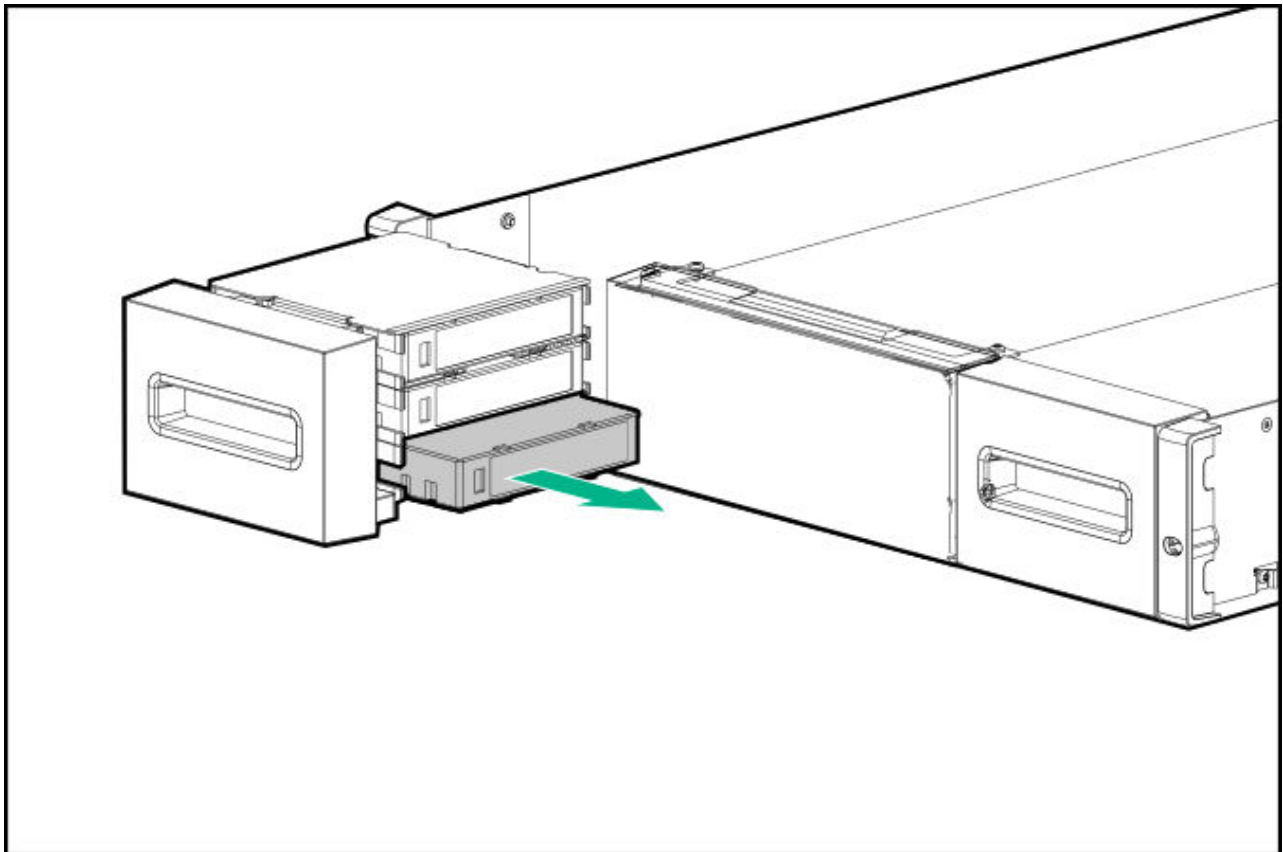


NOTE

The Unlock Mailslot menu is only displayed when the mailslot is enabled.

Procedure

1. Login to the OCP as Administrator, then press **Next** until the screen displays **Operation**. Press **Enter** to select.
2. The library will unlock the mailslot. Once the display reads mailslot unlocked, pull the mailslot out to access the tapes.
3. Push the mailslot back into the library.



The mailslot cannot be opened

Symptom

The **Operation > Open Mailslot** does not display an **Open** button for the mailslot.

Solution 1

Cause

The mailslot is not enabled.

Action

The mailslot must be enabled before it can be opened. To enable a mailslot, see [Enabling or disabling mailslots](#).

Solution 2

Cause

A host application set the Prevent Media Removal (PMR) setting for a mailslot. In this case, the library displays **Removal Prevented** instead of the **Open** button.

Action

If you need to open the mailslot, have the application release the PMR setting for the mailslot.

Upgrading and servicing the library



WARNING: Hazardous Moving Parts

Hazardous moving parts exist inside this product. Do not insert tools or any part of your body into the tape library to avoid injury.

Only personnel with appropriate technical and product safety training (referred to as "users" in this document) may access or operate the tape library.



CAUTION

A discharge of static electricity can damage static-sensitive devices or microcircuitry. Proper packaging and grounding techniques are necessary precautions to prevent damage.

To prevent electrostatic damage, observe the following precautions:

- Transport products in static-safe containers such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free stations.
- Cover the device with approved static-dissipating material. Provide a wrist strap connected to the work surface and properly grounded tools and equipment.
- Keep the work area free of nonconducting materials, such as ordinary plastic assembly aids and foam packing.
- Make sure that you are always properly grounded when touching a static-sensitive component or assembly.
- Avoid touching pins, leads, or circuitry.
- Use conductive field service tools.



WARNING

The MSL2024 weighs approximately 17 kg (37.4 lb) with drives and without media and up to 22 kg (48.4 lb) with media (24 cartridges).



WARNING

To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- Extend only one rack component at a time. If more than one component is extended, a rack can become unstable.

Subtopics

Possible tools needed

Secure Mode

Installing or replacing a tape drive

Removing and replacing a magazine

Replacing the power supply

Removing and replacing the library controller

Removing and replacing the chassis

Installation and replacement of the library rack kit

Tape drive cleaning

Possible tools needed

To service the library, you might need one or more of the following tools:

- Flat-blade screwdrivers (large and small)
- Short-handle #1 Phillips screwdriver
- #2 and #3 Phillips screwdrivers
- Torque driver
- Ground strap
- Paper clip or pin (for manual magazine removal)
- [Diagnosing problems with Library & Tape Tools](#)

Secure Mode

Secure Mode is a setting in the tape drive that only permits encryption settings to be established by the library that enabled Secure Mode using secure methods. Once a partition has been configured for FIPS Support Mode, the library will enable Secure Mode for all LTO-6 drives in the partition each time the library is powered on, and it will disable Secure Mode for all the drives in the partition each time the library is powered off using a soft power off. The library also disables Secure Mode for a drive when it is powered off from the RMI.

Subtopics

Disabling Secure Mode for an LTO-7 or later tape drive

Disabling Secure Mode for an LTO-7 or later tape drive

About this task

LTO-7 and later generation tape drives have separate firmware images that enable or disable Secure Mode when the firmware image is loaded onto the drive.



NOTE

For a current list of products that are FIPS 140-2 validated, see the NIST FIPS 140-2 Crypto Module Validation List. If FIPS 140-2 validation is required, verify the validation status before purchasing the product.

Procedure

Download and install the firmware image without Secure Mode.

Installing or replacing a tape drive

Prerequisites

#2 Phillips screwdriver

About this task

Install or replace the tape drive from the back of the library.



NOTE

- The library assigns the WWNames used by Fibre Channel drives to the drive locations. When you replace a tape drive, the WWName is reassigned to the replacement drive.

The library assigns SAS World Wide IDs to the drive locations. When you replace a SAS tape drive, the World Wide ID is reassigned to the replacement drive.

- You do not need to power off the library to replace a drive.



CAUTION

Powering off the master drive interrupts SCSI communication to the library and robotics.

Procedure

1. Remove the drive bay cover or remove the tape drive.
2. Install the tape drive.
3. Connect the FC cable or connect the SAS cable.
4. Configure the drive.
5. Verify the tape drive installation.

Subtopics

Removing a drive bay cover for new drive installation

Removing a tape drive

Installing the new tape drive

Verifying the tape drive installation

Removing a drive bay cover for new drive installation

Procedure

1. Locate the designated drive bay. Install the first tape drive in the lowest available bay. For any additional tape drives, place each one in the next open bay directly above the previous installation.



IMPORTANT

If you install a new drive below any existing tape drives, the drive numbering sequence of the current drives might change. In this case, you might need to reconfigure your backup software.

2. Using the correct screwdriver, remove one half-height drive bay cover to install a half-height drive or two half-height covers to install a full-height drive.

Removing a tape drive

Procedure

1. Verify that backups are not occurring on the drive you are replacing.



NOTE

If backups are running on another drive and you need to replace the master drive, ensure that the library cannot be accessed through this drive during the replacement process.

2. Verify that the tape drive does not contain a cartridge.
3. Navigate to **RMI > Operation > Move media** to move tape cartridges from the tape drives to storage slots or mailslots. For more information, see [Move media](#).
4. Use the [RMI to power off the drive](#).
5. Verify that the LED on the tape drive back panel is off.
6. Disconnect all cables from the tape drive.

7. Loosen the blue captive thumbscrews on the tape drive. While supporting the bottom of the drive, grasp the drive handle and pull straight back to slide the drive out of the library.

**CAUTION**

Support the bottom of the tape drive when removing it to avoid damage to the internal connections.

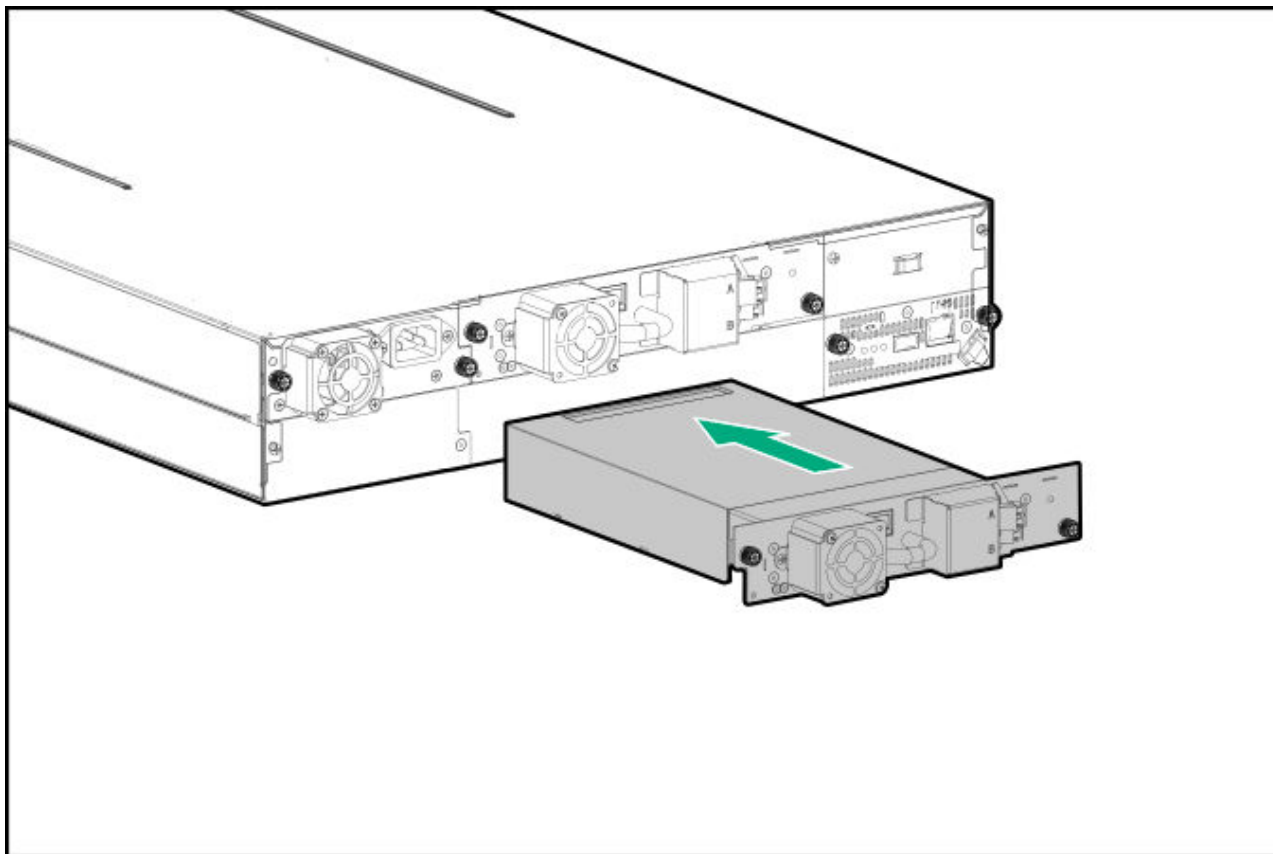
Installing the new tape drive

Prerequisites

Before installing the new drive, inspect the connectors on the tape drive. Ensure that the connectors are intact, free of any foreign objects, and have no cracks or deformed or bent contacts.

Procedure

1. Align the guides on the side of the drive assembly with the guide rails in the drive bay.
2. Slowly insert the new tape drive into the drive bay while supporting the drive assembly.
3. The tape drive is fully inserted when its back panel is flush with the back panel of the library.



4. To secure the tape drive to the chassis, tighten the drive sled mounting screws (the blue captive thumbscrews). You can use either a #2 Phillips screwdriver or a torque driver.

If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not over tighten. If using a torque driver, tighten to a recommended torque of 6-inch pounds or 0.68 N m. If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



IMPORTANT

Under certain conditions of external shock and vibration, if the thumbscrews are not tightened, drive performance issues might occur. So, tighten the thumbscrews to the recommended torque.

5. If the tape drive is new, plan the configuration:
 - **FC:** See [FC connection information](#).
 - **SAS:** See [SAS connection information](#).
6. If the tape drive is new, connect the tape drive to the host:

- **FC:** Plug one end of the FC cable into a port on the tape drive. Plug the other end of the cable into the HBA or switch.
- **SAS:** The cable recommended for use with the SAS library can connect up to four SAS tape drives to an HBA. Any tape drive can be connected with any of the four tape drive ends of the cable. Plug one of the unused SAS connectors on the tape drive end of the cable into the connector on the tape drive.

Verifying the tape drive installation

Procedure

1. Install a drive bay cover on any unused drive bay to ensure proper operation.
2. Attach the cables, if necessary, which was removed from the old tape drive.
3. Power on the drive from the RMI, if necessary.
4. Confirm that the library recognizes the new tape drive in **OCP > System Status**.

If recognized, the new drive will show **Ready, RDY**, or **Empty** status.

5. Use the RMI to add the drive to an existing partition, or create a new partition that includes the drive to make the drive visible to hosts and associated with the library.
6. Use L&TT to verify that the host sees the tape drive.

You can download L&TT without charge from: <https://www.hpe.com/support/TapeTools>.

7. Use the OCP or RMI to verify that the library sees the tape drive and to update the drive firmware, if necessary.

Removing and replacing a magazine

The library has removable magazines. Magazine access is password protected. For safety reasons, the robotic motion is stopped when a magazine is removed. The magazines can be released using the OCP, the RMI, or by a manual release. When possible, release the magazine using the OCP or RMI.



IMPORTANT

To release a magazine manually, see [Releasing the magazines manually](#). However, only use this manual process if the magazine cannot be released using the OCP or the RMI, and the device no longer has power.

Subtopics

[Removing a magazine using the MSL2024 OCP](#)

[Releasing magazines using the RMI](#)

[Releasing the magazine using the manual magazine release](#)

Removing a magazine using the MSL2024 OCP

Prerequisites

Administrator password



IMPORTANT

When removing a magazine using the OCP, once a magazine is removed, the robot cannot perform any other operation.

Procedure

1. Log in to the Operator Control Panel (OCP) as Administrator:
 - a. Press any key.
 - b. Select **User: "ADMINISTRATOR"**, and press **Enter**.
 - c. Enter the PIN using the **Previous**, **Next**, and **Enter** buttons.
2. Click **Next** until the screen displays Operation.
 - a. Press **Enter**.
 - b. Press **Next** to display Magazine Unlock Right or Magazine Unlock Left.
 - c. Press **Enter** to release the desired magazine.

The screen displays Magazine Unlocked for 30s.

3. Pull the unlocked magazine out of the library.
4. Remove the tape cartridges from the magazine, noting their locations so each can be replaced in the proper slot.
5. Install the tape cartridges into the replacement magazine in the same slots that they were removed from.

The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

Releasing magazines using the RMI

Prerequisites



IMPORTANT

When removing a magazine using the RMI, once a magazine is removed, the robot cannot perform any other operation.

Procedure

1. Log in to the RMI as the administrator user.
2. Navigate to **Operation > Open Magazine**.
3. Use the Open button to release each magazine. When a magazine is unlocked, the OCP displays Magazine unlocked.
4. Pull the unlocked magazine out of the library.
5. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot.
6. Install the tape cartridges into the replacement magazine in the same slots that they were removed from.
7. When the OCP screen displays Magazine Removed, slide the replacement magazine completely into the library.

The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

Releasing the magazine using the manual magazine release

About this task

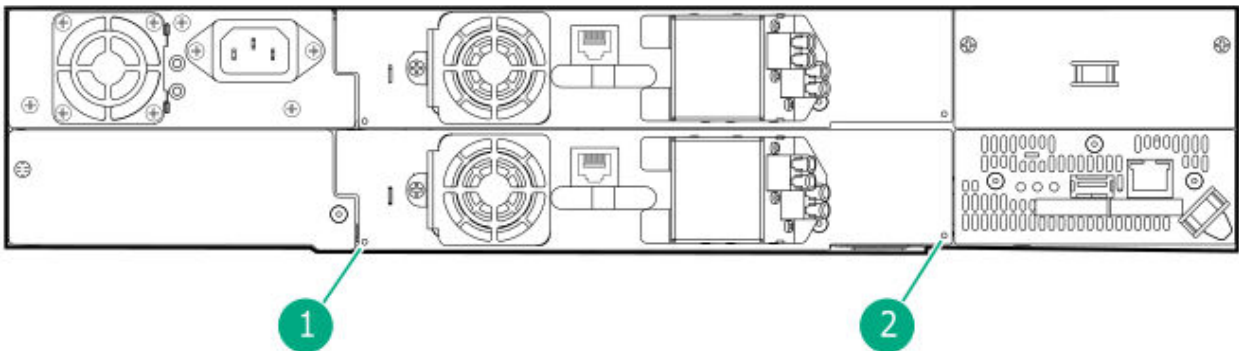


IMPORTANT

Only use this manual process if the magazine cannot be released using the OCP or the RMI and the device no longer has power.

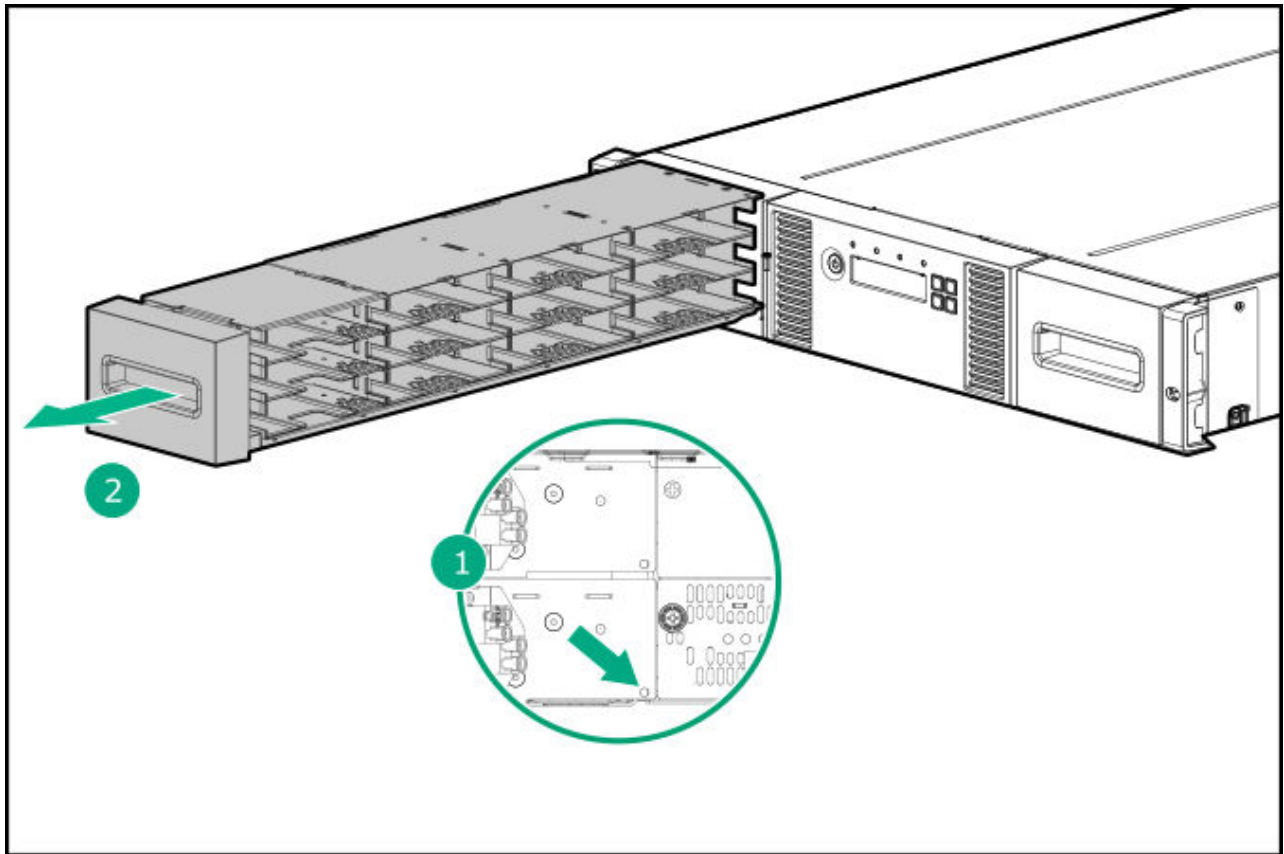
Procedure

1. From the back of the library, locate the magazine release hole associated with the magazine being released. The magazine release latches are accessed from the magazine release holes on the bottom tape drive plate.



Item	Description
1	Release hole for right magazine
2	Release hole for left magazine

2. Insert a straightened paper clip or small metal pin about 1.5 cm (0.6 inch) into the magazine release hole. Have another person pull out the magazine out of the library and set it aside.



Item	Description
------	-------------

- | | |
|---|----------------------------------|
| 1 | Insert a pin into access hole. |
| 2 | Release and remove the magazine. |

**IMPORTANT**

Do not force the pin once you encounter resistance. Doing so can damage the library.

3. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot.
4. Install the tape cartridges into the replacement magazine in the same slots that they were removed from.
5. Install the replacement magazine into the library.

