



Hewlett Packard
Enterprise

HPE StoreEver MSL6480 Tape Library User and Service Guide

Abstract

This guide provides information on installing, configuring, upgrading, and troubleshooting the library. This guide is intended for system administrators and other users who need physical and functional knowledge of the library.

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent 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 vendor's standard commercial license.

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

Acknowledgments

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation 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.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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



Contents

Overview.....	9
Front panel	9
Back panel	10
Tape drive back panels.....	11
LTO-5 and LTO-6 Fibre Channel tape drive back panels.....	11
LTO-5 and LTO-6 SAS tape drive back panel.....	11
LTO-7 and LTO-8 FC tape drive back panel.....	12
LTO-7 and LTO-8 SAS tape drive back panel.....	12
Power supply LEDs.....	13
USB ports.....	13
Element numbering.....	13
Encryption.....	14
HPE StoreEver 1/8 G2 Tape Autoloader and MSL Tape Libraries Encryption Kit	15
Integration with an ESKM or KMIP key manager.....	16
Data cartridges.....	16
LTO-7 Type M media for LTO-8 drives.....	16
Guidelines for using and maintaining data cartridges.....	17
Recommended practices for labeling tape cartridges.....	17
Write-protecting data cartridges.....	18
Read and write compatibility.....	19
Supported media.....	20
HPE StoreEver Management Software.....	21
Path failover features.....	22
Secure Manager.....	23
Installing the library.....	25
Planning the installation.....	25
Preinstallation checklist.....	25
Location requirements.....	26
Module and rack layout guidelines.....	27
FC connection information.....	27
SAS connection information.....	28
Library partition guidelines.....	29
Network configuration information.....	30
Preparing the host.....	30
Unpacking the shipping containers.....	31
Installing the rack rails	31
Installing the base module in the rack.....	34
Preparing the top and bottom modules.....	35
Installing the expansion modules in the rack.....	37
Aligning and connecting modules.....	38
Installing tape drives.....	40
Connecting the Fibre Channel cables.....	41
Connecting the SAS cable.....	41
Connecting cables for Data Verification.....	42
Powering on the library.....	42
Initiating the configuration wizard.....	43



Verifying the host connections.....	44
Labeling tape cartridges.....	44
Loading the tape cartridges	45
Verifying the installation.....	46
Downloading product firmware.....	47
Configuring additional features.....	47

Operating the library..... 49

Library user interfaces.....	49
Logging in to the library.....	50
Library users.....	51
The library RMI main screen.....	51
Configuring the library.....	54
Configuring the simplest configuration.....	54
Using the Initial Configuration Wizard.....	56
Managing the library configuration.....	56
Managing the library date and time.....	58
Configuring media barcode compatibility checking.....	60
Using unlabeled media.....	61
Managing license keys.....	61
Configuring the system language.....	61
Configuring the RMI timeout.....	61
Configuring the library network settings.....	62
Using the Configuration > Network Management screen.....	62
Configuring remote logging.....	65
Configuring event notification parameters.....	66
Configuring HPE Systems Insight Manager for the library.....	67
Configuring HPE SIM for manual discovery.....	67
Configuring tape drives.....	67
Enabling or disabling mailslots.....	69
Partition wizards.....	69
Configuring the encryption key manager type.....	75
MSL Encryption Kit configuration.....	75
ESKM Wizard prerequisites.....	79
Using the ESKM Wizard.....	79
Using the KMIP wizard.....	80
Configuring FIPS Support Mode.....	82
Secure Mode.....	83
Disabling Secure Mode for an LTO-6 tape drive.....	83
Disabling Secure Mode for an LTO-7 or later tape drive.....	84
Configuring local user accounts.....	84
Enabling OCP/RMI session locking.....	86
Configuring LDAP user accounts.....	86
Configuring Command View for Tape Libraries integration.....	88
Enabling Data Verification.....	89
Preparing the library for Data Verification	89
Enabling secure communications.....	90
Adding a signed certificate for SSL/TLS connections.....	90
Configuring Secure Manager.....	91
Maintaining the library.....	95
Performing the system test.....	95
Performing the slot to slot test.....	96
Performing the element to element test.....	96
Performing the position test.....	97



Performing the wellness test.....	97
Performing the robotic test.....	98
Testing and calibrating the OCP.....	98
Viewing log files.....	99
Downloading log and trace files.....	99
Managing library firmware.....	99
Managing drive firmware from the RMI.....	100
Downloading a tape drive support ticket.....	101
Downloading a library support ticket.....	101
Rebooting the library.....	102
Rebooting a tape drive.....	102
Controlling the UID LED.....	102
Moving the robotic assembly to the base module.....	102
Calibrating the library.....	102
Operating the library.....	103
Moving media.....	103
Opening the mailslot	103
Opening a magazine	104
Cleaning a tape drive.....	105
Rescanning the cartridge inventory.....	106
Forcing a drive to eject a cartridge.....	106
Viewing status information.....	107
Viewing library and module status.....	107
Viewing library or partition configuration settings.....	110
Viewing drive status.....	111
Viewing network status.....	113
Command View TL status parameters.....	114
Viewing encryption status.....	115
Viewing Secure Manager status.....	115

Upgrading and servicing the library..... 117

Possible tools needed.....	117
Identifying a failed component	118
Moving a module within the rack or to a nearby rack.....	118
Installing or replacing a tape drive.....	119
Removing a tape drive.....	119
Removing a drive bay cover.....	120
Installing the new tape drive.....	121
Verifying the tape drive installation.....	121
Adding an expansion module.....	121
Powering off the library.....	122
Installing the rails in the rack.....	122
Moving a cover to the new module.....	123
Installing the module.....	123
Verifying the installation and configuration.....	123
Replacing a power supply.....	124
Preparing to remove the power supply.....	124
Removing the power supply	124
Installing the new power supply.....	125
Verifying the power supply installation and operation.....	125
Replacing a controller board.....	126
Saving the configuration.....	127
Powering off the library.....	127
Preparing to remove the controller board.....	127



Removing the base or expansion module controller.....	127
Installing the base or expansion module controller	128
Verifying the module controller replacement	129
Powering on the library.....	130
Replacing the chassis fan assembly.....	130
Removing the chassis fan assembly.....	130
Installing the new chassis fan assembly.....	131
Verifying the chassis fan assembly installation.....	131
Replacing a drive power board.....	132
Preparing to remove the drive power board.....	132
Removing the chassis fan assembly and drive power boards	132
Installing the new drive power board.....	133
Verifying the drive power board installation.....	134
Replacing a magazine.....	135
Unlocking the magazine.....	135
Removing the tape cartridges.....	138
Removing the magazine.....	139
Installing the magazine.....	140
Verifying the magazine installation and operation.....	140
Replacing a module.....	140
Powering off the library.....	142
Removing the data cartridges.....	142
Removing the module cables	143
Removing the tape drives	143
Removing the empty module from the rack	143
Moving library cover plates.....	144
Installing the replacement module into the rack	145
Replacing the module components and cables.....	147
Verifying the library configuration.....	148
Replacing the robotic assembly and spooling mechanism.....	148
Powering off the library.....	148
Preparing to remove the robotic assembly and spooling mechanism from the base module.....	149
Removing the robotic assembly and spooling mechanism from the base module.....	150
Installing the robotic assembly and spooling mechanism into the base module.....	152
Completing the robotic assembly and spooling mechanism installation.....	154
Verifying the installation.....	155
Replacing the front bezel or OCP.....	155
Removing the bezel.....	155
Installing the bezel.....	156
Powering on the library.....	157
Replacing magazine access doors.....	157
Removing the magazine access doors.....	157
Installing the magazine access doors.....	157

Troubleshooting tools, procedures, and information..... 159

Library tests.....	159
Library & Tape Tools.....	159
Diagnosing problems with Library & Tape Tools.....	160
L&TT support tickets.....	160
Generating an L&TT support ticket or report from L&TT	161
Downloading a support ticket from the library.....	161
Viewing a support ticket with L&TT.....	162
Finding event information.....	162
Fibre Channel connection problems.....	162



Detection problems after installing a SAS drive.....	163
Operation problems.....	164
The library does not power on.....	166
No messages on the OCP.....	167
The LCD displays a warning or error icon.....	167
The LCD displays an error code.....	167
Cartridge stuck in drive.....	167
Cartridge stuck in storage slot.....	168
Cartridge incompatible with drive.....	169
Cannot read or write to data cartridge.....	169
The library reports an obstruction in a storage slot or does not see a data cartridge.....	170
The attention and cleaning LEDs are illuminated.....	170
A particular cartridge sets off the cleaning light.....	171
A cartridge recently imported from a different environment is causing issues.....	171
The attention LED is illuminated but the cleaning LED is not illuminated after a cartridge load.....	171
The cleaning LED is illuminated after using a cleaning cartridge.....	171
A particular cartridge sets off the attention LED and possibly the cleaning LED.....	172
The library displays incorrect barcodes.....	172
Cannot connect to the RMI.....	172
Cannot load a cleaning cartridge.....	173
Performance problems.....	173
Average file size.....	174
File storage system	174
Connection from the backup server to the disk array.....	174
Backup/archive server.....	174
Backup/archive software and method.....	174
Connection from the archive/backup host server to the library.....	175
Data cartridges.....	175
Tape drive read or write performance seems slow.....	175
Magazines.....	176
Unlocking a magazine using the OCP or RMI.....	176
Opening a magazine using the manual release.....	177
Locking or unlocking the robotic assembly manually.....	177
Returning the robotic assembly to the base module.....	178
Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is near the base module or is stopped directly between two modules.....	179
Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is not near the base module or it cannot move vertically.....	180
Clearing obstructions from the library.....	181

Library shipping procedures..... 183

Shipping a library in a rack with the original packaging.....	184
Shipping a library that was field-installed in a square-hole rack.....	189
Shipping a module outside of a rack.....	192

Event codes..... 195

Error events.....	195
Warning events.....	219
Configuration change events.....	237
Informational events.....	240

Technical specifications..... 243



Physical specifications.....	243
Environmental specifications.....	243
Electrical specifications.....	244
Regulatory specifications.....	244
Regulatory compliance identification numbers.....	245
Default and restore defaults settings.....	246
Electrostatic discharge.....	249
Preventing electrostatic damage.....	249
Grounding methods.....	249
Websites.....	250
HPE StoreEver library websites.....	250
Support and other resources.....	251
Accessing Hewlett Packard Enterprise Support.....	251
Accessing updates.....	251
Remote support.....	252
Warranty information.....	252
Regulatory information.....	252
Documentation feedback.....	253



Overview



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the library.

Read all documentation and procedures before installing or operating the library.

Hazardous moving parts exist inside this product. Do not insert any tools or any part of your body into the tape library while it is operating.



WARNING: Install the library in a computer rack and verify that the front and rear doors are secure before operating the tape library.

The library provides a compact, high-capacity, low-cost solution for simple, unattended data backup. This unique design houses up to 80 data cartridges for each 6U of height, with easy access to data cartridges via removable mailslots and fully extendable magazines. Library capacity can be increased with 6U expansion modules and additional tape drives. Supported tape drives can be transferred from other Hewlett Packard Enterprise MSL tape libraries.

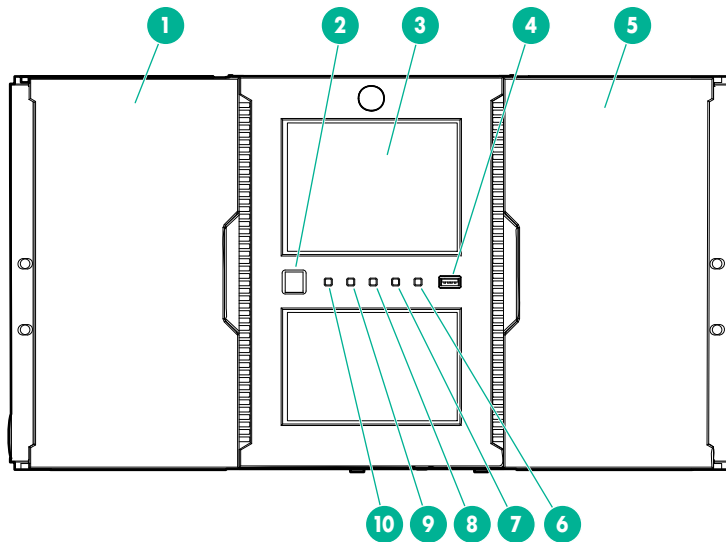
Operating system compatibility

The library is compatible with most operating systems. For full-featured support, the library requires either direct support from the operating system or a compatible backup application to take advantage of its many features. To verify compatibility, see the compatibility matrix at: <https://www.hpe.com/storage/StoreEverSupportMatrix>

Partitioning the library

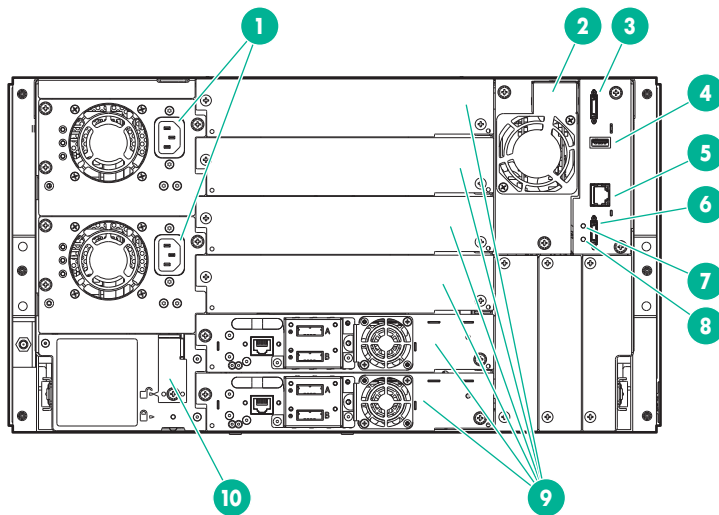
A library with multiple tape drives can be configured into partitions. Each partition is configured independently, allowing use by different backup applications and with different backup policies. For example, one partition could perform a backup operation for one department, while the second partition restores data for another department. Data cartridges in one partition cannot be shared with other partitions.

Front panel



1. Magazine access door
2. Power button
3. LCD touch screen
4. USB port
5. Mailslot, magazine access door
6. Error LED, amber
7. Attention LED, amber
8. Clean LED, amber
9. Ready LED, green
10. Unit Identification (UID) LED, blue

Back panel



1. Power supplies
2. Chassis fan
3. Expansion module interconnect port
4. USB port (base module only)
5. Ethernet port (base module only)
6. Expansion module interconnect port
7. Controller health status LED, green. The controller health status LED pulses on and off in approximately one second cycles during normal operation. If the LED is solid green or not illuminated while the library is powered on, the controller is not operating correctly.
8. UID LED, blue

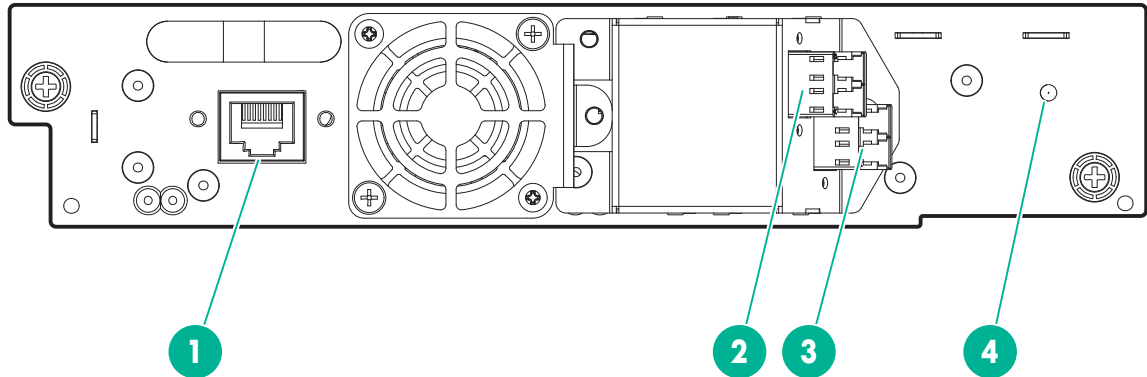


9. Half-height tape drive locations

10. Module alignment mechanism

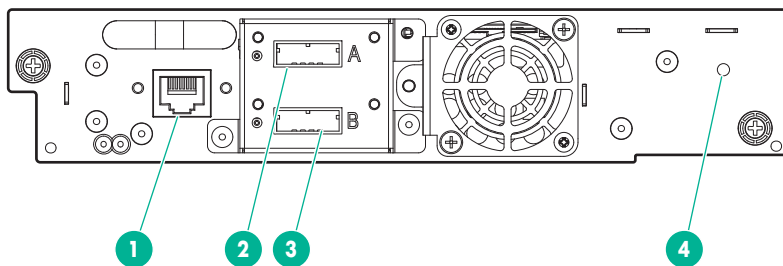
Tape drive back panels

LTO-5 and LTO-6 Fibre Channel tape drive back panels



1. Tape drive Ethernet port
2. FC port A
3. FC port B (LTO-6 only)
4. Tape drive power LED, green

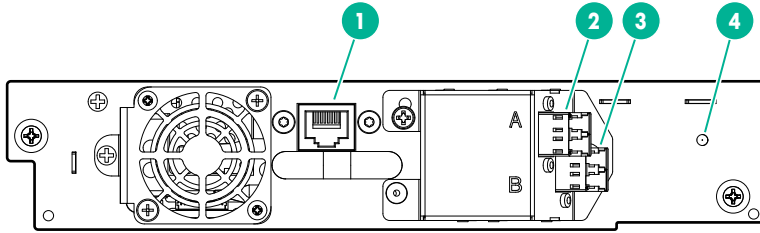
LTO-5 and LTO-6 SAS tape drive back panel



1. Tape drive Ethernet port
2. SAS port A
3. SAS port B (LTO-6 only)
4. Tape drive power LED, green

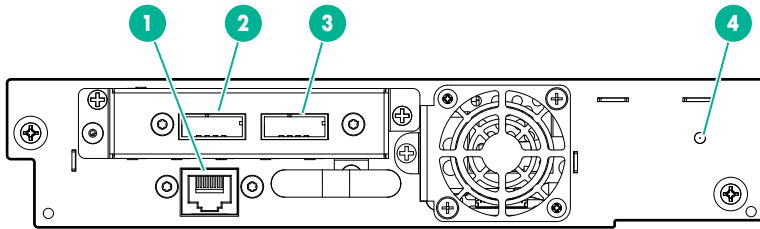


LTO-7 and LTO-8 FC tape drive back panel



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

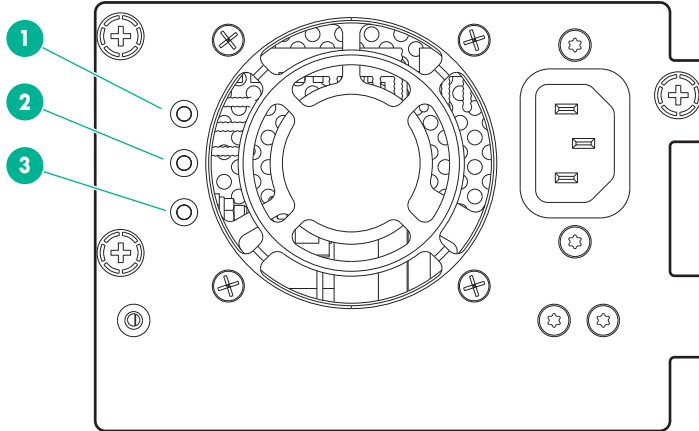
LTO-7 and LTO-8 SAS tape drive back panel



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



Power supply LEDs



1. White	AC power is connected.
2. Amber	The power supply has experienced a fault condition, such as the fan not running, temperature too hot, or producing power that is outside specifications.
3. Green	The power supply is operating correctly.

USB ports

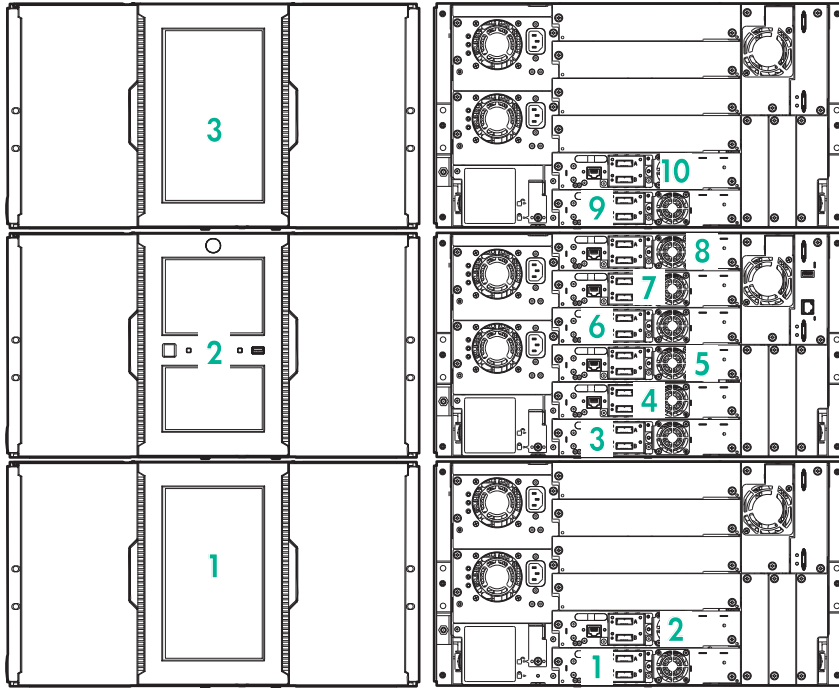
The library has two USB ports — one on the OCP and one on the back panel. You can update firmware, save or restore configuration settings, or download support tickets with a USB thumb drive in either USB port.

The encryption kit token, which is part of the MSL Encryption Kit, is fully functional only when inserted into the back USB port.

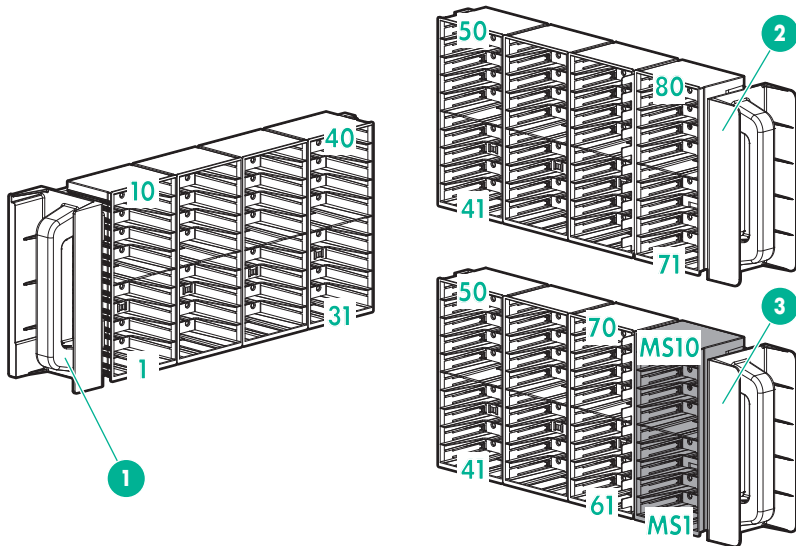
Element numbering

Modules, tape drives, and storage slots are numbered from the bottom of the library up, starting with one.





Storage slots and mailslot elements are numbered as shown.



1. Left magazine

2. Right magazine with the mailslot disabled

3. Right magazine with the mailslot enabled

Encryption

Encryption protects data from unauthorized access and use. The data is changed into a form that can only be read with the key used to encrypt the data.

The LTO-4 and later generation tape drives can encrypt data while writing, and decrypt data when reading. Hardware-based data encryption can be used with or without compression while maintaining the full speed and capacity of the tape drive and media. LTO tape drives use the 256-bit version of the industry-standard AES encrypting algorithm to protect your data.



To use the tape drive hardware-based encryption feature, you need all the following:

- The “HPE 1/8 G2 Tape Autoloader and MSL Tape Libraries Encryption Kit” or a supported key server or a backup application that supports hardware-based data encryption.
- The associated feature license when using an ESKM or KMIP key manager.
- LTO-4 or later generation media. The tape drive will not encrypt data when writing to LTO-3 or earlier generation media.

The tape drives can read encrypted data from and write encrypted data to some earlier generation media. The following table shows backward compatibility for encrypted data.

Table 1: Read and write compatibility for encrypted data

Media	LTO-4 drive	LTO-5 drive	LTO-6 drive	LTO-7 drive	LTO-8 drive
LTO-4 media (encrypted data)	Read/Write with encryption key	Read/Write with encryption key	Read only with encryption key	Incompatible	Incompatible
LTO-5 media (encrypted data)	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Read only with encryption key	Incompatible
LTO-6 media (encrypted data)	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Incompatible
LTO-7 media (encrypted data)	Incompatible	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key
LTO-8 media (encrypted data)	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write with encryption key

Your company policy will determine when to use encryption. For example, encryption might be mandatory for company confidential and financial data, but not for personal data. Company policy will also define how encryption keys are generated and managed. Backup applications that support encryption will generate a key for you.

HPE StoreEver 1/8 G2 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 StoreEver 1/8 G2 Tape Autoloader or MSL2024, MSL3040, MSL4048, MSL6480, MSL8048, and MSL8096 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 will need to 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 in 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 the encryption kit user guide, which is available from the Hewlett Packard Enterprise Information Library at <https://www.hpe.com/info/storage/docs>.



Integration with an ESKM or KMIP key manager

The library supports integration with the ESKM and encryption key management servers using the KMIP standard. These key management servers support sharing encryption keys with different Hewlett Packard Enterprise libraries, which can be in different physical locations.

ESKM is a Hewlett Packard Enterprise encryption key manager for enterprise tape libraries. With ESKM, encryption keys can be shared with other Hewlett Packard Enterprise tape libraries.

The following table lists the licenses required for the ESKM and KMIP features.

Table 2: MSL6480 ESKM and KMIP licenses

Part number	License description
TC469A	HPE StoreEver MSL6480 ESKM Encryption License
TC469AAE	HPE StoreEver MSL6480 ESKM Encryption E-License
D4T76A	HPE StoreEver MSL6480 KMIP 1.2 Key Manager License
D4T76AAE	HPE StoreEver MSL6480 KMIP 1.2 Key Manager E-License

Use the Expert Partition Wizard to configure the use of a key manager. The library supports the use of one key manager type at a time. You can enable the configured key manager independently for each partition.

Data cartridges

LTO-3 and later generation tape drives support both rewritable and WORM data cartridges.

- Rewritable data cartridges are useful when you want to erase or overwrite the existing data, such as making periodic backups or transferring data between libraries in different physical locations.
- WORM data cartridges protect data from accidental or malicious alteration of the data on the cartridge. An application can append data after the existing data to use the full capacity of the data cartridge, but cannot erase or overwrite the data on the cartridge. WORM data cartridges can be identified by their distinctive, two-tone cartridge color.

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

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 revisions 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' bar code label applied, it can be initialized as LTO-7 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' bar code 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>.

Guidelines for using and maintaining data cartridges

⚠ CAUTION: Do not degauss LTO data cartridges! The data cartridges are prerecorded with a magnetic servo signal, which is required to use the cartridges with LTO tape drives. Keep magnetically charged objects away from data cartridges.

To ensure the longest possible life for your data cartridges, follow these guidelines:

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

⚠ CAUTION: Use only Ultrium universal cleaning cartridges.

- 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 the library is 10°C to 35°C. The data cartridge storage temperature range is 16°C to 32°C in a dust-free environment in which relative humidity is between 20% and 80% percent (noncondensing). For archival storage requirements, see the data cartridge 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 for 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, which can render the cartridge unusable.
- Place identification labels only in the designated area on the cartridge.

Recommended practices for labeling tape cartridges

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

💡 TIP: The bar code scanner scans each tape or the back of the storage slot until it reads the bar code label for the cartridge or storage slot, or determines that the slot is empty. The bar code 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 extremely long. Even if you do not need the bar code information, use bar code labels to speed up inventory time.

A proper bar code label includes the Media ID in the last two characters of the bar code. 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.

The host software might track the following information through the associated bar code:

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

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 bar code label. Only apply labels as shown:

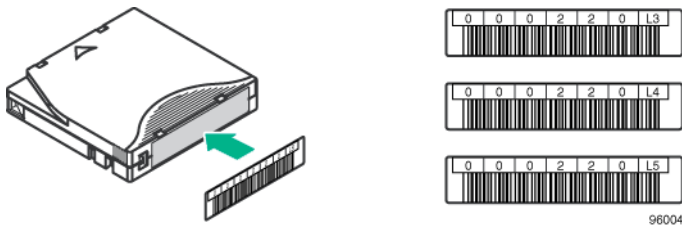


Figure 1: Apply the label within the recessed area.

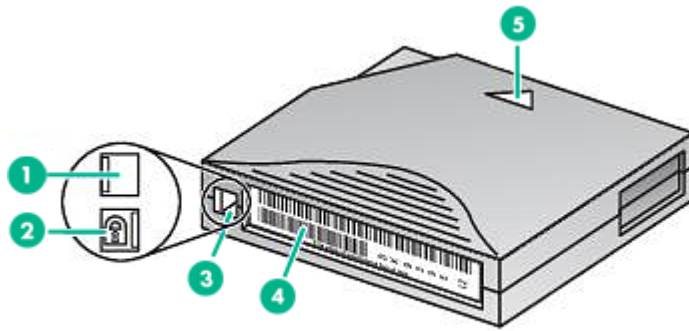
! **IMPORTANT:** Only apply the bar code label as shown, with the alphanumeric portion facing the hub side of the tape cartridge. Never apply multiple labels onto a cartridge because extra labels can cause the cartridge to jam in a tape drive.

Write-protecting data cartridges

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

Procedure

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



10454

1.	Write-protect switch in the unlocked position
2.	Write-protect switch in the locked position
3.	Write-protect switch
4.	Barcode label
5.	Directional arrow. Insert the cartridge into the magazine with the arrow pointing into the storage slot.

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

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-3 drive	LTO-4 drive	LTO-5 drive	LTO-6 drive	LTO-7 drive	LTO-8 drive
LTO-1 media	Read only	Incompatible	Incompatible	Incompatible	Incompatible	Incompatible
LTO-2 media	Read/Write	Read only	Incompatible	Incompatible	Incompatible	Incompatible
LTO-3 media	Read/Write	Read/Write (no encryption)	Read only	Incompatible	Incompatible	Incompatible
LTO-4 media — unencrypted	Incompatible	Read/Write	Read/Write	Read only	Incompatible	Incompatible
LTO-4 media — encrypted	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Read only with encryption key	Incompatible	Incompatible
LTO-5 media — unencrypted	Incompatible	Incompatible	Read/Write	Read/Write	Read only	Incompatible
LTO-5 media — encrypted	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Read only with encryption key	Incompatible
LTO-6 media — unencrypted	Incompatible	Incompatible	Incompatible	Read/Write	Read/Write	Incompatible

Table Continued

	LTO-3 drive	LTO-4 drive	LTO-5 drive	LTO-6 drive	LTO-7 drive	LTO-8 drive
LTO-6 media — encrypted	Incompatible	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Incompatible
LTO-7 media — unencrypted	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write	Read/Write
LTO-7 media — encrypted	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key
LTO-7 Type M media — unencrypted	Incompatible	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write
LTO-7 Type M media — encrypted	Incompatible	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write with encryption key
LTO-8 media — unencrypted	Incompatible	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write
LTO-8 media — encrypted	Incompatible	Incompatible	Incompatible	Incompatible	Incompatible	Read/Write with encryption key

CAUTION: LTO-2 and LTO-3 tape drives require the most recent firmware to identify LTO-4 media immediately. Without the most recent firmware, loading an LTO-4 cartridge into an earlier generation drive can result in a long media identification and unload time. The drive might not identify the media and then return a load error before the application software times out waiting for the load. For proper operation, keep tape drives updated to the most recent firmware.

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/storage/storagemedia>

Cleaning cartridge for all supported tape drives

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

LTO-4 data cartridges

Cartridge type	Part number
HPE LTO-4 Ultrium 1.6TB RW Data Cartridge, green	C7974A
HPE LTO-4 Ultrium 1.6TB WORM Data Cartridge, two-tone (green and gray)	C7974W

LTO-5 data cartridges

Cartridge type	Part number
HPE LTO-5 Ultrium 3 TB RW Data Cartridge, blue	C7975A
HPE LTO-5 Ultrium 3 TB WORM Data Cartridge, two-tone (blue and gray)	C7975W

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

HPE StoreEver Management Software

HPE StoreEver Management Software provides an easy-to-use interface for efficiently managing, monitoring, and configuring an entire tape library environment. The HPE StoreEver Management Software solution is made up of HPE Command View for Tape Libraries (CVTL), HPE StoreEver TapeAssure Advanced and HPE StoreEver Data Verification. CVTL provides the centralized platform for TapeAssure Advanced reporting and Data Verification analysis, CVTL also provides remote management, diagnostics, and configuration for all MSL Tape Libraries from across the room or across the globe. HPE StoreEver TapeAssure Advanced provides the analytics element that implements and presents automated and predictive health, performance, and utilization-related monitoring of all tape drives and cartridges. HPE StoreEver Data Verification Software proactively validates and scans, nondisruptively, the quality of data stored on LTO tape cartridges. This validation ensures that a successful restore is possible when critical business data is needed.

HPE StoreEver TapeAssure Advanced and Data Verification Software can also be tried for free once the CVTL Software has been installed. Download CVTL from <https://www.hpe.com/support/cvctl> and get a 60 day instant-on period to experience TapeAssure Advanced features, and trial Data Verification for the MSL3040 & MSL6480 Tape Libraries with a 10 cartridge-slot license.

For more information about HPE StoreEver Management Software, visit: <https://www.hpe.com/storage/storeevermanagementsoftware>

For information on installing and using CVTL, see the HPE StoreEver Interface Manager and Command View for Tape Libraries user guide, available from the Hewlett Packard Enterprise website at: <https://www.hpe.com/support/cvtl>

Path failover features

The library supports data path failover and control path failover with LTO-5 and later generation tape drives.

- **Data path failover**—Both tape drive ports are connected to the SAN. Only one of the ports is used at any one time and the second port is a standby port. When a link failure on the active port is detected, the second port is used. Data path failover requires a dual-port drive.
- **Control path failover**—Depending on the drive, one or both ports on the control path drive are configured to present a path to the library controller and a second drive is configured as a standby library control path drive.