Replacing the power supply

About this task

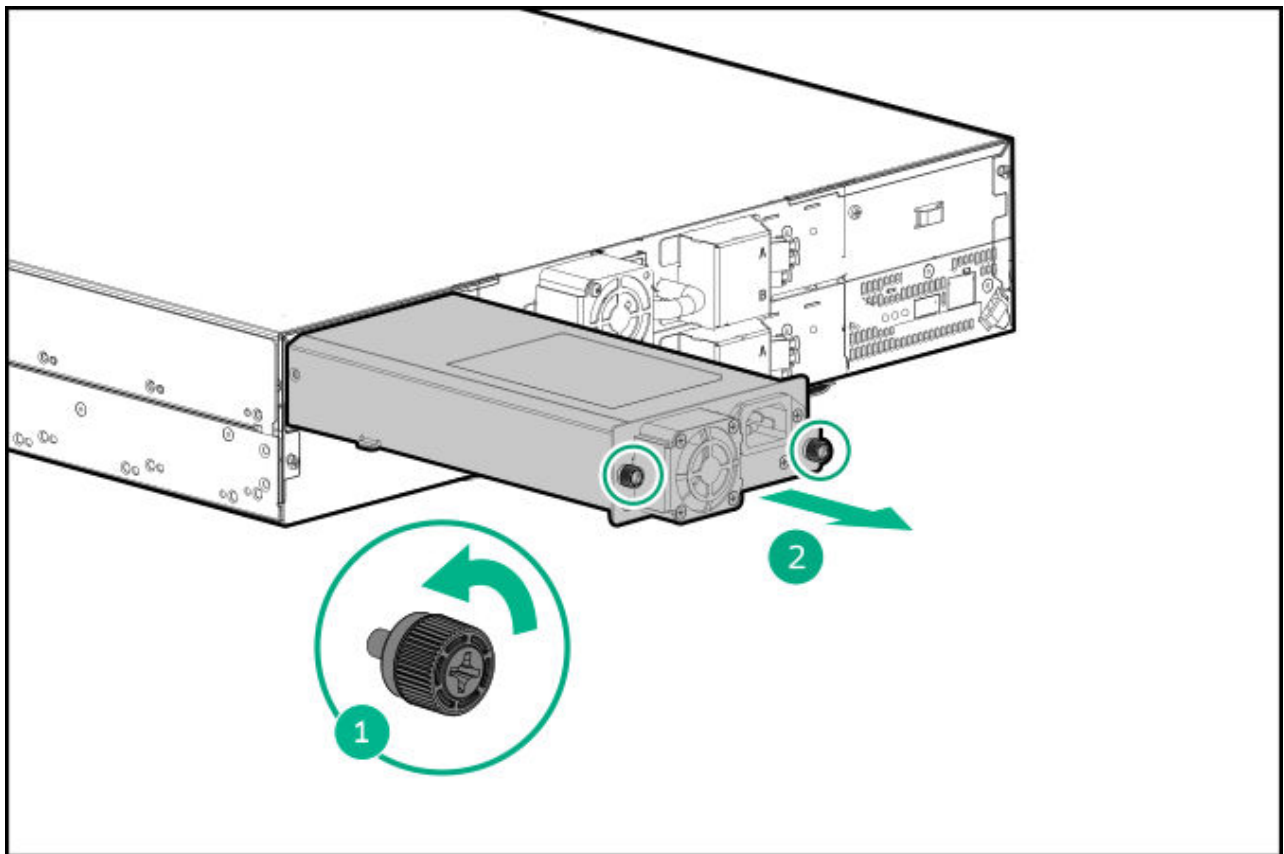


CAUTION

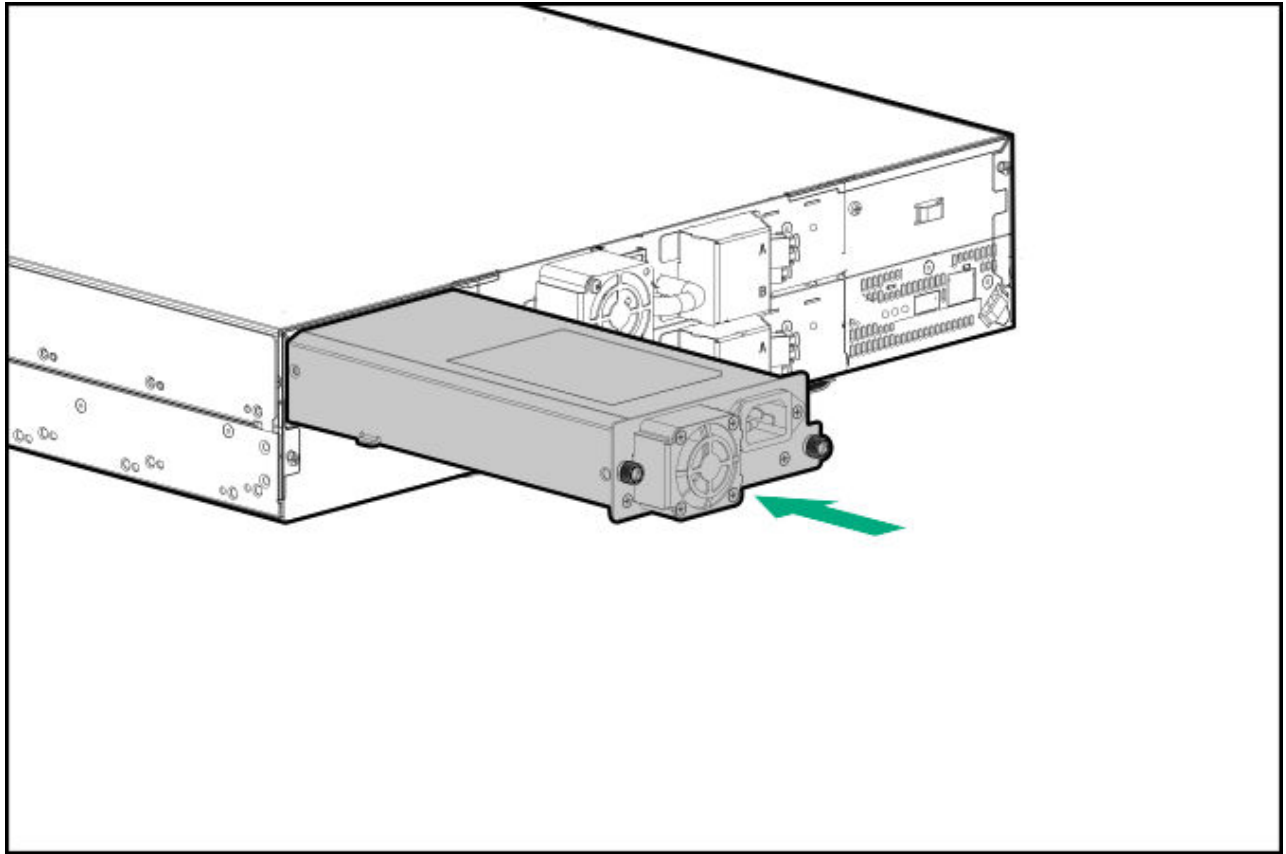
Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed. Ensure that you are properly grounded when touching static-sensitive components.

Procedure

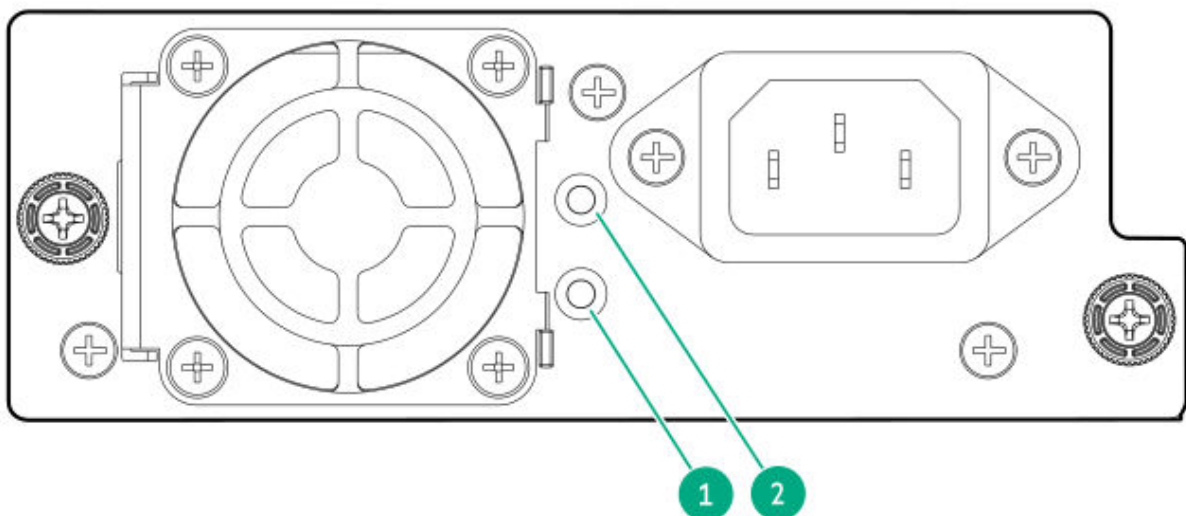
1. Power off the library from the front panel and then remove the AC power cord.
2. Loosen the two captive thumbscrews on the power supply. Grasp a thumbscrew stem on each side of the power supply and while supporting the bottom, pull the power supply out of the library.



3. Position the new power supply on the alignment rails and slide it into the library until it is flush with the back panel. Tighten the two blue thumbscrews to secure the power supply.



4. Attach the AC power cord to the replacement power supply.
5. Power on the library by pressing the power button near the OCP on the front.
6. Verify that the power supply is operating properly.
 - When a power supply with LEDs is operating properly, the white and green LEDs on the power supply module are lit.



Item	Color	Description
1	Green	Module is powered on
2	White	AC power is connected

7. If the UID LEDs are still illuminated, deactivate them using the OCP or RMI.

Removing and replacing the library controller



CAUTION

- Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed. Ensure that you are properly grounded when touching static-sensitive components.
- This part is not hot-pluggable. Power off the library before replacing the library controller.

Subtopics

Identifying the failed component

Saving the library configuration

Powering off the Library

Preparing to remove the controller board

Removing a library controller board

Replacing the library controller

Completing the library controller replacement

Verifying the library controller installation

Identifying the failed component

Procedure

1. Check the RMI **Maintenance > Logs and Traces > View Logs** to get details of the errors and help identifying the issue.
2. Activate the UID LED from the RMI **Maintenance > UID LED Control**.

To help locate the component, turning on the UID LEDs makes it easier to locate the library from the back of the rack.

Saving the library configuration

From the RMI **Configuration > System > Save/Restore Configuration**, you can save the library configuration settings to a file, restore the settings, or reset the library configuration to the default settings. The saved configuration database will make it easier to recover the library configuration in the case of a controller replacement.

Procedure (RMI)

1. Navigate to **Configuration > System > Save/Restore Configuration**.
2. Click **Save**. As a result, the Save Configuration process starts and once the file is ready, press **Download** to save the file to the system you are running the browser on.

Procedure (OCP)

1. Insert the USB flash drive in the USB port on the back of the library.
2. Log in to the OCP as Administrator, then press **Previous** or **Next** until the screen displays Configuration. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Library**. Press **Enter**.
4. Press **Previous** or **Next** until the screen displays Save Config to USB Device. Press **Enter** to save.
5. When saved, remove the USB flash drive from the USB port.

Powering off the Library

Procedure

1. Verify that all host processes are idle.
2. From the front panel, depress the power button and hold it for five seconds.
3. If the library does not perform a soft shutdown, depress and hold the power button for 10 seconds.

Preparing to remove the controller board

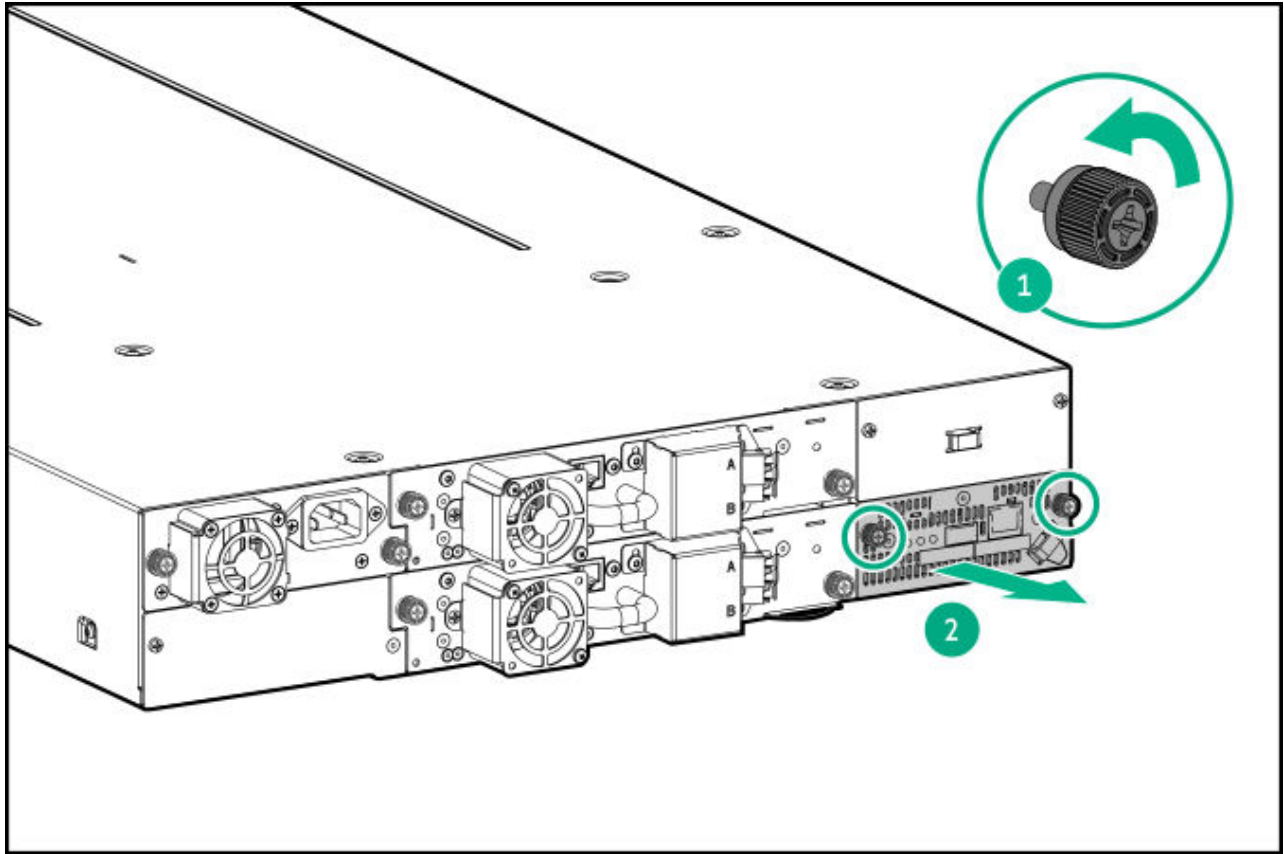
Procedure

1. Unplug the AC power cable from the library.
2. Remove the Ethernet cables, and the USB device from the failed controller board, if present.

Removing a library controller board

Procedure

1. Loosen the two blue captive thumbscrews on the controller board.

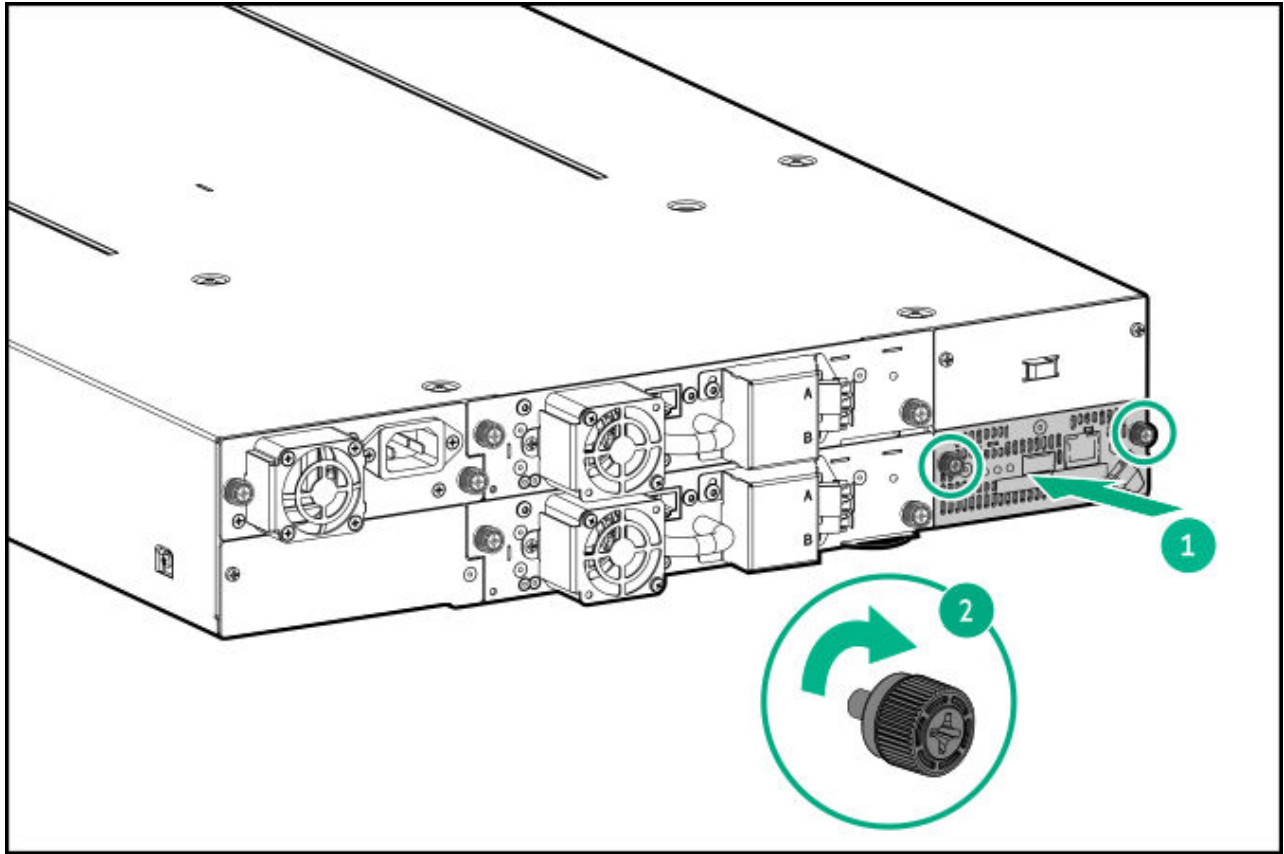


2. Using the thumbscrews, slowly remove the controller board from the library.

Replacing the library controller

Procedure

1. Position the new controller board in the alignment rails.



2. Slide the controller board into the library until firmly seated.
3. Tighten the two thumbscrews with your fingers or a Phillips #2 screwdriver until they are finger tight. Do not over tighten.

Completing the library controller replacement

Procedure

1. If necessary, connect the Ethernet cable and insert the USB device if one was removed.
2. Replace the AC power cord for the library.

Verifying the library controller installation

Procedure

1. Power on the library.
2. Check the overall library status from the RMI **Status > Library Status** or on the OCP from the **Information/Status > Library Status**.
3. Using the RMI, check for events; clear the event that indicated the controller was faulty.
4. Upgrade the firmware if necessary.

After replacing the controller, the firmware version will be the firmware version shipped on the replacement controller. The firmware version shipped on the replacement controller might be earlier than the firmware running on the library before the replacement. In this case, update the library firmware to the version previously installed on the library or the available firmware version.

To find the version of firmware installed on the library, check the upper left corner of the RMI or the **Information/Status > Library Status** screen on the OCP. Update the firmware from the RMI **Maintenance > Firmware Upgrades > System Firmware**.

5. Verify that the library configuration is correct from the RMI **Status > Partition Map > Configuration Status**.

If the library configuration is incorrect after replacing the controller, restore the previous settings from the RMI **Configuration > System > Save/Restore Configuration** or the OCP **Configuration > Library > Restore Config from USB**, or reconfigure the library.

If using the MSL Encryption Kit, you might need to enter the token password in the RMI **Configuration > Encryption** while logged into the RMI as the Security User.

6. If the UID LED is still illuminated, deactivate it using the RMI **Maintenance > UID LED Control**.
7. Resume host applications.

Removing and replacing the chassis

Prerequisites

If the library is managed by Command View for Tape Libraries (CVTL), remove the library from the managed library list in the CVTL Management Station **before** you power off the chassis that is being replaced. After the chassis is replaced, see [Configuring HPE Storage Command View for Tape Libraries integration](#) to add the library back to CVTL.

About this task



WARNING

The library weighs approximately 17 kg (37.4 lb) with drives and without media and approximately 22 kg (48.4 lb) with media (24 tape cartridges). When moving the library, to reduce the risk of personal injury or damage to the library:

- Observe the local health and safety requirements and guidelines for manual material handling.
- Always remove all tapes to reduce the overall weight of the library.
- Obtain adequate assistance to lift and stabilize the library during installation or removal.



WARNING

To reduce the risk of personal injury or damage to equipment:

- Extend the leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install the rack stabilizer kit on the rack.
- Extend only one rack component at a time. Racks might become unstable if more than one component is extended.
- Slide or rail-mounted equipment is not to be used as a shelf or a workspace.
- Parts can be damaged by electrostatic discharge. Keep parts in electrostatic containers until needed.
- Ensure that you are properly grounded when touching static sensitive components.



CAUTION

Discharge of static electricity can damage static-sensitive devices or microcircuitry. Proper packaging and grounding techniques are necessary precautions to prevent damage.

To prevent electrostatic damage, observe the following precautions:

- Transport products in static-safe containers such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at

Procedure

1. Saving the library configuration.
2. Remove the tape cartridge from the tape drive.
3. Remove the cables, magazines, and tape drive.
4. Remove the power supply and library controller.
5. Remove the chassis from the rack.
6. Unpack the new chassis and place it on a sturdy table. Save the packaging materials to return the old chassis.
7. Install the replacement chassis in the rack.
8. Replace the library components and cables.
9. Verify the chassis replacement.

Subtopics

Removing the tape cartridge from the tape drive
Removing the cables, magazines, and tape drive
Removing the power supply and library controller
Removing the library controller
Removing the chassis
Verifying the chassis replacement
Replacing the shipping lock on the old chassis
Repackaging the old chassis

Removing the tape cartridge from the tape drive

About this task

If tape cartridges are installed in the library, follow the instructions to avoid damaging the tape cartridge or tape drive.



CAUTION

If you cannot remove the tape cartridge from the tape drive, handle the tape drive gently during the rest of the procedure to avoid damaging the tape and losing data.

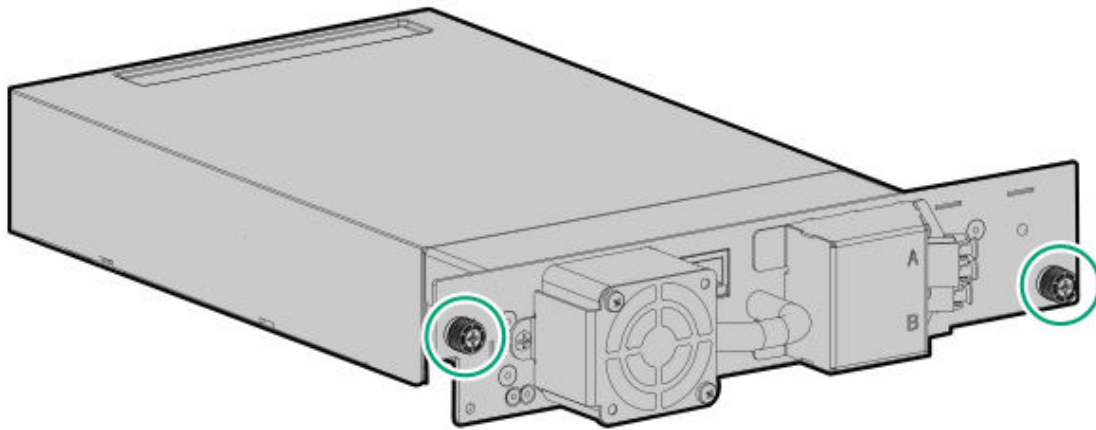
Procedure

Navigate to **RMI > Operation > Move media** to move tape cartridges from the tape drives to storage slots or mailslots. For more information, see [Move media](#).