Path failover implementations

Path failover uses features built into the library and tape drive firmware, and some implementations also use operating system drivers. The library supports three path failover implementations, which are presented in the library user interface as:

- **Basic failover**
 - Is supported with LTO-5 and LTO-6 FC tape drives. Data path failover requires a dual-ported drive.
 - Is supported by a combination of tape drive and library firmware features. Does not require host driver features.
 - Creates a Fibre Channel path to a drive or library when the original path is lost.
 - Most applications recognize the new path and some applications will automatically retry commands after the original path is lost. Some applications might require user intervention to begin using the new path.
 - Requires the LTO-5 and LTO-6 failover licenses.
- **Advanced failover**
 - Is only supported with LTO-6 FC tape drives.
 - Requires host driver features, along with tape drive and library firmware features.
 - Manages multiple paths across multiple SANs, presents a single drive or library path to applications, and transfers commands automatically to the new path if the original path is lost.
 - The transfer to the failover path is invisible to most applications, avoiding the need for user intervention.
 - Requires the LTO-5 and LTO-6 failover licenses.
- **LTO-7+ failover**
 - Is only supported with LTO-7 and later generation FC tape drives.
 - Requires host driver features, along with tape drive and library firmware features.
 - Manages multiple paths across multiple SANs, presents a single drive or library path to applications, and transfers commands automatically to the new path if the original path is lost.
 - The transfer to the failover path is invisible to most applications, avoiding the need for user intervention.
 - Requires the LTO-7+ failover license.

Path failover feature licensing

Failover features are licensed and can only be enabled after the applicable license has been added to the library.

- Separate licenses are available for control path failover and data path failover. Each license enables both basic and advanced path failover.
- A single license supports both control path failover and data path failover.

Path failover licenses

Table 3: Failover licenses for LTO-5 and LTO-6 drives

Part number	License name before June 10, 2014	License name as of June 10, 2014
TC359A	StoreEver MSL6480 Control path failover License	MSL6480 High Availability Control Path Failover License
TC359AAE	StoreEver MSL6480 Control path failover E-License	MSL6480 High Availability Control Path Failover E-License
TC360A	StoreEver MSL6480 Data path failover License	MSL6480 High Availability Data Path Failover License
TC360AAE	StoreEver MSL6480 Data path failover E-License	MSL6480 High Availability Data Path Failover E-License

Table 4: Failover licenses for LTO-7 and later generation drives

Part number	License name
P9H33A	HPE MSL6480 LTO-7+ Path Failover LTU
P9H33AAE	HPE MSL6480 LTO-7+ Path Failover E-LTU

Path failover configuration and status

Control path and data path failover are configured and enabled with the expert partition wizard.

Control path failover is configured independently for each partition. The configuration settings are displayed on the **Status > Partition Map > Configuration Status** screen.

Data path failover is configured for a tape drive. The configuration settings are displayed in the **Status > Drive Status** screen.

Failover documentation

HPE StoreEver Tape Libraries LTO-5 and LTO-6 Failover User Guide and the *HPE StoreEver Tape Libraries LTO-7+ Failover User Guide* on the Hewlett Packard Enterprise website at <https://techlibrary.hpe.com/us/en/storage/info-library/>.

Secure Manager

With Secure Manager, you can configure hosts and drives into access control groups that are managed by the library. With Secure Manager enabled, the drives are not visible to hosts that are logged in to the SAN and so the host will not see the drives by default. For the host to see a drive, the host must be configured into an access control group with the drive.

Secure Manager only supports LTO-4 and later generation FC drives; LTO-3 and SAS drives are not supported. The RMI displays LTO-3 drives, SAS hosts, and SAS drives with gray text. The only Secure Manager function you can perform on the unsupported items is to change the name of a SAS host.

To use Secure Manager, you must understand your FC environment and which hosts to group with which drives. Once Secure Manager is enabled, you will not see drives or libraries from hosts that are outside their group. Without Secure Manager enabled, a host will see a drive as soon as the link is up.

Secure Manager is a licensed feature and can only be enabled after the license has been added to the library.

Table 5: Secure Manager licenses

Part number	Description
D4T75A	HPE StoreEver MSL6480 Secure Manager License
D4T75AAE	HPE StoreEver MSL6480 Secure Manager E-License



Installing the library

**WARNING:**

Each library module weighs 41 kg (90 lb) without media or tape drives and 71.4 kg (157.4 lb) with media (80 cartridges) and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the library:

- Observe local health and safety requirements and guidelines for manual material handling.
 - Remove data cartridges from tape drives before moving a module.
 - Remove all data cartridges from the library to reduce the overall weight of the library and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
 - Obtain adequate assistance to lift and stabilize the library during installation or removal.
-

**WARNING:**

When placing the library into a rack, to reduce the risk of personal injury or damage to equipment:

- Extend the rack 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 may become unstable if more than one component is extended.
-

**CAUTION:**

Slide/rail mounted equipment is not to be used as a shelf or a work space.

Planning the installation

Preinstallation checklist

Procedure

1. **Select a location**
2. **Plan the module and rack layout**
3. **Plan the Fibre Channel configuration** or **Plan the SAS configuration**
4. **Plan library partitions**



Location requirements




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

Table 6: 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	6U for the base library and each expansion module
Operating temperature	10-35° C (50-95° F) for the tape library. Some tape drives have a more limited temperature range when operating at high altitudes. Verify the tape drive operating requirements before installing a tape drive in a high altitude environment.
Power source	AC power voltage: 100-127 VAC; 200-240 VAC Line frequency: 50-60 Hz Place the library near an AC outlet. The AC power cord is the product's main AC disconnect device and must be easily accessible at all times.
Weight without drives or media	41 kg (90 lb)
Weight with drives and media	71.4 kg (157.4 lb)
Air quality	The library should be placed 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-71.04-1985 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants.
Humidity	20-80 percent relative humidity noncondensing
Clearance	As recommended by the rack documentation.

 **TIP:** Temperature and humidity specifications are more tightly controlled for tape media, tape drives, and tape libraries 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.



Module and rack layout guidelines

When possible, install the base module near the middle of the rack at a convenient height for viewing and operating the OCP and accessing the mailslot. If the library will be sharing the rack with other equipment, place heavy devices, such as disk arrays, in the bottom of the rack to reduce the chance of the rack tipping.

The library supports up to three expansion modules above and three modules below the base module, for a total of seven modules. Each module occupies 6U.

For maximum library expansion, install the base module as the centered module of the rack, allowing 18U above the top of the base module and 18U below the bottom of the base module.

Table 7: Rack layout for fully expanded library in a 42U rack

U Volumes	Module
37 — 42	Expansion module
31 — 36	Expansion module
25 — 30	Expansion module
19 — 24	Base module
13 — 18	Expansion module
7 — 12	Expansion module
1 — 6	Expansion module

FC connection information

Connect the FC tape drive directly to the server with an HBA or indirectly through a SAN with an FC switch.

Table 8: FC drive interface speeds

LTO generation	Supported speeds
LTO-3, LTO-4	1 Gb, 2 Gb, 4 Gb
LTO-5, LTO-6, LTO-7, LTO-8	2 Gb, 4 Gb, 8 Gb

Most 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, or 16 Gb FC HBA. A 4 Gb HBA is recommended for LTO-4 tape drives. An 8 Gb or faster HBA is recommended for LTO-5 and later generation tape drives. To verify that an HBA is supported on your server and qualified for the tape drive, see the compatibility matrix at: <https://www.hpe.com/storage/StoreEverSupportMatrix>

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 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-5 HH*	OM3, OM4	0.5 - 300 m	0.5 - 150 m	0.5 - 50 m
All except LTO-5 HH	OM3, OM4	0.5 - 500 m	0.5 - 380 m	0.5 - 150 m

* The LTO-5 Ultrium 3000 half-height drive is shown as **LTO-5 HH**.

SAS connection information

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

Table 9: SAS drive interface speeds

LTO generation	Supported speeds
LTO-4	1.5 Gb, 3 Gb
LTO-5, LTO-6, LTO-7, LTO-8	1.5 Gb, 3 Gb, 6 Gb

The library uses two 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 the StoreEver Support Matrix: <https://www.hpe.com/storage/StoreEverSupportMatrix>

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.

About SAS

SAS is a computer bus technology for transferring data to and from storage devices, including disk drives and tape drives. SAS-1, which is used for LTO-4 tape drives, is designed to transfer data at 3 Gb/s. SAS-2, which is used for LTO-5 and later generation tape drives, is designed to transfer data at 6 Gb/s.



⚠ CAUTION: 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 data rates. Do not use equalized cables with LTO-5 or later generation tape drives unless these cables are verified for 6 Gb/s data rates.
- For optimal performance, only use cables of the length specified as qualified for your products. Do not use a SAS cable longer than 6 meters.

Cable requirements

SAS uses serial connections, with a direct connection between the host server and each of the storage devices. This method eliminates the need to configure SCSI buses and assign SCSI IDs, as is required for parallel SCSI devices.

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.

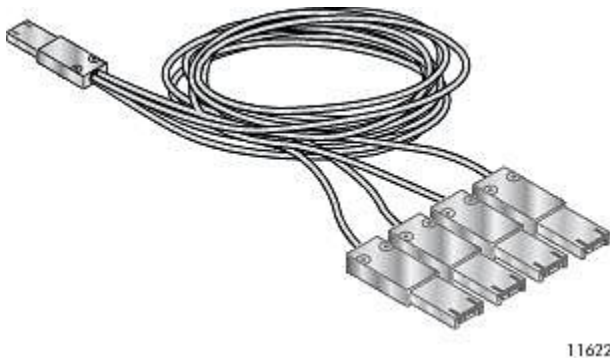


Figure 2: Example SAS fanout cable

Connectors

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

The tape drive has a mini-SAS connector. The 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.

World Wide identifiers

A unique identifier called a World Wide Name (WWN) or World Wide Identifier (WWID) identifies a SAS tape drive. The library assigns the World Wide identifier to the drive bay. When a tape drive is replaced, the World Wide identifier is reassigned to the new tape drive.

The operating system tracks the World Wide identifier for the drive on each HBA channel. Each of the drive connectors on a fanout cable is associated with an HBA channel. Once a drive has been connected, keep it on the same channel to retain the association between the HBA channel and World Wide identifier.

Library partition guidelines

You can partition a tape library with multiple tape drives into logical libraries. Each logical library must contain at least one tape drive. Each logical library is configured independently, allowing use by different backup applications and with



different backup policies. For example, one logical library could perform a backup operation for one department while the second logical library restores data for another department. Data cartridges in one logical library cannot be shared with other logical libraries.

The library partitioning scheme is very flexible. Slots can be assigned in five-slot groups, and the groups do not need to be in contiguous locations. One or more tape drives can be assigned to each logical library and the drives do not need to be contiguous or even installed in the same module. The mailslot on each module can either be assigned to a logical library or shared.

For ease of use and optimal performance, configure the logical libraries as simply as possible, and use the flexibility to adjust logical library capacity as the organization requirements change.

- Assign groups of contiguous slots to each logical library.
- Locate the slots and drives for a logical library near each other, ideally within the same module. If a logical library will span modules, locating the slots and elements as close together as possible will improve performance.

Network configuration information

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. This port can be disabled by the administrator when the library is not being serviced.
80 (TCP)	Bidirectional	Remote management interface (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.

Preparing the host

- !** **IMPORTANT:** Use proper procedures to prevent electrostatic discharge (ESD). Use wrist-grounding straps and anti-static mats when handling internal components.

Procedure

1. Coordinate with the system administrator before powering off the host computer.
2. For a library with SAS drives, install a SAS HBA with an external SAS connector that supports multiple LUNs. Refer to the manuals for the host computer and the HBA for installation information.
3. For a library with FC drives, install an FC HBA or verify that you have sufficient ports available on a compatible Fibre Channel switch.
4. Install application software and compatible drivers on the host computer. For installation and configuration information, see the application software manuals.



Unpacking the shipping containers

Before you begin, clear a level work surface near where you will place the library modules. If you are installing a library with multiple modules and have limited work space, locate and unpack the base module first, along with the rack rails and accessory kits for all of the expansion modules.

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

Procedure

1. Inspect the container for shipping damage. If you notice any damage, report it to the shipping company immediately.
2. Cut the bands on the outside of the container and remove them.
3. Slide the cardboard box up. It is not secured to the pallet.
4. Remove the cardboard sleeve covering the module.
5. Remove the rack rails.
6. Remove the accessory box.
7. Remove the two foam pieces from the top of the module.
8. With assistance, lift the module out of the carton, remove the plastic wrapping from the module, and then place the module on the work surface.
9. Save the packaging for future use.
10. Verify that you received the following components:
 - a. Library module
 - b. Two rack rails
 - c. Accessory package
 - Two packets of rack mounting hardware
 - Expansion interconnect cable (expansion modules only)
 - Two power cords for connecting to a PDU

For Fibre Channel libraries you must provide a cable for each FC tape drive. For SAS libraries, you must provide a SAS cable with the correct connector for your HBA. Hewlett Packard Enterprise recommends using a SAS fanout cable that connects up to four tape drives to the SAS HBA. For ordering information for supported cables, see the MSL QuickSpecs at: <https://www.hpe.com/info/tape>

Installing the rack rails

Library modules install easily into HPE G2 Enterprise Series, Enterprise Series, G2 Advanced Series, Advanced Series, Standard Series, and other HPE square hole or round hole racks.

💡 TIP: When installing a library with multiple modules, starting from the lowest rack location makes it easier to position each set of rails.



Prerequisites

T10 Torx driver

Procedure

1. Note the location for installing the rack rails.

The module requires 6U and the rails are installed in the lower 2U of the module location.

- When installing the module **above** another module or other device in the rack, install the rack rails directly above the device.
- When installing the module **below** another module or other device in the rack, install the rack rails so the bottoms of the rails are 6U below the bottom of the device. The lower hook will be in the middle hole of the lower U volume.

2. When installing the rails in a round-hole rack, install a round-hole adaptor in each of the four locations where the rails will be secured to the vertical supports.

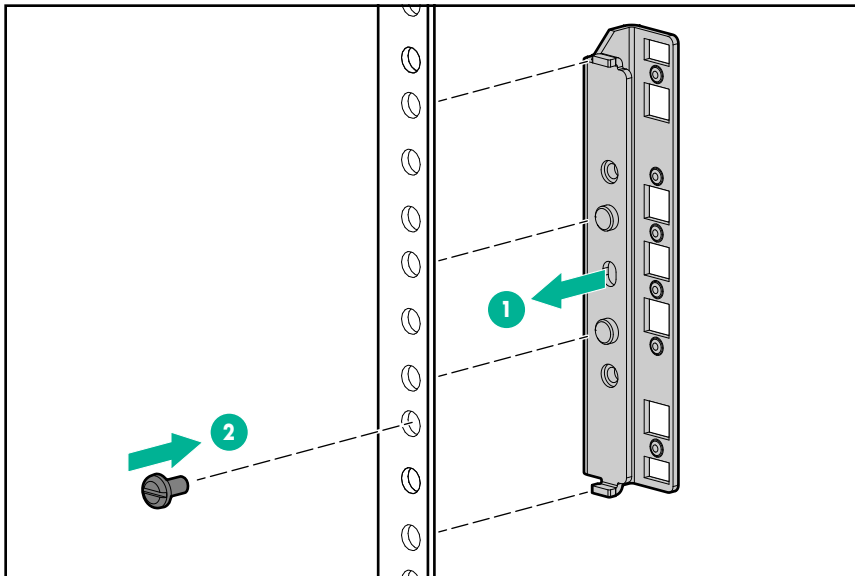
a. Locate the packet labeled **Round-hole rack adapter kit**.

Verify that the packet contains four brackets and eight screws.

b. From the inside of the rack, insert the tabs and pins on one of the brackets into the holes on the vertical support in the location shown.

c. Use two screws to secure the bracket to the vertical support.

d. Repeat steps b and c to install the other brackets.



3. From the front of the rack, insert the rack rails into the back and then front vertical supports.

a. Position a rail according to the left-right front-rear orientation information stamped on the rail.

b. Rotate the front of the rail up while inserting the rear rail hanger into the middle hole of the marked U section in the rear vertical support, and then lower the front of the rail until it is nearly level.

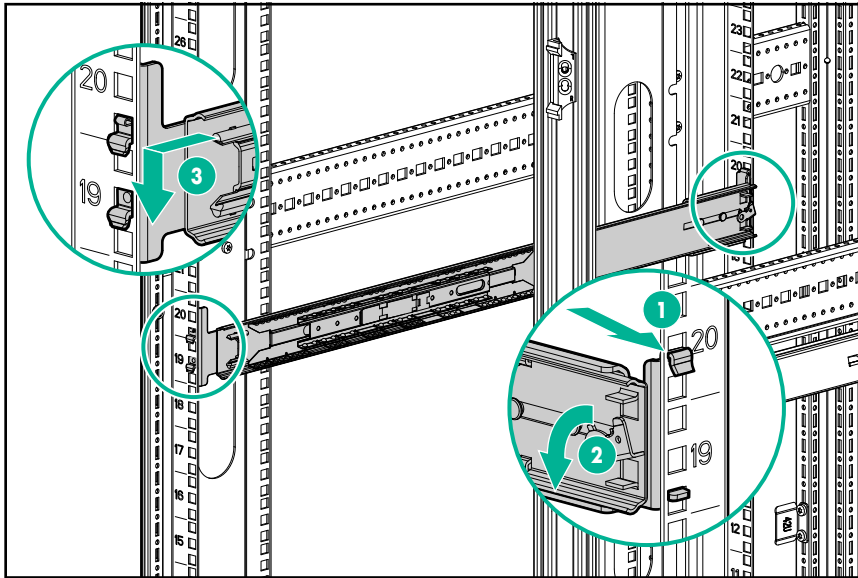
c. Extend the front of the rail until the hangers come through the holes in the vertical support and the retention spring snaps into place. The top hangers of both the front and rear of each rail will be in the same U volume, but in different positions within the U volume.



Verify that the rail is level front to back to confirm that the rail has been installed in the correct holes. If the rail is not level, check the location of the rear of the rails. When properly installed, the top hanger in the rear will be in the middle hole of the marked U section.

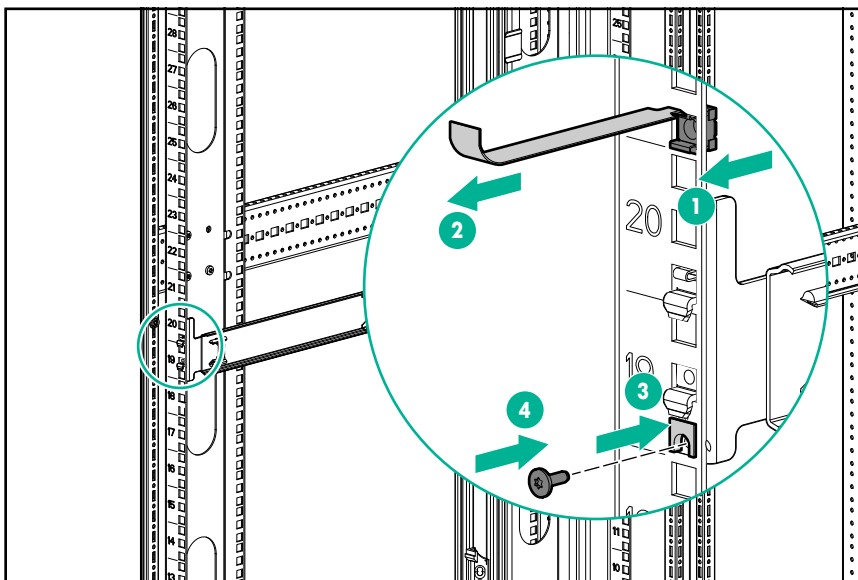
- d. Repeat substeps a, b, and c with the other rail.

NOTE: In these illustrations, the rack rails are installed in the 19 and 20 U locations, which places the module in the center of a 42U rack in U locations 19 through 24. Notice that the top hangers of the front and rear of each rail are in different positions within the U volume.



- 4. On the front of both rails in a square-hole rack, install a clip nut above the mounting bracket. In this illustration, the clip nut is being installed with a clip nut installation tool.

For increased stability, install the retention inserts from the packet labeled **Retention inserts** using a T10 Torx driver.



- 5. If you are installing a library with expansion modules, repeat this procedure to install the rails for all of the modules.



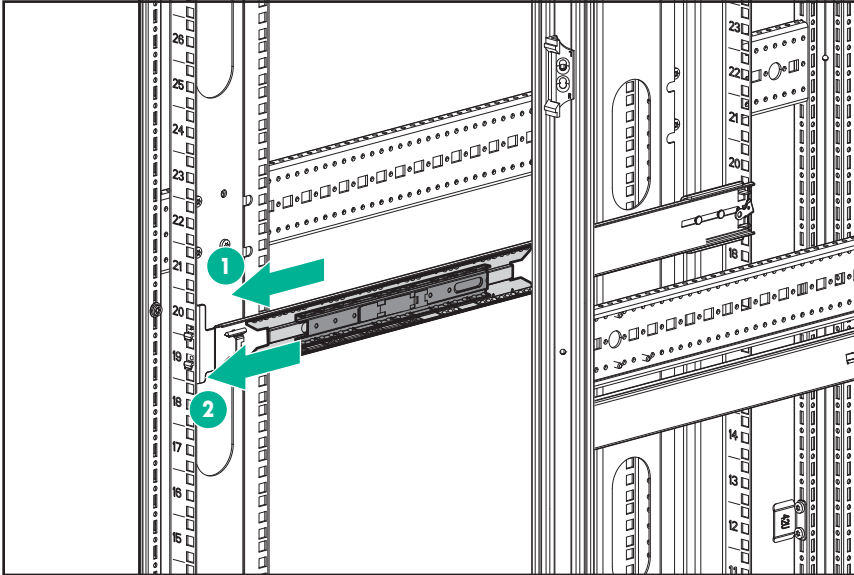
Installing the base module in the rack

The library has a three-part rail system:

- Outer rail is installed in the rack.
- Middle rail connects to the inner and outer rails so the module can be slid out of the rack.
- Inner rail is attached to the module.

Procedure

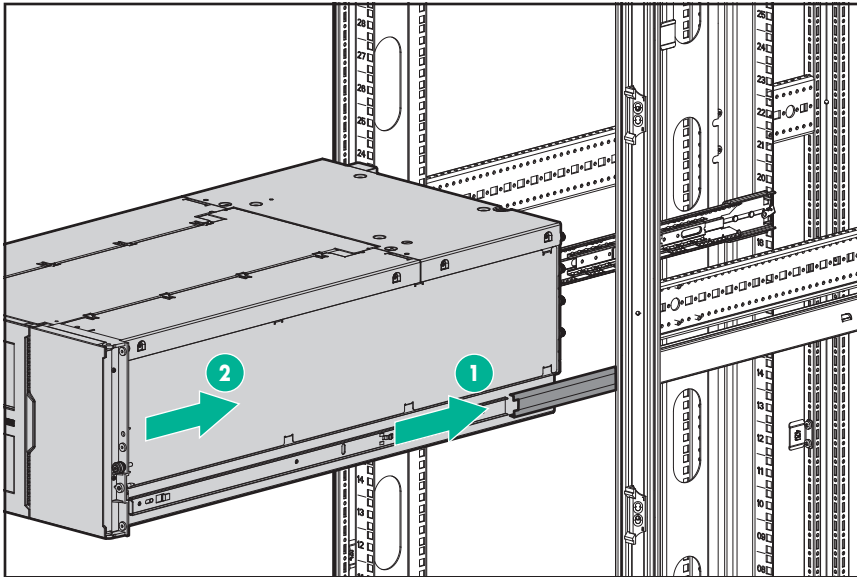
1. Extend the middle rails until they lock into place. Slide the bearing assembly to the front of the middle rails.



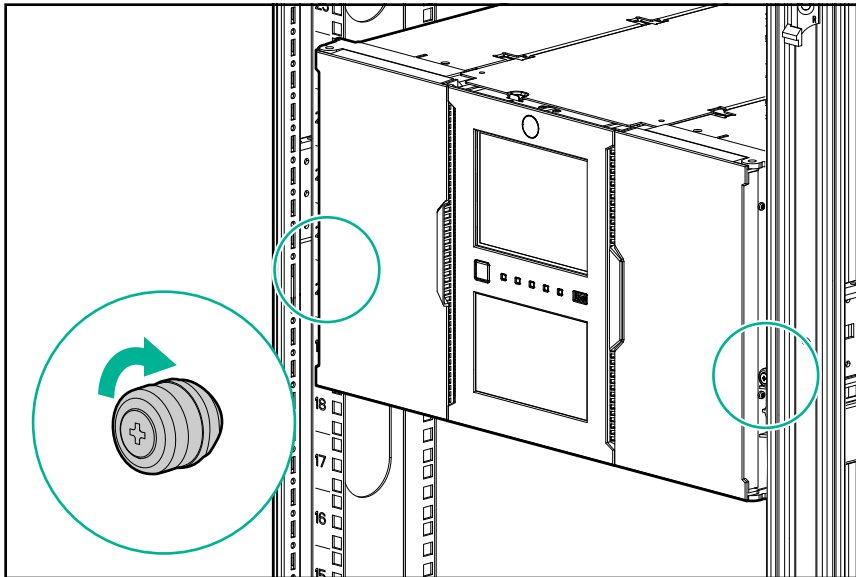
2. Slide the inner rails into the middle rails. Slide the module into the rack.
 - a. Once the module is secure on the rails, remove the protective tape on the front of the module around the thumbscrews.
 - b. Depress the release clips on both rails and then slide the module completely into the rack.

If the module does not go fully into the rack the first time, pull the module back out to the lock position and insert it again.





3. If you are not installing expansion modules, use your fingers or a #2 Phillips screwdriver to tighten the captive fasteners on each side of the module until they are finger tight. Do not over tighten.



4. If you are not installing expansion modules, you can remove the protective film from the front of the base module and then continue with **Installing tape drives**.

Preparing the top and bottom modules

Skip this step if you are installing a library without expansion modules.





WARNING: Each library module weighs 41 kg (90 lb) without media or tape drives and 71.4 kg (157.4 lb) with media (80 cartridges) and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the device:

- Observe local health and safety requirements and guidelines for manual material handling.
- Remove all tapes to reduce the overall weight of the device and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
- Obtain adequate assistance to lift and stabilize the device during installation or removal.

The base module has removable top and bottom covers. You will need to transfer one or both covers from the base module to expansion modules. The covers are identical and the procedure to transfer a cover is the same for both top and bottom covers.

- When installing expansion modules **below** the base module, move the bottom cover from the base module to the expansion module that will be installed at the bottom of the library.
- When installing expansion modules **above** the base module, move the top cover from the base module to the expansion module that will be installed at the top of the library.

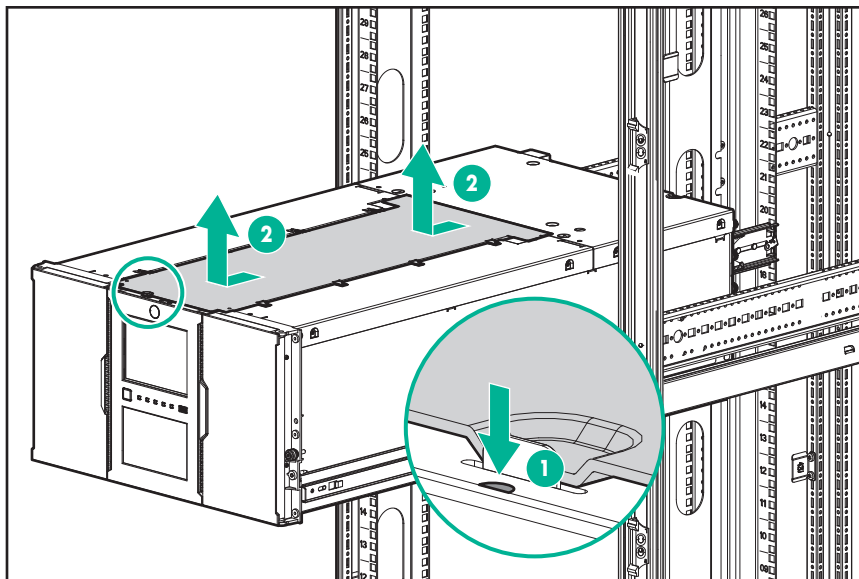
NOTE: Do not touch internal mechanical or electrical components while the top or bottom of the base module is open.

Prerequisites

A small flathead or Torx screwdriver

Procedure

1. Remove the library cover plate from the base module.
 - a. Extend the base module from the rack.
 - b. Insert a small flathead screwdriver or Torx screwdriver into the hole and retract the spring lock. Slide the cover until it reaches the tool, remove the tool and continue sliding the cover to the front of the module until all the tabs are released.

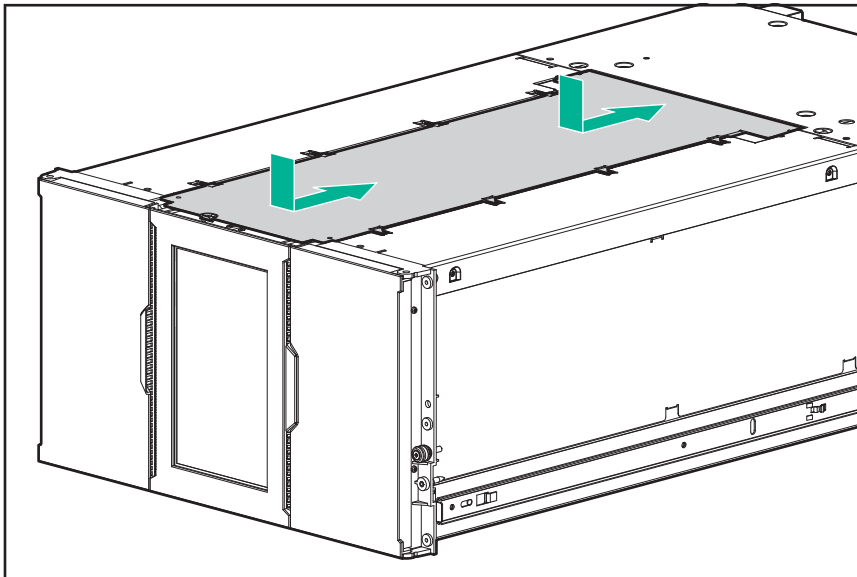


- c. Remove the cover from the module.
- d. Depress the release clips on both rails and then slide the base module completely into the rack.
If the module does not slide fully into the rack the first time, pull the module back out to the lock position and insert it again.
- e. Use your fingers or a #2 Phillips screwdriver to tighten the captive fasteners on each side of the base module until they are finger tight. Do not over tighten.

2. Install the cover on the expansion module.

- a. Place the expansion module on the work table. If the module will be the bottom module in the library, gently turn the module over so you can access the bottom of the module.
- b. Align all eight tabs on the cover with the slots on the module, gently push it down, and then slide the cover towards the back of the module until the spring lock at the front of the module engages by popping out.

NOTE: In this illustration, the top cover from the base module is being installed on the top of the expansion module that will be installed at the top of the library.



- c. If the expansion module is upside down, gently return it to its normal position.

Installing the expansion modules in the rack

Skip this step if the library does not have expansion modules.

Install the lower expansion modules first, working your way from the base module to the bottom of the library, and then install the upper expansion modules, working your way from the base module to the top of the library.



TIP: Installing the modules from the base module to the bottom of the library, and then from the base module to the top of the library minimizes rework in case of an alignment issue.



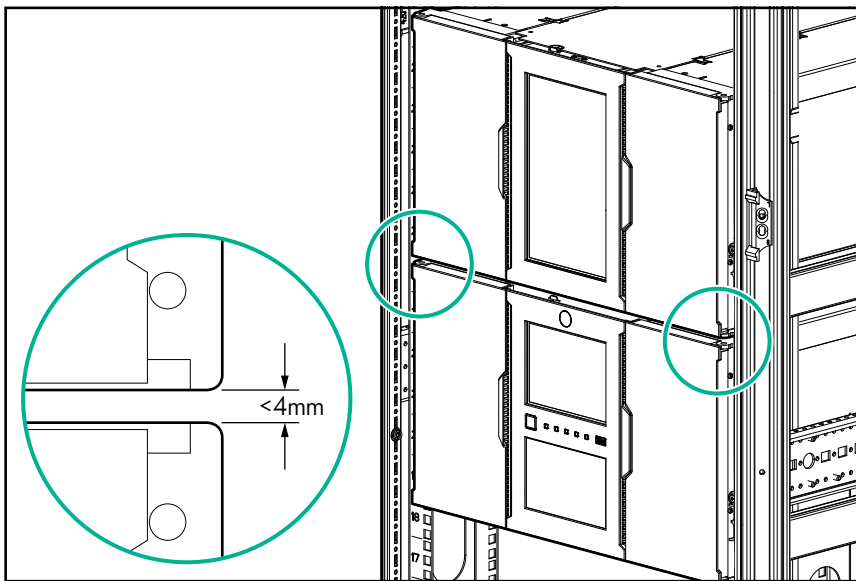
Procedure

1. Extend the middle rails until they lock into place. Slide the bearing assembly to the front of the middle rails. For illustrations, see **Installing the base module in the rack**.
2. Slide the inner rails into the middle rails. Slide the module into the rack.
 - a. Once the module is secure on the rails, remove the protective tape on the front of the module around the thumbscrews.
 - b. Depress the release clips on both rails and then slide the module completely into the rack.

If the module does not go fully into the rack the first time, pull the module back out to the lock position and insert it again.
3. Verify that this module has been installed directly above or below its adjacent module and is contained within the correct 6U volume.

Verify that the gap between modules is less than 4mm on both sides of the front of the modules. The gap in the back must be less than 5mm. If the gap is larger or varies side to side:

 - Confirm that both rack rails are properly located within the U volume.
 - Confirm that both rack rails are properly seated in the rack vertical column.
 - Verify that the top hanger for the rear of each rack rail is in the middle hole of the marked U section.
 - Check the rack vertical columns for bending.
 - Confirm that the rack is an approved model. See **Location requirements**.
 - Verify that the revision level printed on the rack rails is identical on each side.



4. Use your fingers or a #2 Phillips screwdriver to tighten the captive fasteners on each side of the module until they are finger tight. Do not over tighten.
5. After installing all of the expansion modules, you can remove the protective film from the front of the base module.

Aligning and connecting modules

Skip this step if the library does not have expansion modules.



Aligning the modules ensures that the robot can move freely between the modules. The library will not operate unless the alignment mechanism is in the locked position.

⚠ CAUTION: Do not use the alignment mechanism to force the modules into alignment.

The alignment mechanism is designed to hold the modules in position once they are aligned, but is not intended to adjust the module positions.

Procedure

1. From the front of the library, loosen the thumbscrews on each of the modules two full turns.
2. From the back of the library, starting with the bottom pair of modules, align each module with the module below. Repeat for each pair of modules.

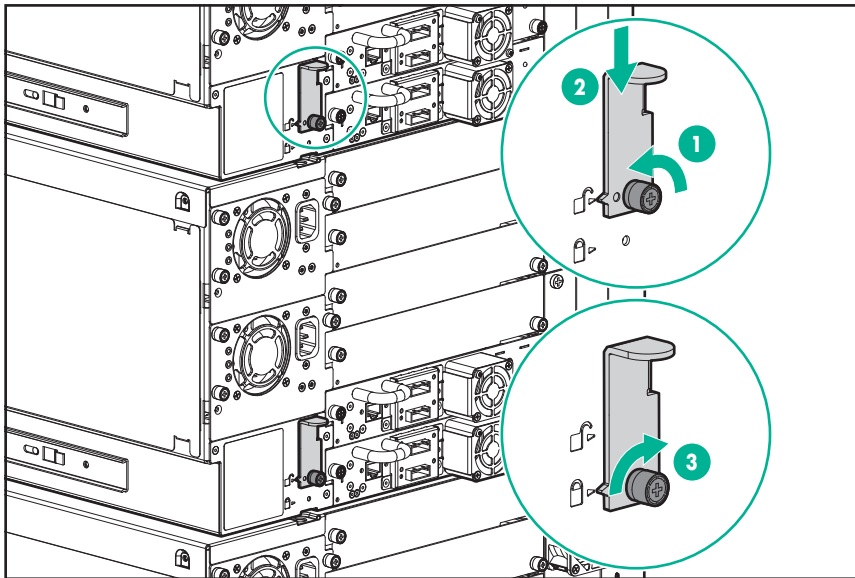
⚠ CAUTION: The alignment mechanism on the lowest module must be secured in the unlocked position. The library will not operate with the bottom mechanism in the locked position.

- a. Loosen the thumbscrew on the module alignment mechanism.
- b. Lower the alignment mechanism. If you encounter resistance, adjust the position of the upper module so the pin in the alignment mechanism moves into the hole in the lower module.

If the resistance continues, check the following:

- From the front of the rack, verify that the thumbscrews securing the modules to the rack have been loosened.
- Verify that the rack is level side-to-side and front-to-back.
- Check the rack for any obstructions or damage that could prevent the modules from aligning.

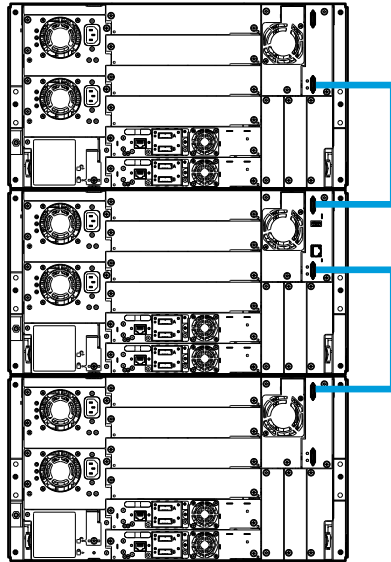
When the alignment mechanism is in the locked position, tighten the thumbscrew.



3. Verify that the lowest module in the library has its alignment mechanism secured in the unlocked position with the thumbscrew.



4. From the front of the library, use your fingers to tighten the thumbscrews on each of the modules to secure the modules to the rack.
5. From the back of the library, connect the lower module of each pair to its adjacent module using the expansion interconnect cable as shown.



Installing tape drives

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.



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the library.

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

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the drive bay openings.



CAUTION: All drive bays without tape drives installed must have drive bay covers installed.

Procedure

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

NOTE: Full height tape drives can only be installed in the top, bottom, or middle pair of half-height drive bays. A full-height drive cannot be seated in other locations and will not operate. If the drive will not seat completely, verify that it is located in one of the three full-height drive locations.

2. Remove the face plate covering the drive bay by removing the screws holding it in place.



Remove one drive bay cover to install a half-height tape drive; remove two drive bay covers to install a full-height tape drive.

3. Holding the tape drive by the handle and supporting it from the bottom, slide the tape drive along the alignment rails 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 blue captive 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.

Connecting the Fibre Channel cables

NOTE: 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

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 six meters.

Procedure

1. Attach the HBA end of the SAS cable into the connector on the HBA. If you are using a SAS fanout cable, the end of the cable with only one connector should be plugged into the HBA.
2. Connect the drive end of the cable.
 - When using a cable with a single connector on each end, attach the other end into the connector on the tape drive.
 - When using a SAS fanout cable, attach one mini-SAS connector into the connector on each tape drive. 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 tape drives, or coil and secure them to the rack to minimize stress on the connectors.



TIP: When using a SAS cable not specified for the library, do not force a SAS cable's mini-SAS connector into the tape drive mini-SAS connector because it might be keyed differently.

NOTE: Each of the tape drives uses one channel and the fanout 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.



Connecting cables for Data Verification

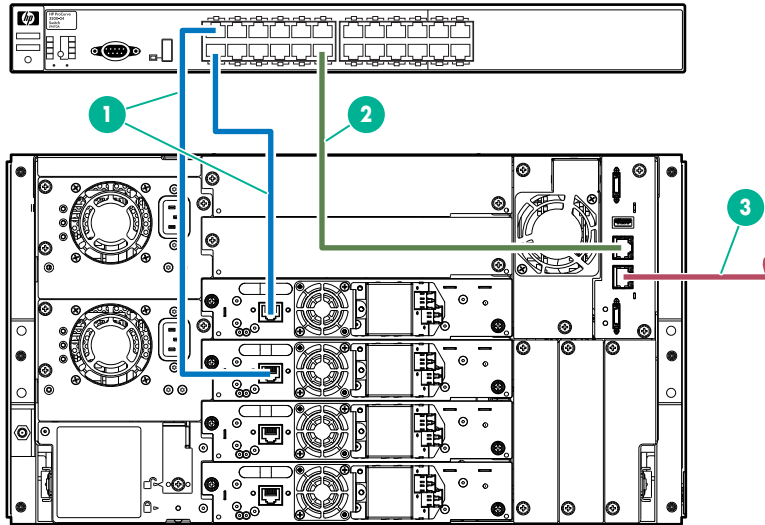
To configure the library for Data Verification, create a private network for the library and the tape drives that will be used for Data Verification.

Procedure

1. If necessary, install a switch with enough Ethernet ports for the library and the tape drives that will be used for Data Verification.

For example, if two tape drives will be used for Data Verification, the switch must have at least three available ports.

2. Using an Ethernet cable, connect the library DIAG port to the switch.



1. Tape drive Ethernet ports are connected to the private network for the Data Verification feature.
 2. Library DIAG port is connected to the private network for the Data Verification feature.
 3. Library Ethernet port is connected to the site LAN to provide user access through the RMI.
3. Using Ethernet cables, connect each tape drive that will be used for Data Verification to the switch.
 4. Regardless of whether you are using a dedicated switch or a VLAN for the data verification network, ensure that only the drive Ethernet ports and the DIAG port are connected to the private network, and that no other hosts or devices are sharing the network.
 5. Verify that the tape drive SAS or FC ports are NOT connected.

Powering on the library

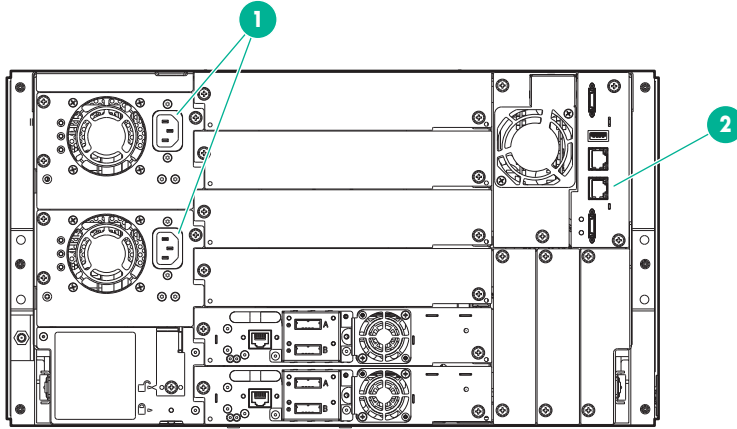
WARNING: To reduce the risk of electric shock or damage to the equipment:

- Use an approved power cord. If you have questions about the type of power cord to use, contact your authorized service provider.
- 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. Plug the power cables into the power connectors on each module and into AC power outlets.



1. Power connectors

2. Ethernet connector (Base module only)



TIP: The library has dual redundant power supplies. To increase redundancy, plug each power cord into a different AC power circuit.

2. To use the RMI, connect an Ethernet cable from the Ethernet port on the library module controller to your network.
3. Power on the library by pressing the power button on the base module just below the OCP.

When the library powers on, it performs the following tasks:

- Illuminates the green light on the front panel
 - Confirms the presence of expansion modules
 - Inventories the tape cartridges in the magazines
 - Checks the firmware version on all modules
 - Configures the tape drives
4. Verify that the library initializes properly and becomes ready

Initiating the configuration wizard

Procedure

Initiate the **Initial Configuration Wizard** from the OCP.

The wizard will guide you through configuring the timezone, date and time, and network settings, setting the administrator password, and then start an initial system test. You can skip items and stop the wizard at any time. Once you have configured the network settings and set the administrator password, you can initiate the wizard from the RMI to complete the remaining configurations.



If the wizard does not start automatically or you want to restart the wizard, navigate to **Configuration > Configuration Wizard** to initiate it manually.

Verifying the host connections

Procedure

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

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

For compatibility information, see the compatibility matrix at: <https://www.hpe.com/storage/StoreEverSupportMatrix>

2. Verify the connection between the library and the host using the host server operating system utilities or Library and Tape Tools (L&TT).

L&TT verifies that the unit is connected and communicating with the host server. It also verifies that the device is functioning and provides diagnostic information. L&TT is available without charge at: <https://www.hpe.com/support/TapeTools>

Labeling tape cartridges

Using unlabeled media can significantly increase the inventory scan time and is therefore not recommended for normal operation. See [Guidelines for using and maintaining data cartridges](#).

- ❗ **IMPORTANT:** Misusing and misunderstanding bar code technology can result in backup and restore failures. To ensure that your bar code labels meet Hewlett Packard Enterprise quality standards, always purchase them from an approved supplier and never print bar code labels yourself.

Procedure

Apply a high-quality preprinted bar code 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 bar code label.

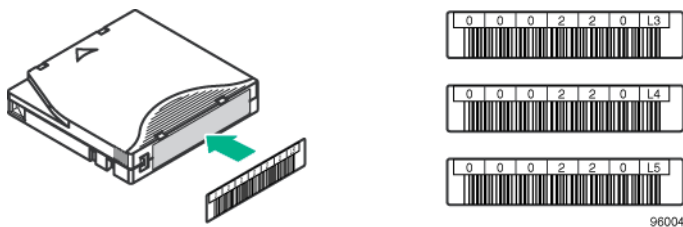


Figure 3: Apply the label within the recessed area





IMPORTANT: Only apply the bar code 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.

Loading the tape cartridges

The library will power on without cartridges, but needs cartridges before performing data read and write operations, or any tests or operations that transfer cartridges.

By default, the library requires that each tape cartridge has a proper bar code label and does not detect unlabeled media. Detection of unlabeled media can be enabled from the **Configuration > System > Allow Unlabeled Media** screen.

Using unlabeled media can significantly increase the inventory scan time and is therefore not recommended for normal operation.



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.



TIP: If the mailslot is enabled, you can use it to load cartridges into the library. On the home screen, tap **Open Mailslot**, open the magazine access door, and then pull out the mailslot.

Procedure

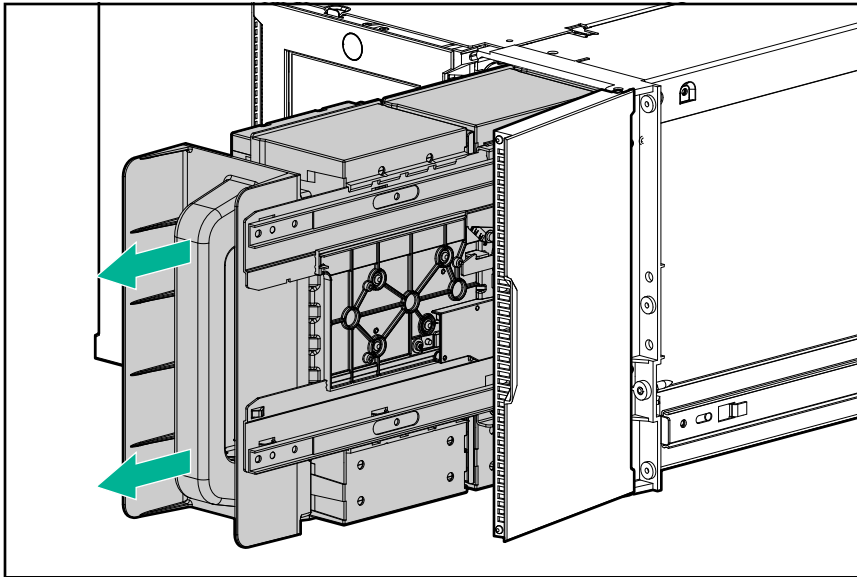
1. Extend one of the magazines from the library.

a. From the OCP or RMI, select the module and then select **Open Magazine**.

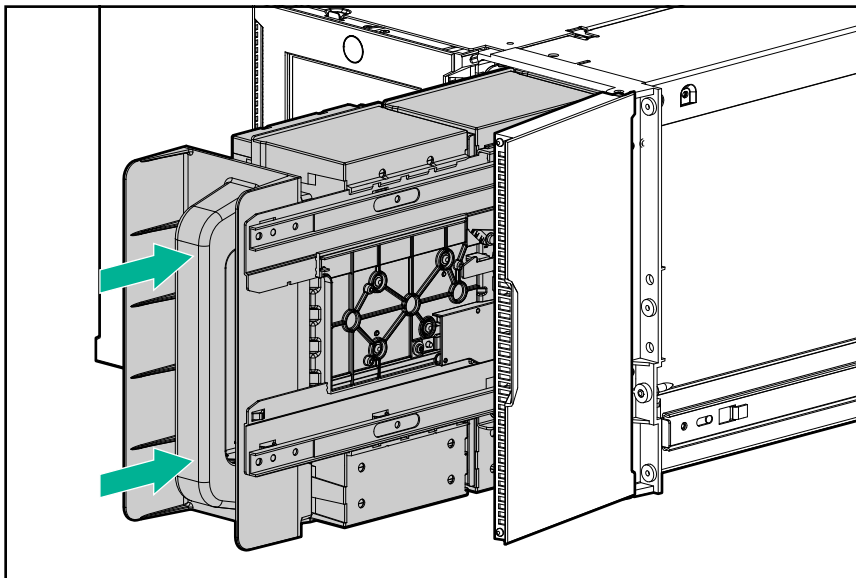
Wait until the OCP or RMI indicates that the magazine has been unlocked before attempting to remove it. Pulling on the handle while the library is unlocking the magazine might damage the library.

b. Open the magazine access door.





- c. Slowly pull the magazine handle until the magazine is fully extended.
2. Load the tape cartridges into the magazine starting with the back of the magazine. Push the magazine in the library as each bin is filled.
3. Push the magazine handle slowly until the magazine release latch snaps into place. The magazine locks into place.



4. Repeat steps 1 through 3 for each of the other magazines.

Verifying the installation

Procedure

1. Verify that the library and drives have the current firmware revision.
The library firmware revision is displayed in the top left corner of the OCP and RMI screen.



The drive firmware version is displayed on the RMI **Status > Drive Status** screen and the OCP **Status > Drive** screen.

2. If necessary, update the library firmware from the OCP or RMI **Maintenance > Firmware Upgrades > System Firmware** screen.
3. After configuring the library, you can save the configuration settings to a USB flash drive from the OCP **Configuration > Save/Restore > Save Configuration File** or to a file on your computer from the RMI **Configuration > System > Save/Restore** screen.

Having a backup of the library configuration is helpful when recovering from a configuration error or if the library needs service.

4. Set the security user password from the **Configuration > User Accounts** screen.

! **IMPORTANT:** The security user password must be changed before the security user or any LDAP users with the security role can log in to 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.

Downloading product firmware

Procedure

1. Navigate to the HPE Support website: <https://www.hpe.com/support/storage>

! **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

To view and update your entitlements, and to link your contracts and warranties with your profile, navigate to: <https://www.hpe.com/support/AccessToSupportMaterials>

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

To upgrade firmware from the OCP, copy the firmware image onto a FAT-32 formatted USB flash drive.

Configuring additional features

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

Procedure

- Enabling the mailslot.
- Configuring partitioning and additional library parameters using one of the partitioning wizards.
 - Basic Partition Wizard — Use the Basic Partition Wizard to configure partitions that will have similar resources or to configure the number of bar code characters to report to the host application and whether to report them from the left or right end of the label for a library with a single partition.
 - Expert Partition Wizard — Use the Expert Partition Wizard to configure partitions that will have different resources or to adjust resource assignments for existing partitions or those partitions created with the Basic Partition Wizard.
- Modifying the default tape drive settings.



NOTE: When using LTO-7 and LTO-8 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.

- Enabling and configuring SNMP network management.
- Enabling and configuring Command View TL integration and Data Verification.
- Setting up email event notification.
- Using the MSL Encryption Kit.



Operating the library

Library user interfaces

The library provides two main interfaces:

- Operator control panel (OCP)—With the OCP, you can monitor, configure, and control the library from the front panel.
- 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.

Status icons



The green **Status OK** icon indicates that the library is fully operational and that no user interaction is required.



The blue exclamation point **Status Warning** icon indicates that user attention is necessary, but that the library can still perform most operations.



The red X **Status Error** icon indicates that user intervention is required and that the library is not capable of performing some operations.

The OCP and RMI are similar in design and functionality. Differences are noted in this chapter.

Using the OCP

The OCP has a power button, an LCD touch screen, and five LEDs. With the OCP you can monitor, configure, and operate most library functions from the library front panel. To navigate the OCP, tap on the LCD touch screen.

To power on the library, press the power button. To power off the library, press the power button for 5 seconds and then release it. With library firmware versions 4.40 and newer, use the touch screen to select the parking position for the robotic assembly.

- **The default parked position** — This option is applicable in most cases and best for all service options. With this option, the robotic assembly returns to its home position behind the OCP.

If a parking position is not selected within 10 seconds in firmware versions 4.40 through 4.80, the library will park the robotic assembly in this location.

- **The shipping position**—With this option the robotic assembly will move to the bottom of the base module above the bottom cover. Select this option when the base module will be removed from the rack for shipping or when the base module is the bottom module in a library that is shipping in a rack.

If a parking position is not selected within 10 seconds in firmware versions 4.90 and later, the library will park the robotic assembly in this location.



IMPORTANT: Only select this option when the base module has a bottom cover.

Before moving or shipping a library, see **Moving a module within the rack or to a nearby rack**.



Table 10: LED indicators on the OCP

UID	Blue when activated. The unit identification (UID) LEDs are controlled by the user through the OCP and RMI Maintenance > UID LED Control screen. The UIDs on the OCP and back panel are activated and deactivated together. The UIDs are helpful for locating the library in a data center.
Ready	Green, steady when power is on, blinking with tape drive or library robotic activity.
Clean	Amber when a tape drive cleaning operation is recommended.
Attention	Amber if the library has detected a condition for which user attention is necessary, but that the library can still perform most operations.
Error	Amber if an unrecoverable tape drive or library error occurs. A corresponding error message is displayed on the LCD screen. User intervention is required; the library is not capable of performing some operations.

Using the RMI

With the RMI, you can monitor, configure, and operate most library functions from a web browser.

Hewlett Packard Enterprise recommends that, when possible, the RMI is used as the primary library interface because the web interface provides access to additional features, includes online help, and is easier to use. However, the RMI is not required to use the product, except to configure advanced features, such as SNMP, IPv6, encryption, LTFS, HPE TapeAssure, and partitions.

Before using the RMI, you must configure the library network settings and set the administrator and security user passwords with the OCP. You can configure the network settings and set the administrator password with the Initial Configuration Wizard. See **Using the Initial Configuration Wizard**. The security user password can be set from the **Configuration > User Accounts** screen. See **Configuring local user accounts**.

To start the RMI, open a supported HTML browser and enter the IP address of the library in the browser address bar.



TIP: See the online help in the RMI for additional information. The help pages are updated with firmware updates and often contain up-to-date technical details that might not be contained in this document. To access RMI help, click the ? icon on the right side of the RMI top banner.

Logging in to the library

Prerequisites



TIP: By default, the administrator password is unset; all of the digits are null. You must set the administrator password from the OCP to protect the administrator functions on the OCP and access the administrator functions on the RMI.

By default, the security password is set to `security`. You must update the security password from the OCP to protect the security functions on the OCP and access the security functions on 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.


Procedure

1. Access the user interface.



- **OCP**—If the OCP screen saver is on, tap the screen. The OCP dims when not being used.
 - **RMI**—Open a supported web browser and enter the IP address of the library in the browser address bar.
2. Select the **User**.
 3. If required, enter the **Password**.
 4. Click **Login**.

Library users

- **User**—No password is required (leave the **Password** blank unless the user password has been set).
The user account provides access to status information, but not configuration, maintenance or operation functions.
 - **Administrator**—The administrator password is required to log in as the administrator user. The same administrator password is used for the RMI and OCP. There is not a default administrator password; the administrator password must be set with the OCP before administrator functions can be used with the RMI. If the administrator password is lost, contact support to generate a temporary password that will grant administrator access for a limited time.
The administrator user has access to all functionality except for the security and service features.
 - **Security**—The security password is required to log in as the security user. The default security password is `security`. The security user password must be changed from the OCP before the library will allow security user access from the RMI. If the security password is lost, both the administrator and service passwords are required to change the security password.
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.
The security user has access to all administrator functionality and can also configure security features and change the security user password.
-
-  **IMPORTANT:** Hewlett Packard Enterprise highly recommends changing the security user password during product installation. Leaving the password with the default value can cause a security risk to the library and data.
-
- **Service**—**Access to this user is by service personnel only.** The service password is set at the factory. The same service password is used for the RMI and OCP. Both the administrator and service passwords are required for a service person to enter the service area.

The library RMI main screen

The library main screen 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 and module status.
- **Center pane**—Provides access to operate and configure the library and to view additional status information.
- **Right pane**—Displays a log of recent events.



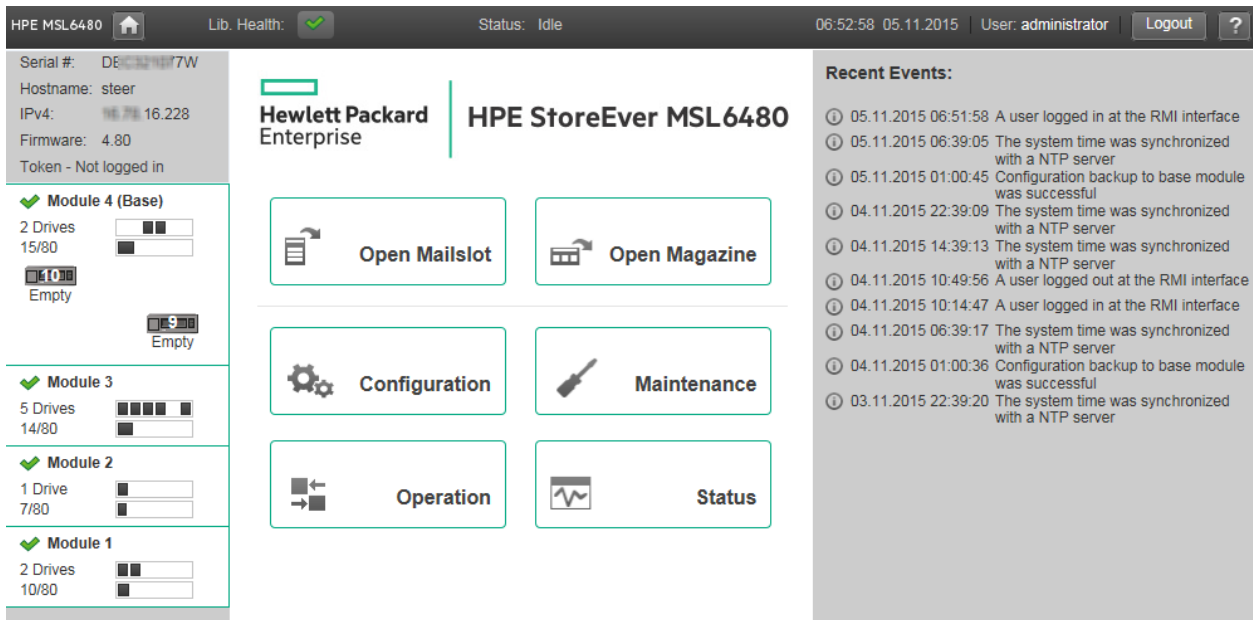






Figure 4: Main screen

Top banner elements

-  Home icon—Returns to the library main screen
- **Library health**—An icon indicating the overall health status of the library
 -  The green check mark **Status OK** icon indicates that all library components are fully operational and that no user intervention is required.
 -  The yellow triangle exclamation point **Status Warning** icon indicates that user attention is necessary, but that the library can still perform most operations. To display the event ticket log, click the icon.
 -  The red circle X **Status Error** icon indicates that 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
 - **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.
- 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**—Logs out of this session.
- **?**—Accesses online help



Left pane elements

- Library status—Overall library configuration and status
 - **Serial #**—The base library serial number
 - **Hostname**—The library hostname
 - Network configuration—The IP version (IPv4 or IPv6) and IP address
 - **Firmware**—The library firmware version
 - **EK Token**—Information about the key server token when using the encryption kit
- Module status overviews—a summary of configuration and health of each module

To select a module, click or tap the module status area.

- Module health icon
 - The green check mark **Status OK** icon indicates that the module and each of its components are fully operational and that no user intervention is required.
 - The yellow triangle explanation point **Status Warning** icon indicates that user attention is necessary, but that the library can still perform most operations.
 - The red circle X **Status Error** icon indicates that user intervention is required and the module is not capable of performing some operations.
- Module number—Modules are numbered based on their location in the physical library. The bottom module is **Module 1**. The base library module is annotated with **(Base)**.
- Drive status—The number of drives installed in the module and the health of each drive
 - To display drive configuration and status information in the center pane, 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 available and the number in use
- Drive operation status—The current drive activity for each drive in the module. The drive operation status is only displayed for the selected module.
 - **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.
 - **Encryp**—the drive is writing encrypted data.



Center pane

- **Open Mailslot**—(Administrator user only) Click or tap to unlock the mailslot on the selected module. Mailslots must be enabled before the slots can be used as mailslots.
- **Open Magazine**—(Administrator user only) Click or tap to unlock a magazine in the selected module. 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.
- **Service Area**—(Service user only) Click or tap to access functionality restricted to service engineers. Both the service and administrator passwords are required to log in as the service user.

Configuring the library

When the library powers on the first time, it is configured with the default settings. The library must be configured before use.

Configuring the simplest configuration

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, run the **Initial Configuration Wizard** from the **Configuration** area of the OCP. You can skip the other configurations and complete them from the RMI.

2. Log in to the RMI as the 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. 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. On the Home screen, click **Configuration**.

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.

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

5. In the **Information** screen, click **Proceed** and then click **Next**.



Create Partition Scheme

Free Resources That Will Be Used by the Partition Scheme

Slots :	140
Mailslots :	20
Drives :	6
Max. Partitions :	6

Partition Settings

Partition Count (max. 20)	1 ▼
Barcode Label Length Reported To Host	8 ▼
Barcode Label Alignment Reported To Host	Left ▼
Auto Clean	<input type="checkbox"/>

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

- The library has one partition.
 - Eight bar code 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 bar code 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.



Finish Configuration

Partitions

No	Slots	Mailslots	Drives	Drive Hosting Lib. LUN	Info	Done
1	140	20	6	1		

7. Click **Finish.**

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

Using the Initial Configuration Wizard

The wizard guides you through setting the administrator password, configuring the timezone, date and time, and library network settings, and then starting an initial system test. You can skip items and stop the wizard at any time.

Procedure

1. Configure the network settings and set the administrator password from the OCP.
2. Initiate the wizard from the RMI or OCP to complete the remaining configurations.

Managing the library configuration

NOTE: The library only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.

Procedure

- **Save the library configuration to a file**
- **Restore the library configuration from a file**
- **Reset the library configuration to the default settings**
- **Save the library configuration to a file**



Saving the library configuration

From the **Configuration > System > Save/Restore Configuration** screen 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 base module or base module controller replacement.

Procedure

1. Navigate to the **Configuration > System > Save/Restore Configuration** screen.
2. If saving the configuration to a USB device on the library, insert a USB flash drive into one of the USB ports on the base module.

NOTE: The library only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.

3. Select the destination location:
 - **RMI**—(RMI only) Downloads the configuration file to the browser or system running the RMI.
 - **USB Device Front**—Downloads the configuration file to a USB flash drive inserted into the USB port on the front of the library.
 - **USB Device Rear**—Downloads the configuration file to a USB flash drive inserted into the USB port in the back of the library.
4. Click **Save**.

Restoring the library configuration from a file

From the **Configuration > System > Save/Restore Configuration** screen you can save the library configuration settings to a file, restore the settings, or reset the library configuration to the default settings. If the base module or base module controller must be replaced, the saved configuration database will make it easier to recover the library configuration.

NOTE: The library only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.

Procedure

1. If restoring the configuration file from a USB device, prepare the files on the USB device.
 - a. Copy the configuration file you want to restore onto a USB device.
 - b. Remove any other configuration files from the USB device.
2. Navigate to the **Configuration > System > Save/Restore Configuration** screen.
3. When restoring the configuration file from a USB device, insert the USB flash drive containing the configuration file into a USB port on the base module.
4. Select the source location:



- **RMI**—(RMI only) Restores the configuration file from the computer running the RMI. Click **Browse** and then navigate to and select the configuration file.
- **USB Device Front**—Restores the configuration file from a USB flash drive inserted into the USB port on the front of the library.
- **USB Device Rear**—Restores the configuration file from a USB flash drive inserted into the USB port in the back of the library.

5. Click **Browse**.

Resetting the library configuration to the default settings

Procedure

From the **Configuration > System > Save/Restore Configuration**, click **Reset Default Settings**. For the default settings, see [Default and restore defaults settings](#).

Resetting the list of known drives and modules

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

Procedure

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

NOTE:

This operation will renumber all of the modules and drives, which can impact element addressing to the hosts. After the operation completes, use one of the partition wizards to verify and update the drive and module assignments as necessary. Other library settings are not affected by this operation.

Managing the library date and and time

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

Procedure

- [Set the timezone](#)
- [Set the date and time format](#)
- [Set the date and time](#)
- [Enable SNTP \(Simple Network Time Protocol\) synchronization](#)



Setting the timezone

Procedure

1. Navigate to the **System > Date and Time Format** screen.
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 timezone list, as necessary, until a location with the appropriate timezone is visible.
4. Select a location with the appropriate timezone.
5. Click **Submit**.

Setting the date and time format

Procedure

1. Navigate to the **System > Date and Time Format** screen.
2. Click **Date/Time Format**.
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

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 the **System > Date and Time Format** screen.
2. Click **Set Date/Time**.
3. Set the time and date.
4. 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.
5. To synchronize the time and date with the computer running the browser, click **Now**.
6. Click **Submit**.



Enabling SNTP (Simple Network Time Protocol) synchronization

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

Procedure

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

Time is synchronized with the SNTP server every 61 seconds.

Configuring media barcode compatibility checking

When Barcode Media ID Restriction is enabled, the library will only allow appropriate data cartridges to be loaded into tape drives. The barcode media ID is the last two characters of the barcode. For example, the library will not move an LTO-6 labeled cartridge into an LTO-4 tape drive.

When 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.

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).

Procedure

- **Enable media barcode compatibility checking**
- **Disable media barcode compatibility checking**

Enabling media barcode compatibility checking

When media barcode compatibility checking is enabled, the library will only allow appropriate data cartridges to be loaded into tape drives.

The barcode media ID is the last two characters of the barcode. For example, the library will not move an LTO-6 labeled cartridge into an LTO-4 tape drive.

When 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.

Procedure

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

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 checking

When **Barcode Media ID Restriction** is enabled, the library will only allow appropriate data cartridges to be loaded into tape drives. The barcode media ID is the last two characters of the barcode. For example, the library will not move an LTO-6 labeled cartridge into an LTO-4 tape drive. When 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.

NOTE: With Barcode Media ID Restriction disabled, the library will allow a single move of an incompatible data cartridge to a tape drive before it will proactively block known incompatible moves that would otherwise fail.

Procedure

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

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. Click **Barcode Media ID Restriction**.
3. Click **Submit**.

Using unlabeled media

By default, the library requires that each data cartridge have a proper barcode label and does not detect unlabeled media.

Detection of unlabeled media can be enabled from the **Configuration > System > Allow Unlabeled Media** screen.

Using unlabeled media can significantly increase the inventory scan time and is therefore not recommended for normal operation.

Managing license keys

License keys register licensed library functionality.

Procedure

1. Navigate to the **Configuration > System > License Key Handling** screen.
2. In the **Add License Key** pane, enter the **License Key**, and then click **Add License**.

Configuring the system language

The RMI is available in English and Japanese.

Procedure

From the **Configuration > System > Language** screen, select the language for the RMI, including the online help.

Configuring the RMI timeout

Procedure

1. Navigate to the **Configuration > Web Management > Session Timeout** screen.
2. Select one of the available settings.



The default is 30 minutes.

3. Click **Submit**

Configuring the library network settings

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

Procedure

1. Navigate to the **Configuration > Network** screen.
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 **Stateless** method.
5. Configure the **Max Link Speed** for the base module library controller Ethernet ports. This setting configures the maximum speed to which both ports will automatically negotiate. The default, 1 Gbit, is applicable for most cases.
If the library is in a network with very high broadcast network traffic, setting a lower value can be useful when diagnosing unexpected network failure events.
6. Click **Submit**.

Using the Configuration > Network Management screen

Procedure

- **Add an SNMP target**
- **Edit information for an SNMP target**
- **Delete an SNMP target**
- **Clear all SNMPv3 options**

SNMP options

The library supports both SNMP configuration and SNMP traps.

- **SNMP Enabled**—When selected, computers listed in the SNMP Target IP Addresses field can manage the library. SNMP must be enabled to work with Command View for Tape Libraries.
- **Community Name**—A string used to match the SNMP management station and 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**—Select the level of severity of events to be sent as SNMP traps. The default is **+Warning**.
 - **Inactive**—No events are sent as SNMP traps.
 - **Critical**—Only Critical events are sent as SNMP traps.
 - **+Warning**—Critical and Warning events are sent as SNMP traps.



- **+Configuration**—Critical, Warning, and Configuration events are sent as SNMP traps.
- **+Informational**—All events are sent as SNMP traps.
- **SNMP Targets**—List of configured SNMP targets.

Adding an SNMP target

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 the **Configuration > Network Management** screen.
2. Click **Edit** next to a target without an IP/Hostname.
3. Enter the target IP address or hostname.
4. Enter the port.
5. Select the SNMP version.
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**.

Editing information for an SNMP target

Procedure

1. Navigate to the **Configuration > Network Management** screen.
2. Click **Edit** for the appropriate SNMP target.
3. Enter the target IP address or hostname.
4. Enter the port.
5. Select the SNMP version.
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 the **Configuration > Network Management** screen.
2. Click **Delete** for the target to be deleted.
3. Click **Submit**.

Clearing all SNMPv3 options

Procedure

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

Configuring remote logging

This feature allows for sending library events to a remote syslog server. The data sent only includes the ticket information generated by library software. No low level logs generated by the Linux and other applications will be sent to the remote server.