Removing the cables, magazines, and tape drive

Procedure

1. [Removing the magazines using the RMI or OCP](#).
2. [Power off the library](#).
3. After powering off the library, look through the shipping lock slot in the top cover. Confirm that the robotic shipping lock slot is immediately below and in vertical alignment with the top cover shipping lock slot. If not and if possible, power cycle the library and recheck the alignment of the two slots.
4. If necessary, remove the USB thumb drive or MSL encryption kit from the controller.
5. Remove the power cord and other cables from the library.
6. If the chassis are faulty, it is possible that the magazines could not be removed through RMI or OCP. In such case, if the magazines have not been removed, remove the magazines from the library using the manual process (see [Releasing the magazines manually](#)).
7. Loosen the blue captive thumbscrews on the drive.



8. While supporting the bottom of the tape drive, pull straight back on the tape drive handle to remove the tape drive from the library.

Place the drive on a static-safe surface, noting its position in the library.

9. Remove any additional tape drives following the same procedure.

Removing the power supply and library controller

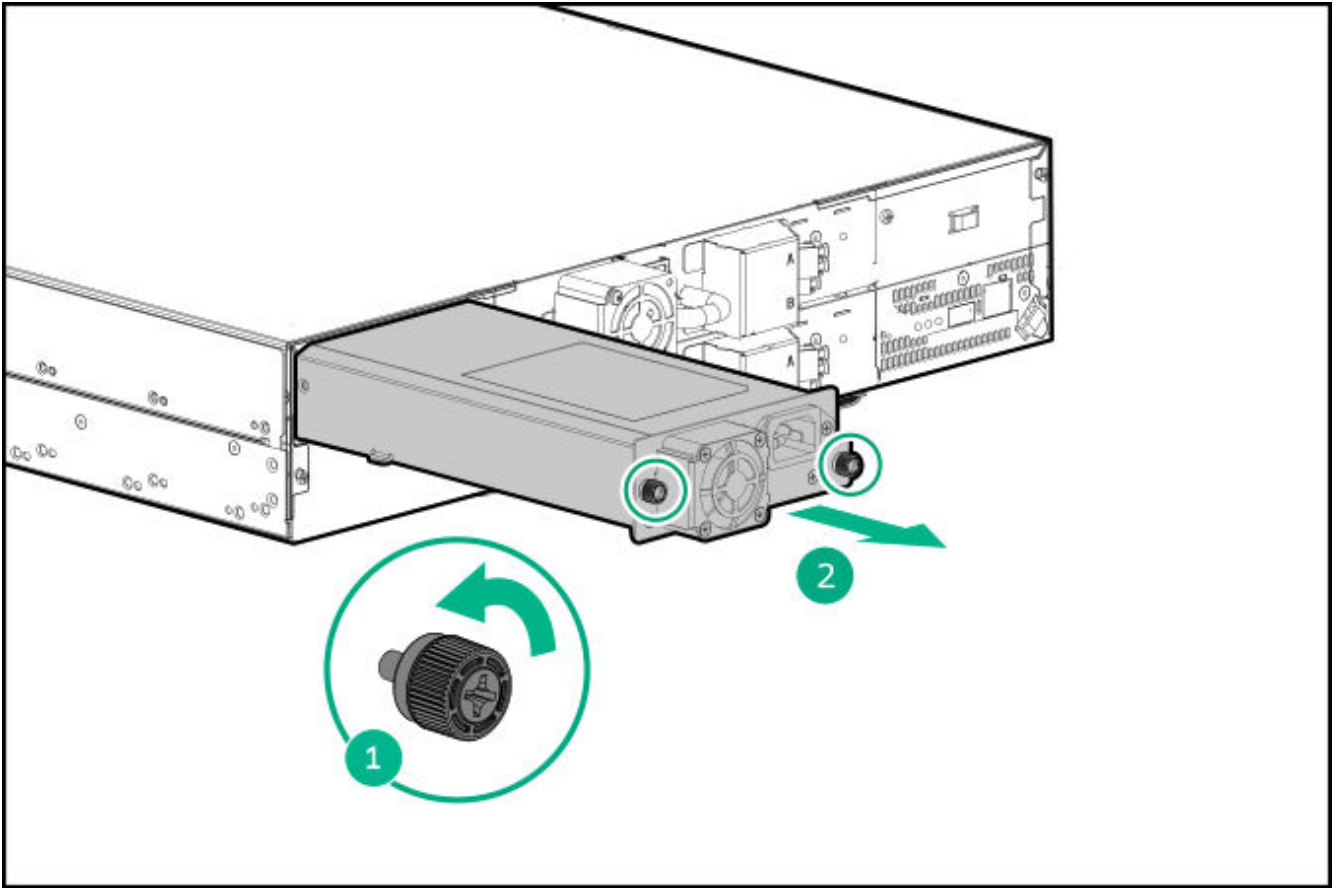
About this task

The power supply and library controller are moved to the new chassis.

Procedure

Remove the power supply.

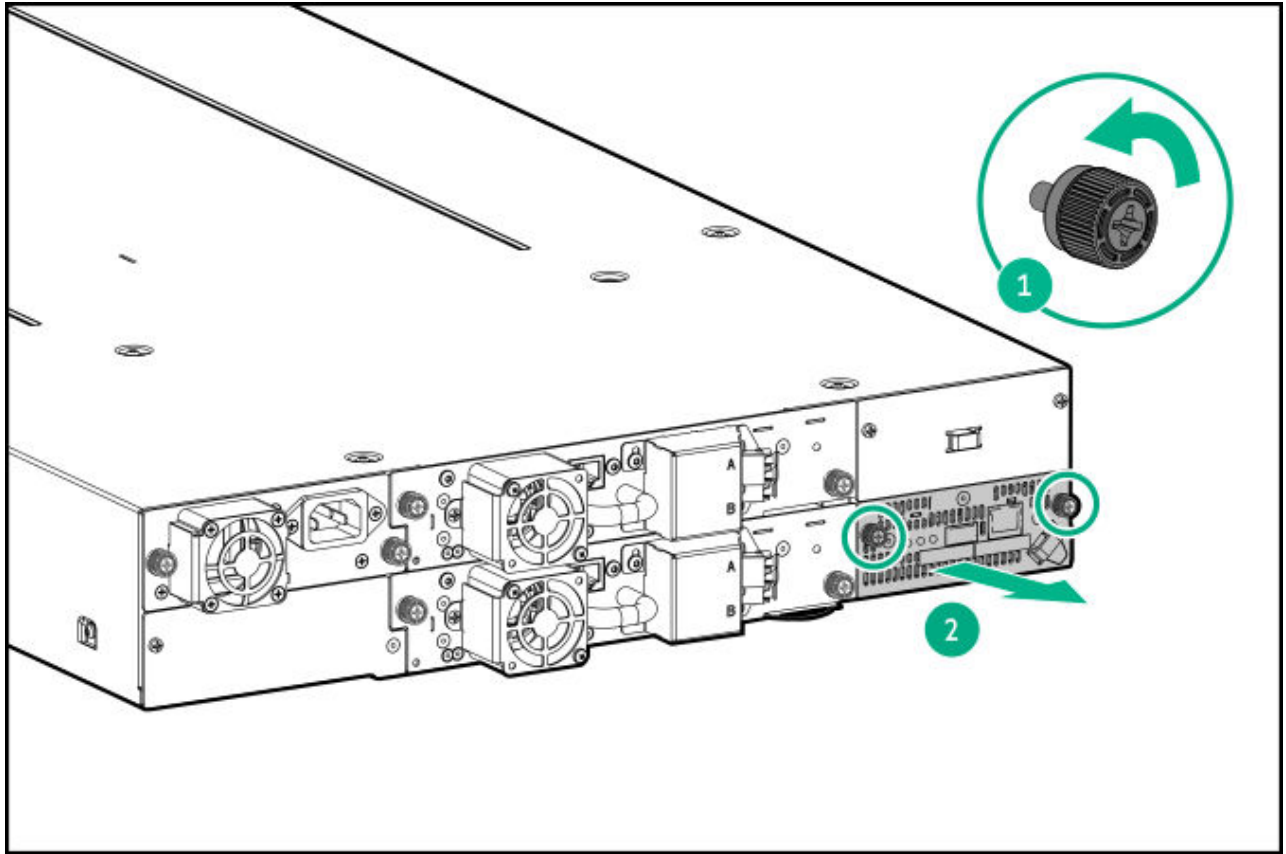
1. Loosen the two captive thumbscrews on the power supply.
2. Grasp a thumbscrew stem on each side of the power supply. Support the bottom while pulling the power supply out of the library.



Removing the library controller

Procedure

1. Loosen the two blue thumbscrews on the library controller and remove it from the library.



2. Place the library controller into a static safe bag.

Removing the chassis

Prerequisites

- #2 Phillips screwdriver
- Obtain adequate assistance to lift and stabilize the library during removal and replacement.

About this task



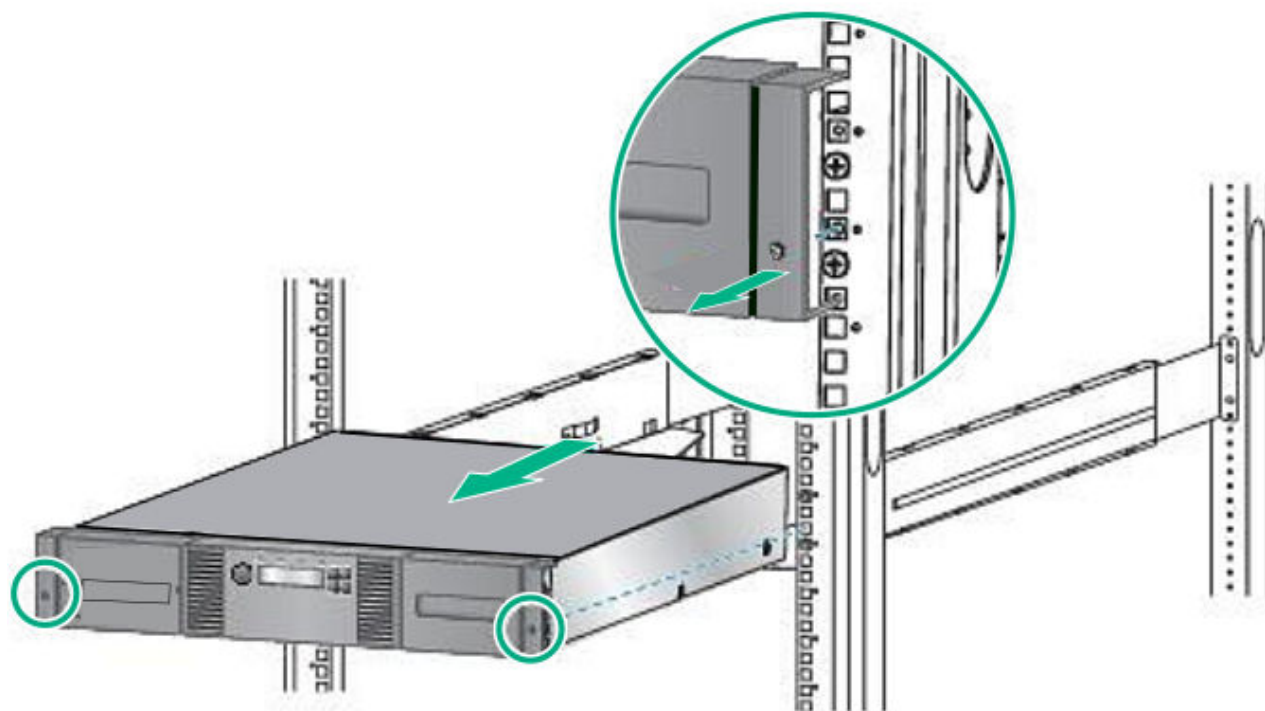
CAUTION

Lift the library from the side edges. Lifting the library from the magazine or tape drive openings can damage the library.

Procedure

From the front of the library:

1. Loosen the screws inside the left and right front bezel (these screws are captive and cannot be removed).
2. Slide the library out, using assistance.



11344

3. Place the chassis on a stable, static-free surface after removal.

Verifying the chassis replacement

About this task

This topic describes the steps to verify the status and configuration of the library after chassis replacement.

Another aspect of replacement is the serial number, which is stored electronically in the chassis and in the controller and physically on the chassis pull-out tab. The replacement chassis will have a different serial number from the original chassis. However, when the existing controller is placed in the new chassis and the chassis is powered on, the controller updates the serial number electronically in the chassis. Electronically, the serial number matches the original serial number and all library data, support tickets, warranty data, and any licenses tied to the original serial number remain valid. The serial number on the chassis pull-out tab is physically printed, it will **not** match the electronic serial number. The mismatch does not affect the ongoing service. HPE retains records of replacements and the library will continue to be identified by the electronic serial number.

Procedure

1. Power on the library.
2. Check the overall library status from the RMI **Status > library** or on the OCP from the **Information/Status > Library Status**.
3. Using the RMI, check for events; clear any events that indicated the chassis was faulty.
4. Upgrade the firmware if necessary.

After replacing the controller, The firmware version shipped on the replacement chassis might be different than the firmware running on the library before the replacement. In this case, update the library firmware to the latest available firmware version.

To find the version of firmware installed on the library, check the upper left corner of the RMI or the **Information/Status > Library Status** screen on the OCP. Update the firmware from the RMI **Maintenance > Firmware Upgrades > System Firmware**.

5. Verify that the library configuration is correct from the RMI **Status > Partition Map > Configuration Status**.

If the library configuration is incorrect after replacing the chassis, restore the previous settings from the RMI **Configuration > System > Save/Restore Configuration** or the OCP **Configuration > Library > Restore Config from USB**, or reconfigure the library.

If using the MSL Encryption Kit, you might need to enter the token password in the RMI **Configuration > Encryption** while logged into the RMI as the Security User.

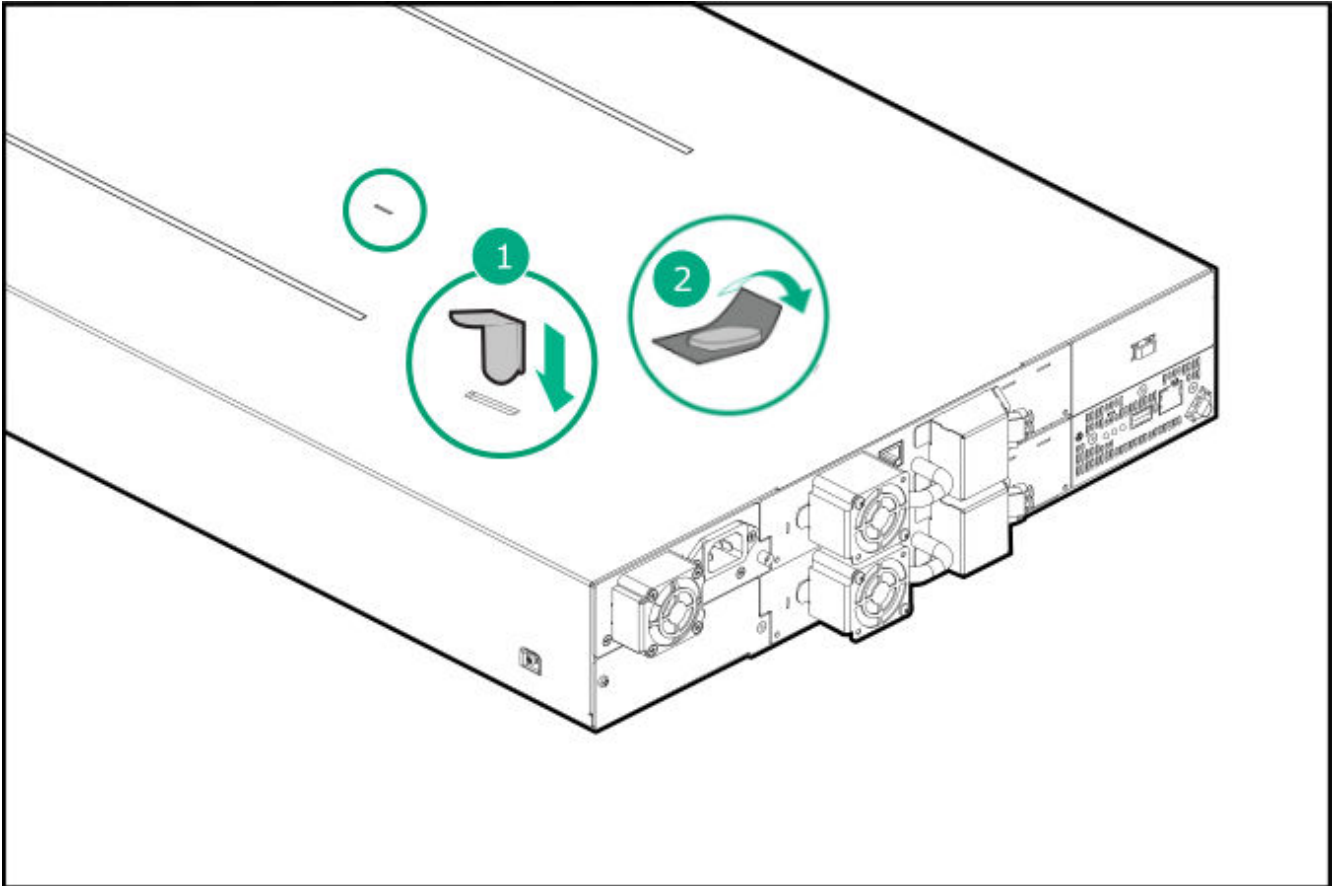
6. If the UID LED is still illuminated, deactivate it using the RMI **Maintenance > UID LED Control**.
7. Resume host applications.

Replacing the shipping lock on the old chassis

Procedure

1. Locate the shipping lock that was set aside from the replacement chassis.
2. Place the shipping lock in the shipping position on top of the old chassis (callout 1).
3. Tape the shipping lock to the chassis to keep it in place during shipping (callout 2).

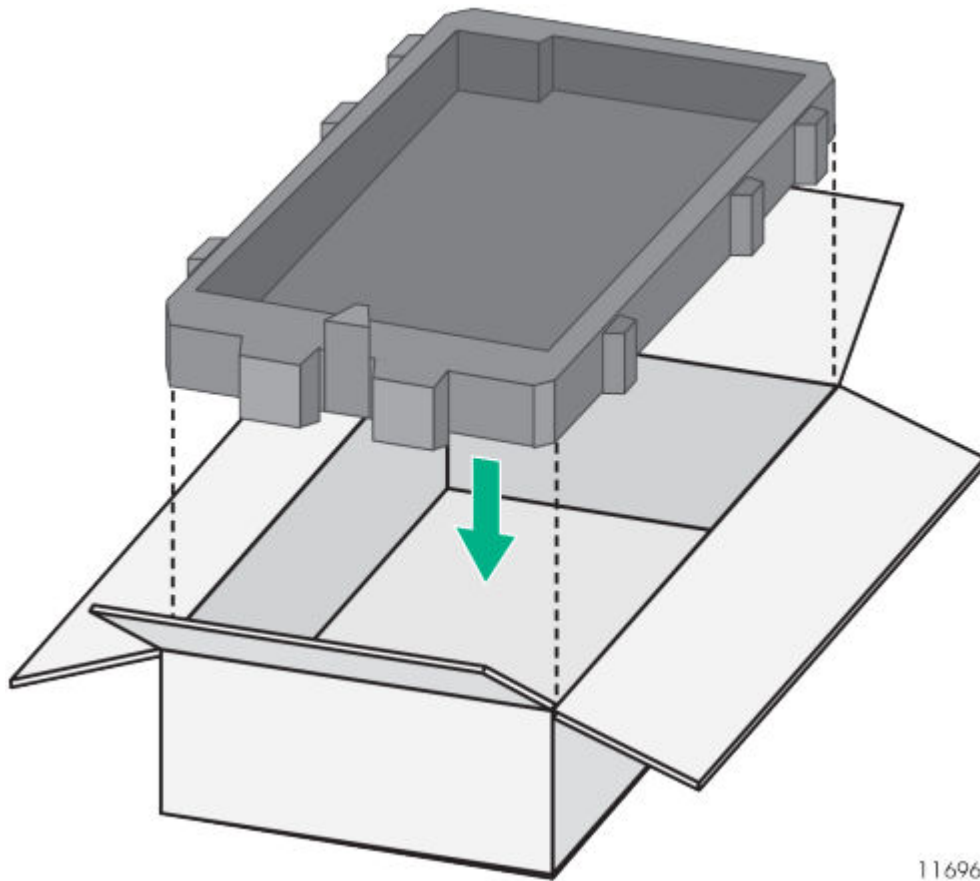
Results



Repackaging the old chassis

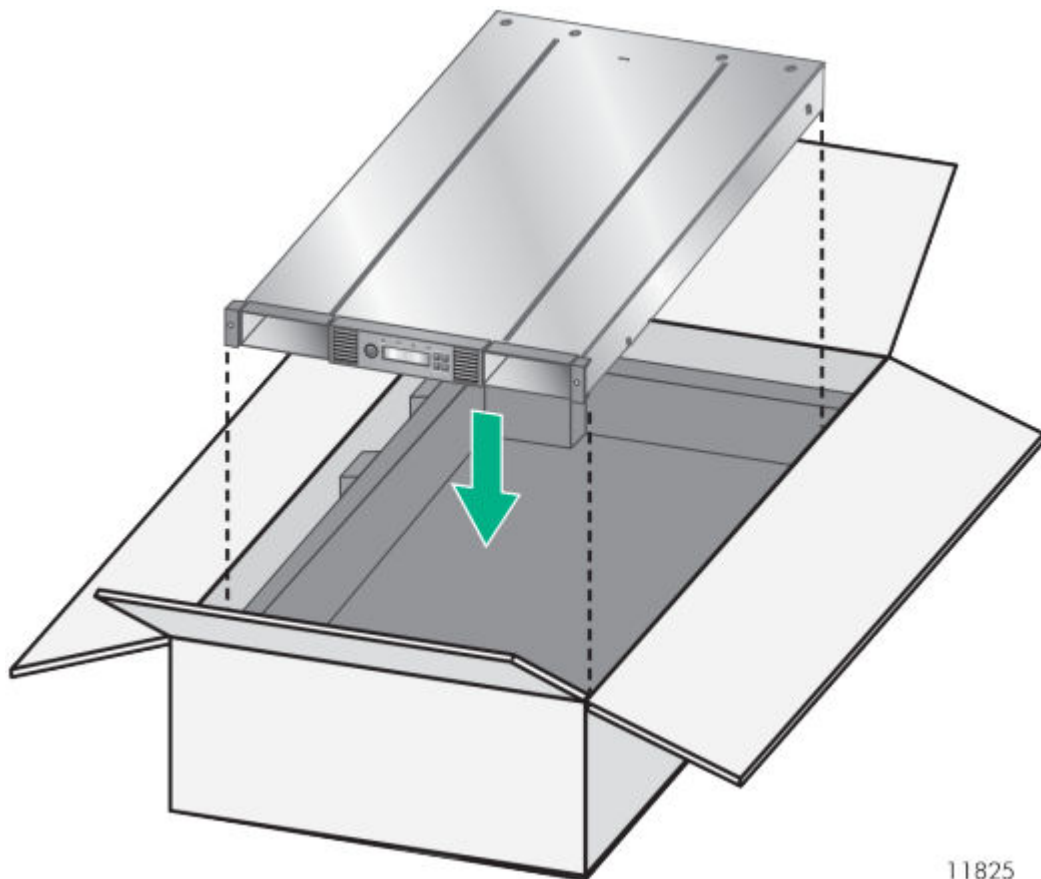
Procedure

1. Place the box from the replacement chassis on a sturdy surface. Slide the bottom foam piece into the box.



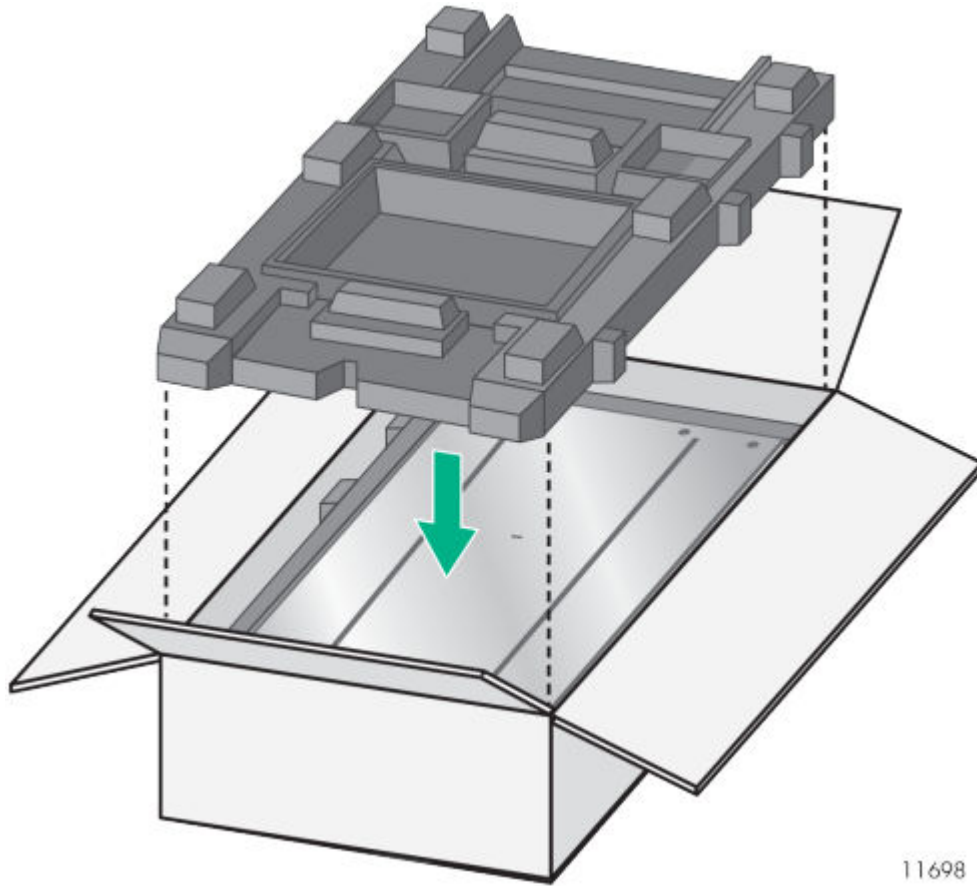
11696

2. If a thin layer of protective foam is included in the replacement shipment, rewrap the chassis in the foam to prevent cosmetic damage. Lower the chassis in the box.