Only non-encrypted remote logging is supported.

Procedure

1. Navigate to the **Configuration > Network Management > Remote Logging (rsyslog)** screen.
2. Enable remote logging, if necessary, by selecting **Remote Logging Enabled**.

When **Remote Logging Enabled** is selected, the library can send library events to the configured **Remote Logging Server** server.

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.
- **+Informational**-All events are sent.

4. In the **Server** field, enter the remote syslog server hostname or IP address.

5. Configure the **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.

6. Configure the **Transport Protocol**.



TCP and UDP are supported. The default is TCP.

7. Click **Submit**.

Configuring event notification parameters

From the **Configuration > Network Management > SMTP** screen, you can enable SMTP (Simple Mail Transfer Protocol) functionality and configure e-mail notification of library events. The library must have network access to an SMTP server.

Procedure

1. Navigate to the **Configuration > Network Management > SMTP** screen.
2. If SMTP is not enabled, click **SMTP Enabled**.
3. When enabled, the remaining configurations are active.
4. Configure SMTP options:
 - a. **Notification Level** — The types of events for which the library should send e-mail
 - **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.
 - b. **SMTP Server** —Hostname or IP address of the SMTP server.
 - c. **Security** —Security protocol for accessing the SMTP server.
 - **None**
 - **SSL/TLS**
 - **STARTTLS**
 - d. **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.
 - e. **To Email Address** —The address to receive the reported events (for example `firstname.lastname@example.com`). Only one email address can be configured.
 - f. **Mailer Name** —Name of the sender of the e-mail.
 - g. **Email Subject** —Subject line for the e-mail message.
 - h. **Email Address** —Return address to use for the e-mail message.
 - i. **Authentication Required** —When selected, a username and password are required to access the SMTP server.
 - j. **Username** —User account for logging in to the SMTP server when authentication is required.
 - k. **Password** —Password associated with the Username when authentication is required.
5. Click **Submit**.



Enabling SMTP

The library must have network access to an SMTP server.

Procedure

1. Navigate to the **Configuration > Network Management > SMTP** screen.
2. Click **SMTP Enabled**.

Configuring HPE Systems Insight Manager for the library

The library uses the HPE NetCitizen MIB, which is supported by HPE Systems Insight Manager (SIM) 7.4 and newer versions, and many other applications. To detect the library using a remote management application, such as HPE SIM, you must first add the IP address for the management system as an SNMP target. SNMP queries are only accepted from configured targets.

Procedure

1. To configure the library for use with HPE SIM:
2. From the RMI, add the HPE SIM management station as an SNMP target.
3. If the library address is in an HPE SIM automatic discovery IP address list, the SIM management station will detect the library at the next scheduled scan.

Configuring HPE SIM for manual discovery

Procedure

1. In the HPE SIM toolbar, click **Options > Discovery**.
2. Click the **Manual** tab.
3. Enter the library IP address or system name.
4. SIM 7.4 will automatically detect the system type and product name.

Configuring tape drives

Procedure

1. Navigate to the **Configuration > Drives > Settings** screen.
2. Modify any of the configurable values.
 - Drive number—Drives are numbered from the bottom of the library up beginning with one. 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. The reassigned the values are based on the new location within the library.



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 3—Ultrium 920, Ultrium 960
 - LTO 4—Ultrium 1760, Ultrium 1840
 - LTO 5—Ultrium 3000, Ultrium 3280
 - LTO 6—Ultrium 6250
 - LTO 7—Ultrium 15000
 - LTO 8—Ultrium 30750
- Drive form factor
 - HH—half height
 - FH—full 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 powered 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.
- **Power On**—Selected when the drive is powered on.

NOTE: Always power off a tape drive before removing it from the library or moving it to a new location within 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 LTO-7 and LTO-8 FC 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.



- **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**.

Configuring barcode handling

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

Procedure

- **Use the basic partition wizard**
- **Use the expert partition wizard**

Changing the control path drive manually

When Basic CPF is enabled and both an active and passive drive are configured, you can change the control path drive from the RMI. Changing the control path drive before powering off the active control path drive ensures that library communication continues during the transition. Using this screen is easier than changing the active and control path drives in the Expert Partition Wizard.

NOTE: This feature only applies to Basic CPF and is not used when Advanced CPF is enabled.

Procedure

1. Navigate to the **Configuration > Drives > Manual Control Path Failover** screen.
2. Click **Failover**.
3. Click **Submit**.

Enabling or disabling mailslots

The **Configuration > Mailslot** screen lists each of the mailslots and shows whether each is enabled or disabled.

Procedure

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

Slots not enabled as mailslots are available as storage slots.

Partition wizards

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

- Each partition must have at least one tape drive. One drive in each partition will host the library LUN for the partition.
- The maximum number of partitions is 20.



- Magazine slots are allocated in five-slot groups in most library modules. Slots allocated from the bottom module in the library are allocated in four-slot groups.
- Mailslots must be enabled for a module 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 off line.

Although the mailslot magazine is shared between partitions, the mailslot elements are assigned individually to partitions.

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. Any extra drives or slots are assigned to the first partition.

Use the Basic Partition Wizard to configure partitions that will have similar resources or 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 a library with a single partition.

- **Expert Partition Wizard**—You add or remove partitions from the current partitions configuration and then edit each partition configuration to add or remove library resources.

Use the Expert Partition Wizard to configure partitions that will have different resources or to adjust resource assignments for existing partitions or partitions created with the Basic Partition Wizard.

Also use the Expert Partition Wizard to configure Control Path Failover and Data Path Failover.

Using the basic partition wizard

When Data Verification is enabled from Command View TL, Command View TL creates a partition called “DVP” on the library, which is used to import media into the library for Data Verification. Hewlett Packard Enterprise recommends only deleting or modifying the DVP partition from the Command View TL user interface rather than from the library RMI. Do not name a partition “DVP” because this name is reserved for Command View TL.

The library will go off line while partitions are being configured. Ensure that all host operations are idle before running a partition wizard.

Procedure

1. From the **Configuration** area, click **Basic Wizard** in the **Partitions** menu to start the wizard.

The **Information** screen displays the existing partitions, which will be deleted by the wizard.

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

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

NOTE: If you want to enable or disable the mailslots, **Cancel** out of the wizard and update the mailslot configuration before configuring partitioning.

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 maximum length is 16 and the default is 8. This configuration will apply to all partitions.



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 library will report 123456. If 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 instead of creating a warning event when a drive requires cleaning. LTO-7 and later generation tape drives might request cleaning 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. 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.

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 bar code media identifier and will allow moves of cleaning cartridges 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** screen displays the proposed allocation of library resources into partitions.
 - a. To update the configuration, click **Back**.
 - b. To have the wizard configure 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

When Data Verification is enabled from Command View TL, Command View TL creates a partition called “DVP” on the library, which is used to import media into the library for Data Verification. Hewlett Packard Enterprise recommends only deleting or modifying the DVP partition from the Command View TL user interface rather than from the library RMI. Do not name a partition “DVP” because this name is reserved for Command View TL.



CAUTION: The library will go off line while partitions are being configured. Ensure that all host operations are idle before running a partition wizard.

NOTE: If you want to enable or disable the mailslots, **Cancel** out of the wizard and update the mailslot configuration before configuring partitioning.



NOTE: Failover features are licensed and can only be enabled when a valid license has been added to the library. If you want to enable these features and have not added the license to the library, **Cancel** out of the wizard and add the license to the library before configuring partitioning.

Procedure

1. From the **Configuration** area, click **Expert Wizard** in the **Partitions** menu to start the wizard.

The **Create Partition Scheme** screen 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.

NOTE: Do not name the partition “DVP” because this name is reserved for the use of Command View TL.

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 maximum length is 16 and the default is 8. This configuration will apply to all partitions.

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 library will report 123456 . If 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 instead of creating a warning event when a drive requires cleaning. LTO-7 and later generation tape drives might request cleaning 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. 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.



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 bar code media identifier and will allow moves of cleaning cartridges 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 **LTO7+ Multi-initiator SCSI Conflict Detection**.

LTO-7 and later generation tape drives track which hosts (SCSI initiators) are sending commands to the drive. When **LTO7+ Multi-initiator SCSI Conflict Detection** is enabled for a partition, the library monitors the initiator lists for all of the LTO-7 and later generation drives in that partition. If the library detects more than a single host WWNN for a drive, the library generates an LTO7+ Multi-initiator SCSI Conflict Detection warning event. The event lists all of the host WWNNs for the given tape drive, so the administrator can remove access to any host that should not be sending commands to the drive.

The **LTO7+ Multi-initiator SCSI Conflict Detection** setting only appears if one or more LTO-7 or later generation drives are detected in the library.

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.

8. Click **Next**.

9. In the **Assign Storage Slots** screen, use the >> and << buttons to assign slots to the new partition and then click **Next**.

10. In the **Assign Mailslots** screen, use the >> and << buttons to assign mailslots to the new partition and then click **Next**.

Individual mailslot elements cannot be shared between partitions. Importing or exporting cartridges in a partition without an assigned mailslot will require magazine access, which will take the library off line.

11. In the **Assign Drives** screen, use the >> and << buttons to assign drives to the new partition and then click **Next**.

12. In the **Select Control Path Failover Type** screen, select the failover feature for the partition.

- **None - Control Path Failover Disabled** —When selected, the library will not transfer control to another tape drive if communication with the active control path drive for the partition is interrupted.
- **Enable - Basic Control Path Failover (CPF)** —When selected, the library will attempt to reassign control to the configured passive control path drive if communication with the active control path drive for the partition is interrupted. All worldwide names and configuration settings are retained after the reassignment.



TIP: This option is only selectable when the following requirements are met:

- The partition has two or more LTO-5 or LTO-6 dual-ported FC drives of the same LTO generation and form factor. For example, you can configure an LTO-5 full-height FC drive as the control path failover drive for another LTO-5 full-height FC drive, but not for an LTO-6 drive.
- The host connection is through a SAN switch with NPIV enabled for associated ports.
- The HPE MSL6480 LTO-5&6 Control Path (CtrlP) Failover license has been added to the library.

All drive port types, A and B for full height drives, must be configured as Fabric. Any drive that is not set to Fabric will be configured as Fabric by the Expert Partition Wizard. If CPF is disabled, the ports remain in Fabric mode until they are manually reconfigured.



- **Enable—LTO6 Advanced Control Path Failover (ACPF)**—When selected, the failover driver on the backup host operating system and library work together to handle error recovery and path failover for the partition at a level below the backup application. ACPF includes both port-to-port failover on a single control path drive and drive-to-drive failover of the library LUN.



TIP: This option is only selectable when the following requirements are met:

The partition contains at least two LTO-6 FC tape drives. SAS and other FC tape drives can be in the same partition, but cannot be configured for ACPF.

NOTE: LTO-6 High Availability Path Failover requires a driver to be installed on all backup application servers that will access the partition. For information about High Availability Path Failover, including installing and using operating system drivers, see the LTO-5 and LTO-6 failover user guide.

- **Enable-LTO7+ Control Path Failover (LTO7+ CPF)** —When selected, the failover driver on the backup host operating system and library work together to handle error recovery and path failover for the partition at a level below the backup application. LTO-7+ control path failover includes both port-to-port failover on a single control path drive and drive-to-drive failover of the library LUN.



TIP: This option is only selectable when the following requirements are met:

- The partition contains at least two LTO-7 or later generation FC tape drives. For example, an LTO-7 FC drive can fail over to an LTO-8 FC drive.

SAS and LTO-6 and earlier generation FC tape drives can be in the same partition, but cannot be configured for LTO-7+ failover.

- The HPE MSL6480 LTO-7+ Path Failover License has been added to the library.
-

NOTE: LTO-7+ Path Failover requires a driver to be installed on all backup application servers that will access the partition. For information about LTO-7+ Path Failover, including installing and using failover software, see the LTO-7 and later generation failover user guide.

13. In the **Select Control Path Settings** screen, select the **Active Control Path Drive**. If CPF or ACPF is enabled, also select the **Passive Control Path Drive**. Click **Next**.

14. In the **Select Data Path Failover Settings** screen, select the Data Path Failover settings for each tape drive.

- **None** —When selected, the drive will not attempt to transfer the data path to the other port if it detects a failure on the primary port.
- **LTO6 Adv. DPF**—The Advanced Data Path Failover features of LTO-6 drives are enabled. With ADPF, the failover driver on the backup host operating system and library work together to detect a failed drive port and transfer the data path to the other drive port as quickly as possible, resulting in most recoveries completing before the standard command timeout.





TIP: This option is only selectable when the following requirements are met:

- The drive is an LTO-6 dual-ported FC drive.
- Basic CPF is NOT enabled for the partition containing the drive.
- The HPE MSL6480 LTO-5&6 Data Path (DataP) Failover License has been added to the library.

- **LTO7+ DPF** —The LTO-7+ data path failover features are enabled. With LTO-7+ data path failover, the failover driver on the backup host operating system and library work together to detect a failed drive port and transfer the data path to the other drive port as quickly as possible, resulting in most recoveries completing before the standard command timeout.



TIP: This option is only selectable when the following requirements are met:

- The drive is an LTO-7 or later generation FC drive.
- Basic CPF or LTO-6 Advanced Control Path Failover is NOT enabled for the partition containing the drive.
- The HPE MSL6480 LTO-7+ Path Failover License has been added to the library.

NOTE: LTO-7+ Path Failover requires a driver to be installed on all backup application servers that will access the partition. For information about LTO-7+ Path Failover, including installing and using failover software, see the LTO-7 and later generation failover user guide.

15. Verify the partition configuration and then click **Finish**.
16. After the wizard reconfigures the partition, the library will come on line automatically.

Configuring the encryption key manager type

The **Configuration > Encryption** screen displays the available data encryption key manager types along with the status of each type. Only one encryption manager type can be configured for the library at a time and it will be used for all tape drives and partitions.

NOTE: Encryption configuration changes cannot be made while media is loaded in any drive in the library.

Prerequisites

Logged in to the RMI as the security user.

Procedure

1. Navigate to the **Configuration > Encryption** screen.
2. Select the partition and encryption method.
3. Click **Submit**.

MSL Encryption Kit configuration

The **Configuration > Encryption > USB—MSL Encryption Kit** screen 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 StoreEver MSL Encryption Kit User Guide* on the Hewlett Packard Enterprise Support website: <https://www.hpe.com/info/storage/docs>. The terms “token PIN” and “token password” are used interchangeably in the encryption kit documentation.

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

Procedure

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

Procedure

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



CAUTION:

The key server token protects the encryption keys with a password. 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.

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

Procedure

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

Configuring automatic key generation when using the MSL Encryption Kit

When automatic key generation is enabled, the library will automatically request the key server token to generate a new key periodically, according to the policy you configure. Be aware that when new keys are created automatically they are not backed up until you do so manually. To avoid only having one copy of the new key, set the automatic key generation policy for a time when you can back up the new key before data cartridges are written using the new key.

Procedure

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

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 off at a time when a new key would have been automatically generated. To prevent a new key from being generated in this case, disable automatic key generation before powering off the autoloader or library.

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

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 the **Configuration > Encryption > USB—MSL Encryption Kit** screen.
2. Expand the **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.
5. Click **Save**.

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

Procedure

1. Navigate to the **Configuration > Encryption > USB—MSL Encryption Kit** screen.
2. Expand the **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. Browse to the location of the key server token backup file on the local computer.
5. Click **Restore**.

Configuring an automatic key generation policy when using the MSL Encryption Kit

Procedure

1. Navigate to the **Configuration > Encryption > USB—MSL Encryption Kit** screen.
2. Expand the **Key Management** section.
3. Set the day of the week, time of day and frequency. A new key can only be generated when no media is in any tape drive in the library, so when possible select a time when all drives in the library are unloaded.
4. Select **Enabled**.
5. Click **Submit**.

Enabling encryption when using the MSL Encryption Kit

Encryption is enabled or disabled for all partitions and tape drives in the library.

Procedure

1. Navigate to the **Configuration > Encryption > USB—MSL Encryption Kit** screen.
2. Expand the **Enable/Disable Encryption** section.
3. Click **Enable** or **Disable**.
4. Click **Submit**.

Disabling encryption when using the MSL Encryption Kit

Encryption is disabled for all partitions and tape drives in the library.

Prerequisites

Logged in to the RMI as the security user.



Procedure

1. Navigate to the **Configuration > Encryption > USB—MSL Encryption Kit** screen.
2. Expand the **Enable/Disable Encryption** section.
3. Click **Submit**.

Configuring the key server token log in behavior when using the MSL Encryption Kit

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 the **Configuration > Encryption > USB—MSL Encryption Kit** screen.
2. Click **Keep Token Logged In Across Reboots**.
3. Click **Submit**.

ESKM Wizard prerequisites

With the ESKM Wizard, you can configure use of the HPE Enterprise Secure Key Management server with the library. Access the wizard from the **Encryption** menu on the RMI, which is only available to the security user and requires that the ESKM license has been added from the **Configuration > System > License Key Handling** screen.

NOTE: The library only allows one encryption key manager type to be used at a time. For example, if ESKM is enabled and in use, the encryption kit cannot also be used for encryption key generation and retrieval.

For additional information on configuring ESKM for use with the library, see the *HPE Enterprise Secure Key Manager User Guide*.

Procedure

- The library configuration is complete, including defining all library partitions.
- A 1024-bit or 2048-bit server certificate for each ESKM device in the cluster has been created.
- The ESKM server certificate has been signed by the Certificate Authority (CA) you intend to use and has been installed on the ESKM.
- SSL is enabled on the ESKM KMS server.
- The ESKM Management Console is open and ready for use. The ESKM Management Console and library RMI are used together to configure the library for ESKM.

Using the ESKM Wizard

Prerequisites

ESKM Wizard prerequisites



Procedure

1. In the **Configuration** area, click **ESKM Wizard** in the **Encryption** menu to start the wizard.
2. The **Wizard Information** screen displays information about the wizard. If the library configuration is complete, click **Next**.
3. The **Certificate Authority Information** screen displays prerequisites for using the ESKM certificate. When the prerequisites are met, click **Next**.
4. The **Certificate Authority Certificate Entry** screen displays instructions for obtaining the certificate for the ESKM server. 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 prerequisites for generating and signing the certificate for the library. When you have verified that SSL has been enabled on the ESKM device and that the ESKM management console is open and ready for use, click **Next**.
6. In the **ESKM Client Configuration** screen, enter the username and password that the library will use to communicate with the ESKM.
7. If the username and password have not already been set up on the ESKM device, follow the instructions in the *HPE Enterprise Secure Key Manager User Guide* to create a client account for the library.
8. Enter the client username and password, and then click **Next**.
9. The **Certificate Generation** screen displays the current library certificate, if one exists. Select whether to keep the current certificate or generate a new one and then click **Next**.
10. In the **ESKM Tier Selection** screen, you can group ESKM devices into tiers so the library will attempt to connect with ESKM devices in the top tier first, and then failover to connect with ESKM devices in a lower priority tier if necessary. For example, you might put ESKM devices in the same data center as the library in Tier 1 with ESKM devices in remote data centers in Tiers 2 and 3.
11. One tier is used by default. To add a tier, click **Add Tier**.
12. Enter the IP address or fully qualified hostname and port number for up to six ESKM devices in each tier. To verify access to the ESKM devices, click **Connectivity Check**.
13. When the tier configuration is complete, click **Next**.
14. 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 setting or address issues, either click **Back** to reach the applicable screen or **Cancel** out of the wizard to fix the issues and return later.
15. If the settings are correct and there are no errors, click **Finish**.

Using the KMIP wizard

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

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

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 **Configuration > System > License Key Handling** screen.
- The security user is logged in to the RMI.

Procedure

1. In the **Configuration** area, click **KMIP Wizard** in the **Encryption** menu to start the wizard.
2. The **Wizard Information** screen displays information about the wizard. If the library configuration is complete and the KMIP server is available on the network, click **Next**.
3. The **Certificate Authority Information** screen displays prerequisites for using the KMIP certificate. When the prerequisites are met, click **Next**.
4. The **Certificate Authority Certificate Entry** screen displays instructions for obtaining the certificate for the KMIP server. 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 provides 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 passing for authentication, select **Enable KMIP Certificate-only authentication**.
Only select this option if you are using a KMIP server that requires it and you do not have a client username and password.
7. Click **Next**.
8. The **Certificate Generation** screen displays the current library certificate, if one exists.
 - 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 hostname 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

- ❗ **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.
-

- **Disable Secure Mode for an LTO-6 tape drive**
- **Disable Secure Mode for an LTO-7 or later tape drive**

Prerequisites

FIPS Support Mode prerequisites

Procedure

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

The **Partition FIPS Support Mode Status** screen lists all library 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**.



7. The **Finish** screen lists each partition that will have a configuration change and whether FIPS Support Mode will be enabled or disabled. To complete FIPS Support Mode configuration, click **Finish**.
8. The wizard updates the screen as it configures each partition. When the wizard is finished, click **Exit**.

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.

Procedure

- All library partitions must be defined.
- Encryption configuration must be complete and encryption enabled for the partition. The partition must use library-managed encryption (ESKM, KMIP, or the MSL Encryption Kit).
- All drives in the partition must be LTO-6 or later generation and running a firmware version that supports Secure Mode.
 1. Remove any LTO-5 or earlier generation tape drives from the partition.
 2. 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
 3. 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.

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 disable Secure Mode for all the drives in the partition each time the library is powered off via a soft power off. The library also disables Secure Mode for a drive when it is powered off from the RMI.

Disabling Secure Mode for an LTO-6 tape drive

To disable Secure Mode for an LTO-6 tape drive, verify that the tape drive is installed in the library that enabled Secure Mode and then either power off the drive, or power off or reboot the 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 the OCP or RMI **Configuration > Drives > Settings** screen.
2. Power off the library from the library OCP by holding the power button on the front panel for five seconds.
3. Reboot the library from the RMI **Maintenance > System Reboot** screen.
4. To identify the library that enabled Secure Mode, install the tape drive in any MSL6480 tape library with 4.70 or later firmware or any MSL3040 tape library. The serial number of the library that enabled Secure Mode is shown in the RMI **Status > Drive Status** screen for the drive in the common name (CN) field.

Disabling Secure Mode for an LTO-7 or later tape drive

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.

Configuring local user accounts

Procedure

- **Configure user account settings**
- **Add a local user account**
- **Set or modify a user password**
- **Allow magazine and mailslot access for the “user” user**
- **Remove a local user account**

Configuring user account settings

Procedure

1. Navigate to the **Configuration > User Accounts > User Accounts Settings** screen.
2. Configure the settings to meet the organization 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 (!@#\$%^&**()_+=[]\|;:"<>?,./) - default is 0
- Maximum number of identical consecutive characters - default is Unlimited
- Maximum number of failed logins before password is locked - default is Unlimited
- Maximum number of days before password must be changed - default is Unlimited
- Number of password changes before an old password can be used again - default is Unlimited

3. Click **Enter**.

Adding a local user account

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

Procedure

1. Navigate to the **Configuration > User Accounts > Local User Accounts** screen.
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 or Administrator.
 - **Password**
4. Click **Add**.

Setting or modifying a user password

Procedure

1. Navigate to the **Configuration > User Accounts > Local User Accounts** screen.
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 substring "tr" will return both "administrator" and "Tristan".
3. Enter the user password in both password fields.
4. Click **Modify**.

Allowing magazine and mailslot access for the “user” user

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 to access to the magazines and mailslots.



Procedure

1. Navigate to the **Configuration > User Accounts > User Account Settings** screen.
2. Configure access.
 - a. To allow access the magazines, select **Allow magazine access by the User role**.
 - b. To allow access to the mailslots, select **Allow mailslot access by the User role**.
3. Click **Submit**.

Removing a local user account

Procedure

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

Enabling OCP/RMI session locking

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 is terminated.

When **OCP/RMI Session Locking** is enabled, a new session will not terminate 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 the **Configuration > Web Management** screen.
2. Click **OCP/RMI Session Locking**.
3. Click **Submit**.

Configuring LDAP user accounts

Prerequisites

Prerequisites for configuring LDAP user accounts

Procedure

1. Navigate to the **Configuration > User Accounts > LDAP** screen.
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.
 - b. Enter all of the requested LDAP configuration settings in the **Primary Server** area.



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. 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.
- **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 by your organization, select **Use SSL** and then paste the appropriate CA certificate.

c. Enter the **Secondary/Backup Server** host address and port number.

d. 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
```

e. Enter the Attribute Mapping parameters.

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

f. Click **Test Connection** to verify the configuration.

g. When the library successfully connects to the LDAP server, click **OK**.

3. In the **LDAP User** area, click **Add User**.

4. The RMI displays the **Add User** dialog.

5. Click **Query LDAP Servers** to see a list of available users.

6. Select the user name and then assign the user a role (User, Administrator, or Security). Click **OK**.

Prerequisites for configuring LDAP user accounts

By default the library has three predefined user accounts: administrator, security, and user. 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 a role based on the predefined user accounts, and this role determines the access level for the LDAP user.

Procedure

- 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.



- 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 using the wizard, you will need to know:
 1. IP address and port for the primary and backup LDAP servers
 2. Common Name for the library administrator
 3. Base Distinguished Name and Domain.
 4. Distinguished Name for the library administrator. These are parameters needed to search for potential library users in the LDAP server. For example, `OU=internal,OU=Users,OU=RW,DC=libgroup,DC=local`.
 5. Attribute Mapping, Username. For most Windows Active Directory environments, the **Username** field under **Attribute Mapping** should be set to `sAMAccountName`.
 6. If SSL is required for the LDAP server. This field is likely required for newer versions of LDAP servers.

Configuring Command View for Tape Libraries integration

For more information about Command View TL, see the *HPE StoreEver Interface Manager and 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 the **Configuration > Command View TL** screen. Do not add the CVTL Management Station as an SNMP Target using the **Configuration > Network Management > SNMP** screen.

Procedure

1. Verify that SNMP is enabled.
2. Navigate to the **Configuration > Command View TL Configuration** screen.
3. Configure the library information.
 - **Name**—The name of the library that will be displayed in the Command View TL interface. The default is `HPMSL6480 <serial number>`.
 - **Serial Number**—The serial number of the base module. This cannot be modified.
 - **Management URL**—The URL of the management station, including port. For example: `http://192.0.2.24:8099`.
4. Configure the product information.
 - **Name**—MSL6480. This cannot be modified.
 - **Version**—Library firmware version.
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. If using the Data Verification feature, configure the Data Verification information.



- **Enable Data Verification and 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 Data Verification and the REST interface does not enable full SSH access for the console or other uses.
- **Data Verification and 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**.
- **Data Verification and Library REST Interface Password**—This password must be the same as the Data Verification 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**.

Enabling Data Verification

Procedure

Enable Data Verification from the Data Verification information area of the **Configuration > Command View TL Configuration** screen.

Preparing the library for Data Verification

The Data Verification feature provides an automated process to validate media readability and data integrity of backup data cartridges. Data Verification is a feature of Command View that is supported by the library and requires a license to be installed on the Command View TL management station. Data Verification is only supported with Command View TL 3.8 and newer versions. For more information on Data Verification, see the *HPE Command View for Tape Libraries User Guide* on the [Command View TL website](#).

The Data Verification feature uses a partition called “DVP” for the storage slots and tape drives used for Data Verification. Command View TL moves the cartridges between the storage slots and tape drives in the DVP partition for media verification read purposes. When Command View TL is performing move operations, the library RMI and other library partitions can still be used. This partition is created and configured from the Command View TL interface.

Before enabling Data Verification with Command View TL, prepare the library by freeing up resources needed for the DVP partition and creating a private network for the tape drives and library.

Procedure

1. Use the Expert Partition Wizard to prepare the library for the data verification partition.
 - a. If the library already has a partition named “DVP” that is not used for Data Verification, rename the partition. The partition name “DVP” is reserved for use by Command View TL.
 - b. Unassign the tape drives that will be used for Data Verification from their current partition.
 - c. Unassign the storage slots that will be used for Data Verification from their current partition.
 - d. If you want to use a mailslot to import and export media, verify that a free mailslot is available.
 - e. Verify that each DVP partition has a valid cleaning cartridge with a barcode beginning with “CLN” that can be used for cleaning operations.
2. Create a private network for the tape drives and library that will be used for Data Verification.
 - a. Ensure that each tape drive that will be assigned to the DVP partition has an Ethernet connection to a switch.



NOTE: Use a true switch for the connections from the drives. DO NOT use a hub, which replicates data to all ports on the hub.

- b. Ensure that the DIAG port of the base module controller has an Ethernet connection to a switch.
-

NOTE: Use a true switch for the connections from the drives. DO NOT use a hub, which replicates data to all ports on the hub.

- c. When the private network is cabled correctly, each drive will obtain an IP address from the library on the 16.1.9.X subnet.

The drive IP address can be viewed on the RMI **Status > Drive Status** screen. For a cabling diagram, see the user guide.

If the drive does not report an IP address, check the cabling of the private network and verify that the library is running 4.40 or later firmware.

- d. Verify that no other hosts or network connections are included in the private network. Only the drives that are used for Data Verification should have their Ethernet port connected to the same private network as the library DIAG port.
-

! **IMPORTANT:** Do not cable or connect the FC or SAS ports for drives that are used for Data Verification. These ports must be left uncabled to prevent host interference with Data Verification operations.

Enabling secure communications

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

When SSH is enabled, the library will only accept SSH connections. The default is disabled. A service user login is required to enable SSH.

NOTE: When Data Verification is enabled, Command View TL communicates with the library though SSH even when SSH is disabled in this screen. However, when SSH is disabled in this screen, console and remote access for SSH connections is disabled.

Procedure

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

Adding a signed certificate for SSL/TLS connections

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 Data Verification connections to Command View TL.

NOTE: ESKM and KMIP SSL/TLS connections will not use this certificate because they use a different set of certificates that are paired with the ESKM or KMIP server.

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** screen.
3. Read the **Information** screen and then click **Next**.
4. In the **Certificate Signing Request** screen, create the certificate.
 - a. Enter the information about the library 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 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** screen, click **Next**.
7. In the **Signed Certificate** screen, paste the signed certificate into the **Signed Certificate** pane and then click **Finish**.
8. 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.

Configuring Secure Manager

Secure Manager is a feature for configuring hosts and drives into access control groups that are managed by the library, without requiring modifications to the SAN layout. Secure Manager is a licensed feature and can only be enabled after the license has been added to the library.

Procedure

- **Enable Secure Manager**
- **Create an access group**
- **Change the name of an access group**
- **Delete an access group**
- **Add a host to an access group**
- **Remove a host from an access group**
- **Configure device access**
- **Create a host**



- **Change the name of a host**
- **Delete a host**

Secure Manager

Secure Manager is a feature for configuring hosts and drives into access control groups that are managed by the library, without requiring modifications to the SAN layout. Secure Manager is a licensed feature and can only be enabled after the license has been added to the library.

Secure Manager only supports LTO-4 and later generation FC tape drives. Hewlett Packard Enterprise recommends only including supported tape drives in partitions using Secure Manager.

SAS drives are not supported by Secure Manager and remain visible on the SAN to all hosts. If an unsupported drive is hosting the library control path, the library will also be visible on the SAN. The Secure Manager RMI screens display SAS hosts and SAS drives with gray text. The only Secure Manager function you can perform on the items is to change the name of a SAS host.

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

NOTE: Using Secure Manager with LTO-4 full-height FC tape drives requires the tape drive have version H6EW or later firmware. If Secure Manager is enabled when using an LTO-4 drive with firmware earlier than version H6EW, the drive will remain visible to all hosts.

! **IMPORTANT:** 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 a library that is not using Secure Manager, reset the tape drive access method to the default open state by disabling Secure Manager.

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

Enabling Secure Manager

Procedure

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

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 the **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 RMI that is being used can also be referenced to see the WWPN-to-port association to help determine which servers are attached.

5. In the **Access Group Hosts** screen, 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 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 into the SAN later.

6. Click **Finish**.

Changing the name of an access group when using Secure Manager

Procedure

1. Navigate to the **Configuration > Secure Manager** screen.

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 the **Configuration > Secure Manager** screen.

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 the **Configuration > Secure Manager** screen.

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 into the SAN later. .

Removing a host from an access group when using Secure Manager

Procedure

1. Navigate to the **Configuration > Secure Manager** screen.
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 the **Configuration > Secure Manager** screen.
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

 **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 the **Configuration > Secure Manager** screen.
2. Click **Edit** next to **Host Configuration**.
3. Click **Create Host**, and then click **Next**.



4. Enter a name for the host for use within Secure Manager and the WWPN, and then click **Finish**.

NOTE: The wizard does not verify that the host exists or is accessible.

NOTE: 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 the **Configuration > Secure Manager** screen.
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 within Secure Manager, and then click **Finish**.
5. Click **Submit**.

Deleting a host when using Secure Manager

Procedure

1. Navigate to the **Configuration > Secure Manager** screen.
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 readded if they are rediscovered and added to an access control group.

Maintaining the library

From the Home screen, click or tap on **Maintenance** to access the library maintenance features.

Performing the system test

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 return it to its original slot. You can select the number of cycles for the test. If the test is cancelled, 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 off line.

Prerequisites

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


To remove a tape from a tape drive, first try using the backup application or Move Media command from the OCP or RMI. If neither of these methods work, see **Forcing a drive to eject a cartridge.**

Procedure

1. Navigate to the **Maintenance > Library Tests > System Test** screen.
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

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.

 **CAUTION:** The test can move cartridges between partitions.

For service and diagnostics, use the robotic test. See **Performing the robotic 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.

Procedure

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

Performing the element to element test

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.

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.

Procedure

1. Navigate to the **Maintenance > Library Tests > Element to Element Test** screen.
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 into 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


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

Performing the wellness test

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

 **CAUTION:** The test can move cartridges between partitions. Especially if the library is configured for encryption, ensure that all cartridges are returned to their original partitions after the 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.
- Each library module must have at least one cartridge installed.
- All backup operations are stopped.

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

Procedure

1. Navigate to the **Maintenance > Library Tests > Wellness Test** screen.
2. Click **Start Test**.

Performing the robotic test

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

Procedure

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

Testing and calibrating the OCP

Procedure

- **Test the front panel LEDs**
- **Calibrate the front panel touch screen**

Testing the front panel LEDs

Procedure

1. Navigate to the **Maintenance > Library Tests > OCP Test** screen.
2. Select **LED Test**.
3. Click **Start**.
4. Follow the instructions on the screen.

Calibrating the front panel touch screen

Procedure

1. Navigate to the **Maintenance > Library Tests > OCP Test** screen.
2. Select **Touch Panel Calibration**.
3. Click **Start**.
4. Follow the instructions on the screen.



Viewing log files

Procedure

1. Navigate to the **Maintenance > Logs and Traces > View Logs** screen.
2. Select one of the logs.
 - a. **Event Ticket Log**—Records library error and warning events
 - b. **Information Log**—Records library information warnings
 - c. **Configuration Log**—Records configuration changes
3. **Show All**—Displays all of the above logs.

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.

The format for the date and time is: YY.MM.DD HH.MM.SS.s.s.

- YY.MM.DD—The date displayed as Year.Month.Day
- HH.MM.SS.ss—The time displayed as Hour.Minute.Second.Hundredths of a second

Downloading log and trace files

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. From the RMI, navigate to the **Maintenance > Logs and Traces > Download Logs and Traces** screen.
2. Click **Save**.

Managing library firmware

The firmware version currently installed on the library is displayed in the library status area on the Home page. Update the library firmware from the **Maintenance > Firmware Upgrades > System Firmware** screen.

NOTE: The library only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.

When you update the library firmware, the library will update the firmware of the expansion modules to a compatible version.

Procedure

- **Update library firmware from the RMI**
- **Update library firmware from the OCP**



Updating library firmware from the RMI

Procedure

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

When you update the library firmware, the library will update the firmware of the expansion modules to a compatible version.

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. In the OCP, navigate to the **Maintenance > Firmware Upgrades > System Firmware** screen.
4. Insert the USB thumb drive into the USB port on the front of the library.
5. The library detects the USB drive.
6. Select the firmware file.
7. Click **Start Upgrade**.

When you update the library firmware, the library will update the firmware of the expansion modules to a compatible version.

Managing drive firmware from the RMI

Drive firmware can be updated on multiple drives of the same type at the same time. Drive firmware can only be updated from the RMI. Each drive will only accept appropriate firmware.

Procedure

1. In the RMI, navigate to the **Maintenance > Firmware Upgrades > Drive Firmware** screen.
2. The tape drives are organized by drive type.
3. Expand the appropriate drive type and select one or more of the tape drives.
4. Click **Choose File**, and then select the firmware file from the local computer.
5. Click **Submit**.

More information

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



Downloading a tape drive support ticket

Procedure

1. Navigate to the **Maintenance > Download Support Ticket** screen.
2. Expand the drive support ticket list, if necessary, by clicking the down arrow on the left side. The drive list displays:
 - **Drive**—The drive number. Drives are numbered starting with one from the physical bottom of the library to the top.
 - **Type**—The drive form factor (half height or full height) and interface
 - **Firmware**—The current drive firmware version
 - **Serial**—The drive serial number
 - **Unit**—The module containing the tape drive
 - **Partition**—The logical library associated with the tape drive
3. 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 are 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.

NOTE: Drive support tickets can only be pulled for LTO-4 and later generation tape drives.

4. Select the drive.
5. Click **Save**.

Downloading a library support ticket

Procedure

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



Rebooting the library

Procedure

From the **Maintenance > System Reboot** screen, click **Reboot**.

Rebooting a tape drive

Procedure

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

Controlling the UID LED

The UID LEDs are a pair of blue LEDs—one on the OCP and the other on the base module controller. The UID LEDs are useful for identifying the library in a data center. The UID LEDs are operated synchronously and controlled by the user.

Procedure

1. Navigate to the **Maintenance > UID LED Control** screen.
2. To change the LED status, click the **On** or **Off** button.
3. Click **Submit**.

Moving the robotic assembly to the base module

Before extending a module from the rack, the robotic assembly must return to its park position in the base module. Under normal circumstances, when the library is powered off using the front power button the robot automatically parks and locks into the base module behind the OCP. After powering off the library and before proceeding with extending a module from the rack, look inside the base module window to verify that the robotic assembly is behind the OCP.

If the library did not move the robotic assembly to its park position, you can do so from the screen.

Procedure

1. Navigate to the **Maintenance > Move Robotic to Base Module** screen.
2. Click **Submit**.

Calibrating the library

The Auto Calibration routine is only needed in some corner case situations. Auto calibration should not be run as part of normal setup or configuration. Only run auto calibration if instructed to do so by a service engineer.

NOTE: The Auto Calibration routine can take up to 15 minutes per module. The library will be offline to hosts while the routine is running.



Procedure

1. Navigate to the **Maintenance > Auto Calibration** screen.
2. Click **Start Auto Calibration Wizard**.
3. Select the modules for calibration.
4. Click **Finish**

Operating the library

Click or tap the **Operations** button on the Home screen to access the operations features.

Moving media

Procedure

1. Navigate to the **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.

Tape drives are listed at the top of each element list and listed in the order of their drive numbers. Tape drives are numbered from the physical top of the library starting with Drive (1).

Slots are listed in the order of the slot numbers. Slots are numbered $m . s$, where m is the module number and s is the slot within the module.

3. To see a subset of the cartridges in the library, click **Barcode Filter On**, enter some or all of 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 of 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 the mailslot



WARNING MOVING PARTS: Hazardous moving parts exist inside this product. Do not insert tools or any portion of your body into the interior of the library through the mailslot safety door.

Procedure

1. Navigate to the **Operation > Open Mailslot** screen.
2. Click **Open** for the appropriate mailslot and then click **Submit**.



The library will release the lock. On the MSL3040, the library will illuminate the magazine release button LED.

3. Pull the mailslot out of the library to access the mailslot.

NOTE: The mailslot will relock after 30 seconds.

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.

Opening a magazine



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

-
- 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 a magazine, 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 the **Operation > Open Magazine** screen.
2. Click **Open** for the magazine.

The library will release the lock.

The library will release the lock. On the MSL3040, the library will illuminate the magazine release button LED.

3. When the OCP displays a message saying that the magazine has been unlocked, open the door and pull the magazine out of the library to access the storage slots.



WARNING: To avoid damaging the library, wait until the OCP displays a message saying that the magazine has been unlocked before pulling the handle.

Unlocking multiple magazines

Normally the library inventories each opened magazine when it is closed. With the Unlock Multiple Magazines wizard, you can access multiple magazines without an inventory between magazines. Only one magazine in the library can be open at a time.

Procedure

1. From the OCP, navigate to the **Operation** screen.
2. Click the **Unlock Multiple Magazines** wizard.
3. Follow the instructions on the screen.

Cleaning a tape drive

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** screen or configure auto cleaning from one of the partition wizards.

Procedure

- **Configure auto cleaning**
 - **The auto cleaning feature**
- **Initiate a drive cleaning operation**

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 of the cleaning cartridges, the library will choose the one with the highest usage count.



Configuring auto cleaning

You can configure auto cleaning with the basic or expert 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.

Procedure

- [Use the basic partition wizard](#)
- [Use the expert partition wizard](#)

Initiating a drive cleaning operation

Procedure

1. Navigate to the **Operation > Clean Drive** screen.
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 a tape drive not listed, move the cartridge out of the drive.
6. Click **Submit**

Rescanning the cartridge inventory

Procedure

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

The library will change to Scanning status and will be unavailable to perform other operations until the scan is complete. The library displays a progress indicator in the top banner while performing a full library inventory.

Forcing a drive to eject a cartridge

The force drive media eject operation attempts to force the tape drive to eject the cartridge and place it into an open slot. Access to this feature requires the administrator password.

Before performing this operation, attempt to eject the data cartridge using the backup software or using the library move media operation through the RMI or OCP. 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 the **Operation > Force Drive Media Eject** screen.
2. Select the drive in the **Source Elements** list.



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

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,

Viewing status information

To access the status area, from the Home screen, click or tap **Status**.

Viewing library and module status

Procedure

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

Status > Library Status screen parameters

Library information

- **Vendor**—HP
- **Serial Number**—Library serial number
- **Robotic Hardware Revision**
- **Barcode Reader Hardware Revision**
- **WWide Node Name**—A worldwide unique identifier that the library reports over SCSI and can be used by operating systems or software applications to identify and track the library.
- **Product ID**—MSL6480
- **Firmware Revision**—Version of the currently installed library firmware
- **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 Firmware Revision**—Version of the currently installed barcode reader firmware. The barcode reader firmware is bundled and installed with the library firmware.

Library status



- **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.
- **Cartridge in Transport**—When applicable, displays the barcode label of the cartridge currently in the robotic assembly
- **Total Power On Time**—Total time that the base module has been powered on since it was manufactured
- **Odometer**—Robotic assembly move count
- **Robotic Location**—The module where the robotic assembly is currently located. The home location for the robotic assembly is in base module behind the OCP.
- **Shipping Lock**—The shipping lock is part of the robotic assembly. Under normal operation, the library will lock and unlock the shipping lock as needed when the robotic assembly is in the base module. For instructions on locking or unlocking the shipping lock manually, see the user guide.

Module status

- **Base Controller Revision** or **Module Controller Revision**—Hardware revision of the controller board currently installed in the module.
- **Power Supply Status**—Displays the status of power redundancy.
- **Lower Power Supply Fan**—Displays the status of the lower power supply fan. If a fan is not operating correctly, the library generates a warning event.
- **Upper Power Supply Fan**—Displays the status of the upper power supply fan. If a fan is not operating correctly, the library generates a warning event.
- **Left Drive Power Board Status**—Status of the drive power board (DC-DC converter) for the top three half-height drive slots in the module.
- **Right Drive Power Board Status**—Status of the drive power board (DC-DC converter) for the lower three half-height drive slots in the module.
- **Chassis Fan**—Displays the status of the chassis fan. If a fan is not operating correctly, the library generates a warning event.

Using the cartridge inventory modular view

Procedure

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

Using list views