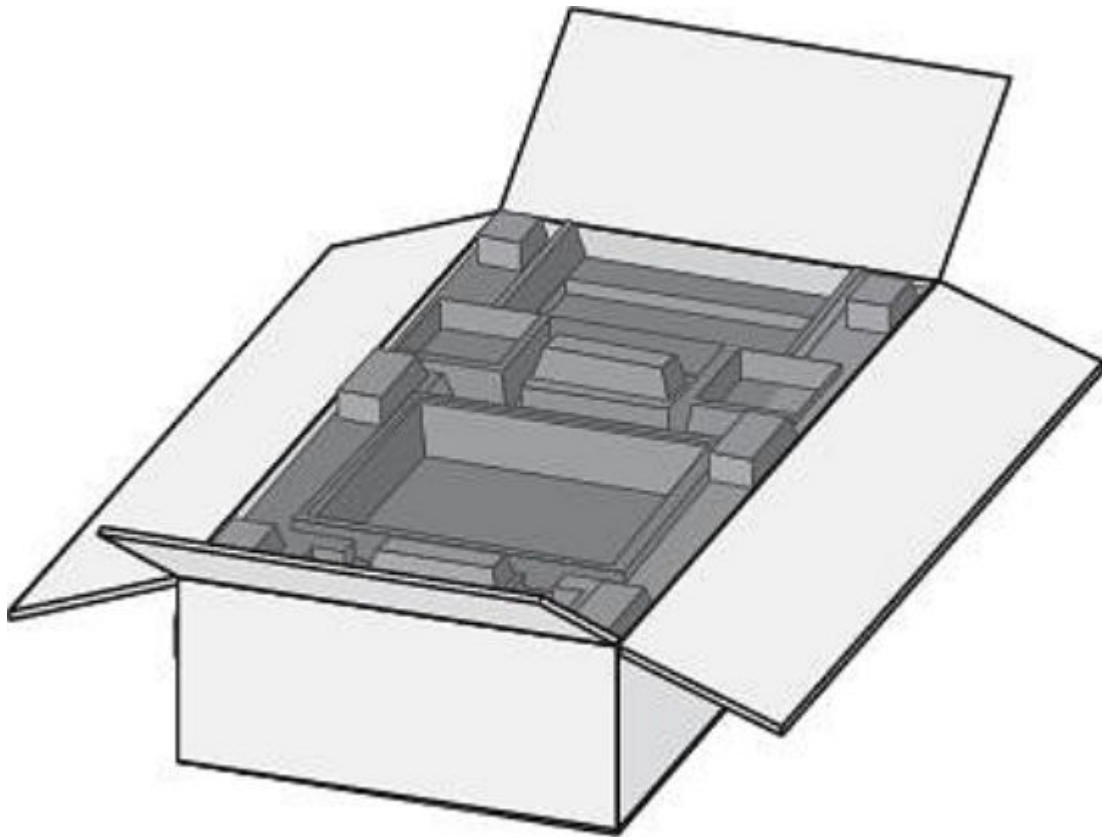


11825

3. Place the top piece of foam on top of the chassis.



4. The top piece of foam should be level with the top of the box.



11699

Installation and replacement of the library rack kit

- When installing a new HPE Storage MSL2024 G4 Library, start with [Securing the rails to the rack](#).
- When replacing the rack rails on a tape library that might contain tape cartridges or has support feet attached, it is a best practice to allow the backup application to complete and return the tape cartridges to the storage slots. After the backup application has completed, start with [Removing the cartridges from tape drives](#).

You will need the following for this procedure:

- #2 and a #3 Phillips screwdriver for this procedure.

**WARNING**

To reduce the risk of personal injury or damage to equipment:

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- In multiple-rack installations, secure the racks together.
- Extend only one rack component at a time. Racks may become unstable if more than one component is extended.

**WARNING**

The MSL2024 weighs approximately 17 kg (37.4 lb) with drives and without media and up to 22 kg (48.4 lb) with media (24 cartridges).

Subtopics

Removing the cartridges from tape drives

Removing the cartridges from the magazines using the OCP

Removing the cartridges from the magazines using the RMI

Removing the cartridges from the magazines using the manual release

Removing the library

Removing the old rails

Securing the rails to the rack

Installing the library

Removing the cartridges from tape drives

About this task

If tape cartridges are installed in the library, follow the instructions to avoid damaging the tape cartridge or tape drive,

Procedure

1. Navigate to **RMI > Operation > Move Media** to move tape cartridges from the tape drives to storage slots or mailslots.
2. Proceed to remove all tape cartridges from the library using the RMI or the OCP.

Removing the cartridges from the magazines using the OCP

About this task



IMPORTANT

When possible, unlock the magazines using the OCP or RMI. However, if the OCP or RMI process fails or a magazine needs to be removed when the power is off, you can release the magazines manually. See [Removing the cartridges from the magazines using the manual release](#).

Procedure

1. Log in to the OCP as Administrator:
 - a. Press any key.
 - b. Select **User: "ADMINISTRATOR"**, and press **Enter**.
 - c. Enter the PIN using the **Previous**, **Next**, and press **Enter**.
2. Click **Next** until the screen displays `Operation`.
 - a. Press **Enter**.
 - b. Press **Next** to display `Magazine Unlock Right` or `Magazine Unlock Left`.
 - c. Press **Enter** to release the desired magazine.

The screen displays `Magazine Unlocked for 30s` message.

3. Pull the unlocked magazine out of the library.
4. Remove the tape cartridges from the magazine, noting their locations so each can be replaced in the proper slot.
5. When the screen displays `Magazine Removed` message, slide the magazine completely into the library.

The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

6. Repeat this procedure to remove the tape cartridges from the other magazine.



IMPORTANT

When removing a magazine using the OCP, once a magazine is removed, the robot cannot perform any other operation. The removed magazine must be reinserted to allow removal of the other magazine.

Removing the cartridges from the magazines using the RMI

About this task



IMPORTANT

When possible, unlock the magazines using the OCP or RMI. However, if the OCP or RMI process fails or a magazine needs to be removed when the power is off, you can release the magazines manually.

Procedure

1. Navigate to **Operation > Open Magazine**.
2. Use the **Open** button to release each magazine.

When a magazine is unlocked, the OCP displays `Magazine unlocked` message.

3. Pull the unlocked magazine out of the library.
4. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot.
5. When the OCP displays `Magazine Removed` message, slide the magazine completely into the library.



IMPORTANT

When removing a magazine using the RMI, once a magazine is removed, the robot cannot perform any other operation. The removed magazine must be reinserted to allow removal of the other magazine.

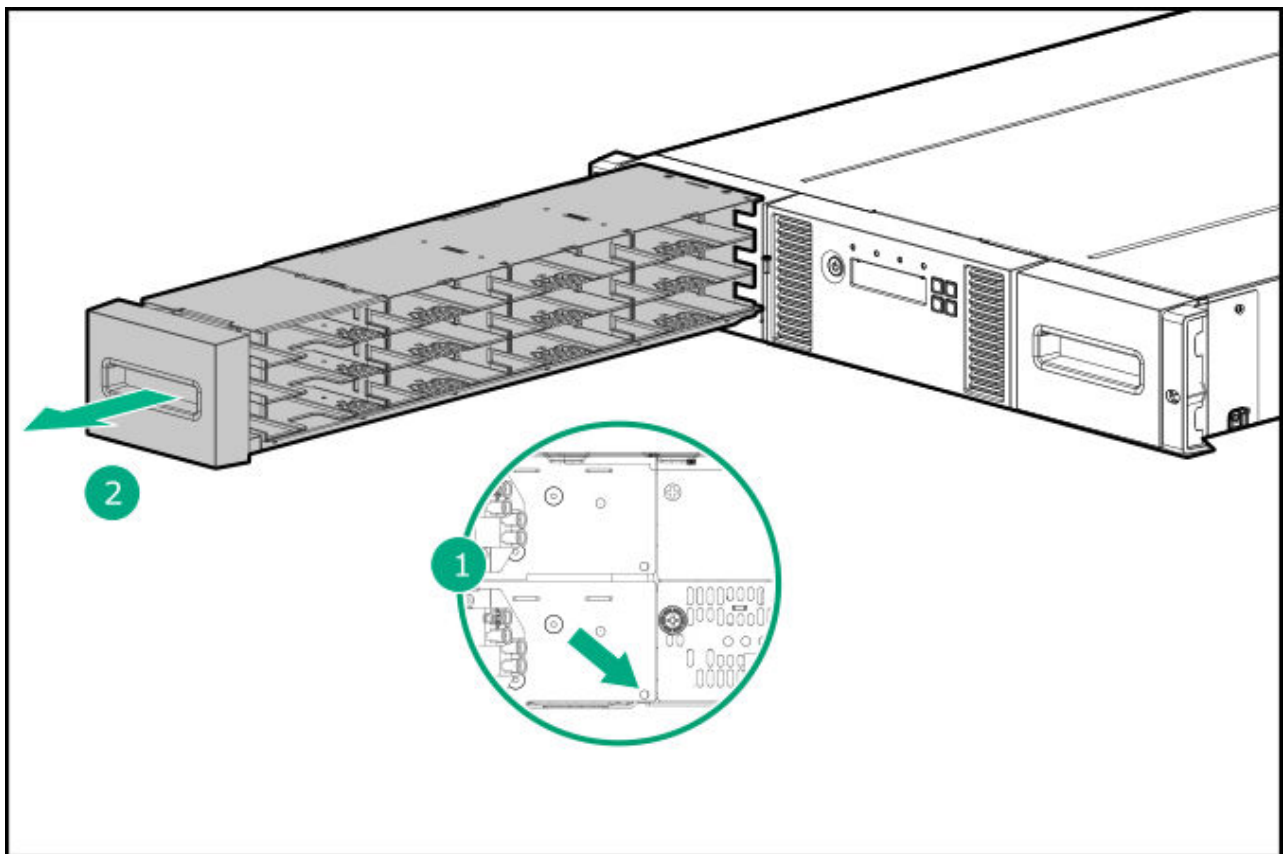
The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

6. Repeat this procedure to remove the tape cartridges from the other magazine.

Removing the cartridges from the magazines using the manual release

Procedure

1. Insert a small metal pin or straightened paper clip about 1.5 cm (0.6 inch) into one of the release holes on the back of the library, while another person grasps the magazines from the released side and removes them from the library.



IMPORTANT

Do not force the pin once you encounter resistance. Doing so can damage the library.

2. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot, then reinsert the magazines into the library. The magazines will lock into place once it is correctly installed.

3. Repeat this step to remove the magazines from the other side.

Removing the library

About this task

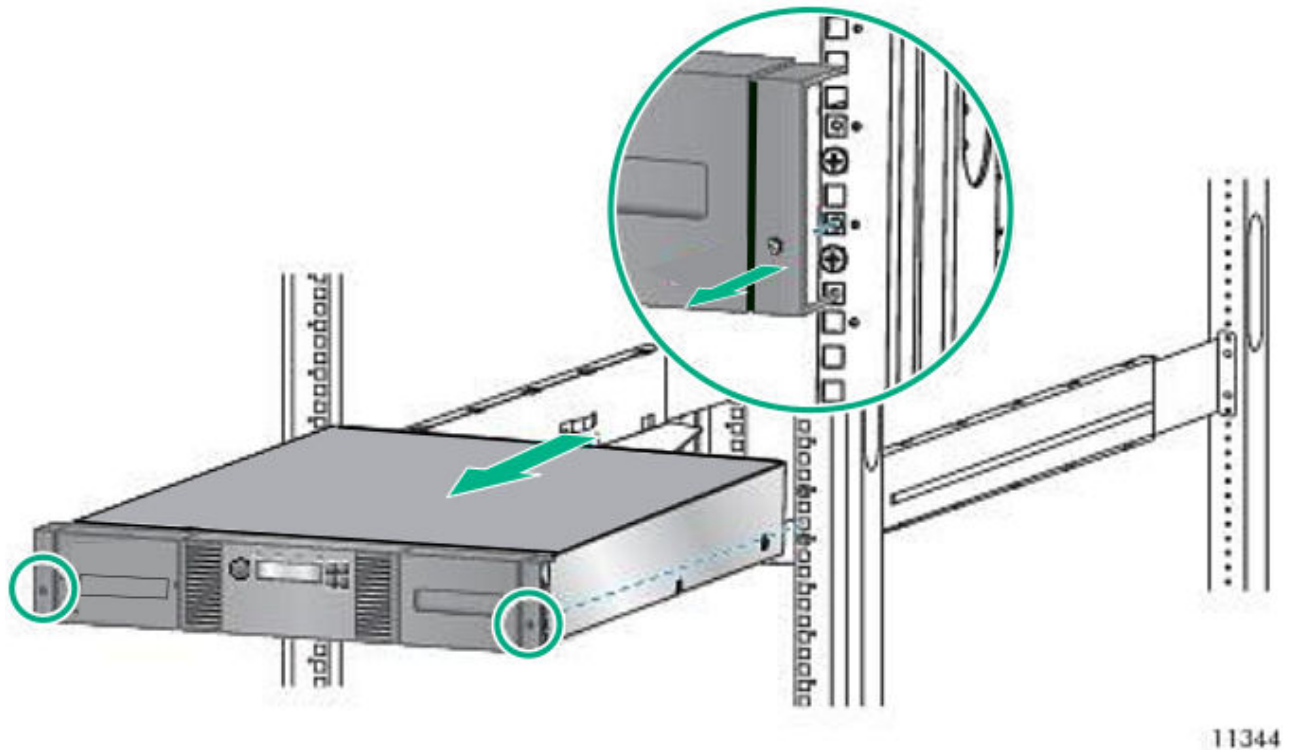


CAUTION

When lifting the library, hold it under its side edges. Lifting it from the drive or magazine openings can damage the chassis and cause errors.

Procedure

1. With a #2 Phillips screwdriver, loosen the captive screws on the front bezel. The library has one screw on each side.



2. With assistance, slide the library out of the rack.

Removing the old rails

With a #3 Phillips screwdriver, remove the screws holding the rails to the rack.

Securing the rails to the rack

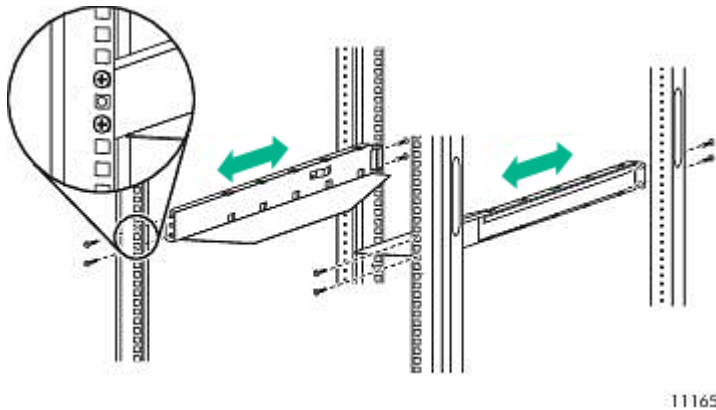
About this task

The rack kit includes two packets of hardware. Select the packet for your rack.

- **Packet label Applicable racks 7.1 mm Round-Hole Rack** HPE supported racks with 7.1 mm round holes in the rack column
- **9.5 mm Square-Hole Rack** HPE supported racks with 9.5 mm square holes in the rack column

Procedure

1. Using the screws from the hardware packet for your rack and a #3 Phillips screwdriver, secure the front of one rail to the front of the rack. The support platform of each rail is tapered, narrowing towards the rear.



11165

2. Extend the rail and then use two screws to secure the other end of the rail to the rear rack column.
3. Repeat steps 1 and 2 to secure the other rail.

Installing the library

About this task

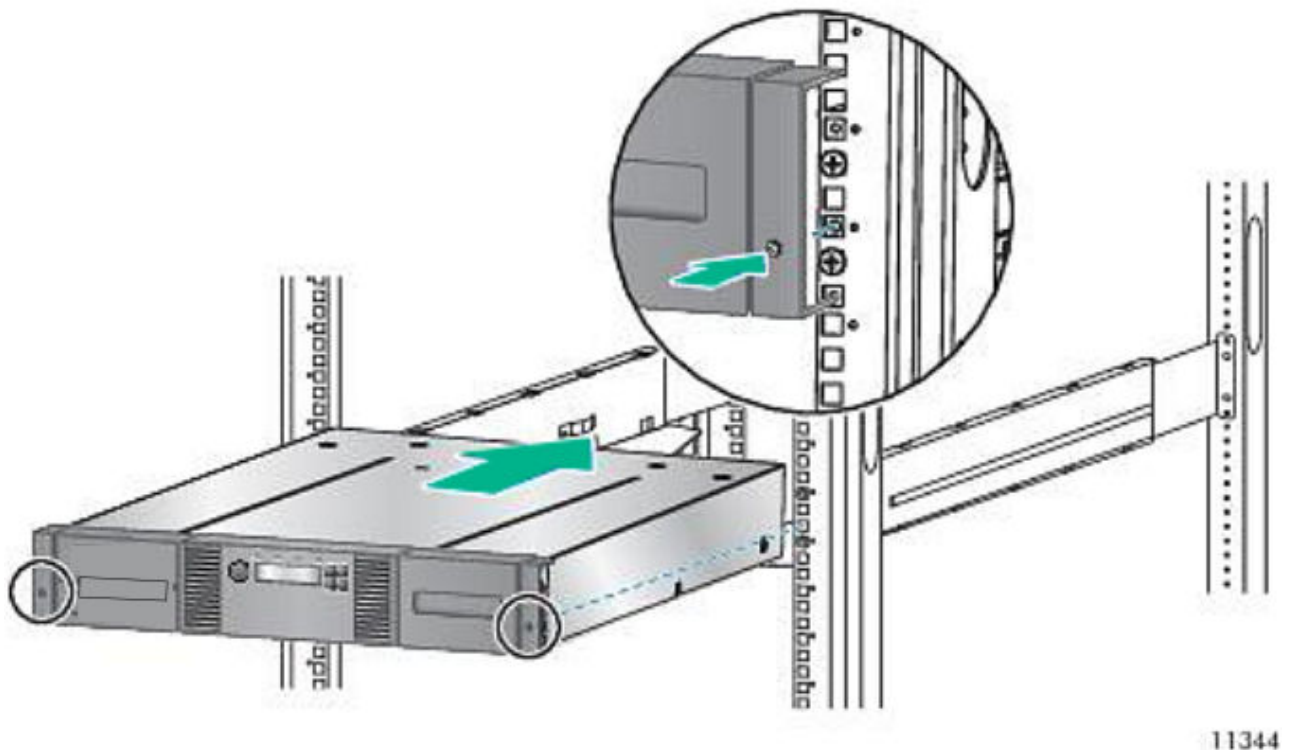


CAUTION

When lifting the library, hold it under its side edges. Lifting it from the drive or magazine openings can damage the chassis and cause errors.

Procedure

1. For new library installation, see [Installing the tape library](#).
2. Slide the library onto the rails.
3. From the front of the library, secure the front bezel to the rack. You can use either a #2 Phillips screw driver or torque driver. Place the tool through the small holes in the mounting bracket. Tighten the captive screws on each side of the library until they are seated. If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not over tighten. If using a torque driver, the recommended torque is six-inch pounds or 0.68 N m.



4. Verify that the library is contained within the 2U rack volume.

5. Load the cartridges into the magazines if necessary.
6. Slide the magazines into the library if necessary.
7. Attach or reattach any SAS, FC, and Ethernet cables.
8. Insert or reinsert the USB device if required.
9. Attach or reattach the power cord.
10. Power on the library.

Tape drive cleaning

The tape drive monitors its need for cleaning, reporting a cleaning request as an event. You can either initiate a drive cleaning operation manually from the **Operation > Clean Drive** or configure auto cleaning from one of the partition wizards.

- [The auto cleaning feature](#)
- [Configuring auto cleaning](#)

Subtopics

[**The auto cleaning feature**](#)
[**Auto cleaning configuration**](#)

The auto cleaning feature

When auto cleaning is enabled, the library must have an unexpired labeled cleaning cartridge loaded. The label must begin with the letters “CLN” for the library to recognize it as a cleaning cartridge. The cleaning cartridge can be in a partition slot or in a slot that is not part of a partition.

The usage count for a cleaning cartridge is maintained in the cartridge memory. The library reads the usage count the first time the cartridge is loaded into a tape drive and records the usage count with the cartridge inventory information. When multiple cleaning cartridges are available, the library will choose a cleaning cartridge whose usage count is not available in the cartridge inventory information. If the library knows the usage count for all the cleaning cartridges, the library will choose the one with the highest usage count.

Auto cleaning configuration

You can configure auto cleaning with the basic or expert partition wizards, see [Partition wizards](#). When auto cleaning is enabled, the library automatically initiates a cleaning operation when media is unloaded from a drive that requires cleaning instead of creating a warning event when a drive requires cleaning.

Troubleshooting



CAUTION

Shipping Lock: The shipping lock must be removed for the robotics to operate properly on the MSL2024. The library displays a robot move error if the shipping lock is not removed (see [Removing the shipping lock](#)).

Subtopics

[The library displays errors](#)

[Fibre Channel connection problems](#)

[Detection problems after installing a SAS drive](#)

[Operation problems](#)

[Performance problems](#)

[The wellness test](#)

[Error codes](#)

[Diagnosing problems with Library & Tape Tools](#)

The library displays errors

Symptom

The library displays library errors and the library edges are not properly supported.

Cause



CAUTION

This library is designed to operate when installed in a rack using the included rack rails. Operating the library without installing it in the rails, such as on a table or rack shelf, could result in library errors. Placing any weight on top of the library might also cause errors.

Fibre Channel connection problems

Use the **Status** screen to check the link connection for your tape drive.

If the screen shows **Logged Out**:

- Check that the Fibre speed is set to Automatic (on the RMI) or Auto Detect (on the OCP), or that the correct fibre speed is selected. If you are unsure of the speed of the HBA or switch that the library is connected to, try Automatic (on the RMI) or Auto Detect (on the OCP).
- Check that the correct port type, fabric, or loop, is selected. Loop requires additional configuration. If you are unsure of the correct port type, try Automatic (on the RMI) or Auto Detect (on the OCP).

If the screen shows **No Link**, the Speed Status is – and the Link LED on the back of the drive is off:

- The speed is probably set incorrectly. Try setting the speed to **Automatic** (on the RMI interface) or **Auto Detect** (on the OCP).
- If there are still issues, change the port type to Auto Detect.

If the screen shows **No Light**:

- The cable is not plugged in correctly. Check that it is connected correctly to Port A of the tape drive.
- The cable is damaged. FC cables are delicate. If the cable has been bent or twisted sharply, it might be broken and must be replaced.

If the screen shows **ALPA Conflict**:

- There might be a conflict with the ALPA address on Loop ports. Select **Soft** for the Loop mode to allow the system to select an available address each time the tape drive connects to the FC fabric. If your server configuration does not support changing addresses, try using the **Hard Auto-Select** option for the Loop mode. This allows the system to select an available address when it first connects, and then retain that address for future connections.

Detection problems after installing a SAS drive

Problems encountered after installation are often caused by improper SAS cable connections, application software configuration errors, or an incorrectly configured operating system. If the application software or operating system does not communicate with the library or drive after installation, determine the extent of the detection problem:

- Does the application software detect the tape drive?

- Does the application software detect the library?
- Does the operating system detect the tape drive?
- Does the operating system detect the library?
- Does the operating system detect the library, but list it as a generic device?

Based on the extent of the detection problem, check the following:

- If neither the application software nor operating system detects the tape drive, or they do not detect both the tape drive and the library:
 - Verify that all SAS cables are securely connected on both ends. If the mini-SAS connectors that connect to the tape drive and some HBAs will not plug in, check the key. The mini-SAS connector on the tape drive is keyed at location four, which is the standard location for end devices. If the connector on the cable is keyed in a different location, the connector not plug-in and the cable probably will not work.
 - Check the length and integrity of your SAS cabling. For reliable operation, do not use a SAS cable longer than 6 meters. Do not use a cable adapter or converters between the HBA and the library.
 - Check the SAS connectors for damage or debris.
 - Verify that your HBA is supported by the host computer and qualified with the library. For current HBA compatibility information, see the compatibility matrix at [Accessing the compatibility matrix](#).
 - Verify that your HBA has the latest firmware.
- If the application software or operating system detects the tape drive, but not the library:
 - Verify that multiple LUN support is enabled on the HBA. The device uses two Logical Unit Numbers (LUNs) to control the tape drive (LUN 0) and robotic (LUN 1). The device requires an HBA with multiple LUN support, and thus multiple LUN support must be enabled on the host computer. When multiple LUN support is not enabled, the host computer can see the tape drive, but not the library.



NOTE

Many RAID or array controllers do not provide multiple LUN support.

- If the application software or operating system does not detect any devices on the HBA:
 - Verify that the SAS host adapter is installed correctly. See the manual that came with your host adapter for installation and troubleshooting instructions. Pay particular attention to any steps describing configuration settings. Ensure that the host adapter is properly seated in the motherboard slot, and it is correctly detected by the operating system.
 - Verify that the proper device driver is installed for the SAS host adapter.

- If the library is detected by the operating system, but not by the application software:
 - See the documentation included with your backup application for instructions on how to verify proper installation. Some backup software packages require an additional module to communicate with the robotics.
- If the library is detected by the operating system, but is listed as an unknown or generic device:
 - Make sure that the proper device driver, if applicable, is installed for the device. Check your software provider website for the latest drivers and patches.



NOTE

Many backup applications use their own drivers. Before installing a driver, make sure that it is not in conflict with the application software.

If you continue to have problems with a SAS library, check the following:

- Ensure that the device is compatible with the SAS host adapter and backup application you plan to use. For a list of compatible SAS host bus adapters and application software, check with your SAS host adapter manufacturer, backup application vendor, or the compatibility matrix at [Accessing the compatibility matrix](#).
- Verify that your HBA is supported by the host computer and qualified with the library. For current HBA compatibility information, see the compatibility matrix at [Accessing the compatibility matrix](#).
- Ensure that you are using a compatible, high-quality cable. See the product **QuickSpecs** for a list of supported cables.

Operation problems

Problem	Solution
Device does not power on.	1. Check all power cord connections. 2. Make sure that the power button on the front panel has been pressed, and the green READY LED is illuminated. 3. Make sure that the outlet has power. Try another working outlet. 4. Replace the power cord.
No display messages appear.	1. Make sure that the power cord is connected.

Problem	Solution
	2. Make sure that the power button on the front panel has been pressed, and the green READY LED is illuminated. 3. Power cycle the device. 4. If the display is still blank but the device seems to be powered on, try to get the device status or error information from the RMI.
All power supply LEDs are off.	1. Check all power cord connections. 2. Make sure that the power button on the front panel has been pressed, and the green READY LED on the front panel is lit. 3. Make sure that the outlet has power. Try another working outlet. 4. Replace the power cord.
The power button has been pressed, the blue power supply LED is lit, and green power supply LED is off.	The blue LED is lit when the power supply is plugged into a good outlet. The green LED is lit when the power supply is producing good power. 1. Replace the power supply.
Yellow power supply LED is lit.	The yellow LED is lit when the power supply fan is not rotating at an acceptable speed. 1. Check the power supply fan for obstructions. 2. Replace the power supply.

Failure/attention indications displayed on the front panel

Problem	Solution
"!" in operator panel inventory display.	Export the data cartridge marked with an ! in the inventory. The cartridge is either damaged, incompatible with the drive, or the wrong type for the attempted operation.
The LCD displays an error code.	Look up the error code, try to resolve the failure, and power cycle the device (see Error codes). On the MSL2024 OCP, press Enter to see the error message for the error code.

Controller health status

Problem

Controller health status LED is solid green or not illuminated (pulsing).

Solution

To determine if the controller is faulty, power cycle the library. When operating normally, the LED pulses on and off in cycles of approximately one second. If, after power cycling the library, the LED remains solid green or is not illuminated (pulsing), review the logs for error codes and details. In the RMI, navigate to **Maintenance > Logs and Traces > View Logs**. For assistance with error codes and next steps, contact HPE Support.

Tape movement problems

Problem

Tape stuck in drive.

Solution

Try the following steps, in this order, to remove the stuck tape.



NOTE

The tape drive must rewind the tape before ejecting it. This can take as long as five minutes, depending on how much tape must be rewound. Once the tape is rewound, the eject cycle will take fewer than 16 seconds.

The **READY** light flashes while the tape rewinds. Wait for the tape to finish rewinding before attempting another operation.

1. Attempt to unload the tape from your backup software.
2. Shut down the backup software and stop the operating system's removable storage services. From the OCP, attempt to unload or move the tape to a slot.
3. Power down the unit, disconnect the cable from the drive, power up the unit, and wait until the tape drive is idle or ready. From the OCP, attempt to unload or move the tape to a slot.
4. Attempt a force eject operation from the RMI. See, [Forcing a drive to eject a cartridge](#).



IMPORTANT

Inspect the tape cartridge that was stuck. Damage or misplaced labels on the cartridge could have caused the

Problem**Solution**

e load/unload failure. Discard any tape cartridge found to have issues.

Tape stuck in storage slot.

To remove a stuck tape from a storage slot:

If the OCP or the RMI is still operational:

1. Move the tapes from the drives to the magazines using the **Move Tape** command.
2. Use the magazine removal process to release the magazine and remove it from the device.
3. Manually remove the cartridge from the magazine by inserting a finger in the hole at the back of the magazine. Some tapes need to be inserted and removed several times to condition them for free movement in and out of the magazine.

Media problems**Problem****Solution**

Cleaning or data cartridge incompatible with drive.

Make sure that you are using data and cleaning cartridges that are compatible with the drive and model of your device (see [Tape cartridges](#)) and that you are using the correct cartridge type for the operation. The device automatically unloads incompatible cartridges, the **Attention** LED flashes, and an exclamation point (!) displays in the inventory display for the indicated slot number. Export the media to clear the state.

Cannot write to or read from tape.

- Make sure that the cartridge is not a WORM cartridge that has already been used.
- Make sure that the cartridge is write enabled (move the write-protect switch to the enabled position).
- Make sure that the data cartridge is compatible with the drive model. (See [Read and write compatibility](#).)
- Make sure that you are using an Ultrium cartridge that has not been degaussed. **Do not degauss Ultrium cartridges!**
- Make sure that the cartridge has not been exposed to harsh environmental or electrical conditions and is not physically damaged in any way.

Problem**Solution**

- Many backup applications do not read or write to cartridges that were created using a different backup application. In this case, you might have to perform an erase, format, or label operation on the cartridge.
- Make sure that you understand any data protection or overwrite protection schemes that your backup application might be using, which could prevent you from writing to a given cartridge.
- Retry the operation with a different, known good tape.
- Clean the tape drive.

Attention LED is illuminated**Problem****Solution**

Both the Attention and Cleaning LEDs are lit.

This is most likely caused by a dirty drive that cannot read a tape and marks the tape invalid.

1. View the inventory with the RMI. Note the slots that have tapes marked with .
2. Remove any magazines that contain tapes marked with .
3. Remove the tapes that were marked with .
4. Inspect each removed tape for damage, check that the tape is compatible with the drive, and ensure that it is not past its usage life. See [Tape cartridges](#). Discard any tapes that are damaged or past their usage life. Do not use cartridges that are incompatible with the tape drive.
5. Reload the magazines with tapes that have passed inspection and new tapes to replace cartridges that did not pass inspection.
6. Replace the magazines.
7. Clean the tape drive.

A particular cartridge sets off the cleaning light.

Check the cartridge for contamination by loose debris.

A cartridge recently imported from a different environment is causing issues.

Media that is moved from one environment to another can cause issues until it has acclimated to the new conditions. A cartridge should be acclimated for at least 24 hours before being used, particularly if it has

Problem	Solution
	been stored at a substantially different temperature or level of humidity than the device.
The Attention LED is lit but the Cleaning LED is not lit after a cartridge load.	The library was unable to complete the requested operation with the selected tape cartridge. • Use only cartridges that are compatible with the drive type (see Tape cartridges). • Use the correct type of cartridges for the operation. For example, use a cleaning cartridge for cleaning. • Make sure that you are using an Ultrium Universal cleaning cartridge (see Tape cartridges).
The Cleaning LED is lit after using a cleaning cartridge.	The cleaning cartridge is expired. A cleaning cartridge will expire after 50 cleaning cycles.
A particular cartridge sets off the Attention LED and possibly the Cleaning LED.	If the Media Attention LED is cleared and the drive has been cleaned, and then immediately redisplayed each time a particular cartridge is reloaded, that cartridge should be suspected as being defective. • If this occurs, export the cartridge and load a known good cartridge. In some cases, a cartridge can be worn out, have a defective Cartridge Memory, or have been formatted as a Firmware Upgrade Cartridge. • Any cartridge that is suspected of being defective or contaminated should NOT be reused in any drive. • If the bad cartridge is a cleaning cartridge, it might be expired.

Inventory problems

Problem	Solution
The inventory labels the cartridge Full instead of showing its barcode	• Verify that the label is a Hewlett Packard Enterprise label. The barcode reader might not be able to read other labels. • Verify that the label is properly applied. See, Recommended practices for labeling tape cartridges. • Verify that the label is not soiled.

Problem**Solution**

The inventory process takes a long time

Apply high-quality Hewlett Packard Enterprise labels to all tape cartridges. During the inventory process, the barcode reader attempts to read the barcode on the cartridge or the barcode on the back of the storage slot until it identifies the cartridge or determines that the slot is empty. The reader can usually identify a properly labeled cartridge the first time, while determining that an unlabeled cartridge is in a storage slot can take four times as long.

RMI network connection issues**Problem****Solution**

Cannot connect to the remote management interface (RMI)

- Verify that the device is connected to the LAN with a CAT 5E, 6, or 6E Ethernet cable.
- Verify that the link LED on the RJ45 (LAN) connector is lit when the device is powered up. If the LED is not lit, the device is not communicating with the LAN. See your network administrator for help.
- Verify that the device has been configured with a valid static network address or DHCP has been enabled so the device can obtain a network address. If using DHCP, write down the device network address from the OCP Information menu. If the device did not obtain a valid address via DHCP, verify that the DHCP server is up and the device has network access to it. If necessary, set a static network address instead.
- Enter the device IP address into the address bar of a web browser connected to the same LAN as the device. If the RMI web page does not display, ping the device IP address. If the ping fails, verify that the device has a valid network address and that there are no firewalls or other obstructions to network traffic between the computer with the web browser and the device. See your network administrator for help.

Cleaning problems

Problem	Solution
Cannot load the cleaning cartridge .	• Make sure that you are using an Ultrium Universal cleaning cartridge (see Tape cartridges) . • Make sure that the cleaning cartridge has not expired. A cleaning cartridge will expire after 50 cleaning cycles. • Ensure that the cleaning cartridge has a cleaning cartridge label installed. For more information on labeling tape cartridges, see . • Power cycle the tape library.

Performance problems

Backing up files involves many system components, from the files in the file system on the disk, through the backup server, and finally saved to the storage library. All of this is managed by software running on your computer's operating system. The backup process can only run as fast as the slowest component in the system.

Performance issues are solved by identifying and addressing performance limitations in your system.

Potential performance limitations:

- [Average file size](#)
- [File storage system](#)
- [Connection from the backup server to the disk array](#)
- [Backup/archive server](#)
- [Backup/archive software and method](#)
- [Connection from the archive/backup host server to the library](#)
- [Data cartridges](#)
- [Tape drive read or write performance seems slow](#)

You can use the L&TT system performance test to assess the performance of simulated backup and restore operations. For information on downloading and using L&TT, see [Diagnosing problems with Library & Tape Tools](#).

Subtopics

Average file size

File storage system

Connection from the backup server to the disk array

Backup/archive server

Backup/archive software and method

Connection from the archive/backup host server to the library

Data cartridges

Tape drive read or write performance seems slow

Average file size

The hard drive must seek to the position of a file before it can start reading. The more time the disks are seeking to files, the lower the performance. Therefore, if the average file size is small, the read performance will be lower.

To determine the average file size, divide the size of the backup by the number of files.

If the average file size is small (64 KB or less), consider using a sequential, image, or block backup method that backs up the whole hard drive or LUN image instead of individual files. The trade-off for using one of these methods is that you might only be able to restore the entire image instead of individual files.



NOTE

File fragmentation will also cause excessive drive seeking, which lowers performance, so ensure that files are regularly defragmented.

File storage system

The file storage system determines the organization of the files on the disks. Using RAID controllers to spread files over multiple disks can improve performance because some disks can be seeking while others are reading. Storing files on a single non-RAID disk results in the slowest performance while storing files on a high-end disk array results in the fastest performance.

Converting standalone disks to RAID can improve performance.

Ensure that the file systems being backed up have no or minimal fragmentation.

Connection from the backup server to the disk array

The connection between the host server and the disks determines how much data can be transferred from the disks to the host computer at one time. A connection with insufficient bandwidth cannot provide enough data for the tape drives to write at full speed. For optimum performance, the storage subsystem must be able to provide data at the tape drive maximum transfer rate.

Backup systems using a low-speed Ethernet network should use multiple network connections.

Backup/archive server

The backup server must have enough RAM and processor power to transfer the files from the disk to the tape drive while also running the backup or archive software and any other processes.

Check the RAM and processor usage during a backup operation. If they are operating at capacity, adding RAM or processor capability can improve performance.

Backup/archive software and method

Each backup method has its own impact on performance, depending on how well it can keep data streaming to the tape drive. In most cases, native applications do not have the features required to maximize performance for LTO tape drives. Hewlett Packard Enterprise recommends using a full-featured backup or archive application with this library.

File-by-file backup or archive methods provide the best restore performance if you only need to restore individual files. However, if the average file size is small, file-by-file methods will significantly reduce performance.

Disk image, flash, or sequential backup methods provide the fastest performance because they back up an entire disk, partition, or LUN, which minimizes disk seeking. The disadvantage is that backup and restore operations work on an entire disk, partition, or LUN. You might not be able to back up a subset of files or restore a single file. If you can restore a single file, the restore process will be slow.

Database backup performance will vary based on the use model. To improve performance when backing up data from a database:

- Use specific backup agents for the database.
- Use the latest versions of the databases.
- Do not back up individual mailboxes.
- Do not back up specific records or do a record-by-record backup.
- Do not back up when the database is in heavy use.

Connection from the archive/backup host server to the library

For the best performance, the connection from the host server to the library must have sufficient bandwidth to provide enough data to keep the tape drive streaming. Current LTO tape drives take advantage of some of the fastest interfaces available so the type of interface used to connect the library to the host server is not likely to be the cause of a performance issue. However, issues with cables and connectors can limit performance.

Verify that the system is using cables that are listed in the QuickSpecs, are in good condition, and do not exceed recommended cable lengths.

Data cartridges

The type and condition of data cartridges can affect backup performance. For best results, use Hewlett Packard Enterprise cartridges that are the same LTO generation as the tape drives. If you suspect cartridge-related performance problems, run the L&TT media assessment test to evaluate the condition of the data cartridges.

Tape drive read or write performance seems slow

Symptom

Tape drive read or write is slower than expected.

Cause

If the tape drive is not properly secured to the chassis or the library is not properly secured to the rack, vibration may cause slow read or write performance. Vibration could come from the cooling fan or external sources.

Action

1. To ensure that the tape drives are securely tightened to the chassis, tighten the drive sled mounting screws (the blue captive thumbscrews). You can use either a #2 Phillips screwdriver or a torque driver.
 - If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not overtighten.
 - If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.

- If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



IMPORTANT

Under certain conditions of external shock and vibration, it has been noted that if the thumbscrews are not tightened, drive performance issues might occur. In that situation, please tighten the thumbscrews to the recommended torque.

2. Ensure that the chassis is securely tightened to the rack.

From the front of the library, use either a #2 Phillips screwdriver or a torque driver to tighten the captive fasteners

If using a #2 Phillips screwdriver, tighten the captive fasteners until a low initial threshold torque achieves a snug tight condition. Do not overtighten. If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.

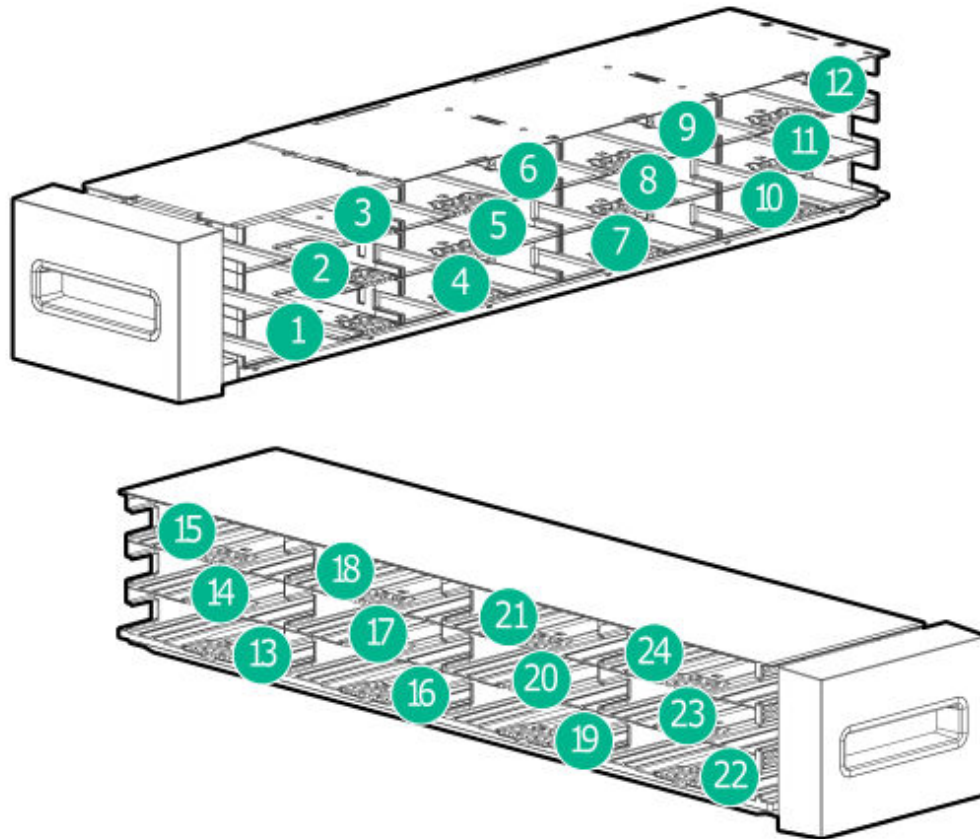
The wellness test

The wellness test exercises all library and tape drive hardware, except the external connections, and is useful for verifying that a library is working correctly.

For complete testing, enable the mailslot and ensure that each top-row corner slot contains a tape cartridge.

The Wellness Test requires at least one enabled and functional drive and one cartridge with barcode label in the library. For more information, see the online help. For a quick test execution, it is recommended to have one functional drive and compatible data cartridges in the corner slots of the library.

Figure 1. MSL2024 top-row corner slots with mailslot disabled: 3, 12, 15, 24



IMPORTANT

The library will remove any tape cartridges from the tape drives and go offline when running the wellness test. Verify that any applications using the library are completed before starting the wellness test.

You can have the library run up to 10 cycles of the wellness test. If the library has more than one tape drive installed, you can select whether to run the test on one or all the tape drives. The wellness test operates on the whole library, without regard to logical libraries.

Subtopics

Running the wellness test

Running the wellness test

Prerequisites

- At least one drive must be empty.
- At least one cartridge that is compatible with the empty drive must be in a magazine slot or mailslot.

If moving a cartridge to or from a tape drive, the cartridge must be compatible with the generation of the tape drive.

- One of the selected element locations must be empty and one of the selected element locations must be full.
- All backup operations are stopped.

The test takes the library offline to hosts for the duration of the test.