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 the **Status > Cartridge Inventory > List View** screen.
 - To see the elements organized by logical library or partition, navigate to the **Status > Partition Map > List View** screen.
2. In the Inventory List you can see:
 - **Module**—The module number
 - **Slot #**—The slot number in the form `<module>.<slot>`, where `module` is the module number and `slot` is 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**.
7. To see all elements, click **Partition** or **Slots**.
8. To change list grouping, click **Group on** or **Group off**.

When the list is grouped, you can expand or contract the list for each group by clicking the triangle next to the number in the first column. Grouping is enabled by default.

To disable grouping, click **Group off**.

To enable grouping, click **Group on**.

Using the partition map graphical view

Procedure

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

This screen displays a graphical representation of the cartridges in the storage slots, mailslots, and tape drives for each module.
2. Expand the module section to see the map for that module.



The partition number is shown for each element.

3. Hover over an element for status and configuration information about the partition or drive.

Viewing library or partition configuration settings

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

Procedure

1. Navigate to the **Status > Partition Map > Configuration Status** screen.

The library displays the current configuration settings for a partition.

2. Expand the sections for additional information.

Configuration Status screen parameters

- **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 12345678, if alignment is left, the library will report 123456. If alignment is right, the library will report 345678.
- **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.
- **Control Path Failover**
 - **Basic** when basic control path failover is enabled.
 - **Advanced** when LTO-6 advanced control path failover is enabled.
 - **LTO7+ CPF** when LTO-7+ control path failover is enabled.
 - **Disabled** when control path failover is not enabled.
 - **Unlicensed** when a control path failover license has not been added to the library.
- **Active Control Path Drive**—The tape drive that hosts the LUN for the partition.



- **Passive Control Path Drive**—The tape drive that the library will use as an alternate if control path failover is enabled and there is a failure of the active control path drive.
- **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 each drive installed in the library.

Drive Status configuration settings

- Drive number—Drives are numbered starting with one from the bottom of the library up. 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 3—Ultrium 920, Ultrium 960
 - LTO 4—Ultrium 1760, Ultrium 1840
 - LTO 5—Ultrium 3000, Ultrium 3280
 - LTO 6—Ultrium 6250
 - LTO 7—Ultrium 15000
 - LTO 8—Ultrium 30750
- Drive form factor
 - HH—Half height
 - FH—Full height
- Drive interface
 - FC—Fibre Channel
 - SAS—Serial Attached SCSI
- Status icon
 - A green circle with a check mark indicates that the drive is fully operational and that no user intervention is required.
 - A yellow triangle with an exclamation point indicates that user attention is necessary, but that the drive can still perform most operations.
 - A red circle with an **X** indicates that user intervention is required or the drive is not capable of performing some operations.
- 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.
- **Encryp**—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
- **Powered**—On or Off
- **Product ID**—Indicates the LTO generation
- **Temperature**—Internal temperature reported by the drive. The normal temperature range is provided for reference and varies depending on the type of tape drive. The tape drive will send out errors if there is any possibility of error due to temperature.

NOTE: This temperature is not the temperature of the tape path in the drive nor is this value the operating environment temperature.

- **Encryption**—Indicates whether the drive is configured for encryption with the encryption kit.
- **IP Address**—IP address of the drive Ethernet port. When the library is configured for Data Verification and the private network with the tape drive and library DIAG port is cabled correctly, the drive obtains an IP address from the library on the 16.1.9.X subnet.

If Data Verification is configured and the drive does not report an IP address, verify the cabling of the private network and ensure that the library is running the latest version of firmware.
- **Module Loc**—Module in which the drive is installed
- **Cooling Fan Status**—When the drive cooling fan is operating correctly, the status will be **Active**.
- **Personality**—A service engineer might request this information.
- **Control Path Failover**
 - **Basic**—Basic Control Path Failover is enabled. The Active and Passive drives are designated.
 - **Disabled**—Control path failover is not enabled for the drive.
 - **Unlicensed**—A control path failover license has not been added to the library.
 - **Advanced**—LTO-6 advanced control path failover is enabled for the drive. The Active and Passive drives are designated.
 - **LTO7+ CPF**—LTO-7+ control path failover is enabled for the drive. The Active and Passive drives are designated.
- **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. 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.
- **Data Compression**—Indicates whether the drive is using data compression.
- **Data Path Failover**
 - **Basic**—Basic Data Path Failover is enabled.
 - **Advanced**—LTO-6 advanced data path failover is enabled.
 - **LTO7+ DPF**—LTO-7+ data path failover is enabled.
 - **Disabled**—DPF is not enabled for the drive.
 - **Unlicensed**—A Data Path Failover license has not been added to the library.
- **Fibre Channel Fabric Log-in Name** (LTO-6 only)
- Port configuration (FC only)—Drive port status
 - **WWPN**—Displays the worldwide port name, a unique identifier for each FC interface.
 - **Speed**—Displays the current interface speed.
 - **Port Type**
 - **Automatic**
 - **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.
 - **Fibre Channel Fabric Log-in Name** (LTO-6 only)
- **Secure Mode**—Indicates whether the drive is running in Secure Mode.

Viewing network status

Procedure

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

Network Status screen parameters

- **Host Name**—Library hostname
- **Domain Name**
- **Protocol**—IPV4 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



IPv4 settings

- **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 was 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**
- **DNS 2**

IPv6 settings

- **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.
- **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**—Base module serial number reported to Command View TL.
- **Management URL**—Management station URL, including port. For example: <http://192.0.2.24:8099>.

Product information

- **Name**—Product name reported to Command View TL. Will always be MSL6480.
- **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



Viewing encryption status

Procedure

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

Encryption status parameters

- **USB—MSL Encryption Kit**—Status of the key server token.

NOTE: The key server token should only be inserted in the **rear** USB port in the base module.

- **KMIP**—Status of the connection to the KMIP server.
- **Key Server Token Status**—Identity of the key server token, if any, present in the rear USB port
- **Partition Encryption Status**—Configured encryption method for each partition. The library only uses one encryption method at a time.
- **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 the **Status > Secure Manager** screen to see the currently defined Secure Manager access groups.

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 one from the bottom of the library up.
- LTO generation
 - **LTO3**—Ultrium 920, Ultrium 960
 - **LTO4**—Ultrium 1760, Ultrium 1840
 - **LTO5**—Ultrium 3000, Ultrium 3280
 - **LTO6**—Ultrium 6250
 - **LTO7**—Ultrium 15000
 - **LTO8**—Ultrium 30750
- 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.



Upgrading and servicing the library



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the library.

Read all documentation and procedures before installing or operating the library.

Hazardous moving parts exist inside this product. Do not insert any tools or any part of your body into the tape library while it is operating.



CAUTION: Slide/rail mounted equipment is not to be used as a shelf or a work space.



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.



WARNING: Each library module weighs 41 kg (90 lb) without media or tape drives and 71.4 kg (157.4 lb) with media (80 cartridges) and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the device:

- Observe local health and safety requirements and guidelines for manual material handling.
- Remove all tapes to reduce the overall weight of the device and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
- Obtain adequate assistance to lift and stabilize the device 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.

Possible tools needed

- #1 Phillips screwdriver—removing drive bay covers
- #2 Phillips screwdriver—securing or removing the round-hole rack adapter bracket
- T10 Torx driver—securing retention inserts in square-hole racks
- Small flat head or Torx screwdriver—retracting the locking screen when moving a library cover, using the magazine manual release
- Small flat head screwdriver—removing a magazine access door
- Clip nut installation tool—inserting or removing clip nuts in square-hole racks while installing or removing rack rails



Identifying a failed component

Procedure

1. Activate the UID (Unit Identification) LEDs from the **Maintenance > UID LED Control** screen.

The blue LED on the front and rear of the base module will illuminate and identify the library containing the failed component.

2. Identify the module within the library that contains the failed component.
 - a. In the upper left corner of the Home screen, locate the module that indicates an error.
 - b. Click or tap the module for information about the failed component.

NOTE: When locating a failed drive power board, there are two drive power boards in each module; the screen will indicate whether the left or right drive power board (as seen from the rear of the library) has failed. On the failed board itself, the amber LED might be illuminated and visible through the fan grating.

Moving a module within the rack or to a nearby rack

Use this procedure when you are moving one or more modules within a controlled environment. In this case, the modules are removed from the rack and each moved individually, if necessary, on sturdy carts in the same area.

Do not use this procedure if the whole rack is being moved or if a module is being transported on a vehicle or between buildings. In these cases, use the shipping procedure applicable to your situation. See **Library shipping procedures**.



WARNING: Each library module weighs 41 kg (90 lb) without media or tape drives and 71.4 kg (157.4 lb) with media (80 cartridges) and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the device:

- Observe local health and safety requirements and guidelines for manual material handling.
- Remove all tapes to reduce the overall weight of the device and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
- Obtain adequate assistance to lift and stabilize the device during installation or removal.



WARNING: When removing a module from the rack or placing a module into a rack, to reduce the risk of personal injury or damage to equipment:

- Extend the rack 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.
-



Procedure

1. Save the library configuration.
2. Remove the data cartridges from the tape drives and magazines, and power off the library.
3. Disconnect the power cords and cables, and unlock the alignment mechanisms.
4. Remove the modules from the rack.
5. Remove the rack rails from the rack.
6. Verify that the destination rack is level side to side and front to back.
7. Install the rack rails in the destination rack.
8. Install the modules in the rack.
9. Replace the cables and lock the alignment mechanisms.
10. Connect the power cords, power on the library, and verify the operation.
11. Replace the data cartridges.

For instructions for these steps, see [Replacing a module](#) and [Installing the library](#).

Installing or replacing a tape drive



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the library.

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

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the drive bay openings.

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 FC drive**.
5. **Verify the tape drive installation**.

Removing a tape drive

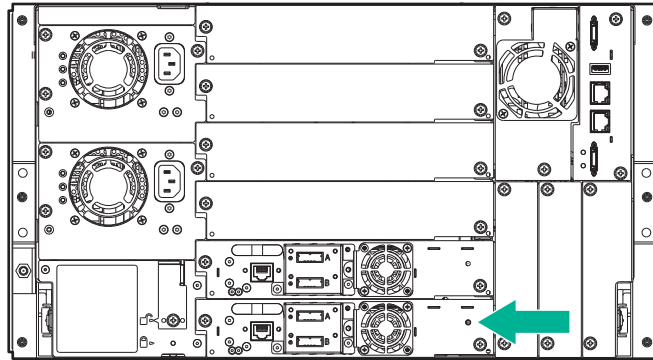
Procedure

1. Verify that the tape drive does not contain a cartridge.
Use the operator control panel (OCP) or the remote management interface (RMI) to move the cartridge to a storage slot or mailslot.
2. Verify that backups are not occurring on the drive you are replacing.

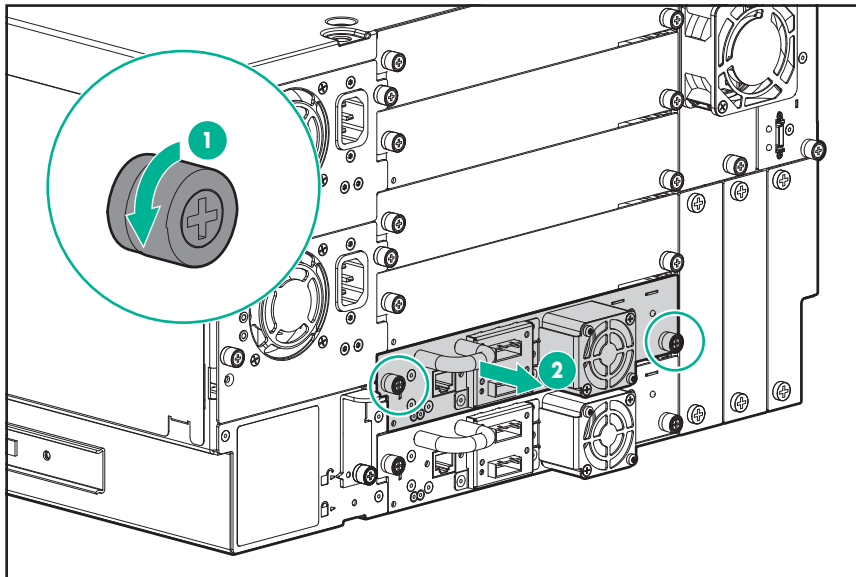


If backups are occurring on another drive and you are replacing the master drive, verify that the library will not be accessed through this drive while the drive is being replaced.

3. Use the OCP or RMI to power off the drive.
4. Verify that the LED on the tape drive back panel is off.



5. Remove all cables from the tape drive.
6. Loosen the blue captive thumbscrews on the tape drive. Pull straight back on the tape drive handle while supporting the bottom of the drive to remove it from the library.



CAUTION: Support the bottom of the tape drive when removing it to avoid damaging any of the internal connections.

Removing a drive bay cover

Procedure

1. Identify the location for the tape drive.

Install the first tape drive in the bottom drive bay. Install an additional drive in the next higher open drive location.





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.

Installing the new tape drive

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.
The tape drive is fully inserted when its back panel is flush with the back panel of the library.
3. To secure the tape drive to the chassis, use a torque driver to tighten the blue captive 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.

Verifying the tape drive installation

Procedure

1. To ensure proper operation, install a drive bay cover on any unused drive bay.
2. Power on the drive from the OCP or RMI, if necessary.
3. Confirm that the library recognizes the new tape drive by checking the System Status screen on the OCP.
If recognized, the new drive will show `Ready`, `RDY`, or `Empty` status.
4. Use Library & Tape Tools (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>
5. Use the OCP or RMI to verify that the library sees the tape drive and to update the drive firmware, if necessary.

Adding an expansion module



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.





WARNING: Each library module weighs 41 kg (90 lb) without media or tape drives and 71.4 kg (157.4 lb) with media (80 cartridges) and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the device:

- Observe local health and safety requirements and guidelines for manual material handling.
 - Remove all tapes to reduce the overall weight of the device and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
 - Obtain adequate assistance to lift and stabilize the device 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.
-

Procedure

1. **Power off the library.**
2. **Install the rails in the rack.**
3. **Move a cover to the expansion module.**
4. **Install the module in the rack.**
5. **Verify the installation and configuration.**

Powering off the library

Procedure

1. Verify that all host processes are idle.
2. Power off the library from the front panel. Depress the power button for 5 seconds and then release it. If the library is idle, you can release the button when the Ready LED begins flashing.

With firmware versions 4.40 and newer, select **The default parked position.**

If the library does not perform a soft shutdown, depress and hold the power button for 10 seconds.

3. Verify that the robotic assembly is located in the base module behind the OCP.

Installing the rails in the rack

Procedure

1. Clear 6U in the rack directly over or under the library, if necessary.



Module and rack layout guidelines

2. Install the rails in the rack.

For instructions, see [Installing the rack rails](#).

Moving a cover to the new module

Procedure

The library has removable top and bottom covers. When adding a module, you must move either the top or the bottom cover to the new module. The two covers are identical and the process for removing and installing them is the same for the top and bottom of the module. See [Preparing the top and bottom modules](#) for details; while this procedure refers to moving a cover from the base module, the information is the same for moving a cover from an expansion module.

Installing the module

Procedure

1. Install the module in the rack.
 - a. Extend the rack rails.
 - b. Slide the module into the rack.
 - c. Verify that the new module is properly aligned and then secure the module to the rack.

For illustrated instructions, see [Installing the expansion modules in the rack](#).

2. Align and connect the module.

Aligning the new module with the library ensures that the robot can move freely between the modules. The library will not operate unless the alignment mechanism is in the locked position.

For illustrated instructions, see [Aligning and connecting modules](#).

3. Connect the power cords.

Plug the power cords into the two power supplies in the new module.



TIP: The module has dual redundant power supplies. To increase redundancy, plug each power cord into a different AC power circuit.

Verifying the installation and configuration

Verify that the library powers on and initializes correctly, and that the status is Ready. From the OCP or RMI, verify that the new module is visible.

Check the library configuration settings related to the additional storage slots, mailslots, and tape drives, and update if necessary.

The expansion module will operate using the existing library firmware. Hewlett Packard Enterprise recommends always updating the library to the latest firmware version. You can download the latest library firmware from the Hewlett Packard Enterprise Support website: <https://www.hpe.com/support/hpesc>.

You can update firmware from the RMI or OCP **Maintenance > Software Upgrades > System Firmware** screen.



Replacing a power supply

- ⚠ 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.

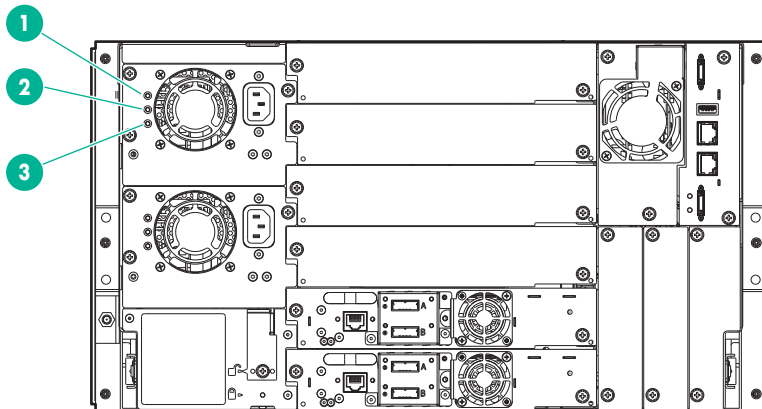
Procedure

1. **Prepare to remove the power supply.**
2. **Remove the power supply.**
3. **Install the new power supply.**
4. **Verify the power supply installation and operation.**

Preparing to remove the power supply

Procedure

1. Locate the failed power supply on the rear of the library by the LEDs; either the amber LED (2) will be illuminated or none of the three LEDs will be illuminated.



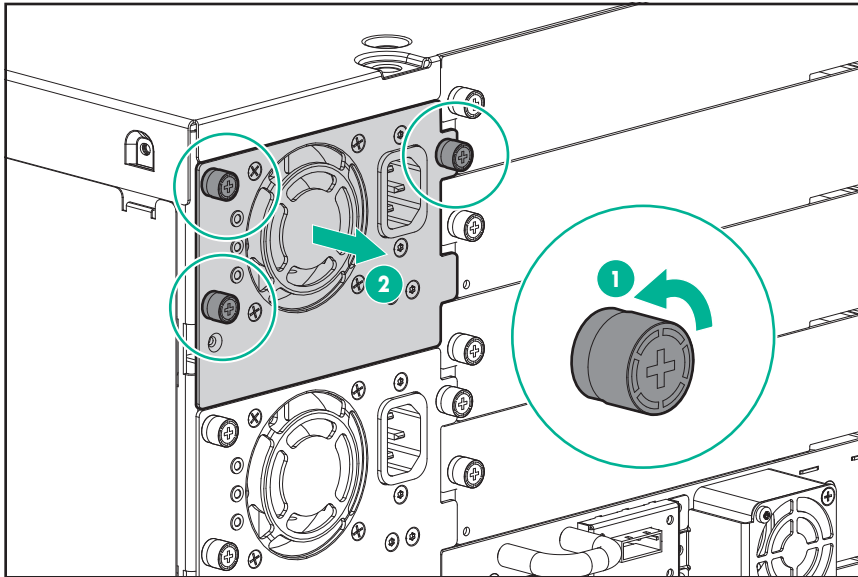
2. Unplug the AC power cord from the power supply you are replacing.

Removing the power supply

Procedure

1. Loosen the three blue captive thumbscrews with your fingers on the power supply.
2. Using the thumbscrews (one on each side), slowly pull the power supply approximately 10 cm (4 inches) from the back of the library.
3. Use one hand to remove the power supply from the module while using the other hand to support the bottom.

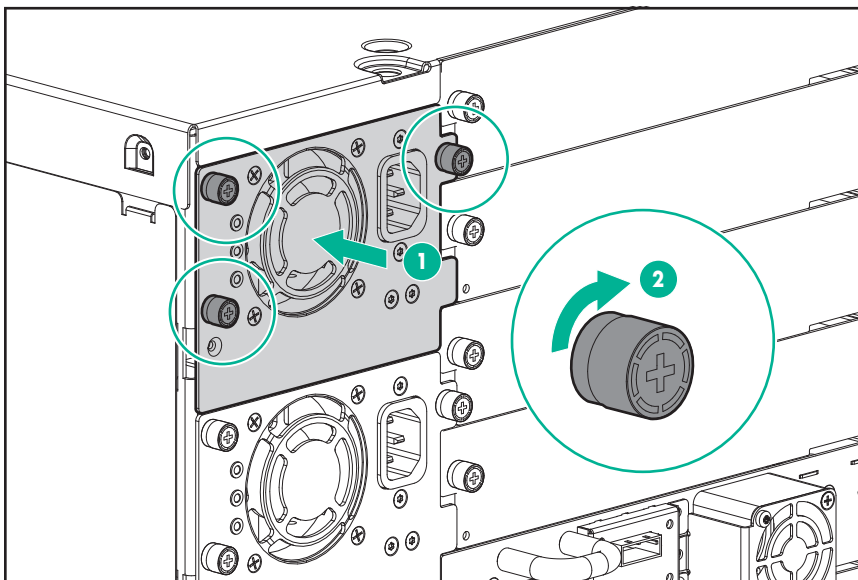




Installing the new power supply

Procedure

1. Position the new power supply onto the alignment rails.
2. Slide the power supply into the library until it is flush with the back panel of the library.
3. Tighten the blue captive thumbscrews with your fingers to secure it to the library.
4. Attach the AC power cord to the new power supply.



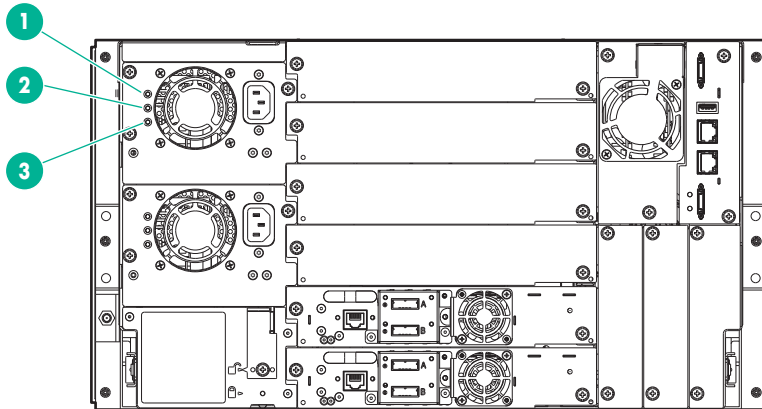
Verifying the power supply installation and operation

Procedure

1. Verify that the new power supply is operating properly by checking the power supply LEDs:



- a. The white (1) and green (3) LEDs should be illuminated.
- b. The amber (2) LED should not be illuminated.



2. Using the OCP or RMI, confirm that the power supply is operating correctly; the event that indicated the power supply was faulty should be cleared.
3. If the UID LEDs are still illuminated, deactivate them using the OCP or RMI.

Replacing a controller board

-
- ⚠ **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.
-
- ⚠ **CAUTION:** Power off the library before installing or replacing this part or damage may occur.
-
- ⓘ **IMPORTANT:** Do not replace both the base chassis and the base module controller with repair components in the same procedure. If both components are replaced at the same time, the firmware will prevent the library from operating. The library WWID and serial number are saved in the controller and within the chassis. When one is replaced, the data from the original component is transferred to the repair component. If replacing both the base chassis and base module controller, you must power cycle the library between component replacements.
-

Procedure

1. **Save the configuration.**
2. **Power off the library.**
3. **Prepare to remove the controller board.**
4. **Remove the controller board.**
5. **Install the replacement controller board.**



6. Verify the replacement.

7. Power on the library.

Saving the configuration

The library configuration settings are on the library chassis and will be restored automatically when the controller is replaced. However, Hewlett Packard Enterprise recommends saving the configuration settings before removing the controller board.

More information

Saving the library configuration

Powering off the library

Procedure

1. Verify that all host processes are idle.
2. Depress the power button on the front panel for 5 seconds and then release it.
If the library is idle, you can release the button when the Ready LED begins flashing.

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

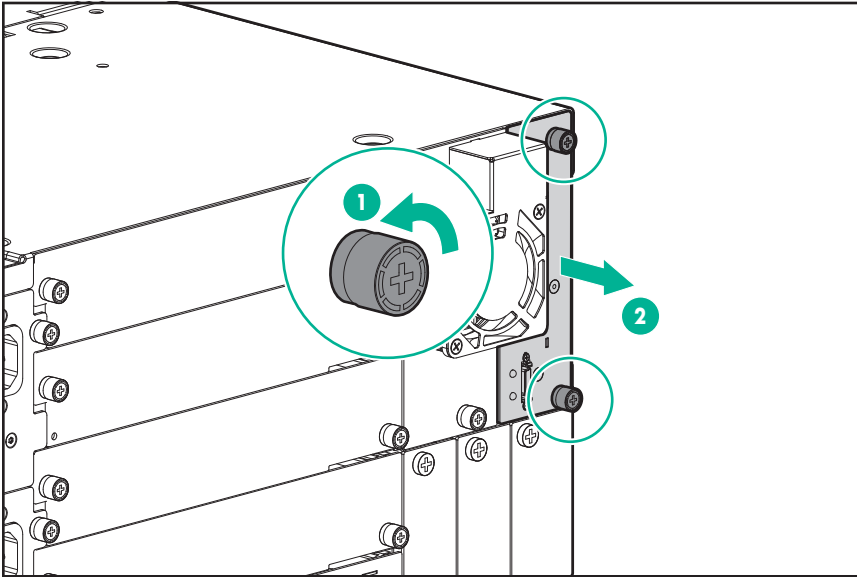
1. Unplug the AC power cables from the module containing the failed controller board.
2. Remove the Ethernet cables, module interconnect cables, and the USB device from the failed module controller board, if present. (An expansion module will not have Ethernet or USB ports.)

Removing the base or expansion module controller

Procedure

1. Loosen the two blue captive thumbscrews on the controller.
2. Using the thumbscrews, slowly remove the controller from the library.
3. Place the controller in a static safe bag.

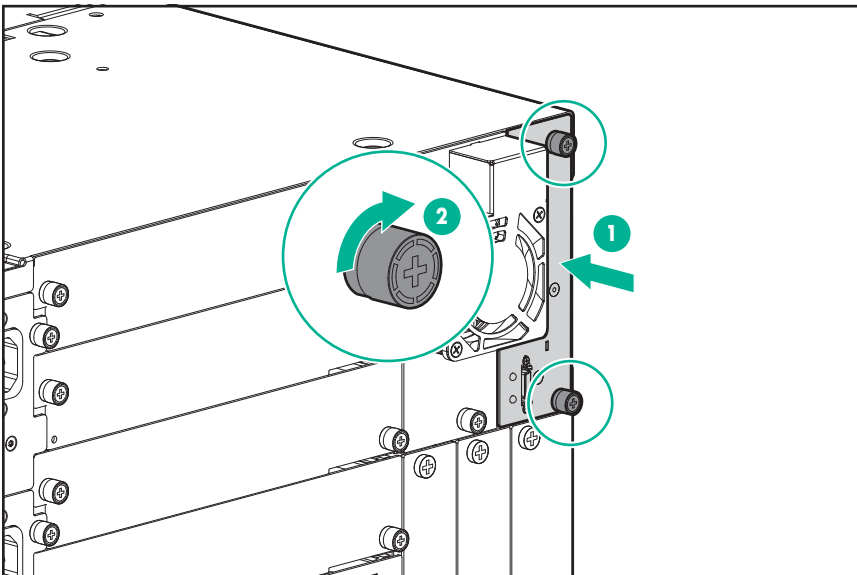




Installing the base or expansion module controller

Procedure

1. Position the new controller on the alignment rails.
2. Slide the controller slowly into the library until it is flush with the back panel of the library.
3. Tighten the blue captive thumbscrews with your fingers to secure it to the library.
4. Replace the expansion interconnect cables, the Ethernet cable, and the USB device removed previously.
5. Plug in the AC power cables.



Verifying the module controller replacement

Procedure

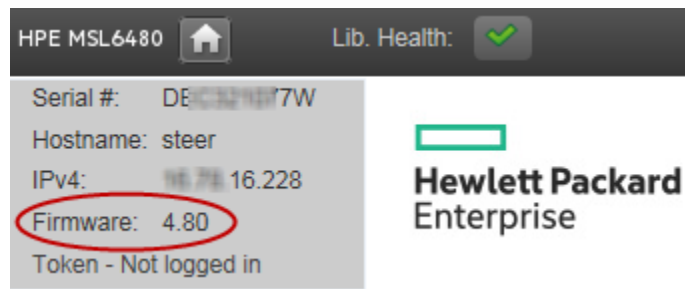
1. Power on the library.

The library will check the firmware version for each of the library modules and install the firmware version from the base module controller on any expansion module controllers that have a different firmware version. This process can take up to 30 minutes depending on the configuration.

- a. If the base module controller was replaced, and replacement has a different firmware version, the library will automatically install the firmware version from the base module controller on any modules with a different version. If the replacement base module controller had an earlier firmware version than the library, this can result in downgrading the firmware in all the expansion modules.
- b. If an expansion module controller was replaced, the library will update the expansion module firmware, if necessary, to match the rest of the library modules.

When this update process completes, the library will reboot itself.

2. The first time the library boots with the new base module controller, the library displays the OCP calibration test. Complete the touch-panel calibration test, ensuring that you only press the location on the OCP that is requested by the test.
3. Using the OCP or RMI, click or tap **Status > Hardware Monitoring** to view the controller status.
4. Using the OCP or RMI, check for events; the event that indicated the controller was faulty should be cleared.
5. Verify that the library has the most up-to-date firmware revision. To find the version of firmware installed on the library, check the upper left corner of the OCP or RMI.



6. If replacing the base module controller, upgrade the firmware if necessary.
To find the most up-to-date firmware version, visit the <https://www.hpe.com/support/hpesc> website. If necessary, download the firmware files.
Update the firmware from the RMI **Maintenance > Software Upgrades > System Firmware** screen.
7. If replacing the base module controller, verify that the configuration settings are correct. If necessary restore the settings from a file of saved settings, or re-enter them using the OCP or RMI.
 - a. If the library has licensed features, verify that the license information was retained and then re-enable the features if necessary.
 - b. Verify the date, time, and timezone information and reset them if necessary.
 - c. Update any configuration settings that changed since the settings were saved.
8. If using the encryption kit, re-enter the PIN.



9. If the UID LEDs are still illuminated, deactivate them using the OCP or RMI.

10. Resume the host applications.

Powering on the library

Procedure

Power on the library by pressing the power button on the base module just below the OCP; the green light will illuminate. When the library is powered on, it inventories the data cartridges in the magazines, checks the firmware version on all modules, configures the tape drives, confirms the presence of the existing modules, and searches for any new modules.

Replacing the chassis fan assembly

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.

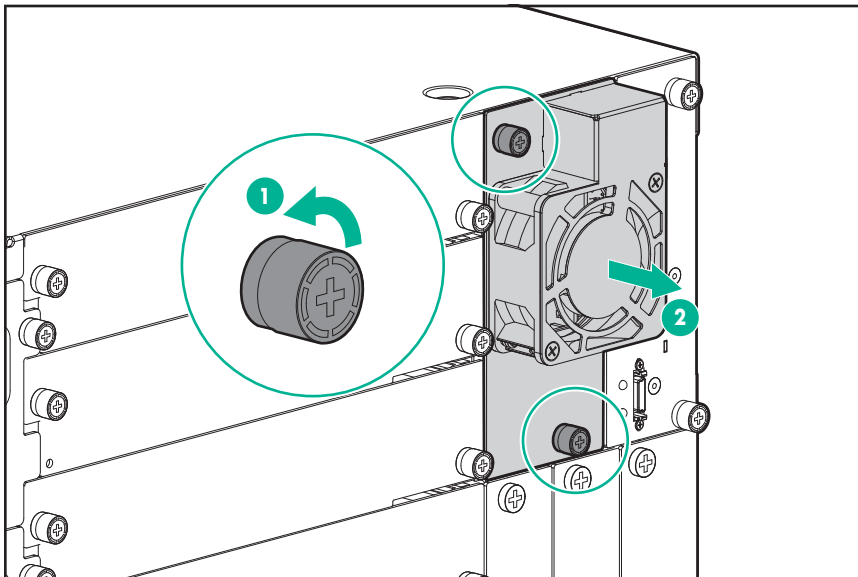
Procedure

1. **Remove the chassis fan assembly.**
2. **Install the new chassis fan assembly.**
3. **Verify the installation.**

Removing the chassis fan assembly

Procedure

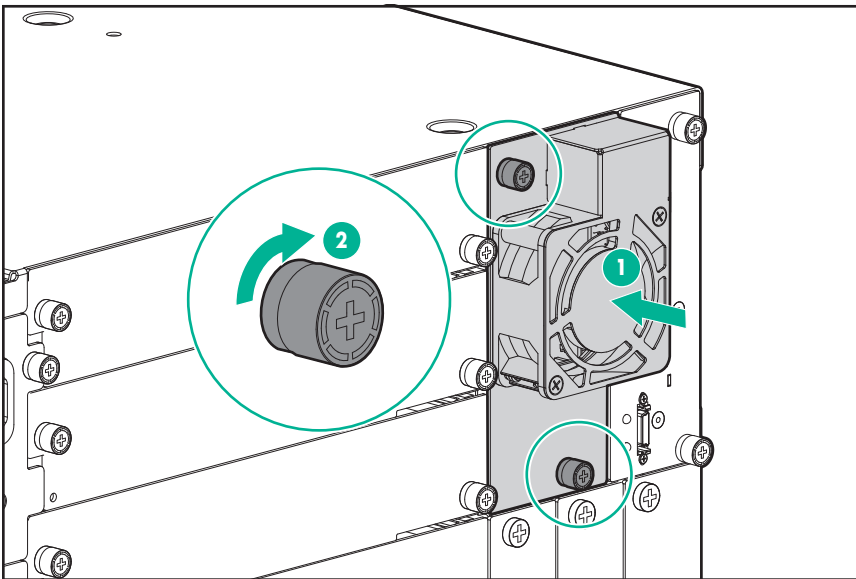
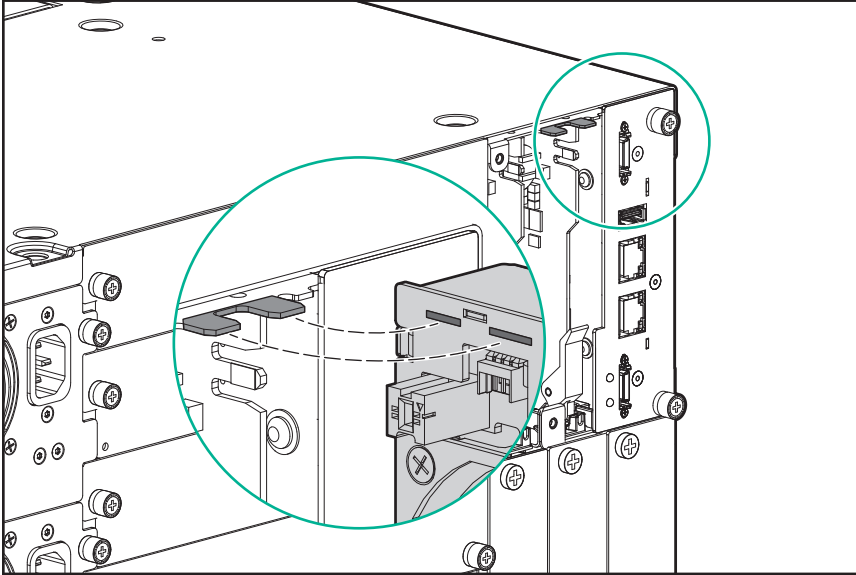
1. Loosen the two blue captive thumbscrews on the chassis fan assembly.
2. Using the thumbscrews, slowly remove the chassis fan assembly from the library.



Installing the new chassis fan assembly

Procedure

1. Align the tabs on the library with the slots at the top of the chassis fan assembly.
2. Push in the chassis fan assembly until it is flush with the back panel of the library.
3. Tighten the blue captive thumbscrews with your fingers to secure it to the library.



Verifying the chassis fan assembly installation

Procedure

1. Verify that the new chassis fan assembly is installed properly by checking the OCP or RMI; the event that indicated the chassis fan assembly was faulty should be cleared.
2. If the UID LEDs are still illuminated, deactivate them using the OCP or RMI.



Replacing a drive power board

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. **Prepare to remove the drive power board.**
2. **Remove the drive power board.**
3. **Install the new drive power board.**
4. **Verify the installation.**

Preparing to remove the drive power board

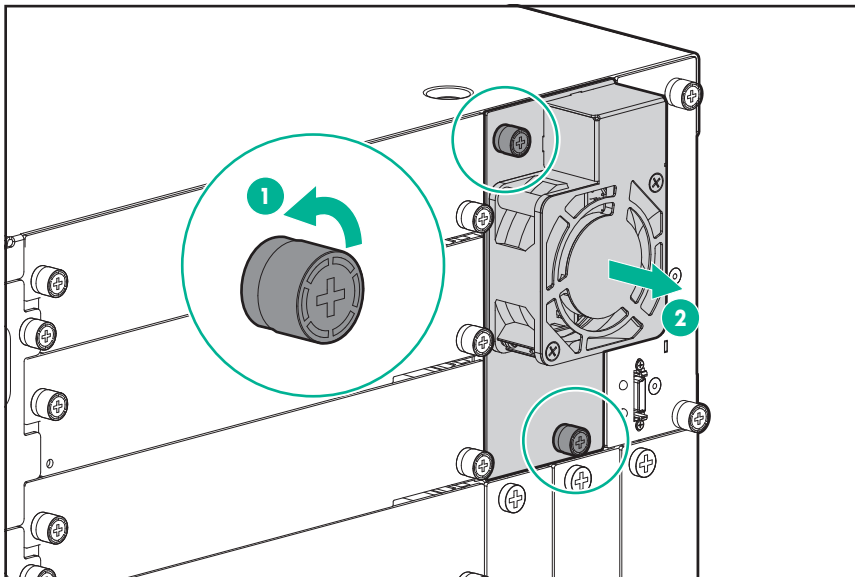
Procedure

Unplug the AC power cords from the module containing the failed drive power board.

Removing the chassis fan assembly and drive power boards

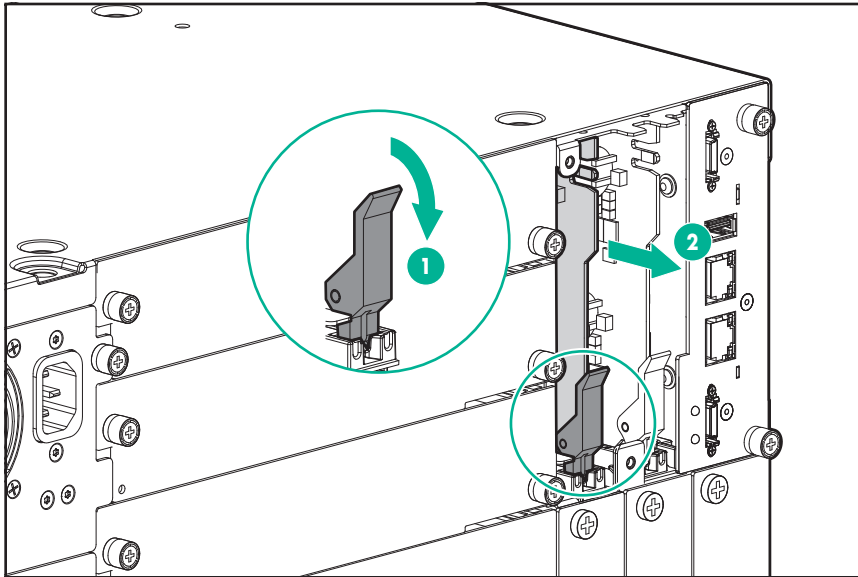
Procedure

1. Loosen the two blue captive thumbscrews on the chassis fan assembly.
2. Using the thumbscrews, slowly remove the chassis fan assembly from the library.



3. Slowly slide the drive power board out of the library.
4. Place the drive power board in a static safe bag.

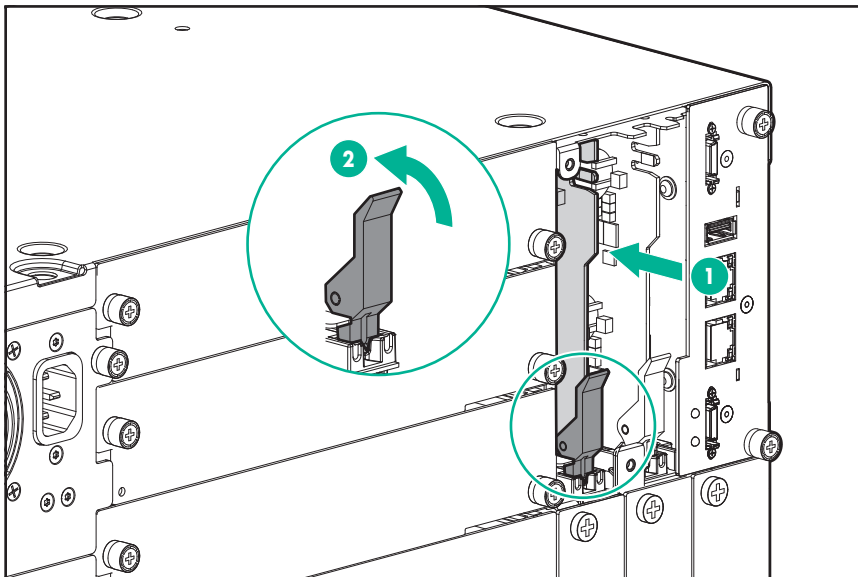




Installing the new drive power board

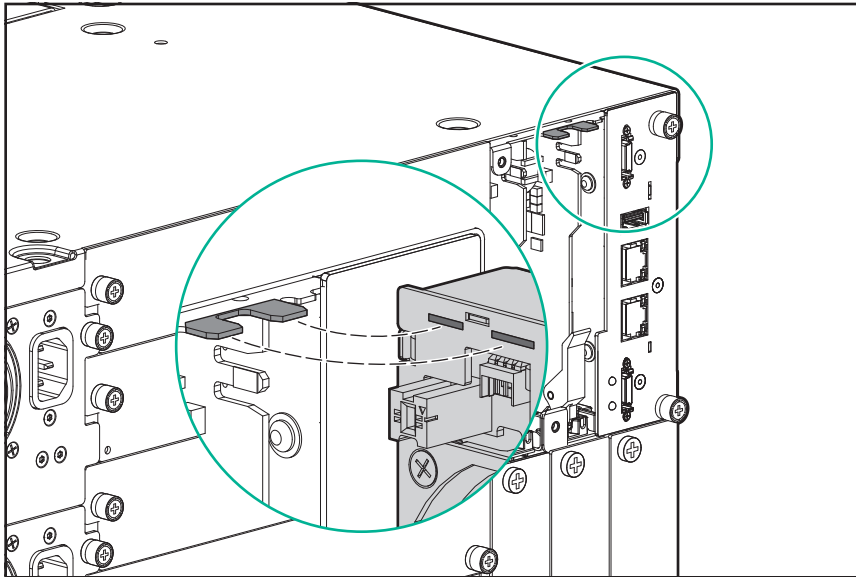
Procedure

1. Position the new drive power board onto the alignment rails.
2. Slide the drive power board into the library until seated firmly. Push the latch up until it snaps into place; when the drive power board is installed correctly, the latch will not be loose.

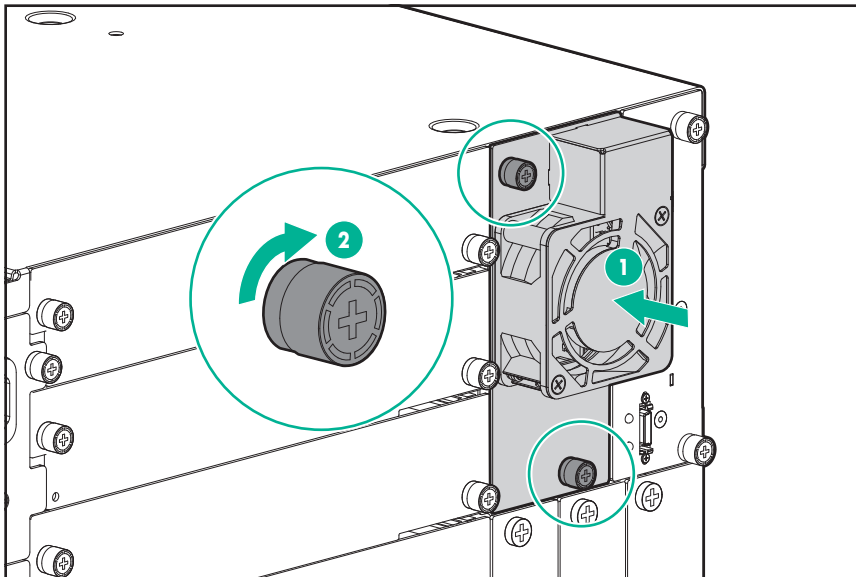


3. Align the tabs on the library with the slots at the top of the chassis fan assembly. Push in the chassis fan assembly until it is flush with the back panel of the library.





4. Tighten the blue captive thumbscrews with your fingers to secure it to the library.



5. Plug in the AC power cords disconnected previously.

Verifying the drive power board installation

Procedure

1. Verify that all drives that are present are powered on:
 - a. Check the OCP or RMI for events.
 - b. From the back of the library, verify that the green LED on each drive is illuminated.
2. Verify that the new drive power board is operating properly by checking the OCP or RMI; the event that indicated the drive power board was faulty should be cleared.



3. If the UID LEDs are still illuminated, deactivate them using the OCP or RMI.
4. Resume the host applications.

Replacing a magazine



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

Procedure

1. **Unlock the magazine.**
2. **Remove the tape cartridges.**
3. **Install the magazine.**
4. **Verify the installation.**

Unlocking the magazine

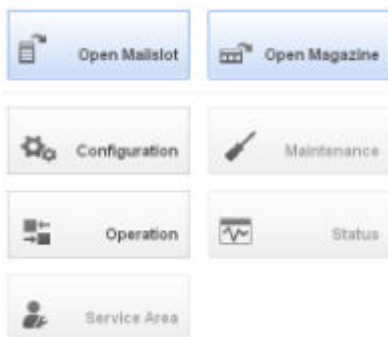
Hewlett Packard Enterprise recommends unlocking the magazine using the OCP or RMI. If these methods fail, power off the library. If a magazine needs to be removed when the power to the library is off, you can release the magazine manually. Only one magazine or mailslot can be open at a time.

NOTE: As a best practice, perform this procedure while applications are idle. While the magazine is extended, the library robotic assembly cannot move media.

Using the OCP

Procedure

1. Log in as an administrator.
2. On the home screen, tap **Open Magazine**.

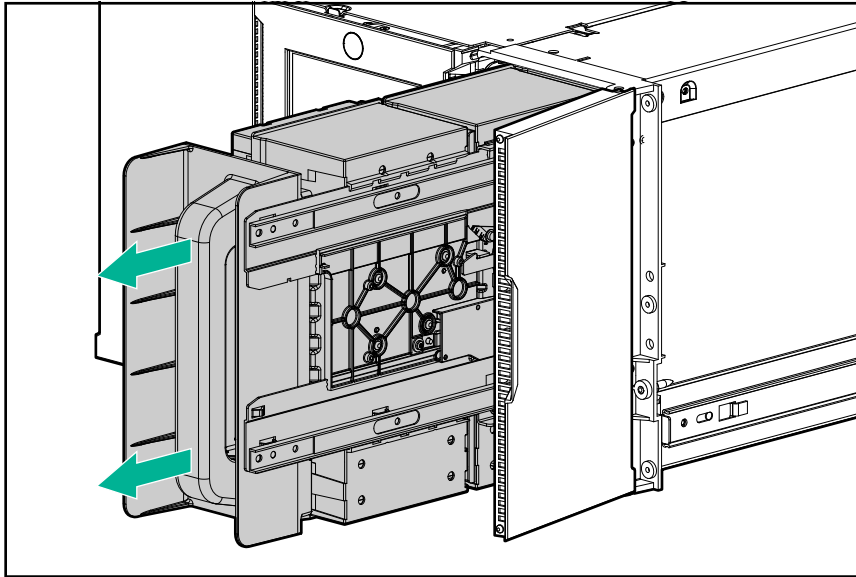


3. Tap the desired module and then tap **Open** in the left or right magazine column within the module containing the magazine to be replaced.



CAUTION: Wait until the OCP indicates that the magazine has been unlocked before attempting to remove it. Pulling on the handle while the library is unlocking the magazine might damage the library.

4. Open the magazine access door.



NOTE: If not removed, the magazines and the mailslot will relock after the time configured on the **Configuration > Mailslots** screen. The default is 30 seconds.

Using the RMI

Procedure

1. Log in as an administrator.
2. On the home screen, click **Open Magazine**.

A screenshot of the HPE StoreEver MSL6480 Remote Management Interface (RMI) home screen. The interface is dark-themed with white and green text and icons. At the top, it displays system information: 'HPE MSL6480', 'Lib. Health: [green checkmark]', 'Status: Idle', '06:52:58 05.11.2015', 'User: administrator', and 'Logout' with a help icon. The left sidebar shows system details: Serial #, Hostname (steer), IPv4 (16.228), Firmware (4.80), and Token status. Below this are drive status sections for Module 4 (Base), Module 3, Module 2, and Module 1, each with a drive count and progress indicator. The main area features a grid of navigation buttons: 'Open Mailslot', 'Open Magazine', 'Configuration', 'Maintenance', 'Operation', and 'Status'. A 'Recent Events' log is visible on the right side of the screen.



3. Click **Open** in the left or right magazine column within the module containing the magazine to be opened.

Operation > Open Magazine

Module	Left	Right
▼ 2	Closed	Closed
▲ Base	Closed	Closed

Open

Open

⚠ CAUTION: Wait until the RMI indicates that the magazine has been unlocked before attempting to remove it. Pulling on the handle while the library is unlocking the magazine might damage the library.

4. Open the magazine access door.

NOTE: If not removed, the magazines and the mailslot will relock after the time configured on the **Configuration > Mailslots** screen. The default is 30 seconds.

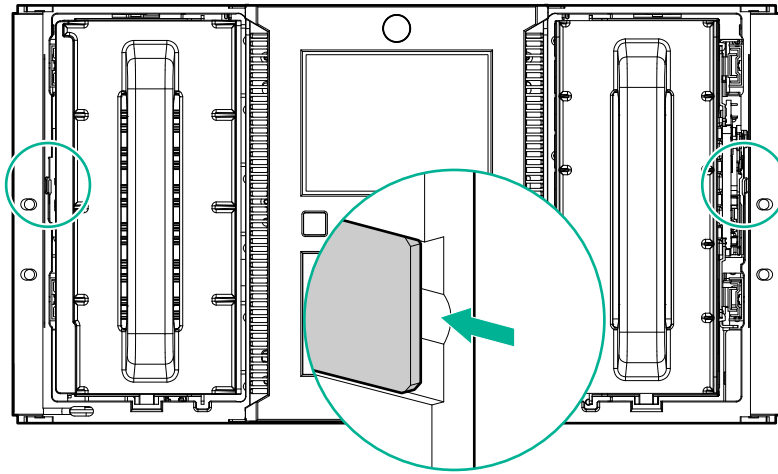
Using the manual release

Procedure

1. Open the magazine access door.
2. Insert a small flat head screwdriver or Torx driver into the appropriate magazine release hole and gently push the tab in.

⚠ IMPORTANT: Do not exert force once you encounter resistance. Doing so can damage the library.



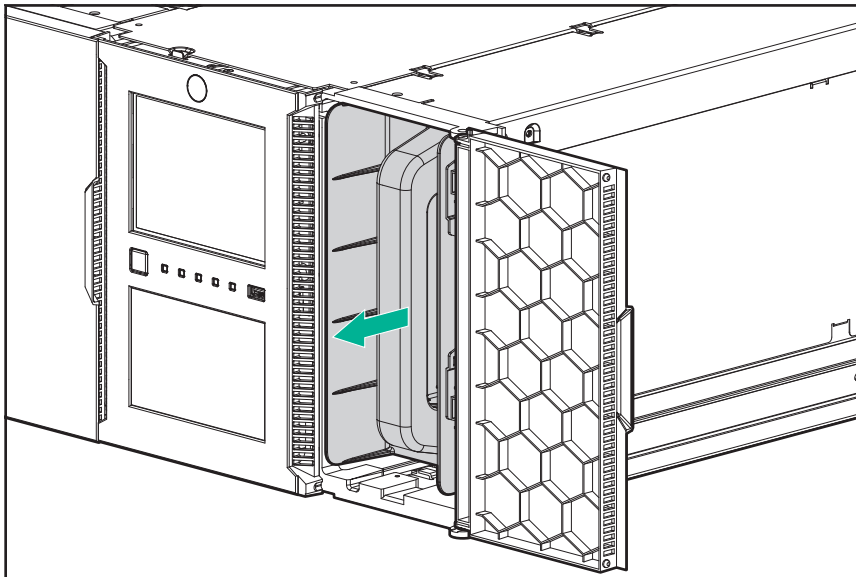


3. Slowly pull the magazine handle until the magazine is free of the latch.

Removing the tape cartridges

Procedure

1. Slowly pull the magazine handle until the magazine is fully extended.



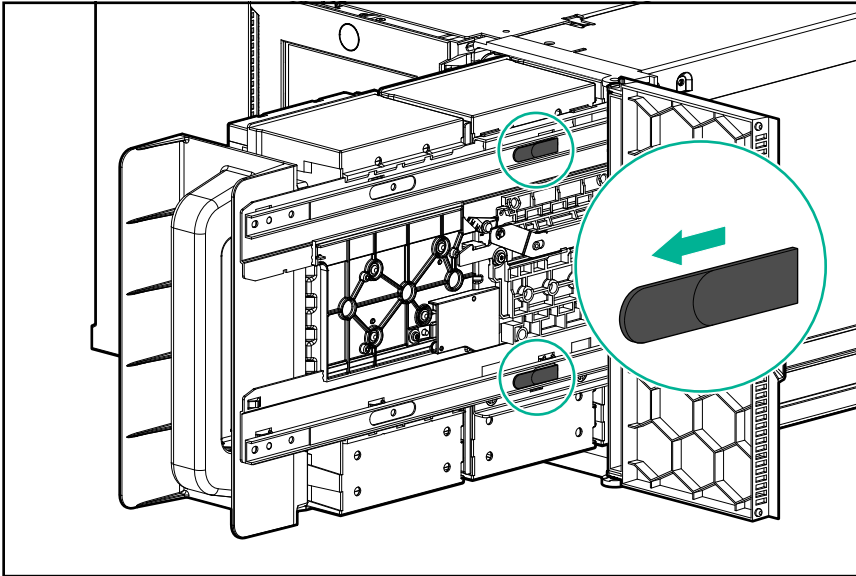
2. Remove the tape cartridges noting their locations within the magazine. You will place them in the same locations in the new magazine after it is installed.



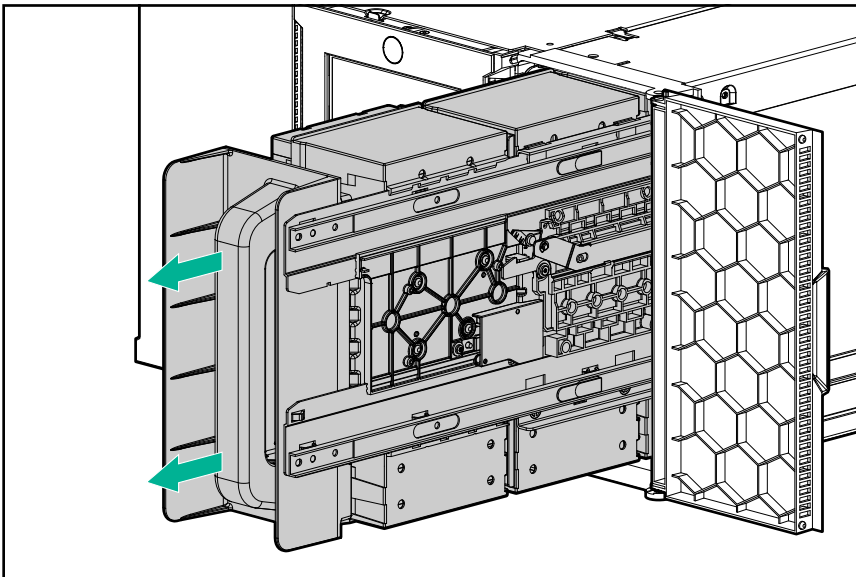
Removing the magazine

Procedure

1. Push the magazine approximately 12 mm (0.5 inches) back into the module to remove tension from the release mechanism.
2. On the back side of the magazine, while pushing the two red latches toward the front of the rack, slide the magazine until clear of the release mechanism.



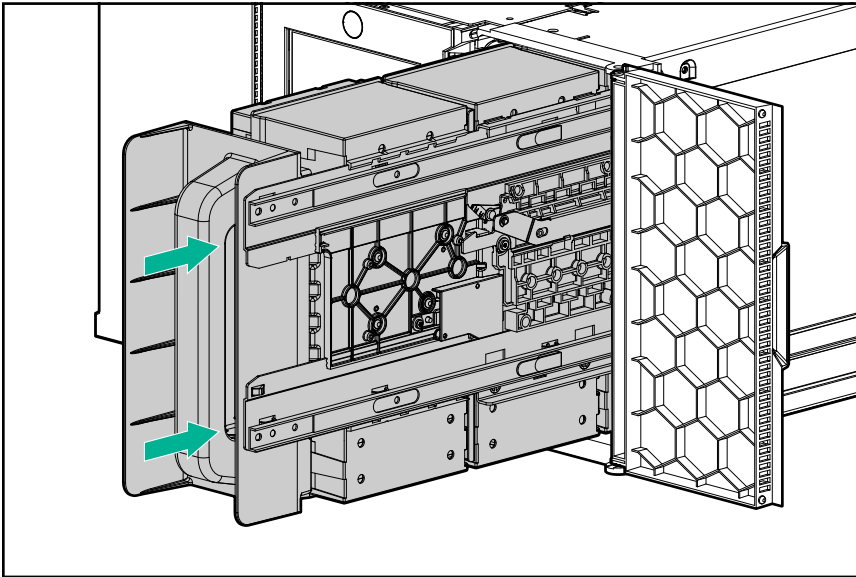
3. Use one hand to remove the magazine from the module while using the other hand to support the bottom.



Installing the magazine

Procedure

1. Position the upper and lower magazine rails onto the alignment rails.
2. Push in slowly until the magazine rails are properly seated and the magazine is only slightly extended (stop before locking the magazine).
3. Pull the magazine back out until fully extended.
4. Load the data cartridges into the new magazine in the same locations they were in previously.
5. Push the magazine handle slowly until the magazine release latch snaps into place. The magazine locks into place after it is correctly installed.



Verifying the magazine installation and operation

Using the OCP or RMI:

Procedure

1. Confirm that the replaced magazine is closed.
2. Confirm that the cartridges in the replaced magazine are inventoried. If you replaced the right magazine, confirm that the cartridges in the mailslot are inventoried.
3. If you replaced the right magazine, unlock the mailslot using the OCP or RMI, pull it out, and push it back in.

Replacing a module



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.





WARNING: Each library module weighs 41 kg (90 lb) without data cartridges or tape drives and 71.4 kg (157.4 lb) with 80 data cartridges and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the library:

- Observe local health and safety requirements and guidelines for manual material handling.
 - Remove all cartridges to reduce the overall weight of the library and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
 - Obtain adequate assistance to lift and stabilize the library during installation or removal.
-



WARNING: When replacing a module in the rack, to reduce the risk of personal injury or damage to equipment:

- Extend the rack 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 may become unstable if more than one component is extended.
-

Process overview

Prerequisites

- #1 Phillips screwdriver for removing the drive bay covers
 - A small flat head screwdriver
 - Several static safe bags for the boards being moved to the replacement chassis
 - Ensure that the rack is level side to side and front to back.
 - Verify that any applications using the library are idle.
 - Verify that the replacement module is the same temperature as the room where it will be installed.
-



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

Procedure

1. Save the library configuration. For instructions, see **Saving the library configuration**.
2. To reduce weight, remove the tape cartridges from the magazines of the module being replaced. For instructions, see **Removing the tape cartridges**.
3. **Power off the library** and verify that the robotic assembly is in the shipping position.
4. **Unlock the magazine from the RMI or OCP**.
5. **Remove the tape cartridges**.
6. **Remove the module cables**.
7. **Remove the tape drives**.



8. **Remove the empty module from the rack.**
9. **Move any library cover plates from the empty module to the replacement module.**
10. **Install the replacement module in the rack.**
11. **Replace the module components and cables.**
12. **Verify the library configuration**

Powering off the library

- ⓘ **IMPORTANT:** After powering off the library and before extending the module from the rack, look through the base module window to locate the robotic assembly. Verify that the robotic assembly is in its shipping position at the bottom of the base module.

If you do not see the robotic assembly completely in the base module, see the instructions for returning the robotic assembly to the base module in the troubleshooting chapter.

Procedure

1. Verify that all host processes are idle.
2. Depress the power button on the front panel for 5 seconds and then release it. When prompted for the robotic assembly parking position, select **The Shipping Position**.

If the library is idle, you can release the button when the Ready LED begins flashing.

If the library does not perform a soft shutdown, press and hold the power button for 10 seconds.

3. If the library has multiple modules, verify that the robotic assembly is in its shipping position at the bottom of the module.

- ⓘ **IMPORTANT:** Continuing this procedure when the robotic assembly is not in the correct position could damage library components.
-

- a. Look through the base module window to locate the robotic assembly.
- b. If you cannot locate the robotic assembly or it is not in its shipping position at the bottom of the base module, see the user guide for troubleshooting information.

Removing the data cartridges

Procedure

Remove the data cartridges while noting their locations within the magazine.



You will place them in the same locations in the new magazine after it is installed. For detailed instructions, see **Removing the tape cartridges**.

Removing the module cables

Procedure

1. Remove the power cords from the module being replaced.
2. Remove the expansion interconnect cables from the module being replaced and from the modules connected to it.

NOTE: Completely removing the cables from both ends prevents damaging the expansion interconnect cables during module removal and replacement.

3. Remove any SAS, FC, or Ethernet cables from the module being replaced.
4. Remove the USB device, if present.

Removing the tape drives

Skip this step if the module does not have tape drives.

Procedure

1. Using your fingers or a #2 Phillips screwdriver, loosen the blue captive thumbscrews on the tape drive.
2. Pull straight back on the tape drive handle while supporting the bottom of the drive to remove it from the module.



CAUTION: Support the bottom of the tape drive when removing it to avoid damaging any of the internal connections.

3. Place the drive on a static-safe surface, noting its position in the module.
The library tracks the drive locations and will issue events if the drives are not in the expected locations.
4. Repeat this procedure for any other drives in the module.

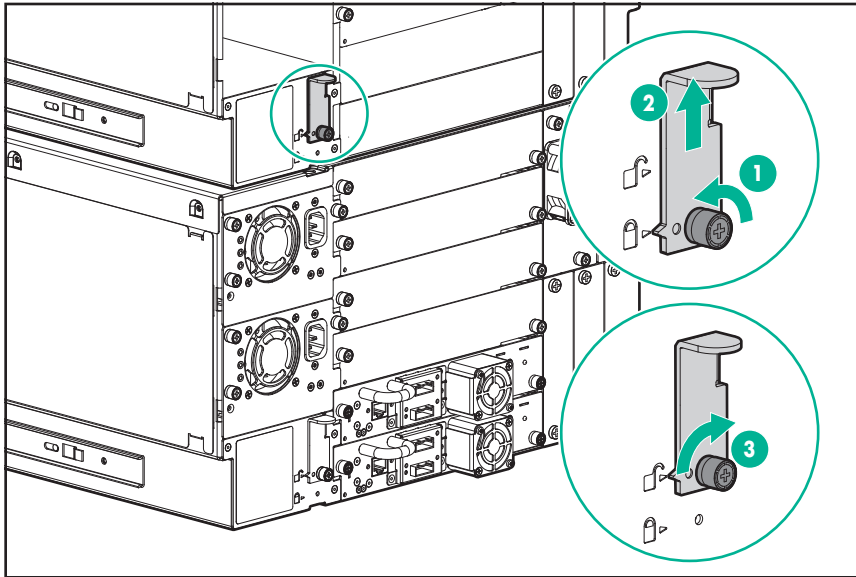
Removing the empty module from the rack

Obtain assistance to lift and stabilize the module during removal and replacement.

Procedure

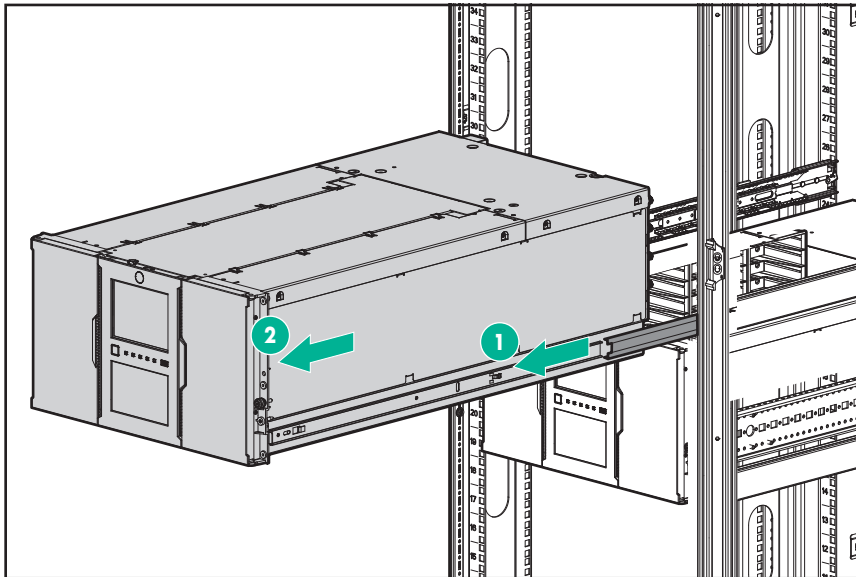
1. If you are removing a module that has a module immediately above and/or below it:
 - a. From the front of the library, use your fingers to loosen the captive thumbscrews two full turns on the module being removed and its adjacent modules.
 - b. From the back of the library, unlock the alignment mechanisms connecting the module being removed with the adjacent modules and secure the alignment mechanisms in the unlocked position.





2. From the front of the library, use your fingers to loosen the thumbscrews on the module to be removed and slide the module out until it stops.
3. With assistance, release the locks on the side of the rails and slide the module out of the rack.

! **IMPORTANT:** To avoid personal injury or damage to the module, always support the bottom of the module where the rack shelf contacts the module. Do not touch internal mechanical or electrical components while moving the module.



Moving library cover plates

The library has removable top and bottom cover plates. The two covers are identical and the process for removing and installing them is the same for the top and bottom of the module.

Procedure

1. Unpack the replacement module and place it on a sturdy work surface.



Save the packaging materials for returning the empty module.

2. Make note of whether the replacement has a top cover plate and/or a bottom cover plate.

If the replacement module has one or both cover plates, you will need to return the failed module with cover plates installed in the same locations.

3. Move the cover plates as necessary so the replacement module has cover plates in the same locations as the failed module.

For instructions, see **Preparing the top and bottom modules**. While this procedure refers to moving a cover from the base module, the information is the same for moving a cover from an expansion module.

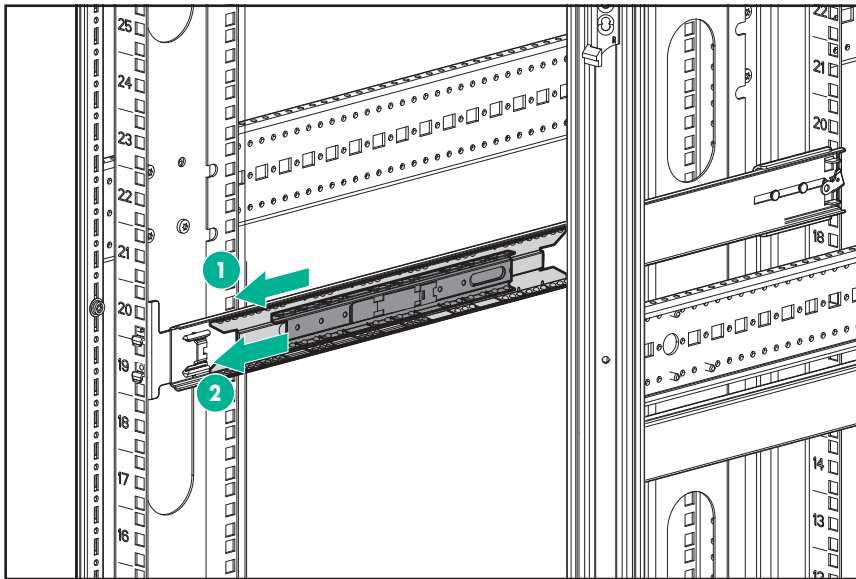
4. If the replacement module arrived with cover plates, install cover plates in the same location on the failed module.

The cover plates protect the module during shipment.

Installing the replacement module into the rack

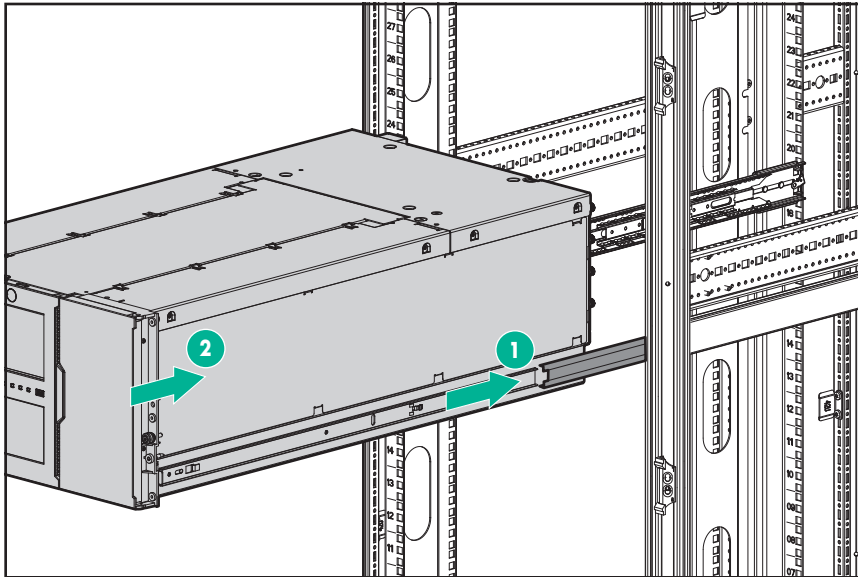
Procedure

1. Extend the middle rails until they lock into place. Move the sliding assembly to the front of the middle rails.

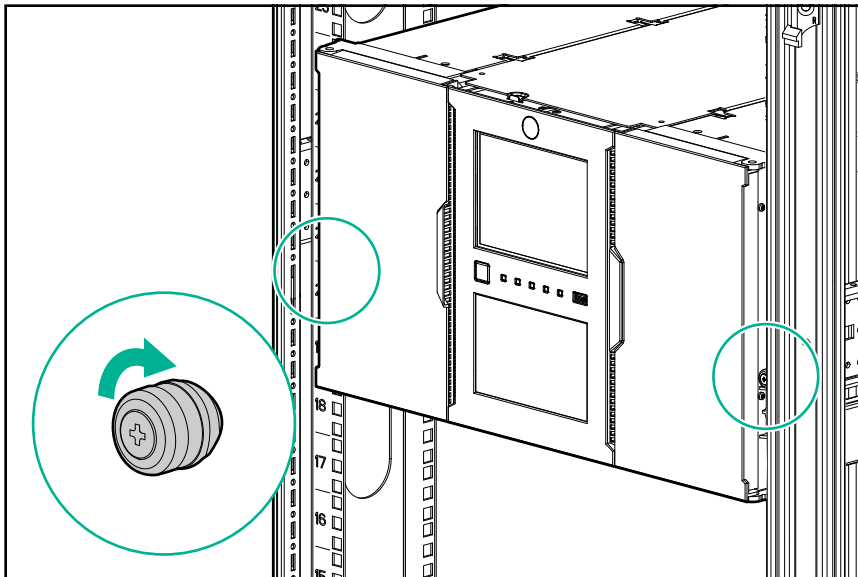


2. Slide the inner rails, which are attached to the module, into the middle rails. Slide the module into the rack.





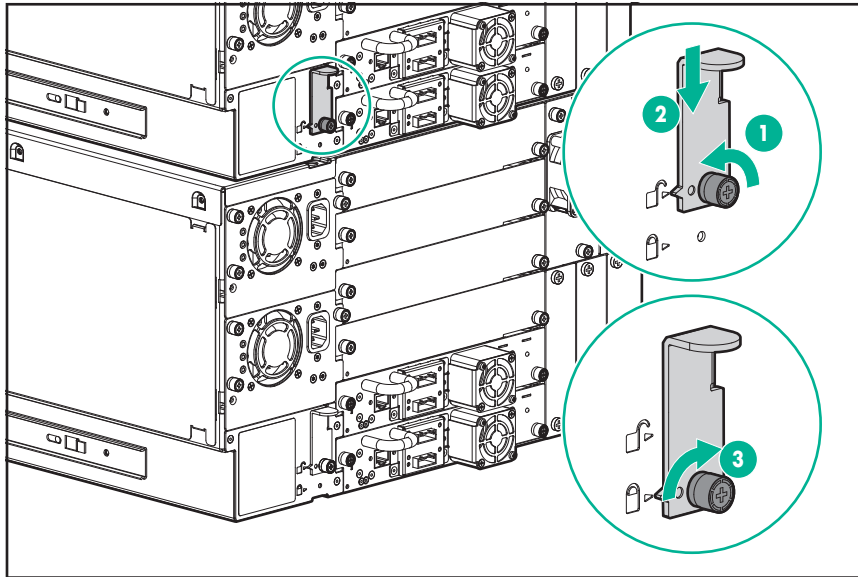
3. Use your fingers or a #2 Phillips screwdriver to tighten the captive fasteners on each side of the module until they are finger tight. Do not over tighten.



4. If there are adjacent modules, align the replacement with the library.
 - a. From the front of the library, use your fingers or a #2 Phillips screwdriver to loosen the captive thumbscrews on the replacement module and all modules above it two full turns.
 - b. From the back of the library, starting with the replacement module and the one under it, align the modules and lock them together. Repeat for each pair of modules.
 - I. Use your fingers to loosen the thumbscrew on the alignment mechanism that will connect the upper module with the lower module.
 - II. Lower the alignment mechanism. If you encounter resistance, adjust the upper module so the pin in the alignment mechanism moves into the hole in the lower module. When the alignment mechanism is in the locked position, tighten the thumbscrew with your fingers.



-
- ⚠ CAUTION:** Do not use the alignment mechanism to force the modules into alignment. The alignment mechanism is designed to hold the modules in position once they are aligned. The alignment mechanism is not intended to adjust the module positions.
-



- c. From the front of the library, use your fingers or a #2 Phillips screwdriver to tighten the captive fasteners on all the modules until they are finger tight. Do not over tighten.

Replacing the module components and cables

Replace the module components by reversing the removal procedures. Align the components carefully in the guide slots. If the thumbscrews cannot be tightened easily, verify that the component is aligned properly.

Procedure

1. Replace the drive power boards and chassis fan assembly.
2. Replace the controller board.
3. Replace the tape drives in the same locations.



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

To secure the tape drive to the chassis, use a torque driver to tighten the blue captive 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.

4. Replace the power supplies.
5. Reattach any SAS, FC, expansion interconnect, and Ethernet cables removed earlier.
6. Reinsert the USB device if you removed it earlier.
7. Reattach the power cords.





Verifying the library configuration

Procedure

1. Power on the library by pressing the button just under the OCP.
2. Verify that the library initializes correctly and that the status is Ready.
3. Verify that the replacement module is visible in the OCP or RMI.
4. Verify the configuration and update it if necessary.
Under normal operation, the library configuration is saved on the base module controller.
5. Replace the data cartridges in the same locations.

Replacing the robotic assembly and spooling mechanism

 **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.

 **IMPORTANT:** Under normal circumstances, when the library is powered off using the front power button the robot automatically parks and locks into the base module behind the OCP. After powering off the library and before proceeding with the robotic assembly and spooling mechanism removal, look inside the base module window to verify that the robotic assembly is behind the OCP.

If you do not see the robotic assembly completely in the base module, see [Returning the robotic assembly to the base module](#) for troubleshooting information.

Procedure

1. **Power off the library.**
2. **Prepare to remove the robotic assembly and spooling mechanism from the base module.**
3. **Remove the robotic assembly and spooling mechanism from the base module.**
4. **Install the robotic assembly and spooling mechanism into the base module.**
5. **Complete the installation.**
6. **Power on the library.**
7. **Verify the installation.**

Powering off the library

Procedure


1. Verify that all host processes are idle.
2. Depress the power button on the front panel for 5 seconds and then release it. When prompted for the robotic assembly parking position, select **The default parked position.**

If the library is idle, you can release the button when the Ready LED begins flashing.



If the library does not perform a soft shutdown, depress and hold the power button for 10 seconds.

3. If the library has multiple modules, verify that the robotic assembly is in its parked position behind the OCP.

 **IMPORTANT:** Continuing this procedure when the robotic assembly is not in the correct position could damage library components.

- a. Look through the base or expansion module windows to locate the robotic assembly.
- b. If you do not see the robotic assembly completely in the base module, see **Returning the robotic assembly to the base module** for troubleshooting information.

Preparing to remove the robotic assembly and spooling mechanism from the base module



WARNING: When extending a module from the library, to reduce the risk of personal injury or damage to equipment:

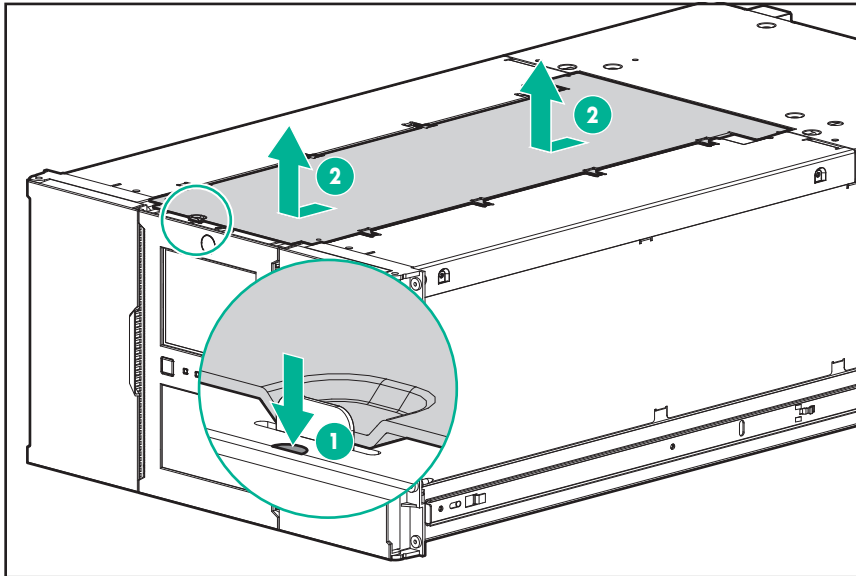
- Extend the rack leveling jacks to the floor.
 - Ensure that the full weight of the rack rests on the leveling jacks.
 - Verify that the rack is level side to side and front to back.
 - Install the rack stabilizer kit on the rack.
 - Extend only one rack component at a time. Racks may become unstable if more than one component is extended.
-

Procedure

1. Loosen the front captive thumbscrews that connect the base module to the rack two full turns.
2. If there are adjacent expansion modules:
 - a. Loosen the front captive thumbscrews two full turns on the adjacent expansion modules.
 - b. On the back of the base module and the module above (if present), loosen the thumbscrews on the alignment mechanisms, move the alignment mechanisms into the unlocked position, and retighten the thumbscrews.
 - c. Disconnect and completely remove the expansion interconnect cables from the base module and from the adjacent modules. Removing the expansion interconnect cables completely prevents damaging the cables when moving the module in and out of the rack.
3. Disconnect the power supply cables on the base module.
4. Disconnect the Ethernet, SAS, and Fibre Channel cables from the base module.
5. Completely loosen the front captive thumbscrews of the base module.
6. Slowly extend the base module from the front of the rack until the rails lock into place.
7. Remove the top library cover plate, if present:



- a. Push a small flat head or Torx screwdriver into the hole to retract the spring lock, slide the cover until it reaches the tool, remove the tool and continue sliding the cover to the front of the module until the tabs are released.
- b. Remove the cover from the module.



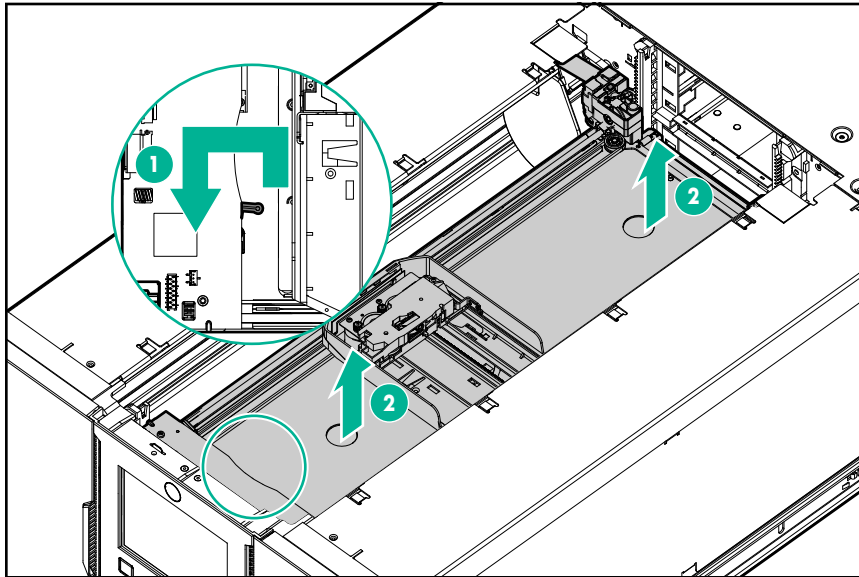
Removing the robotic assembly and spooling mechanism from the base module

Procedure

1. Slide the cartridge carrier toward the center of the robotic assembly to access the robot locking lever.
2. Standing at the front of the module, unlock the robot by moving the blue lever to the left, then toward you, then to the right.
3. Place your fingers into the large holes on the robotic assembly and pull up slowly.

NOTE: The robotic assembly will offer resistance. Lift the robotic assembly no faster than 12 mm (0.5 inches) per second.

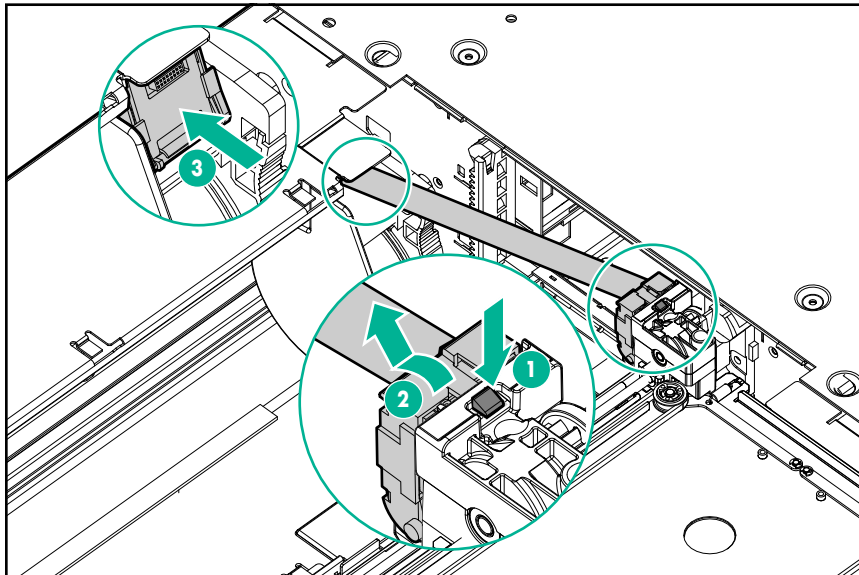




4. Lift the robotic assembly gently from the module and place it on top of the module on the right side (opposite the spooling mechanism) and slightly to the front. Take care not to damage the spooling cable.
5. On the top of the robotic assembly where the spooling cable is attached, use a small flat head screwdriver or Torx driver to press and push the small latch that unlocks the spooling cable.

Note where the end of the spooling cable pivots in the robotic assembly. This is important to know when you attach the new spooling cable to the robotic assembly.

6. Lift the spooling cable from the robotic assembly and place it in its cradle at the top of the spooling mechanism.



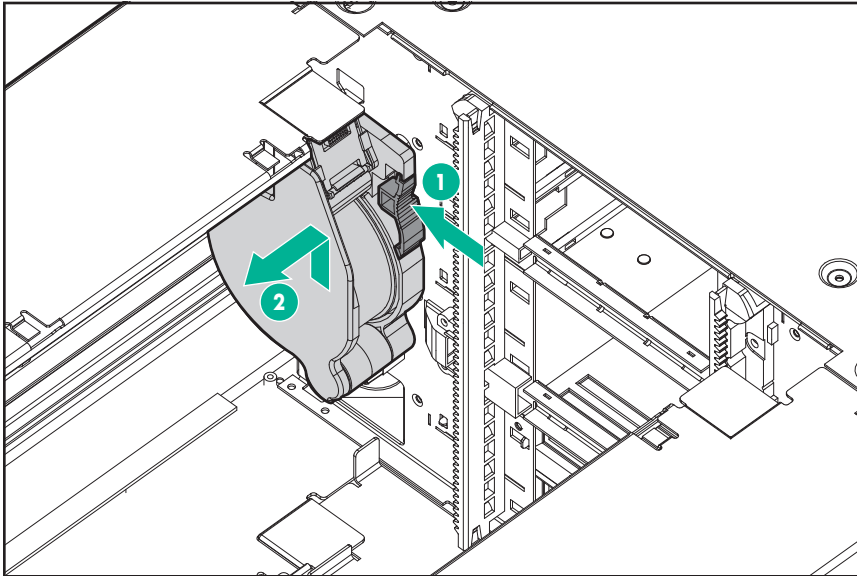
7. Set aside the robotic assembly.

⚠ **IMPORTANT:** If there is a data cartridge still in the cartridge carrier, remove the cartridge by lifting it straight up; you may need to move the cartridge slightly from side to side.

8. Extend the left magazine out of the rack by approximately 15 cm (6 inches).



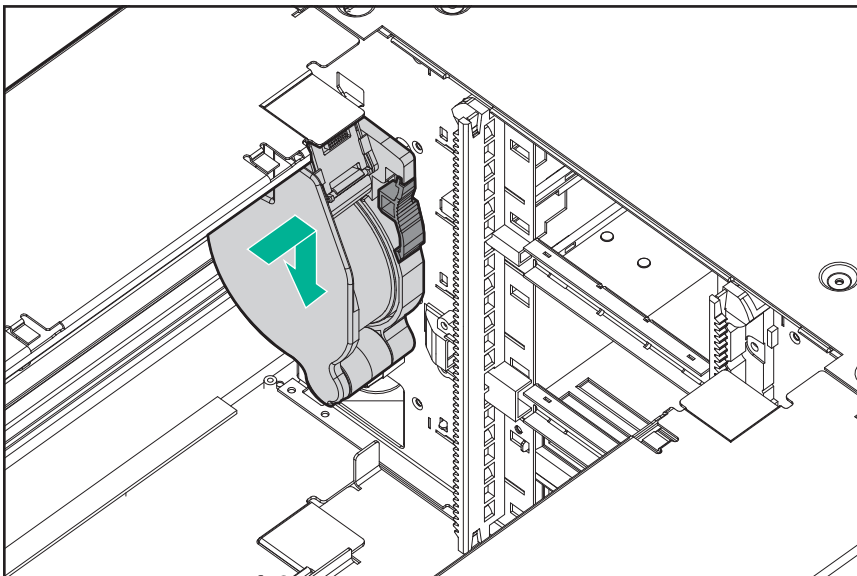
9. While pressing the latch near the top of the spooling mechanism, pull the entire spooling mechanism gently up until you see that it clears the narrow part of the keyhole in the back left of the metal wall. It may help to push up from the bottom with your other hand.
10. Pull the spooling mechanism toward the front of the module until it disconnects and remove it from the module.



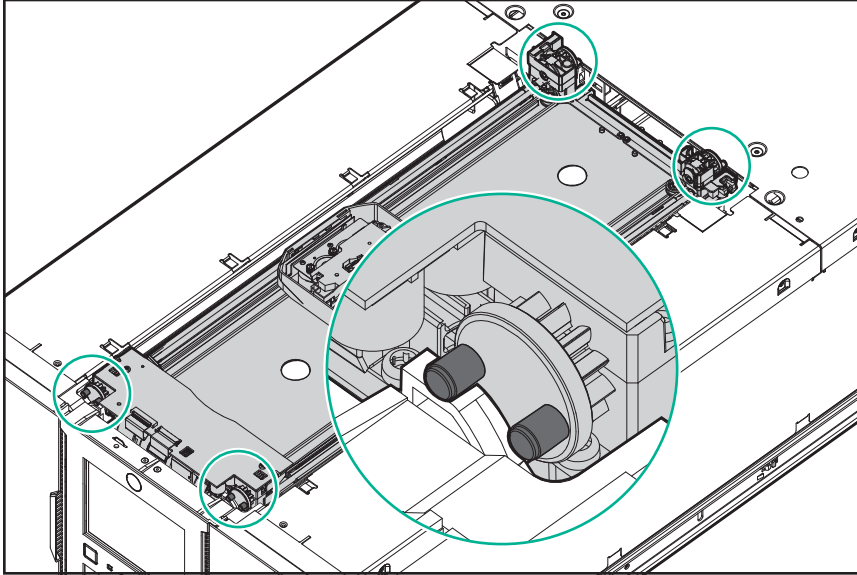
Installing the robotic assembly and spooling mechanism into the base module

Procedure

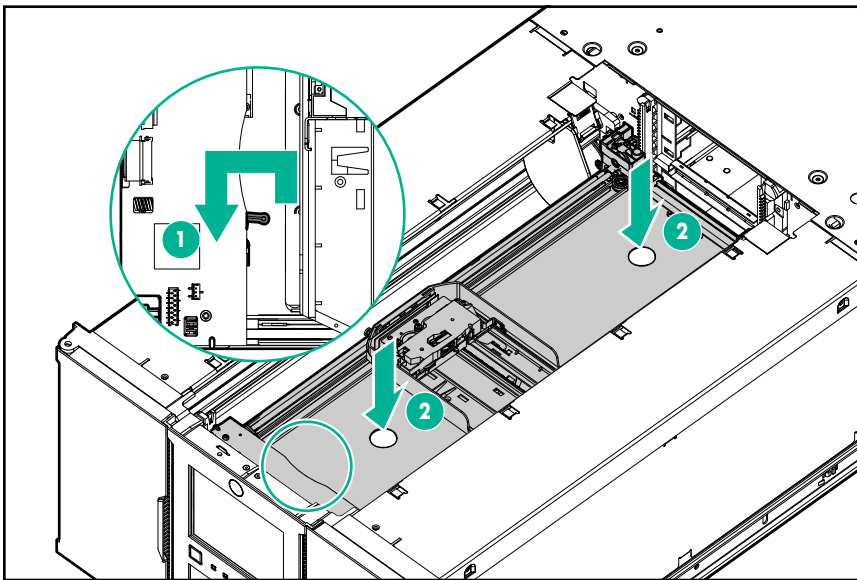
1. Hold the spooling mechanism so that the end of the spooling cable that attaches to the robotic assembly is pointing up.
2. Align the tab on the back of the spooling mechanism with the keyhole in the back left of the metal wall.
3. Push the spooling mechanism in and down until it snaps into place.



4. The robotic assembly is shipped with the robot in the unlocked position. Verify that it is unlocked. If the robot is locked, unlock it; standing at the front of the module, move the blue lever to the left, then toward you, then to the right.
5. Each corner of the robotic assembly has a gear with two protruding pins. Rotate one of the gears on the robotic assembly so that the two pins are aligned horizontally.
6. Place the gears of the robotic assembly into the grooves on the inside corners of the module. Confirm that all of the pins are touching the outside of the grooves.



7. Push the robotic assembly down slowly until the platform of the robotic assembly is approximately 7.5 cm (3 inches) lower than the top of the module.



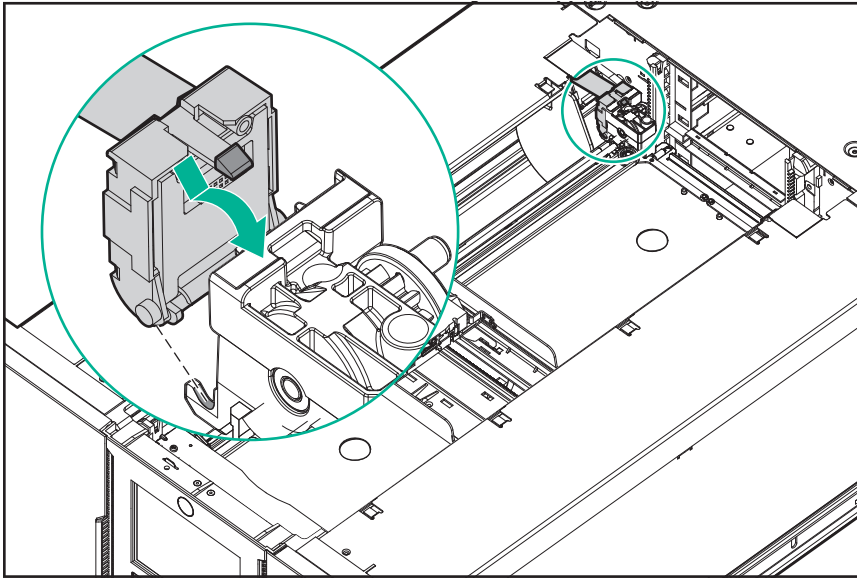
NOTE: The robotic assembly should drop smoothly when applying gentle force. If it does not, check the alignment of the gears.





CAUTION: Lower the robotic assembly no faster than 12 mm (0.5 inches) per second. If the robotic assembly is not aligned properly or you push too hard or too quickly, damage to the robotic assembly and the module may occur.

8. Lock the robot; standing at the front of the module, move the blue lever to the left, then away from you, then to the right.
9. Standing at the right side of the module, remove the end of the spooling cable that connects to the robotic assembly from its cradle.
10. Place the spooling cable into the grooves where it attaches to the robotic assembly and rotate until it snaps into place.



TIP: If the end of the spooling cable drops into the module, unlock the robotic assembly, remove it from the module, return the end of the spooling cable to its cradle, return the robotic assembly to its previous position in the module, relock the robotic assembly, and repeat the procedure.

Completing the robotic assembly and spooling mechanism installation

Procedure

1. Push the left magazine back into the module until it locks into place.
2. Replace the top cover on the base module if you removed one. Align all tabs on the cover with the slots on the module, gently push it down, and then slide the cover toward the back of the module until the spring lock engages.
3. Slide the module into the rack.
4. If there are no adjacent modules, tighten the front captive thumbscrews with your fingers.
5. If there are adjacent modules:
 - a. Loosen the thumbscrews on the alignment mechanisms that you previously unlocked.
 - b. Lower the alignment mechanisms. If you encounter resistance, adjust the upper module so the pin in the alignment mechanism moves into the hole in the lower module. When the alignment mechanism is in the locked position, tighten the thumbscrew with your fingers.



- c. Tighten the front captive thumbscrews with your fingers on all of the modules that had been loosened.
 - d. Reconnect the expansion interconnect cables.
6. Reconnect the Ethernet, SAS, and Fibre Channel cables to the base module.
 7. Reconnect the power supply cables to the base module.
 8. Pack the failed robotic assembly and spooling mechanism to return to Hewlett Packard Enterprise.

Verifying the installation

Procedure

1. Verify that the library powers on and initializes correctly, and that the status is Ready.
2. If the UID LEDs are still illuminated, deactivate them using the OCP or RMI.

Replacing the front bezel or OCP

⚠ 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.
2. **Remove the front bezel.**
3. **Install the front bezel.**
4. **Power on the library.**

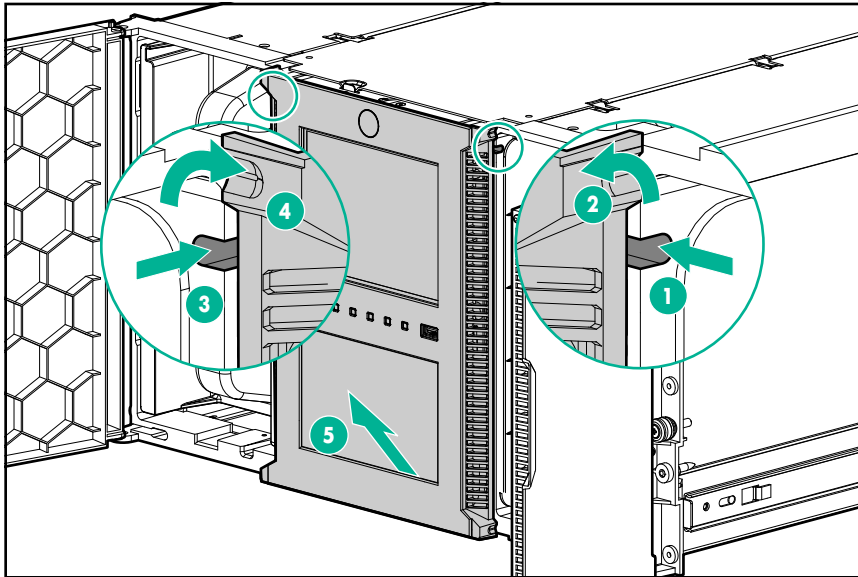
Removing the bezel

Procedure

1. Open the magazine access doors.
2. On one side of the bezel near the top, insert a small flat head or Torx screwdriver into the bezel release hole.
3. Push the screwdriver gently toward the middle of the bezel until that corner of the bezel is released.
4. Release the other top corner in the same manner.
5. Pull the bezel up until clear of the bottom brackets.

NOTE: If removing a base module bezel, pull gently to avoid damaging the OCP cable. Note where the OCP cable is located, routed, and attached.



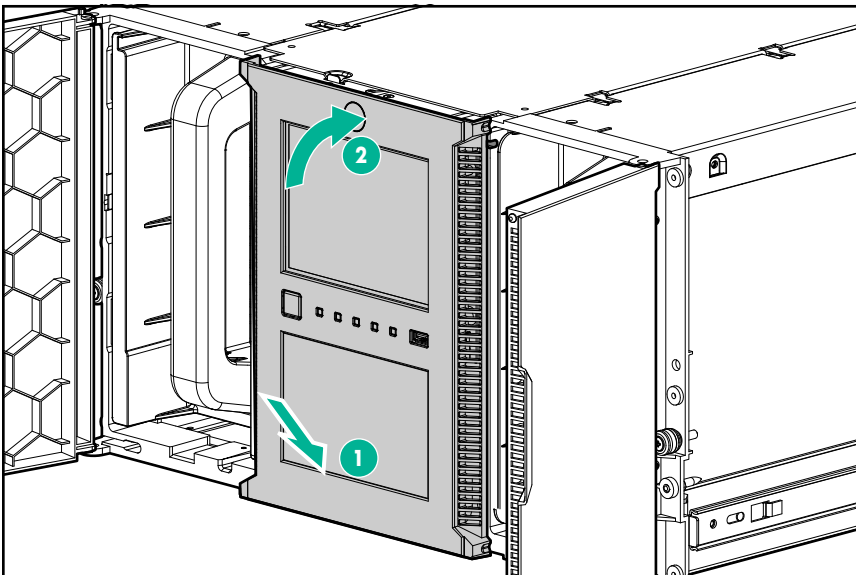