About this task

The wellness test exercises basic library functionality. At the end of the test, cartridges will be in different storage slots.

Procedure

1. Navigate to **Maintenance > Tests > Wellness Test**.
2. Click **Start Test**.

Error codes

If an error occurs during operation, the device stops the current operation and displays an error code on the LCD screen.

To check the overall operation of the device, run the wellness test from the OCP. The wellness test exercises all robotic movements and checks the status of the electrical components and communication.

If the error persists, contact support personnel.

There are three ways to obtain logs from the device:

- On the OCP
- On the RMI
- On an L&TT support ticket or report

For more information on Saving Logs and Tickets from the OCP using a USB drive, see [Saving a Library Support Ticket](#) and [Saving Library Logs Files](#).

Subtopics

Finding library logs on the RMI

Generating a report or support ticket from L&TT

Downloading a support ticket from the library

Viewing a downloaded support ticket

Finding error code information on an L&TT support ticket or report

Error events

Warning events

Configuration change events

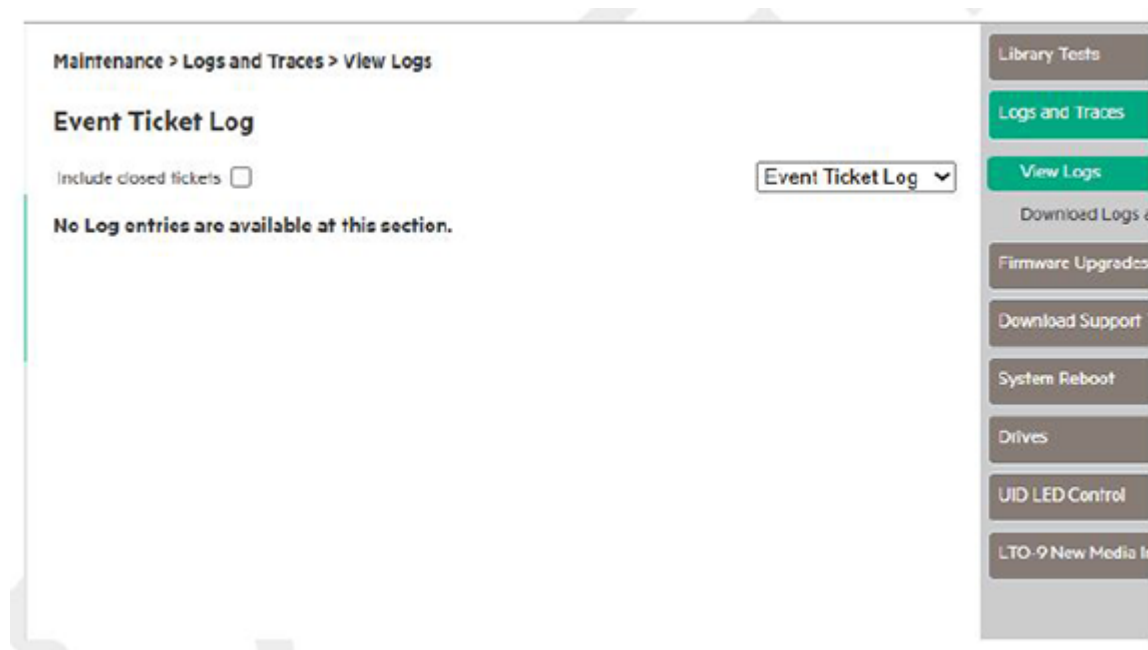
Informational events

Finding library logs on the RMI

You can view or save logs on the RMI **Maintenance > Logs and Traces**. The available logs are: Event Ticket Log, Information Log, Configuration Log, or Show All.

The log entries are displayed in order of most recent to oldest. Log entries will have the Time of the Event, the Event code, and a Description of the Event. Clicking on an individual event will show more details.

A Library support ticket can also be saved from the library RMI from the **Maintenance > Download Support Ticket > Library Support Ticket**. See [Downloading an library support ticket](#).



Generating a report or support ticket from L&TT

Procedure

1. In the L&TT **By Product** or **By Connection** tab, select the device from the device list.

2. Click the **Health** button on the main toolbar to generate and display a standard report, or click the **Support** button on the main toolbar to display the **Support** screen for additional report or support ticket options.

Downloading a support ticket from the library

About this task



TIP

Each support ticket downloaded from the RMI will only contain information for the library itself or one drive. To capture all support information, download a ticket from the library and from each drive. To generate a consolidated support ticket with all support data in a single compressed file, download the support ticket with L&TT.

Procedure

- Navigate to **RMI > Support > Support ticket** and click **Download**.
- Insert a USB flash drive into the USB port on the rear panel and then from the OCP, select **Download support ticket to USB**.

Viewing a downloaded support ticket

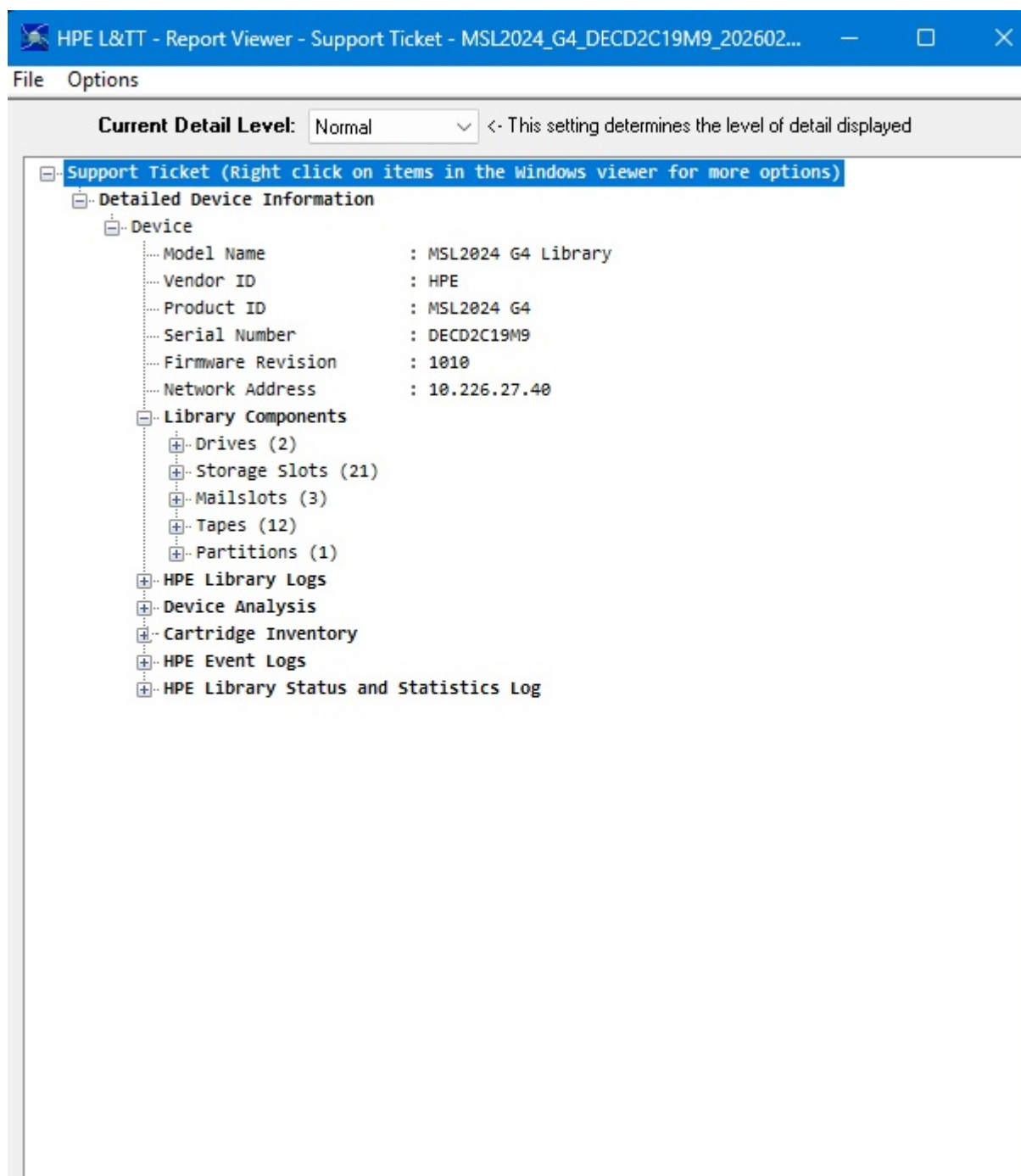
Procedure

1. Navigate to **L&TT > File > Load Support Ticket**.
2. Select the support ticket file in the browser.

Finding error code information on an L&TT support ticket or report

An L&TT support ticket or report contains detailed information about the device configuration, along with errors and warnings. The support ticket and report contain the same information. The report is easier to read, but must be generated and read on the host computer. The support ticket can be downloaded from the device and then viewed on any computer with L&TT installed.

The top of the support ticket contains basic configuration information about the library.



Expand **HP Event Logs** to see events divided into three categories:

- Events in the last 24 hours
- Events in the last 31 days
- Events older than 31 days

Set the **Current Detail Level** to see additional types of events:

- **Normal** will only show critical events or hard errors.
- **More details** will also show warning and configuration events.
- **Everything** shows all events.

Critical events are designated with a STOP sign icon. Expand an event for more information.

The time stamp is in the format hours:minutes:seconds. The hours are in 24-hour clock format.

The date is in the format year/month/day.

The type of event:

- **Crit**—error events
- **Warn**—warning events
- **Config**—configuration events
- **Info**—informational events

The event ID is the number on the header line. It uniquely maps to an error code. For error codes, see [Event codes](#).

The text description in the header is the simple text description of the event.

- The time stamp is in the format hours:minutes:seconds. The hours are in 24-hour clock format. For example, in this case `14` is 2 p.m.
- The date is in the format year/month/day.
- The event ID is the number on the header line, `0x006E` in this example. It uniquely maps to an error code.
- `HE` designates a hard error. The STOP sign icon and the word `Crit` before the event ID also indicate a hard error.
- The text description in the header (“robotic controller error” in this example) is the simple text description of the main error code.
- The main error code `(0x83)` is displayed in parentheses as the **Global error code**. The text after the main error code (`Robotic controller generic problem` in this example) is the text description for the error code.
- The error sub-code `(0x02)` is displayed in parentheses as the **Module error code**. The text after the error sub-code (`Robotic: connection to slave robotic failed` in this example) is name of the component followed by the text description of the error sub-code.
- The **Current command** provides information for factory use only.

Error events

Event code	Event text	Details and solution
2000	Failed to move cartridge	1. Verify the source and destination elements and then retry the move operation. • If the source is a magazine slot, open the magazine with the RMI Operation > Open Magazine page, and manually remove and replace the tape cartridge several times to ensure that it is not stuck. • If the source is a drive, use the RMI to move the tape cartridge to a magazine slot using the Operation > Move Media page of the RMI. If the cartridge still cannot be moved, power cycle the drive using the Configuration > Drives page of the RMI, then retry the move. If the move is unsuccessful, attempt a force drive media eject from the OperationForce Drive Media Eject page in the RMI. If the cartridge still cannot be moved from the drive, power cycle the library and then retry the move. If the move is not successful, attempt a force drive media eject from the OperationForce Drive Media Eject page in the RMI. 2. Ensure that the library and tape drives are running the latest firmware version.
2003	Temperature in library exceeded critical limit	1. Verify that the power supply fan is functioning. 2. Verify that the drive cover plates are installed in all open drive bays. 3. Verify that the ambient room temperature is within the specified limits.

Event code	Event text	Details and solution
		- Verify that there are no obstructions to airflow through the library. - Ensure that the library is running the latest firmware version.
2004	Library startup failure	 IMPORTANT Verify that the shipping lock is removed. - Power off the library and then check inside the library for any obstruction that the robotic assembly may be hitting. - Remove all magazines and ensure that all tape cartridges are pushed fully into the air slots. When reinstalling the magazines, ensure the magazine guides are correctly inserted into the library. - Remove any loose tape cartridges from the elevator. - Check the tape drives for loose, uncontrolled, or stuck tape cartridges. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. - Power on the library. - If the error event persists, ensure that AC power is connected. Using power supply LEDs and controller LEDs, verify that each component is powered on and functioning correctly. - Power cycle the library. - If the error event persists, power off the library. Then power on the library. - If the error event persists, power off the library. If the library was recently moved, the ass

Event code	Event text	Details and solution
		sembly could be out of alignment. Correct if necessary. - Power on the library. - If the error event persists, check the event log for additional events or event details that provide more specific information. - If the issue is corrected, continue with the next debugging step or return the library to its normal operation and clear the event codes.
2009	Library test failed due to robotics assembly problem	- Review the test requirements, address any issues, and then retry the test. - Power off the library and then check inside the library for any obstruction that the robotic assembly could hit. - Clear any obstructions from the bottom of the library. Remove all magazines and ensure that all tapes are pushed fully into their slots. - Remove any loose tape cartridge from the elevator. - Check the tape drives for a loose, unrolled, or stuck tape cartridge. If you find any loose cartridges, put them back into their correct magazine slots. - When reinstalling the magazines, ensure that the magazine guides at the bottom fit properly. Also, verify that the magazine is fully inserted into the library. - Power on the library. - If the error event persists, power off the library.

Event code	Event text	Details and solution
		5. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. If the error event recurs, check the event log for additional events or event details that provide more specific information.
2021	Database access error	An error occurred while accessing the system database. 1. Ensure that the library and tape drives are running the latest firmware version. 2. Power cycle the library. 3. If the error persists, restore the library configuration.
2022	Drive has been hot removed while in active status as LUN master	Tape drives must be powered off before removing them from the library. Ensure the drive is fully seated and secured.
2023	Internal software error	Power cycle the library.
2024	Exception thrown by application not handled	One of the library applications failed with an exception which has not been handled. Retry the operation and if the error persists power cycle the library. If the error persists, update the library firmware.
2027	Move failed pulling cartridge from slot	• Inspect the cartridge and cartridge labels for physical damage that could prevent the cartridge from being inserted into or removed from the slot. • Clear any obstructions from the bottom of the library. • If the source is a magazine slot, manually remove and replace the tape cartridge several times to ensure that it is not stuck.
2028	Move failed inserting cartridge into slot	

Event code	Event text	Details and solution
2029	Initialization failure due to robot front to back positioning error	 NOTE If the cartridge still cannot be moved, power cycle the library and then retry that the robotic assembly move. - Power off the library and then check inside the library for any obstruction that may be hitting. If the cartridge still cannot be moved, power cycle the library and then retry the move. - Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridges from the elevator. - Confirm that the robotics shipping lock is removed. - Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. - When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. Ensure that the magazine is fully inserted into the library. - Power on the library. - Verify that the library is level front-to-back and side-to-side. - If the error event persists, check the event log for additional events or event details that provide more specific information.

Event code	Event text	Details and solution
		- If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. - If the error event reoccurs, replace the chassis assembly.
2032	Initialization failure due to robot rotation positioning error	Confirm that the robotics shipping lock is removed.
2033	Initialization failure due to robot vertical positioning error	- Power off the library and then look inside the library for any obstruction (for example, a cartridge sticking out). - Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridges from the elevator. - Confirm that the robotics shipping lock is removed. - Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. - When reinstalling the magazines, ensure that the magazine guides at bottom are correctly engaged, and ensure that the magazine is fully inserted into the library. - Power on the library. - Verify that the library is level front to back and side to side. Power on the library.

Event code	Event text	Details and solution
		- If the error event persists, view the event log for additional events or event detail that provide more specific information. - If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the robotic assembly event codes. - If the error event reoccurs, replace the chassis assembly.
2035	Initialization failure due to robot gripper positioning error	- Power off the library and then look inside the library for any obstruction. - Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridges from the elevator. - Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to appropriate magazine storage slots. - When reinstalling the magazines, ensure that the magazine guides at the top and bottom are correctly engaged. Ensure that the magazine is fully inserted into the library. - Power on the library. - If the error event persists, view the event log for additional events or event details that provide more specific information. - Power cycle the library and then retry the operation.

Event code	Event text	Details and solution
2036	Unintended termination of application process	One of the application processes unexpectedly terminated.
2037	Robotics firmware version upgrade failed	Power cycle the library and then retry the operation.
2039	Cartridge left in robot gripper, unable to be moved to any open location	The post initialization recovery process was not successful in moving the cartridge from the robotic gripper to an open location. 1. Enable mailslots if necessary. Ensure that some magazine slots are available. Remove tape cartridges from the library to open slots, if necessary. 2. Power cycle the library. 3. Use the OCP to move the cartridge to an open slot.
2040	Wellness test failed with critical error	1. Check for additional events that might provide an indication of the reason for the failure. 2. Retry the wellness test.
2045	Wellness test failed because move media test failed	1. Verify that at least one unloaded drive and one data cartridge compatible with that unloaded drive are installed in that the robotic assembly library. If no drives are unloaded or no compatible cartridge is found, the test will fail and the error event will be generated. 2. Unload all tape drives and then rerun the test. 3. Power off the library and then look inside the library for any obstructions. a. Remove all magazines and ensure that all tape cartridges are pushed fully into the ir slots. When reinstalling the magazines, ensure the magazine guides at the bottom and top are correctly engaged. b. Clear any obstructions from the bottom of the library.

Event code	Event text	Details and solution
		c. Clear any loose tape cartridges from the elevator. d. Check the tape drives for loose, uncontrolled, or stuck tape cartridges. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. e. Power on the library. 4. Verified that the library is level front-to-back and side-to-side. 5. If the error event persists, check the event log for additional events or event details that provide more specific information. 6. If the issue is corrected, continue with the next debugging step or return the library to its normal operation and clear the event codes.
2046	Wellness test failed because drive communication test failed	1. Power off the library. 2. Remove and then reinstall the tape drive to ensure that the drive is fully seated. 3. Power on the library. 4. Verify that the drive is running the most recent firmware version. 5. Use the RMI to pull a drive support ticket and review the device analysis section.
2047	Wellness test failed because the barcode scanning test failed	1. Verify that there is not an obstruction between the robotic assembly and the magazines. 2. Verify that all cartridges have high-quality proper barcode labels. 3. Clear any obstructions from the bottom of the library.
2051	Wellness test failed because of the failing robotic test	1. Verify that the library is level front-to-back and side-to-side.

Event code	Event text	Details and solution
		2. Power off the library and then look inside the library for any obstruction that might be blocking the robotic assembly. a. Remove all magazines and ensure that all tape cartridges are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. b. Confirm that the robotics shipping lock is removed. c. Clear any obstructions from the bottom of the library. d. Clear any loose tape cartridge from the elevator. e. Check the tape drives for loose, uncontrolled, or stuck tape cartridges. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. 3. Power on the library. 4. If the error event persists, view the event log for additional events or event details that provide more specific information. 5. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. 6. If the error event reoccurs, replace the library controller.
2052	An open magazine was detected and as a result that the system was taken offline	1. Ensure that all magazines are inserted completely into the library and properly locked. Do not open magazines using the emergency release while the library is operating and the robot is moving.

Event code	Event text	Details and solution
2056	Initialization failures due to picker push pull positioning error	Look for obstructions in the horizontal pathway of the robotics assembly, such as a cartridge sticking out or a cable impeding movement of the robotics assembly.
2061	Move failed pulling cartridge from drive	1. Verify that the drive is fully seated in the library and that all the thumb screws are tightened. 2. Check for loose barcode labels, cartridge damage, or cartridge misalignments that would prevent the cartridge from coming out of the drive. 3. Use the OCP or RMI to move the tape cartridge to the magazine slot. If the cartridge still cannot be moved with the OCP, power cycle the drive and then retry the move. If the move is not successful, attempt a force drive media eject from the Operation > Force Drive Media Eject screen. If the cartridge still cannot be moved from the drive, power cycle the library, and then retry the move. If the move is not successful, attempt a force drive media eject from the Operation > Force Drive Media Eject screen. 4. Ensure that the library and tape drives are running the latest firmware version.
2062	Move failed inserting cartridge to drive	1. Verify that the drive is seated in the library and that all the thumb screws are tightened. 2. Look for labels or cartridge misalignments that would prevent the cartridge from being inserted into the drive. 3. Use the OCP or RMI to move the tape cartridge to the drive. 4. If the cartridge still cannot be moved with the OCP, power cycle the drive and then retry the move.

Event code	Event text	Details and solution
		- If the cartridge still cannot be moved to the drive, power cycle the library, and then retry the move. - If the move is not successful, attempt a force drive media eject from the Operation > Force Drive Media Eject screen. - Ensure that the library and tape drives are running the latest firmware version. - If the move is not successful, attempt a force drive media eject from the Operation > Force Drive Media Eject screen.
2063	Move failed positioning picker in front of drive	- View the event log for additional events or event detail that provide more specific information. - Power off the library and then look inside the library for any obstruction to the robotic assembly. - Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any obstructions from the bottom of library. - Clear any loose tape cartridge from the elevator. - Inspect the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. - When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. Ensure that the magazine is fully inserted into the library. - Power on the library.

Event code	Event text	Details and solution
		- If the error event persists, power off the library and then verify that the library is level within the rack. - Power on the library.
2064	Library test failed with critical error	- Check for additional events that might provide an indication of the reason for the failure. - Verify that the minimum requirements are met for the test and then retry the test. - To verify robotic movement, perform a slot-to-slot or element-to-element test. - Update the library to the latest firmware.
2065	Library startup process failed because of robotics initialization issue	Power off the library and then look inside the library for any obstruction to the robotic assembly.
2066	Library startup process failed during inventory scan	- Remove all magazines and ensure that all tape cartridges are pushed fully into the slots. - Clear any obstructions from the bottom of the library. Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any loose tape cartridge from the elevator. - Check the tape drives for a loose, unrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. - When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. Ensure that the magazine is fully inserted into the library.

Event code	Event text	Details and solution
		2. Power on the library. 3. If the error event persists, power off the library and then verify that the library is level within the rack. If the library was recently moved, the assembly could be out of alignment. Correct if necessary. 4. Power on the library. 5. If the error event persists, view the event log for additional events or event detail that provide more specific information. 6. If the issue is corrected, continue with the next debugging step or return the library to its normal operation and clear the event codes. 7. If the error event reoccurs, replace the library controller.
2067	For safety reason, the robot movement was halted in place	The library detected a physical opening in the library and stopped movement of the robotic assembly. 1. Ensure that all magazines are inserted completely into the library and properly locked. Do not open magazines using the emergency release while the library is operating and the robot is moving. 2. Ensure that the AC power is connected. Using both power supply LEDs and controller LEDs, verify that everything is powered and functional.
2069	Initialization failure due to barcode reader error	1. View the event log for additional events that provide more specific information. 2. Run the robotic test. 3. Power off the library and then look inside the library for any obstruction the robotic assembly.

Event code	Event text	Details and solution
		mbly. Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridge from the elevator. Verify that all cartridges have high-quality proper barcode labels and that the labels are properly applied. - Inspect the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. Power on the library. - Verify that the library is running the latest firmware version. If not, update the library firmware. - Power cycle the library and see if the issue persists.
2070	Inventory scan failed because of elevator axis problem	- Power off the library and then look inside the library for any obstruction to the robotic assembly. - Remove all magazines and ensure that all tapes are pushed fully into their slots. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridges from the elevator. - Verify that all cartridges have high-quality barcode labels and that the labels are properly applied.

Event code	Event text	Details and solution
		e. Inspect the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. f. When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. Ensure that the magazine is fully inserted into the library. 2. Power on the library. 3. If the error event persists, check the event log for additional events or event detail that provide more specific information. 4. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. 5. If the error event reoccurs, replace the library controller.
2071	Cartridge on picker when trying to scan	1. View the event log for additional events that provide more specific information. 2. Ensure that the library has an open storage slot or mailslot. 3. If a cartridge is in the robotic assembly, remove it manually. 4. Inspect the cartridge for damage. Ensure that the cartridge is properly labeled and that the label is in good condition. 5. Ensure that all the tape drives are fully inserted into the library. 6. Ensure that each drive is secured with both thumbscrews.

Event code	Event text	Details and solution
		- Run the element-to-element test specifying the same elements and media that caused the event. - Run the slot-to-slot test.
2074	The library startup failed due to a GPIO error	Power cycle the library.
2075	The library startup failed due to an error when trying to open the robotics serial port	Verify that the library is running the latest firmware version. If not, update the library firmware.
2076	I2C bus signals invalid	- Remove all tape drives from the affected chassis and then power on the library. If the problem persists, the cause is likely to be in the chassis. - Power off the library. - Reinstall the drive and power on the library. - If the problem persists, the cause could be in the drive. If possible, try a different drive in the drive slot and then try the suspect drive in a different slot to see which part is causing the problem. - If the problem appears to be with the tape drive, use the RMI to pull a drive support ticket and check the device analysis. L&TT must be installed to view a support ticket. For more information, see Diagnosing problems with Library & Tape Tools.
2079	Could not upgrade barcode reader firmware	- Power cycle the library. - If the error persists, see if the event log shows events related to the spooling mechanism or robotic assembly. - If the error event persists, view the event log for additional events or event detail that provide more specific information.

Event code	Event text	Details and solution
2080	Cartridge lost while inserting it into slot/drive	A data or cleaning cartridge came loose from the robotic assembly while the cartridge was being inserted into a magazine slot or tape drive. 1. Retrieve the cartridge from inside the library. It is likely on top of the robotic assembly or on the bottom of the library. 2. Inspect the source and destination elements and ensure that there are no obstructions in the pathway of the robotic assembly, including at the bottom of the library. 3. Inspect the cartridge for signs of physical damage, and if so, discard it from the media pool.
2082	Drive with Secure Mode enabled has been hot removed while in active status as LUN master	An LTO-6 tape drive with FIPS Secure Mode enabled must be powered off before removing it from the library. The library disables Secure Mode in the tape drive during the power off process so the drive can be moved to a different library. 1. Reinsert the tape drive into the same position in the same library from which it was removed. 2. Power off the drive from the Configuration > Drive screen in the RMI. The drive can now be safely removed.
2087	Error accessing the backplane flash memory	Power cycle the library.
2093	Communication to Robotic Controller could not be established	This event is generated during startup when the communication to the robotics controller could not be established and has failed. 1. Power off the library. 2. Power on the library. 3. If the error event persists, replace the library controller.
2094	An emergency stop condition was detected and prevented	This event is generated when an emergency stop condition occurred during inventory scan.

Event code	Event text	Details and solution
	ted the robotic from running the inventory scan	1. Ensure that all magazines are inserted and properly locked. 2. Insert all open magazines before powering on the library. 3. Ensure that the library is powered on.
2095	Inventory scan failed because of robotic positioning problem	1. Power off the library and then look inside the library for any obstruction to the robotic assembly. a. Remove all magazines and ensure that all tapes are pushed fully into their slots. b. Clear any obstructions from the bottom of the library. c. Clear any loose tape cartridge from the elevator. Verify that all tape cartridges have high-quality proper barcode labels and that the labels are properly applied. d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. 2. Power on the library. 3. If the error event persists, check the event log for additional events or event details that provide more specific information. 4. If the issue is corrected, continue with the next debugging step or return the library to its normal operation and clear the event codes. 5. If the error event persists, replace the library controller.

Event code	Event text	Details and solution
2096	Initializing a communication interface on the library controller failed	Power cycle the library. If the error persists, replace the library controller.
2097	Mechanical re-initialization in context of Robotics error recovery has failed	1. Verify that the library is running the latest firmware version. 2. If the error event persists, power off the library and then look inside the library for any obstruction to the robotic assembly. a. Remove all magazines and ensure that all tapes are pushed fully into their slots. b. Clear any obstructions from the bottom of the library. c. Remove any loose tape cartridges from the elevator. d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. 3. Power on the library. 4. If the error event persists, power off the library, and verify that the library is level within the rack. Power on the library. 5. If the error event persists, view the event log for additional events or event details that provide more specific information. 6. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes.

Event code	Event text	Details and solution
		If the error event reoccurs, replace the library controller.
2100	Position to element command failed because of robotic problem	- Power off the library. Confirm that the shipping lock is removed. - Power on the library. - If the error event persists, power off the library and then look inside the library for any obstruction to the robotic assembly. - Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridges from the elevator. - Inspect the tape drives for a loose, uncontrolled, or stuck tape cartridge. - Power on the library. - If the error event persists, power off the library, and verify that the library is level within the rack. Power on the library. - If the error event persists, check the event log for additional events or event details that provide more specific information. - If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. - If the error event reoccurs, replace the library controller.

Event code	Event text	Details and solution
2105	Access or initialization failed due to horizontal positioning problem	1. Power off the library. Confirm that the shipping lock is removed. . 2. Power on the library. 3. If the error event persists, power off the library and then look inside the library for any obstruction to the robotic assembly. a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. b. Clear any obstructions from the bottom of the library. c. Clear any loose tape cartridge from the elevator. d. Inspect the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. 4. Power on the library. 5. If the error event persists, power off the library, and verify that the library is level within the rack. 6. Power on the library. 7. If the error event persists, view the event log for additional events or event details that provide more specific information. 8. If the issue is corrected, continue with the next debugging step or return the library to its normal operation and clear the event codes.

Event code	Event text	Details and solution
		9. If the error event reoccurs, replace the library controller.
2106	An elevator block was detected and as a result the system was taken offline	- Power off the library and then look inside the library for any obstruction to the robotic assembly. - Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. - Clear any obstructions from the bottom of the library. - Clear any loose tape cartridge from the elevator. - Inspect the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. - Power on the library. - If the error event persists, power off the library, and verify that the library is level within the rack. - Power on the library. - If the error event persists, view the event log for additional events or event details that provide more specific information. - If the issue is corrected, continue with the next debugging step or return the library to its normal operation and clear the event codes. - If the error event reoccurs, replace the library controller.

Warning events

Event code	Message and description	Details and solution
4000	A reported drive sled fan speed is too slow	Ensure that there are no obstructions to the drive fans.
4002	A drive sent a clean request	1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem persists with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem persists with both tape cartridges, the drive may be faulty or multiple cartridges may be defective. Review the event logs for drive and tape cartridge interactions that occurred at the same time. Run a drive assessment test using L&TT. Then, use the RMI to pull a drive support ticket, and view the ticket using L&TT. Check the details analysis section for more information. If you have access to another known good drive, use that drive to test the suspect tape cartridge. Based on the information contained in the drive support ticket and the results gathered using the known good drive, determine

Event code	Message and description	Details and solution
		ine whether multiple tape cartridges are faulty or if the drive is faulty. 5. If you have not already done so, consider setting up auto clean in each library partition. For more information about auto cleaning, see Configuring auto cleaning. Make sure that at least one unexpired cleaning cartridge is physically located in each partition.
4003	The drive configuration failed	1. Power off the library. Remove and then re install the tape drive to ensure that the drive is fully seated. Power on the library. Retry the operation. 2. If the drive installed is a different LTO generation than the drive previously installed , reset the list of known drives from Configuration > System in the RMI. 3. Use the RMI to pull a drive support ticket and then view the ticket using L&TT. Check the details analysis section for more information.
4004	The drive status request failed	1. Power off the library. Remove and then re install the tape drive to ensure that the drive is fully seated. Power on the library. Retry the operation. 2. If the problem persists, reset the drive from Configuration > Drives in the RMI. 3. Use the RMI to pull a drive support ticket and check the device analysis section for more information. Use L&TT to view the support ticket.
4005	Drive is reporting a critical TapeAlert	1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the prob

Event code	Message and description	Details and solution
		lem persists, clean the drive again using a n unexpired cleaning cartridge. Retry the operation with a different tape cartridge i n the same drive. 3. If the problem persists with the original ta pe cartridge, but not with the different ta pe cartridge, remove the original cartridg e from use. 4. If the problem persists with both tape car tridges, the drive may be faulty or multipl e cartridges may be defective. Review the event logs for drive and tape cartridge in teractions that occurred at the same time. Run a drive assessment test using L&TT. Then, use the RMI to pull a drive support ticket and view the ticket using L&TT. Che ck the details analysis section for more in formation. If you have access to another known g ood drive, use that drive to test the suspe ct tape cartridge. Based on the information contained in th e drive support ticket and the results gat hered using the know good drive, determ ine whether multiple tape cartridges are faulty or if the drive is faulty.
4006	A drive temperature reported is above the th reshold	1. Verify that the drive fan is spinning and n ot obstructed. 2. Verify that the ambient temperature is wi thin specifications. 3. Verify that the drive cover plates are insta lled in all open drive bays. The drive cove r plates are required for proper airflow wit hin the library.
4007	Cartridge error	1. Clean the drive using an unexpired clean ing cartridge. Power cycle the drive. Rem

Event code	Message and description	Details and solution
		ove the tape cartridge and inspect it for damage. If damaged, remove the cartridge from use. - Assuming the original cartridge is not damaged, retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. - If the problem persists with the original tape cartridge, but not with the different tape cartridge, remove the original cartridge from use. - If the problem persists with both tape cartridges, the drive may be faulty or multiple cartridges may be defective. Review the event logs for drive and tape cartridge interactions that occurred at the same time. Run a drive assessment test using L&TT. Then, use the RMI to pull a drive support ticket and view the ticket using L&TT. Check the details analysis section for more information. If you have access to another known good drive, use that drive to test the suspect tape cartridge. Based on the information contained in the drive support ticket and the results gathered using the known good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.
4008	Cleaning cartridge expired	Discard the cleaning cartridge and retry the cleaning operation with a new unexpired cleaning cartridge.
4010	Drive is not compatible with this library	Power off the library.

Event code	Message and description	Details and solution
		2. Remove the incompatible drive. 3. Install a compatible drive. Only install drives that are supported by the library. 4. Power on the library.
4012	Move cartridge operation failed due to drive or media issue	1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem persists with the original tape cartridge, but not with the different tape cartridge, remove the original cartridge from use. 4. If the problem persists with both tape cartridges, the drive may be faulty or multiple cartridges may be defective. Review the event logs for drive and tape cartridge interactions that occurred at the same time. Run a drive assessment using L&TT. Use the RMI to pull a drive support ticket, and then view the ticket using L&TT. Use L&TT to view the support ticket. Check the device analysis section for more information. If you have access to another known good drive, use that drive to test the suspect tape cartridge. Based on the information contained in the drive support ticket and the results gathered using the known good drive, determine

Event code	Message and description	Details and solution
		rmine whether multiple tape cartridges are faulty or if the drive is faulty.
4014	Library test failed due to a drive issue	1. Verify the test parameters and then retry the test. 2. View the library event log for events associated with this drive. 3. Use the RMI to pull a drive support ticket and check the device analysis section for more information. Use L&TT to view the support ticket.
4016	Backup configuration data to base module failed	1. If possible, save the library configuration to a file. 2. Power cycle the library and retry the operation.
4017	Restore configuration data from chassis failed	1. If possible, save the library configuration to a file. 2. Power cycle the library and retry the operation.
4018	Firmware upgrade failed, tape drive reported an error applying the firmware file	1. Verify that the firmware file is correct for the drive.
4019	General drive firmware bundle upgrade failure	2. Ensure that the drive is in a healthy state and does not have a cartridge. 3. Retry the operation. 4. Power cycle the library and retry the operation.
4020	Database has been reset due to a problem that prevented the library from powering up	Restore previously saved configuration data. If you do not have a saved configuration file, reconfigure the library.
4021	Drive has been hot removed while in active status as data transfer device	Drives must be powered off before removing them from the library. 1. Power off the library.

Event code	Message and description	Details and solution
		- Reinstall the removed tape drive in the same position from which it was removed. - Power on the library.
4025	Library test failed due to a cartridge error	- Remove the cartridge and inspect it for damage. - Retry the operation with another cartridge.
4028	Drive cannot use this media due to it being an unknown or unsupported format. Possibly the media is the wrong generation of media	- Verify that the LTO generation on the barcode label media ID matches the LTO generation of the data cartridge. - Remove cartridges that are incompatible with the drives in the library.
4029	Incompatible media move operation blocked by media barcode ID check	Verify that the LTO generation on the media barcode label matches the LTO generation of the data cartridge. Replace the label if it is incorrect, or remove the incompatible cartridge from the library.
4030	Move cartridge operation failed due to media error	- Power cycle the drive. Remove the tape cartridge and inspect it for damage. If damaged, remove the cartridge from use. Make sure that the destination drive does not already have a tape cartridge loaded. If the drive has a tape cartridge loaded, make sure that the backup application is finished using the drive, then see the Details and solution recommendation under event code 2061. - Assuming the original cartridge is not damaged, retry the operation with the same drive and tape cartridge combination. If the problem persists, retry the operation with a different tape cartridge in the same drive. - If the problem persists with the original tape cartridge, but not with the different ta

Event code	Message and description	Details and solution
		pe cartridge, remove the original cartridge from use. If the problem persists with both tape cartridges, the drive may be faulty or multiple cartridges may be defective. Review the event logs for drive and tape cartridge interactions that occurred at the same time. Run a drive assessment test using L&TT. Then, use the RMI to pull a drive support ticket. You can view the ticket using L&TT. Check the details analysis section for more information. If you have access to another known good drive, use that drive to test the suspect tape cartridge. Based on the information contained in the drive support ticket and the results gathered using the known good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.
4033	Unsupported key generation (keygen) policy	- Check the network connection and ESKM server configuration for the specified partition. - After ensuring that all partitions have the same KeyGenPolicy, rerun the Expert Partitioning wizard for the specified partition. - From the Status > Security screen, verify that all drives and partitions are configured correctly for encryption. Example ESKM server KeyGenPolicy for a three-partition library: - SER1020633_LL01 KT - SER1020633_LL02 KT - SER1020633_LL03 KT

Event code	Message and description	Details and solution
4037	Loss of redundant datapath	Verify that both FC ports are correctly cabled to the SAN.
4038	The drive configuration failed because of unsupported ADPF features selected	Advanced path failover, ADPF and ACPF, are only supported on LTO-6 tape drives. - If the drive is an LTO-6 drive, verify that it is running the latest firmware version and that all drives in the partition support advanced path failover. To update the drive configuration, run the Advanced Partition Wizard. - If the drive is not an LTO-6 drive, either remove it from the partition or disable advanced path failover for the partition. Run the Advanced Partition Wizard to update the partition and drive configuration.
4039	The drive configuration failed because of unsupported ACPF features selected	Use the Partition Wizard to update the partition and drive configuration.
4040	Data path failover occurred	This event applies to Advanced Control Path Failover. Data path failover occurred (the active data path switched from the active port to the failover path). Inspect the cabling and all network components between the affected drive and host computer.
4043	Control path failover occurred	This event applies to Advanced Control Path Failover. The active control path switched from the active path to the failover path. If the failover was unplanned or unexpected, verify that the host still sees both the active and passive drives. If necessary, reconfigure a different passive drive for the partition. Inspect the cabling and all network components between the affected drive and host computer.
4044	One of the library tests failed because a source element or destination element is currently not accessible	The library either could not find the source cartridge or the destination element was unexpectedly full. This error can happen if a cartridge

Event code	Message and description	Details and solution
		dge in the destination element has an unreadable barcode label. 1. See the event details to find the source and destination elements. 2. Open the magazine and inspect the source and destination drives or slots. 3. Unless the library is configured not to use barcode labels, verify that all cartridges have a high-quality barcode label.
4046	The drive configuration failed because of missing DPF license	Disable data path failover or install the DPF license.
4047	The drive configuration failed because of missing CPF license	Disable control path failover or install the CPF license.
4051	A new encryption key could not be created because media is loaded in one or more drives	Unload the media from all drives and then retry the manual key creation again.
4052	A new encryption key could not be created because media is loaded in one or more drives	Unload the media from all drives and then automatic key generation will occur during the next scheduled time frame, or generate a new key server token key manually.
4060	Connection to the KMIP server failed	1. Verify the user name and password configured to log in to the Key Management Interoperability Protocol (KMIP) server. 2. Verify that all necessary SSL certificates have been configured. 3. Verify that the KMIP server is reachable within the network. 4. Verify that the configured IP addresses and/or host names are correct.
4061	Key not found on KMIP server	Verify that the requested key is available on the KMIP server. Review the KMIP server logs for additional details.
4062	Key creation on KMIP server failed	Review the KMIP server logs for additional details.

Event code	Message and description	Details and solution
4063	KMIP configuration invalid	Use the KMIP configuration wizard to verify the KMIP configuration.
4064	KMIP feature not licensed	Disable the KMIP feature or install the necessary license.
4065	A tape alert event was reported by a drive	1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem persists with the original tape cartridge, but not with the different tape cartridge, remove the original cartridge from use. 4. If the problem persists with both tape cartridges, the drive may be faulty or multiple cartridges may be defective. Review the event logs for drive and tape cartridge interactions that occurred at the same time. Run a drive assessment test using L&TT. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information. If you have access to another known good drive, use that drive to test the suspect tape cartridge. Based on the information contained in the drive support ticket and the results gathered using the known good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.

Event code	Message and description	Details and solution
		Verify that the ambient temperature and humidity meet the specifications for the specific drive generations installed.
4066	Automatic control path failover failed because disabling LUN drive failed, partition may be disconnected from host	Inspect cabling and all network components between the affected drive and host computer.
4067	Cleaning cartridge will soon be expired and should be replaced	Replace the cleaning cartridge.
4072	No cleaning cartridge in partition available for auto cleaning	When initiating a cleaning operation, the library will use an unexpired cleaning cartridge from the same partition as the tape drive. If the partition does not contain an unexpired cleaning cartridge, the library will use an unexpired cleaning cartridge from an unpartitioned area of the library. The library will not use a cleaning cartridge from a different partition. When enabling auto cleaning, ensure that either each partition has an unexpired cleaning cartridge or place at least one unexpired cleaning cartridge in an area that is not assigned to a partition. The cleaning cartridge label must begin with the letters "CLN" for the library to recognize it as a cleaning cartridge. - Verify that a properly labeled unexpired cleaning cartridge is available in the same partitions as the drives requesting cleaning or in an unpartitioned area of the library. - Perform a load and unload on any drives that need cleaning to initiate autocleaning.
4073	Medium source element empty	Visually inspect the source slot and then rescan inventory.
4074	Medium source element empty	- Verify that the cartridge has a valid and readable barcode label. - Rescan the inventory from the backup application.

Event code	Message and description	Details and solution
4075	Cartridge lost while extracting it from slot/drive	1. Inspect the source element and ensure that there are no obstructions in the pathway of the robot. 2. Rescan the inventory from the backup application.
4076	Secure Manager feature not licensed	Disable Secure Manager or install the necessary Secure Manager license.
4077	Unlocking the right magazine failed	1. Verify that all magazines are fully inserted in the library.
4078	Unlocking the left magazine failed	2. Power cycle the library and then retry the operation.
4079	Unlocking the mailslot failed	3. If the problem persists, power off the library and then release the magazine manually. 4. Check for obstructions or damage near the magazines.
4080	Wellness test failed with warning	1. Check for additional events that might provide an indication of the reason for the failure. 2. Verify that the library meets the requirements of the test. 3. Retry the wellness test. 4. Run the system test and then check for events with additional information. 5. Verify that media is loaded in the library.
4081	Library test failed with warning	1. Verify that the test requirements are met. 2. Review the Event Logs for any other error. 3. Verify that the firmware is up to date. 4. Retry the test operation.

Event code	Message and description	Details and solution
4084	Failed reading logged in hosts table	1. Verify that the drive is powered on and is communicating with the library. 2. Verify that the drive is running a firmware version that is supported with the library firmware version. 3. If this error persists, disable Secure Manager for the entire library and then re-enable Secure Manager.
4085	Too many retries of drive command needed because of Unit Attention or Not Ready condition	1. Check for additional events that might provide an indication of the reason for the failure. 2. Inspect the data cartridge in the drive for damage and wear. 3. Wait for drive operation to complete and then retry the command.
4086	Move operation failed due to inability to access the internal library database	1. Verify that the network the library is connected to is not experiencing abnormal loads, such as packet storms or excessive polling. 2. Verify that the library is running the latest firmware version. 3. Power cycle the library.
4087	Key server token is over 90% full	Obtain a new key server token and seed it with the keys needed for current use. See the encryption kit user guide for instructions.
4093	Could not obtain an IP address from DHCP server	1. In the RMI, select Status > Network to check the network configuration settings. 2. Verify that the DHCP server is reachable from the library. 3. Trigger an automatic reconfiguration of the network interface by changing the network configuration in the RMI, select Configuration > Network or unplugging the

Event code	Message and description	Details and solution
		e network cable and then plugging it in after a few seconds.  NOTE If this warning displays and you are not using DHCP for your environment, disregard the message.
4094	Drive interface I/O error	Reboot the library to reinitialize the hardware and device drivers.
4095	Library test failed due to load of an incompatible medium	1. Review the cartridge requirements for the test and then ensure that sufficient cartridges are available in the required locations to run the test. 2. Rerun the test.
4098	System time synchronization through SNTP failed	1. Verify that the SNTP server address is valid. In the RMI, select Configuration > System > Date and Time Format. 2. Ensure that the SNTP server is reachable from the library network and not blocked by a firewall.
4099	An unexpected reset of robotics has been detected	Verify that the spooling cable is fully seated in the base module and correctly connected to the robotic assembly.
4101	The drive configuration failed. FIPS Secure Mode is not supported	1. Replace the drive with an LTO-6 or later generation drive or disable FIPS Secure Mode for this partition. 2. If the drive is an LTO-6 or later generation drive, update the drive firmware to the latest version.
4102	The drive configuration failed due to an error during FIPS Secure Mode specific operation	Retry the operation. If the problem persists, verify that the drive is running the latest released firmware version and that the FIPS Support Mode settings on the partition are correct.

Event code	Message and description	Details and solution
4103	The drive configuration failed during disabling FIPS Secure Mode for tape drive	An LTO-6 drive with Secure Mode enabled in a library was removed without first powering off the drive. For additional information and instructions, see Disabling Secure Mode for an LTO-6 tape drive .
4105	Drive configuration failed during enabling FIPS Secure Mode for tape drive	An LTO-6 drive with Secure Mode enabled in a library was removed without first powering off the drive. For additional information and instructions, see Disabling Secure Mode for an LTO-6 tape drive .
4106	The drive configuration failed while enabling FIPS Secure Mode for tape drive	Rerun the FIPS Secure Mode wizard to generate certificates or disable FIPS Support Mode.
4108	Partition has FIPS Support Mode disabled, but a drive in the partition is running FIPS Secure Mode-enabled firmware	To correct this configuration mismatch, either enable FIPS Support Mode for the specified partition or install the FIPS Secure Mode-disabled firmware variant on the LTO-7 or later tape drive.
 NOTE The drive is online and functional, encryption keys will continue to be provided in the correct encrypted format, and the drive status reports FIPS Secure Mode enabled.		
4109	Partition has FIPS Support Mode enabled, but a drive in the partition is running FIPS Secure Mode-disabled firmware	To correct this configuration mismatch, either disable FIPS Support Mode for the specified partition or install the FIPS Secure Mode-enabled firmware variant on the LTO-7 or later tape drive.
 NOTE The drive primary ports are offline and the drive status reports FIPS not supported.		
4111	Drive firmware upgrade failed because the specified image is not FIPS Secure Mode enabled	This event indicates that an attempt was made to load FIPS Secure Mode-disabled firmware.

Event code	Message and description	Details and solution
		e into an LTO-7 or later drive in a partition that has FIPS Support Mode enabled. To correct this configuration mismatch, either disable FIPS Support Mode for the specified partition or install the FIPS Secure Mode-enabled firmware variant on the LTO-7 or later tape drive.
4112	Move cartridge failed due to cartridge not seating properly	1. Look for other events related to drive problems. 2. Retry the operation with the same source and destination combination. If the problem persists, retry the operation with a different cartridge in the same drive. 3. If the problem follows the cartridge, inspect the cartridge for physical damage and remove it from the media pool. 4. If the problem follows the drive, use the library RMI to pull a drive support ticket and review the analysis section for additional information. L&TT must be installed to view the support ticket.
4113	Move cartridge operation failed due to cartridge not properly taken over from drive	Inspect the cartridge for labels or physical damage that would prevent it from being removed easily from the slot or drive.
4115	Internal software error	1. Check for a newer firmware version and upgrade. 2. If error persists, reboot the library (this resets the memory and may clear any memory related issues).
4120	No empty drive available for system test	1. Verify all tape drives are empty. 2. Shut down any ISV applications accessing the library. 3. If needed, manually move tapes from the drive(s) to empty slots using the RMI.

Event code	Message and description	Details and solution
4121	No compatible media available for system test	Verify that the library has properly labeled media that is compatible with the drives installed in the library.
4122	No cartridge available for slot to slot test	Verify that the library has tape media installed.
4123	No empty slot available for slot to slot test	Verify that the library has at least one empty tape slot. Remove one or more tapes if necessary.
4124	Drive or media statistics could not be retrieved when unloading the tape	1. Review the event log for additional events that provide more specific information. 2. If media-related tape alert events are reported, replace the media.
4125	Potential conflict: Tape drive has been accessed by multiple initiators	1. View the list of host WWNN addresses listed in the event text. • If only one host can have access the tape drive, ensure that the other hosts are not allowed to access the tape drive. • If multiple hosts will access the tape drive, disable multi-initiator SCSI detection for the partition with the drive. 2. Close the event and continue normal use of the tape drive.
4127	Drive re-configuration caused by sled reset	1. Reboot the affected drive using the RMI (select Maintenance > Drives > Drive Reboot), then retry the operation. 2. If the error persists, reset the affected drive. a. Power off the library. b. Loosening the thumbscrews of the affected drive. c. Pull the drive partially out of the library and then fully reinsert the drive.

Event code	Message and description	Details and solution
		d. Retighten the thumbscrews as described in the tape drive installation section of the User Guide. e. Power on the library and retry the operation. 3. If possible, move the drive sled to a different slot within the library or to a different library, if the issue follows the drive sled, replace the drive. If possible, using a different drive in the same slot and the issue remains with the chassis, replace the chassis.
4129	Media removal prevented by drive	Check the backup application for how to allow media removal from drive. If unsuccessful, select Operations > Force Drive Media Eject in the RMI.
4130	Wellness test failed because drive not finally initialized	Wait until drive initialization has completed and run the test again.
4138	USB overcurrent detected. As a result the USB port has been disabled	Make sure that the USB device is correctly inserted and that it does not consume more current than specified in manual.
4140	Personality mismatch detected	1. Update the library and drive firmware to the latest version. 2. If the issue persists, replace either the chassis or library controller to ensure all parts in the stack are matching the personality of the main library controller.
4141	Drive requires cleaning	1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive.

Event code	Message and description	Details and solution
		- If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. - If the problem reoccurs with both tape cartridges, the drive may be faulty or multiple cartridges may be defective. Review the event logs for drive and tape cartridge interactions that occurred at the same time. Run a drive assessment test using L&TT. Use the RMI to pull a drive support ticket, and use L&TT to view the support ticket. Check the device analysis section for more information. If a second known good drive is available, check the suspect tape cartridges in this drive. Based on the information contained in the drive support ticket and the results gathered using the known good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty. - If you have not already done so, consider setting up auto clean in each library partition. For more information about auto cleaning, see Configuring Auto Cleaning. Make sure that at least one unexpired cleaning cartridge is physically located in each partition.
4143	Magazine has been removed for more than 15 minutes	The library is offline when a magazine is removed. Reinstall the magazine to move the library online.
4145	Verify that the MSL Encryption Kit token containing the requested key is inserted and logged in	Verify that the MSL Encryption Kit token containing the requested key is inserted and logged in.
4146	LTO7 formatted cartridge with a Type M barcode detected	Replace cartridge barcode label by correct version.

Event code	Message and description	Details and solution
4147	Type M cartridge without a Type M barcode detected	Replace cartridge barcode label by correct version.
4151	Download of drive firmware image completed, but firmware revision did not change after reboot	- Solution 1: Verify that the uploaded firmware image matches your drive type and generation. Ensure that the image file is not corrupted. Download a new image from the drive vendor web site if you are not sure about file integrity. - Solution 2: Power cycle the library, then update the drive firmware.
4152	The selected port on the target machine is not open, the connection is refused	Verify that the server application is running on the target machine and the firewall is not blocking the selected port. Contact your IT personnel to verify the port settings.
4153	The authentication on server side fails, because the client certificate cannot be trusted	Use a client certificate, which is signed by a trusted Certification Authority (CA) or manually select the untrusted certificate on server side and trust it (not available on all servers).
4154	The target machine could not be reached, no network connection possible	Verify the following: - The IP address in the settings is correct. - The target machine is powered and connected to the network. - The network cable. - The Firewall setting on the target machine allows ping requests and responses.
4155	The target machine could not be reached, the network route to the machine is not available	Verify the following: - The IP settings (IP Address, Gateway, and Netmask) and confirm them with your IT personnel. - The Firewall settings on the target machine are correct.

Event code	Message and description	Details and solution
4156	The TLS connection could not be established because of Handshake errors during certificate exchange	Verify the following: • The certificates on server and client side for valid entries and that they are still valid and not expired. • That TLS1.2 is enabled on the server. Check the client and server date/time for current time. • Request new and valid certificates from your IT personnel.
4157	The server certificate is unknown, because the root certificate is missing or not trusted	Run a new certificate request with your server or certificate authority and import the resulting certificate chain.
4158	The host name on the network could not be found. It does not exist or is misspelled	Verify that the entered host name is correct. Verify the DNS address in the network settings. Contact your IT personnel for the verification of the entered data.
4159	The TLS server certificate could not be verified as a valid and trusted certificate	Determine if your server root certificate has changed. Create a new certificate request against your server to generate a new client certificate based on the changed server certificates.
4163	Drive sled discovery timeout, status of drive sleds not available in time	Ensure that the network is not experiencing broadcast storms or other abnormal activity. Reboot or power cycle the system for re-initialization. Power cycle the library.
4164	Inventory has been updated due to an unexpected empty or full slot	If a move fails due to an unexpected empty or full slot, the slot is re-scanned and the inventory is corrected. Power cycle the library.
4174	KMIP CA certificate failure. The CA certificate could not be verified as a valid and trusted certificate	The CA certificate could not be verified as a valid and trusted certificate. • Verify that the correct CA certificate was used. • Verify that the CA certificate on the encryption server is current.

Event code	Message and description	Details and solution
4176	Failed to send CVTL ticket	The tape library is unable to send support tickets to the CVTL server. Check the CVTL configuration of the library. Verify that the CVTL server is online and accessible on the network.
4193	Autocleaning has failed	1. Move a cleaning cartridge into the drive where autoclean has failed. If the cleaning process fails again, review tape alert flags or events for further failure analysis 2. If the event persists, replace the cleaning cartridge.

Configuration change events

Event code	Message and description
8000	The configuration of a drive changed.
8001	The drive was added or removed from the system.
8002	A partition was added/removed or changed.
8003	A mailslot bank was enabled/disabled.
8004	Drive firmware changed due to firmware upgrade.
8005	The configuration of hostname/domain name has changed.
8006	The email configuration settings have been changed.
8007	The configuration of a date/time format changed.
8009	The timezone configuration has changed.
8011	The network settings have changed.
8013	The NTP time synchronization configuration has changed.

Event code Message and description

8014	The SSH access was enabled/disabled.
8015	Level of media generation checking has changed. LTO generation media checking has been enabled or disabled by the user.
8016	Library reset default settings invoked by user. The library settings have been reset to their default values.
8017	Library firmware changed. The firmware process was initiated by a user.
8018	The Unlabeled Media Support configuration has changed.
8019	Robotics firmware version upgraded.
8020	A new key was created automatically. A new security token key was created through the Encryption Kit automatic key generation mode.
8021	Secure Manager status changed.
8022	RMI/OCP Timeout configuration changed.
8024	Mailslot / Magazine access control configuration changed.
8026	Robotics assembly change detected. The robotics assembly has been replaced.
8029	The SNMP configuration changed.
8030	An SNMP target has been added.
8031	An SNMP target has been deleted.
8032	The SNMPv3 settings changed.
8034	Manual drive reset executed. A drive reboot was requested through the RMI or by the library. This process could cause side effects if done while the library is operating.
8040	LDAP server has been added.
8041	LDAP server has been modified.
8042	LDAP server has been deleted.
8043	LDAP user has been added.
8044	LDAP user has been modified.
8045	LDAP user has been deleted.

Event code Message and description

8046	Logout prevention configuration changed.
8047	FIPS Secure Mode configuration changed.
8056	Command View TL configuration changed.
8057	New hardware component added to the library.
8058	Hardware component removed from the library.
8059	A hardware component of the library has been replaced.
8061	New Base Library Controller detected.
8062	Auto calibration successfully finished.
8064	Password rules configuration changed.
8065	User has been added.
8066	User has been deleted.
8067	Persistent reservations have been removed.
8068	Remote Logging configuration changed.
8069	User password has been changed.
8070	Default encryption mode for new partitions has been changed.
8071	The administrator permission for configuring encryption has been changed.
8103	Two-factor authentication has been enabled for user.
8104	Two-factor authentication has been disabled for user.

Informational events

Event code Message

9000	A tape alert flag was reported by a drive.
------	--

Event code	Message
9001	A drive is present in the system but powered off.
9002	The library was powered on.
9003	A move media command was executed.
9004	Inventory scan was performed.
9005	The library was powered down from the front panel.
9006	The network interface was switched on.
9007	The network interface switched off.
9008	The system time was synchronized with an NTP server.
9009	A magazine was unlocked and opened.
9010	A magazine was closed and locked.
9011	A mailslot bank was unlocked and opened.
9012	A mailslot bank was closed and locked.
9013	A user logged in to the RMI interface.
9014	A user logged out of the RMI interface.
9015	A user logged in to the OCP interface.
9016	A user logged out of the OCP interface.
9017	MSL Encryption Kit password has changed.
9018	MSL Encryption Kit password has been requested.
9019	MSL Encryption Kit key has been created.
9020	MSL Encryption Kit password has been set.
9021	MSL Encryption Kit token has been initialized.
9022	MSL Encryption Kit backup has been done. The encryption keys on the key server token have been saved to a key server token backup file.
9023	MSL Encryption Kit restore has been done. The encryption keys have been restored to the key server token from a key server token backup file.

Event code	Message
9024	Drive support ticket created.
9025	Library test started.
9026	Library test successfully finished.
9027	Library test stopped by user.
9028	Configuration backup to base module was successful.
9029	Configuration restore operation from base module was successful.
9031	Library health status changed to status "OK".
9032	Library health status changed to status "Warning".
9033	Library health status changed to status "Critical".
9035	New library chassis detected.
9038	The library was rebooted through the user interface.
9039	Token key creation attempt failed due to media being loaded in one or more drives.
9040	Control path switched over from active to passive drive. This event code is used when the user initiates the failover from the RMI.
9041	Key on KMIP server created.
9043	Drive cleaning was started. There will not be an additional event generated when cleaning successfully finishes. If there was an error, one or more warning events will be generated.
9047	MSL Encryption Kit backup has been initiated
9048	MSL Encryption Kit restore has been initiated.
9049	MSL Encryption Kit partial backup has been initiated.
9050	More than five invalid MSL Encryption Kit PIN attempts.
9051	MSL Encryption Kit key server token contains keys that have not been backed up.
9052	MSL Encryption Kit key server token is full. Adding or generation new keys is prohibited.
9053	MSL Encryption Kit key provided.
9055	MSL Encryption Kit key server token not present.

Event code	Message
9056	MSL Encryption Kit key server token was inserted.
9057	MSL Encryption Kit key server token was removed.
9060	One or multiple configured DNS servers are not responding.
9061	A user account has been locked due to too many invalid login attempts on RMI.
9062	Invalid password used for login.
9064	Backup of certificate created.
9065	Certificate has been restored.
9067	LTO7 formatted cartridge with a Type M barcode detected.
9068	Type M cartridge without a Type M barcode detected.
9071	MSL Encryption Kit has been password set automatically.
9078	Unexpected drive reset occurred.
9079	Media initialization needed.
9085	A user was logged out of the RMI interface due to a timeout.
9086	A user has been logged out of the RMI interface by another user.
9087	A user was logged out of the OCP interface due to a timeout.
9088	A user has been logged out of the OCP interface by another user.

Diagnosing problems with Library & Tape Tools

About this task

With Library & Tape Tools installed on the host server you can:

- Identify all SAS and FC devices connected to your system.
- View detailed configuration, identification, inventory, and drive information for the device.
- Easily update device and drive firmware.

- Run advanced diagnostic tests, including connectivity, read/write, media validation, and testing the functionality of the device.
- View device and drive error logs.
- Generate a detailed support ticket that can be e-mailed or faxed to your support representative for analysis.

The Library & Tape Tools diagnostic provides an intuitive graphical user interface with integrated context-sensitive help. Hewlett Packard Enterprise updates L&TT periodically with new diagnostic features and device support. When using L&TT for troubleshooting, download and update to the current version. You can verify that you are using the latest version and download L&TT without cost from the L&TT website: <https://www.hpe.com/support/TapeTools>.

Procedure

1. Run L&TT on the host server.

You can install L&TT on the host server, or run it from a CD-ROM or USB flash drive on the host server.

2. Pull a support ticket for the device.
3. Look at the device analysis results for additional information about the device operation.

Electrostatic discharge

To prevent damaging the system, be aware of and follow precautions when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Subtopics

Preventing electrostatic damage
Grounding methods

Preventing electrostatic damage

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.

- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly. See the next section.

Grounding methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm (± 10 percent) resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have your Hewlett Packard Enterprise authorized reseller install the part.



NOTE

For more information on static electricity, or assistance with product installation, contact your Hewlett Packard Enterprise authorized reseller.

Technical specifications

Library capacity

Characteristic	MSL2024 G4
Form factor	2U
Maximum cartridge slots	24
Mailslots	0, 3
Maximum half-height tape drives	2

Supported interfaces

LTO generation	Interface
LTO-6, LTO-7, LTO-8, LTO-9	Fibre Channel, SAS

Subtopics

- [Physical specifications](#)
- [Environmental specifications](#)
- [Electrical specifications](#)
- [Regulatory specifications](#)
- [Regulatory compliance identification numbers](#)
- [Default and restore defaults settings](#)

Physical specifications

MSL2024 G4 physical specifications: all models

Characteristics	Product alone (without drives or media)	Packaged (Shipped)
Approximate height	87 mm (3.43 in)	275 mm (10.83 in)
Approximate width	482 mm (19.98 in)	590 mm (23.32 in)
Approximate depth	809 mm (31.85 in)	990 mm (38.98 in)
Approximate weight	12 kg (26.4 lb)	21.5 kg (47.3 lb)

Environmental specifications

Characteristic	Specification		
	LTO-9	LTO-7 and LTO-8	LTO-6
Temperature			

Characteristic	Specification		
	LTO-9	LTO-7 and LTO-8	LTO-6
Operating (Recommended)	15°C to 25°C	20°C to 25°C	
Operating (Allowable)	15°C to 32°C. Derate 1°C / 300m above 900m.	10°C to 35°C up to 3000m and 10°C to 30°C above 3000m and up to 4000m.	10° to 35°C
Non-operating	-30° to 60° C	-30° to 60° C	-30° to 60° C
Maximum rate of change	5° C per hour	10° C per hour	10° C per hour
Humidity			
Operating (Recommended)	20% to 50% RH (non-condensing)	20% to 50% RH (non-condensing)	
Operating (Allowable)	20% to 80% RH (non-condensing, 22°C dew point maximum)	20% to 80% RH (non-condensing, max wet bulb temperature = 26°C)	20% to 80% RH (non-condensing, max wet bulb temperature = 26°C)
Non-operating	10% to 90% RH (non-condensing)	10% to 90% RH (non-condensing)	10% to 95% RH (non-condensing)
Miscellaneous			
Altitude	3048 meters	4000 meters (see Operating temperatures)	4000 meters
Dust concentration	ISO 14644-1 Class 8	ISO 14644 -1 Class 8	Less than 200 microgram / cubic meter

Electrical specifications

Power—MSL2024 G4: 168 Watts (max)

Input Requirements—MSL2024 G4: 100 - 240V AC, 3.7A maximum, 50/60Hz

USB port—USB 2.0

Ethernet port—10BASE-T, 100BASE-TX, 1000BASE-T are supported

Regulatory specifications

Product safety test conditions

Characteristic	Tested condition or value
Equipment mobility	Stationary (rack-mount or desk-top)
Connection to the mains	Pluggable — Type A
Operating condition	Continuous
Access location	Operator accessible
Over voltage category (OVC)	OVC II
Mains supply tolerance (%) or absolute mains supply values	-10%, +10%
Tested for IT power systems	No
IT testing, phase-phase voltage (V)	N/A
Class of equipment	Class I
Considered current rating (A)	20 A (branch circuit protection)
Pollution degree (PD)	PD 2
IP protection class	IPX0
Altitude during operation (m)	Max 5000
Altitude of test laboratory (m)	38
Mass of equipment (kg)	Max 25 kg
Manufacturer's Declared Ambient (°C)	40 °C



NOTE

The product safety test conditions might differ from the product specification limits.

Regulatory compliance identification numbers

For the purpose of regulatory compliance certifications and identification, each product is assigned a unique regulatory model number. The regulatory model number can be found on the product nameplate label, along with all required approval markings and information. When requesting compliance information for the product, always see this regulatory model number. The regulatory model number is not the marketing name or model number of the product.

The Regulatory Compliance label is on the bottom of the library. To view this information from the back of the library, tilt the library up until the label is visible.

Product-specific information:

Regulatory model number: LVLDC-0501, Type: 2U

FCC and CISPR classification: Class A

These products contain laser components. See Class 1 laser statement in Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at [https://www.hpe.com/support/](https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)

Safety-Compliance-EnterpriseProducts

Manufacturer: Hewlett Packard Enterprise Company, 1701 E Mossy Oaks Road, Spring, TX 77389 U.S.

Manufacturer's representative: ZAO Hewlett-Packard A.O.

Default and restore defaults settings

You can save the configuration settings to a file, restore the settings, or reset the configuration to the default settings. Use the RMI to view or change settings. The following table lists the configuration parameters, with their default settings and whether they are reset to default or saved to a file.

Parameter	Default setting	Reset by Set Defaults	Stored in Saved Config file
Tape drive settings			
FC drive configuration	Automatic speed, auto port type	Yes	Yes
Drive power	Drive powered on	Yes	Yes
Auto clean	Disabled	Yes	
Slots			
Active slots	Maximum possible	Yes	
Reserved slots	0	Yes	Yes

Parameter	Default setting	Reset by Set Defaults	Stored in Saved Config file
Mailslot configuration	Mailslot disabled	Yes	Yes
Administrator password required for mailslot removal	Enabled	Yes	Yes
Barcode reader settings			
Barcode reader label length	8	Yes	Yes
Barcode reader alignment	Left	Yes	Yes
Ignore barcode Media ID	Disabled	Yes	Yes
Error and event settings			
Event log levels and filter	Continuous trace and all levels and filters active (for HPE Service only)	Yes	Yes
Error recovery	On	Yes	
E-mail notification	Disabled	Yes, but configurations retained	Yes
Administrator password	Unset	No	Yes
Network settings		No. The network is always enabled and the network addresses are retained.	Yes, including DHCP, DNS, IPv4, and IPv6 addresses
HTTPS	Disabled	Yes	Yes
SNMP	Disabled, but saved addresses do not change	Yes, but saved addresses do not change	Yes
Restricted network access	Enabled	Yes	Yes
Miscellaneous settings			

Parameter	Default setting	Reset by Set Defaults	Stored in Saved Config file
Date and time	Blank or existing	No	
Encryption and security settings	Disabled	Not applicable	Yes
License Keys	None	No	Yes

Websites

General websites

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

<https://www.hpe.com/storage/spock>

Technical papers and analyst reports

<https://www.hpe.com/us/en/resource-library>

For additional websites, see [Support and other resources](#).

Subtopics

[Accessing the compatibility matrix](#)

[HPE Storage library websites](#)

Accessing the compatibility matrix

Procedure

1. Go to <https://www.hpe.com/Storage/TapeCompatibilityMatrix>.
2. On the **Welcome to SPOCK** page, click **Sign in/Register**.
3. Log in with your existing HPE account or create an account.
4. From the SPOCK home page, expand the plus sign (+) next to **Explore HPE Storage Tape Solutions**.
5. Click **HPE Storage Tape Solutions Documents**, and then select the compatibility matrix.

HPE Storage library websites

For more information on Storage products, see <https://www.hpe.com/storage/msl>.

For product information about Command View for Tape Libraries, see <https://www.hpe.com/storage/cvtl>.

To download Command View for Tape Libraries, see <https://www.hpe.com/support/cvtl>.

For more information about TapeAssure Advanced, see <https://www.hpe.com/storage/tapeassure>.

For more information about Data Verification, see <https://www.hpe.com/storage/dataverification>.

Download HPE Library & Tape Tools without charge from <https://www.hpe.com/support/TapeTools>.

Support and other resources

Subtopics

[Accessing Hewlett Packard Enterprise Support](#)

[HPE product registration](#)

[Accessing updates](#)

[Remote support](#)

[Warranty information](#)

[Regulatory information](#)

[Documentation feedback](#)

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

<https://www.hpe.com/info/assistance>

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

<https://www.hpe.com/support/hpesc>

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see <https://www.hpe.com/info/add-products-contracts>.

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

Hewlett Packard Enterprise Support Center

<https://www.hpe.com/support/hpesc>

My HPE Software Center

<https://www.hpe.com/software/hpesoftwarecenter>

- To subscribe to eNewsletters and alerts:

<https://www.hpe.com/support/e-updates>

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

<https://www.hpe.com/support/AccessToSupportMaterials>



IMPORTANT

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Account set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

<https://www.hpe.com/services/getconnected>

HPE Tech Care Service

<https://www.hpe.com/services/techcare>

HPE Complete Care Service

<https://www.hpe.com/services/completecure>

Warranty information

To view the warranty information for your product, see the [warranty check tool](#).

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

<https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

<https://www.hpe.com/info/reach>

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

<https://www.hpe.com/info/ecodata>

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

<https://www.hpe.com/info/environment>

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, click the **Feedback** button on the page of an opened document on the Hewlett Packard Enterprise Support Center portal (<https://www.hpe.com/support/hpesc>). Use this feature to send any errors, suggestions, or comments. This process captures all document information.