6. If removing a base module bezel, disconnect the OCP cable.

Installing the bezel

Procedure

1. If installing a base module bezel, connect the OCP cable to the new OCP.
Ensure that the OCP cable is correctly routed in the channel behind the clear plastic window.
2. Place the bottom tabs of the bezel into the slots in the bottom of the module.
3. Rotate the bezel and snap in the top corners.



Powering on the library

Procedure

Power on the library by pressing the power button on the base module just below the OCP; the green light will illuminate. When the library is powered on, it inventories the data cartridges in the magazines, checks the firmware version on all modules, configures the tape drives, confirms the presence of the existing modules, and searches for any new modules.

Replacing magazine access doors

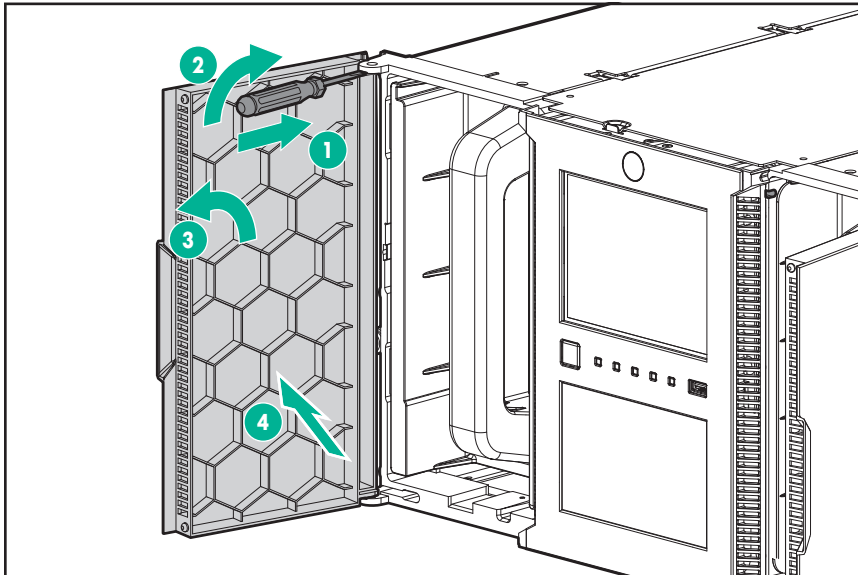
Procedure

1. Remove the magazine access doors.
2. Install the replacement magazine access doors.

Removing the magazine access doors

Procedure

1. Insert a small flat head screwdriver into the slot directly above the top hinge.
2. Use the screwdriver to pry the hinge free of the module while pulling the door toward you.
3. Remove the door from the module.



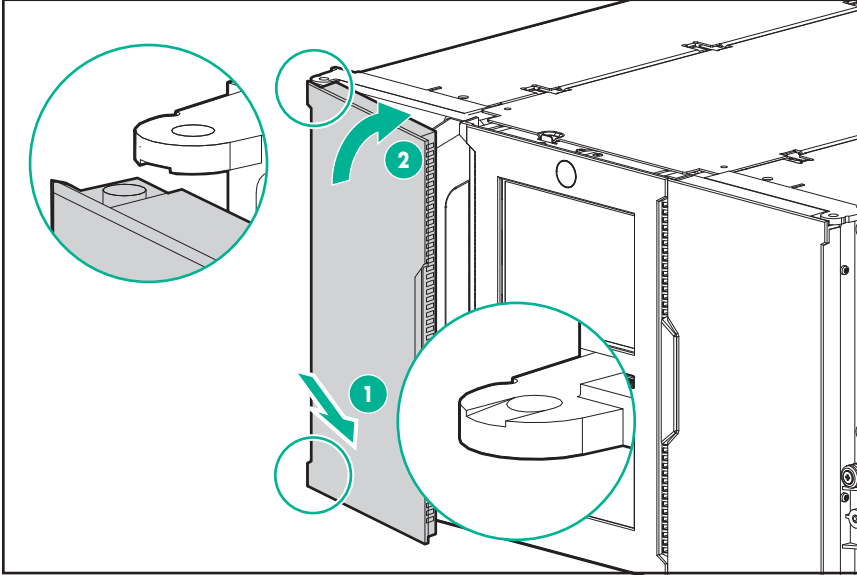
Installing the magazine access doors

NOTE: The doors are identical and can be mounted on either side of the module.



Procedure

1. Orient the door so that the hinges are to the outside of the module.
2. With the door almost closed, insert the bottom hinge into the small recess on the module.
3. Snap the top hinge into place.
4. Verify that the door opens and closes normally.



Troubleshooting tools, procedures, and information



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the library.

Read all documentation and procedures before installing or operating the library.

Hazardous moving parts exist inside this product. Do not insert any tools or any part of your body into the tape library while it is operating.



CAUTION: This library is designed to operate when installed in a rack using the rack rail kit. 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.

Library tests

The library provides diagnostic tests to verify library operations. Each diagnostic test has prerequisites noted on the top of the RMI page, in the online help, and in this document. Before starting a test, review the test prerequisites and verify that they have been met.

- **System test**—exercises overall library functionality by moving cartridges within the library. Cartridges are returned to their original locations.
- **Wellness test**—exercises basic library functionality. Cartridges are NOT returned to their original locations.
- **Slot to slot test**—randomly exchanges cartridges within the library. Cartridges are NOT returned to their original locations.
- **Element to element**—moves a cartridge to a specific element and then returns it to its original location.
- **Robotic test**—performs a full inventory and exercises all robotic assembly movements and sensors.
- **OCP LED test**—illuminates each of the front panel LEDs.

Library & Tape Tools

With Library & Tape Tools (L&TT) installed on the host server you can:

- View detailed configuration, identification, inventory, and drive information for the devices attached to the server.
- 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.

L&TT is a collection of storage hardware management and diagnostic tools for tape mechanisms, tape automation, magneto-optical and archival products. L&TT assembles these tools into a single, convenient program. L&TT 4.26 and newer versions support the library.



Diagnosing problems with Library & Tape Tools

Procedure

1. Install L&TT using the instructions from the L&TT user guide.
L&TT can be downloaded free of charge from <https://www.hpe.com/support/TapeTools>.
2. Generate a support ticket for the library.
3. See the device analysis results for additional information about the library operation.

L&TT support tickets

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. Once downloaded from the device, the support ticket can be viewed on any computer with L&TT installed.

The top of the support ticket contains basic configuration information about the library.



Figure 5: Support ticket in viewer

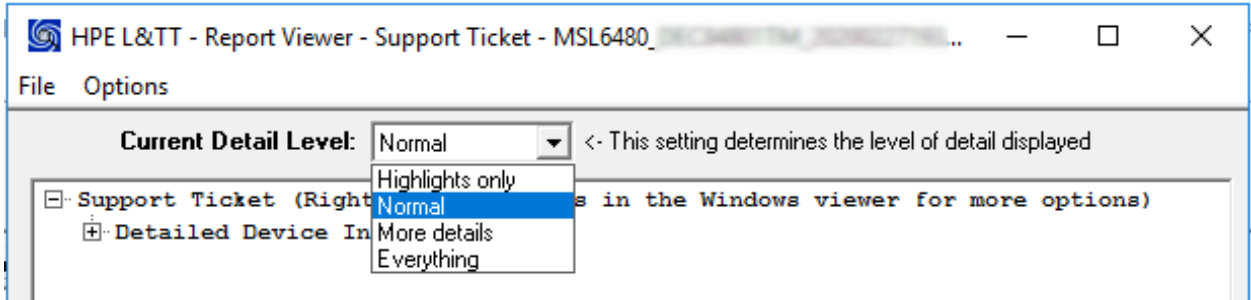
Expand **HP Event Logs** to see events divided into three categories:

- Events in the last 24 hours
- Events in the last 31 days
- Events older than 31 days



Current detail level

To see additional types of events, set the **Current Detail Level** in the Report Viewer.



- **Normal** will only show critical events or hard errors.
- **More details** will also show warning and configuration events.
- **Everything** shows all events.

Event details

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.

Generating an L&TT support ticket or report 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

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

- Download the support ticket from the RMI.
 1. Navigate to the **Maintenance > Download Support Ticket** screen.
 2. Click **Download**.
- Download the support ticket from the OCP.
 1. Insert a FAT-32 formatted USB flash drive into a USB port.
 2. Select **Maintenance > Download support ticket**.
 3. Under the **Library Support Ticket** drop-down, select **Save**.
 4. Once the ticket is saved, remove the USB device.

Viewing a support ticket with L&TT

Prerequisites

- L&TT is installed on the local computer.
- The support ticket has been downloaded to the local computer.

Procedure

1. From the L&TT **File** menu, select **Load Support Ticket**.
2. Select the support ticket file in the browser.

Finding event information

You can find error codes by viewing log files from the **Maintenance > Logs and Traces > View Logs** screen or downloading support tickets from the **Maintenance > Download Support Ticket** screen.

Fibre Channel connection problems

Full height tape drives can only be installed in the top, bottom, or middle pair of half-height drive bays. A full-height drive cannot be seated in other locations and will not operate. If the drive will not seat completely, verify that it is located in one of the three full-height drive locations.

Use the **Status > Drive Status** screen to check the link connection for your tape drive.

If the screen shows Logged Out:

- Verify that the correct Fibre speed is selected or is set to Automatic. If you are unsure of the speed of the HBA or switch that the drive is connected to, try Automatic.
- Check that the correct port type is selected. Loop requires additional configuration. If you are unsure of the correct port type, try Automatic.

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.
- 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 option 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

Frequent causes of SAS detection issues

- Improper SAS cable connections
- Application software configuration errors
- An incorrectly configured operating system

If the application software or operating system does not communicate with the library 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 or 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, not only will the connector not plug in, but 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: <https://www.hpe.com/storage/StoreEverSupportMatrix>

- 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 library uses two Logical Unit Numbers (LUNs) to control the tape drive (LUN 0) and robotic (LUN 1). The library requires an HBA with multiple LUN support and 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. For installation and troubleshooting instructions, see the manual that came with your host adapter. Pay particular attention to any steps describing configuration settings. Ensure that the host adapter is properly seated in the motherboard slot and that the operating system correctly detects the host adapter.
 - 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:
 - For instructions verifying proper installation, see the backup application documentation. 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 application 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 library 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 or backup application vendor, or see the compatibility matrix at: <https://www.hpe.com/storage/StoreEverSupportMatrix>
- 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: <https://www.hpe.com/storage/StoreEverSupportMatrix>
- Ensure that you are using a compatible, high-quality cable.

See the product QuickSpecs for a list of supported cables.

Operation problems

- Power problems



- **The library does not power on**
- **No messages on the OCP**
- Failure/attention indications displayed on the front panel
 - **The LCD displays a warning or error icon**
 - **The LCD displays an error code**
- Tape movement problems
 - **Cartridge stuck in drive**
 - **Cartridge stuck in storage slot**
- Media problems
 - **Cartridge incompatible with drive**
 - **Cannot read or write to data cartridge**
 - **The library reports an obstruction in a storage slot or does not see a data cartridge**
 - **Cannot load a cleaning cartridge**
- Attention LED is illuminated
 - **The attention and cleaning LEDs are illuminated**
 - **A particular cartridge sets off the cleaning light**
 - **A cartridge recently imported from a different environment is causing issues**
 - **The attention LED is illuminated but the cleaning LED is not illuminated after a cartridge load**
 - **A particular cartridge sets off the attention LED and possibly the cleaning LED**
- Inventory problems
 - **The library displays incorrect barcodes**
- RMI network connection issues
 - **Cannot connect to the RMI**
- Data Verification problems



Table 11: Data Verification problems

Problem	Solution
A tape drive used for Data Verification does not report an IP address.	<ul style="list-style-type: none">• Verify that the library has 4.40 or later firmware, which is needed to support Data Verification.• Verify that Ethernet port on the tape drive is connected to the same private network as the library DIAG port.• Verify that only the library DIAG port and drives in the DVP partition are connected to the private network. No other drives or other devices may be connected to the private network.
The library appears unable to communicate with one of the Data Verification drives.	Verify that none of the tape drives in the DVP partition has an FC or SAS port cabled. The drives used for Data Verification should only have an Ethernet cable connected.
The library reports the drive status for one of the Data Verification drives as “configuration failed.”	
The library cannot perform an operation with one of the Data Verification drives, such as pulling a support ticket or moving media to or from the drive.	
Command View TL cannot authenticate to the library	<ul style="list-style-type: none">• Verify that the passwords are the same in the RMI and Command View TL GUI.• Verify that DV is enabled in the RMI.
Command View TL does not pass the connectivity test	<ul style="list-style-type: none">• Verify that SNMP is enabled on the library.• Check the network connections between the library and Command View TL management station.

The library does not power on

Symptom

The library does not power on.

Action

1. Check all power cord connections.
2. Check the LEDs on the power supplies.
3. Make sure that the power button on the front panel has been pressed, and the green **Ready** LED is illuminated.
4. Make sure that the outlet has power. Try another working outlet.
5. Replace the power cord.



No messages on the OCP

Symptom

No messages appear on the OCP display.

Action

1. Verify that the power cord is connected to an active AC source.
2. Verify that the power button on the front panel has been pressed.
3. Verify that the green **Ready** LED is illuminated.
4. Power cycle the library.
5. If the display is still blank but the library seems to be powered on, check the RMI for library status or error information.

The LCD displays a warning or error icon

Symptom

The LCD on the front panel displays a warning or error icon.

Action

Tap the icon to see more information about the event.

The LCD displays an error code

Symptom

The LCD on the front panel displays an error code.

Action

1. Look up the error code in **Event codes**.
2. Use the information about the error to try to resolve the failure.
3. Power cycle the library.

Cartridge stuck in drive

Symptom

A tape cartridge is stuck in a tape drive.

NOTE: The tape drive must rewind the tape before ejecting the cartridge. This process 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.

Cause

Either the tape drive or tape cartridge could be faulty. If multiple tape cartridges are having an issue in an individual drive, the drive might be faulty.



If one tape cartridge is having an issue in an individual drive or multiple drives, inspect the cartridge for damage or a loose label. Discard if necessary.

Use the following actions to remove the cartridge and then continue troubleshooting to determine whether the drive or cartridge need attention.

Action

1. Attempt to unload the cartridge from the backup application.
2. Stop other backup services and then attempt to unload the cartridge from the library RMI or OCP.
 - a. Shut down the backup application.
 - b. Stop the operating system removable storage services.
 - c. From the **Operation > Move Media** screen, attempt to unload or move the cartridge to a slot.
3. If the cartridge still cannot be moved with the RMI or OCP, power cycle the drive.
 - a. Remove the check from the **Power On** box in the **Configuration > Drives Settings** screen and submit.
 - b. Add the check in the **Power On** box in the **Configuration > Drives Settings** screen and submit.
 - c. Wait for the drive to initialize and then retry the move.
4. From the **Operation > Force Drive Media Eject** screen, attempt a force eject or emergency unload operation.
5. Disconnect the library from the host and then attempt to unload the cartridge from the library RMI or OCP.
 - a. Power down the library.
 - b. Disconnect the cable from the drive.
 - c. Power on the library and wait until the tape drive is idle or ready.
 - d. From the **Operation > Move Media** screen, attempt to unload or move the cartridge to a slot.
6. If the move is not successful, attempt a force drive media eject from the **Operation > Force Drive Media Eject** screen.

Cartridge stuck in storage slot

Symptom

A tape cartridge cannot be removed from a storage slot

Action

1. Unlock the magazine from the **Operation > Open Magazine** screen and extend it to access the storage slot.





WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

2. Grasp the cartridge and remove it from the storage slot.

Some cartridges must be inserted and removed several times to condition them for free movement in and out of the magazine.

3. Check the barcode label and verify that it is secure to the cartridge.
4. Check the cartridge for damage.
5. Check the storage slot for damage.

Cartridge incompatible with drive

Symptom

A data or storage cartridge is incompatible with a tape drive.

Action

1. To see which cartridge is incompatible, check the event log.
2. Verify that the data and cleaning cartridges in the library are compatible with the drive.



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

The library automatically unloads incompatible cartridges, the **Attention** LED flashes. Export the media.

3. Verify that the cartridges in the library are the correct type for the operation

Cannot read or write to data cartridge

Symptom

Cannot write to or read from a data cartridge.

Action

1. Make sure that the cartridge is not a WORM cartridge that has already been used.





WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

-
2. Make sure that the cartridge is write enabled (move the write-protect switch to the enabled position).
 3. Make sure that the data cartridge is compatible with the drive model. LTO tape drives can read data cartridges from two generations back and write to data cartridges one generation back. See **Data cartridges**.
 4. Make sure that you are using an Ultrium cartridge that has not been degaussed. **Do not degauss Ultrium cartridges!**
 5. Verify that the cartridge has not been exposed to harsh environmental or electrical conditions.
 6. Inspect the cartridge for physical damage.
 7. Many backup applications do not read or write to cartridges that were created using a different backup application. In this case, you may have to perform an erase, format, or label operation on the cartridge.
 8. Review any data protection or overwrite protection schemes that your backup application may be using. The application could prevent the tape drive from writing to a given cartridge.
 9. Retry the operation with a different, known good cartridge.
 10. Clean the tape drive from the **Operation > Clean Drive** screen.

The library reports an obstruction in a storage slot or does not see a data cartridge

Symptom

The library reports an obstruction in a storage slot or does not see a data cartridge.

Action

The cartridge has a damaged or incorrect label.

All data cartridges must have high-quality labels with valid information.

The attention and cleaning LEDs are illuminated

Symptom

Both the attention and cleaning LEDs are illuminated

Cause

This issue is most likely caused by a dirty drive that cannot read a data cartridge and marks the cartridge invalid.



Action

1. Log in to the OCP or RMI and check the event log to see which drive has reported that it needs cleaning.
2. Clean the drive with an approved Ultrium cleaning cartridge.

A particular cartridge sets off the cleaning light

Symptom

A particular cartridge sets off the cleaning light.

Action

Remove the cartridge from the library.

A cartridge recently imported from a different environment is causing issues

Symptom

A cartridge recently imported from a different environment is causing issues.

Cause

Media that is moved from one environment to another can cause issues until it has acclimated to the new conditions.

Action

Acclimate a cartridge for at least 24 hours before using it if it has been stored at a substantially different temperature or level of humidity than the library.

The attention LED is illuminated but the cleaning LED is not illuminated after a cartridge load

Symptom

The attention LED is illuminated but the cleaning LED is not illuminated after a cartridge load.

Cause

The library was unable to complete the requested operation with the selected tape cartridge.

Action

- Use only cartridges that are compatible with the drive type.
- Use the correct type of cartridges for the operation. For example, use a cleaning cartridge for cleaning.
- Make sure that you are using a Universal cleaning cartridge

The cleaning LED is illuminated after using a cleaning cartridge

Symptom

The cleaning LED is illuminated after using a cleaning cartridge.



Cause

The cleaning cartridge is expired. A cleaning cartridge will expire after 50 cleaning cycles.

Action

Replace the cleaning cartridge with a new cartridge.

A particular cartridge sets off the attention LED and possibly the cleaning LED

Symptom

A particular cartridge sets off the attention LED and possibly the cleaning LED.

Action

1. Retry the operation with a different cleaning cartridge.
2. If the attention LED is cleared and the drive has been cleaned, and then immediately redisplay each time a particular cartridge is reloaded, the cartridge is likely defective.
 - a. 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.
 - b. Do NOT reuse any cartridge that is suspected of being defective or contaminated in any drive.
 - c. If the bad cartridge is a cleaning cartridge, it might be expired.

The library displays incorrect barcodes

Symptom

The library displays incorrect barcodes.

Action

1. Verify that the label is a Hewlett Packard Enterprise label. The barcode reader might not be able to read other labels.
2. Verify that the label is properly applied.
3. Verify that the label is not soiled.

Cannot connect to the RMI

Symptom

You cannot connect to the RMI from a browser.

Action

1. Verify that the Ethernet cable is connected to the base module controller board and to the LAN.
2. Verify that the link LED on the RJ45 (LAN) connector is illuminated.



The library illuminates the link LED when the library is powered on. If the LED is not illuminated, the library is not communicating with the LAN. See your network administrator for help.

3. Verify that the library has been configured with a valid static network address or DHCP has been enabled. The library needs one of these options to obtain a network address.
 - a. If using DHCP, write down the library network address from the OCP login screen.
 - b. If the library did not obtain a valid address through DHCP, verify that the DHCP server is up and the library has network access to it.
 - c. If necessary, set a static network address instead.
4. Browse to the library IP address from a web browser connected to the same LAN as the library.
 - a. If the RMI webpage does not display, ping the library IP address.
 - b. If the ping fails, verify that the library has a valid network address.
 - c. Verify that there are no firewalls or other obstructions to network traffic between the computer with the web browser and the library.
 - d. See your network administrator for help.

Cannot load a cleaning cartridge

Symptom

A tape drive cannot load a cleaning cartridge.

Action

1. Make sure that you are using an Ultrium cleaning cartridge.
2. Make sure that the cleaning cartridge has not expired.

A cleaning cartridge will expire after 50 cleaning cycles.
3. Power cycle the library.

Performance problems

The process of backing up files involves many system components, from the files in the file system on the disk, through the backup server, and out to the library, all managed by software running on an 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**.

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 a 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's maximum transfer rate.

Backup systems using a lower 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, in addition to 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 enough 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 the data cartridges also affect backup performance. For best performance, use Hewlett Packard Enterprise cartridges that are the same LTO generation as the tape drives. If you suspect a performance issue related to data cartridges, use 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. Ensure that the tape drives are securely tightened to the chassis.

Use a torque driver to tighten the thumbscrews on all the tape drives 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. Do not over tighten.

2. Ensure that the chassis is securely tightened to the rack.

From the front of the library, use a torque driver to tighten the captive fasteners to 6 inch pounds or 0.68 N m.

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



Magazines

Hewlett Packard Enterprise recommends unlocking the magazine using the OCP or RMI. If these methods fail, power off the library. If the library is powered off, you can release the magazine manually. Only one magazine or mailslot can be open at a time.

NOTE: As a best practice, perform this procedure while applications are idle. While the magazine is extended, the library robotic assembly cannot move media.

Unlocking a magazine using the OCP or RMI



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

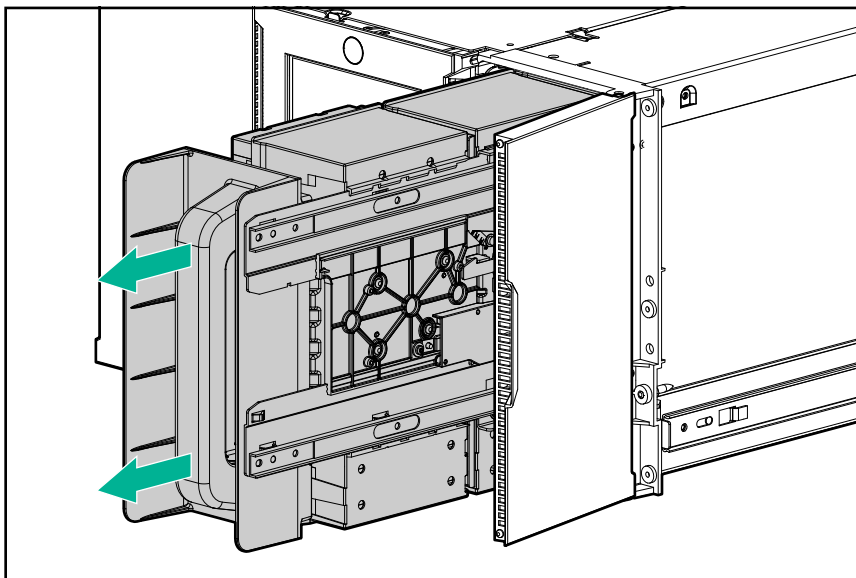
Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

Procedure

1. Log in as an administrator.
2. On the home screen, tap or click **Open Magazine**.
3. Click **Open** in the left or right magazine column within the module containing the magazine to be opened.

CAUTION: Wait until the RMI indicates that the magazine has been unlocked before attempting to remove it. Pulling on the handle while the library is unlocking the magazine might damage the library.

4. Open the magazine access door.



NOTE: If not removed, the magazines and the mailslot will relock after the time configured on the **Configuration > Mailslots** screen. The default is 30 seconds.



Opening a magazine using the manual release



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

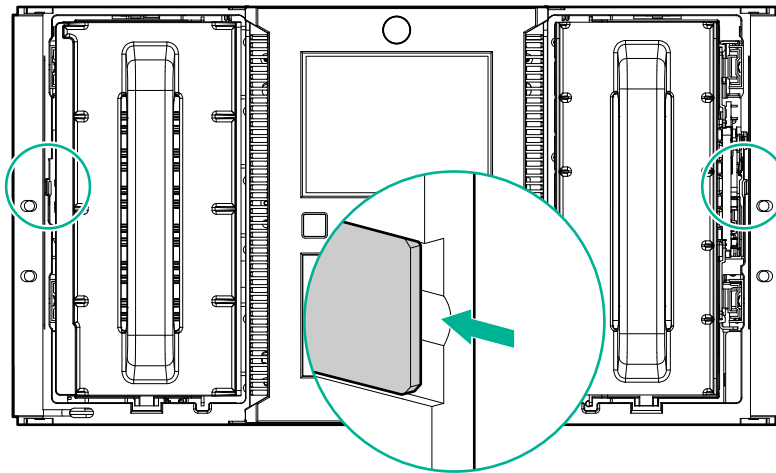
Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

Procedure

1. Open the magazine access door.
2. Insert a small flat head screwdriver or Torx driver into the appropriate magazine release hole and gently push the tab in.



IMPORTANT: Do not exert force once you encounter resistance. Doing so can damage the library.



3. Slowly pull the magazine handle until the magazine is free of the latch.

Locking or unlocking the robotic assembly manually

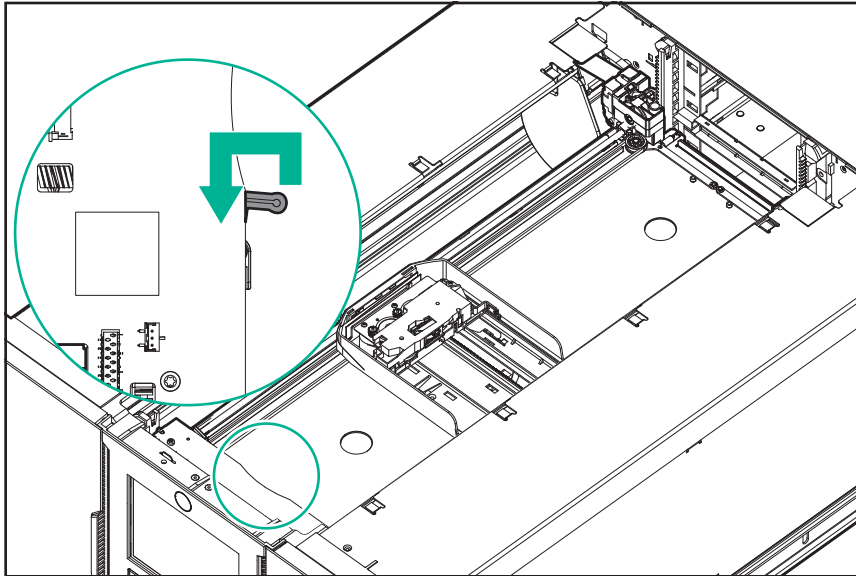
In normal operation, the library returns the robotic assembly to its home position in the base module, behind the OCP, and sets the lock when the library is powered off. You do not normally need to lock or unlock the robotic assembly manually. If the robotic assembly becomes stuck between the locked and unlocked positions, you can set the lock manually.

Procedure

1. Verify that all host processes are idle.
2. Power off the library from the front panel. Depress the power button for 5 seconds and then release it. If the library is idle, you can release the button when the Ready LED begins flashing. If the library does not perform a soft shutdown, depress and hold the power button for 10 seconds.
3. Remove the front bezel from the base module; see [Removing the bezel](#).



4. To lock the assembly, standing at the front of the module, move the blue lever to the left, then away from you, then to the right.



5. To unlock the assembly, move the blue lever to the left, then towards you, then to the right.
6. Reinstall the bezel previously removed; see [Installing the bezel](#).
7. Power on the library from the front panel by pressing the power button.

Returning the robotic assembly to the base module

If you have powered off the library and the robotic assembly did not return to its park position in the base module behind the OCP use this procedure.

Procedure

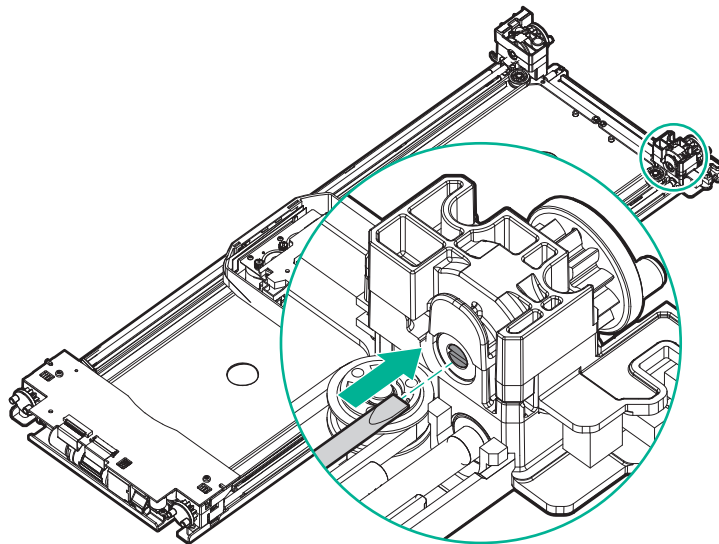
1. Power on the library by pressing the power button on the base module just below the OCP.
2. From the RMI, return the robotic assembly to its park position from the **Maintenance > Move Robotic to Base Module** screen.
3. Power off the library from the front panel. Depress the power button for 5 seconds and then release it. If the library is idle, you can release the button when the Ready LED begins flashing. If the library does not perform a soft shutdown, depress and hold the power button for 10 seconds.
4. If the robotic assembly is still not in the base module, try this procedure: **Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is near the base module or is stopped directly between two modules**
5. If the robotic assembly is still not in the base module, try this procedure: **Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is not near the base module or it cannot move vertically**



Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is near the base module or is stopped directly between two modules

Procedure

1. Remove the front bezel from the base module, the expansion module containing the robotic assembly, and modules in between as needed; see **Removing the bezel.**
2. If the robotic assembly is stopped in a module, try gently and slowly moving the robotic assembly to the next module by hand.
3. To move the robotic assembly into the next module, use a small flat head screwdriver to operate the gear train.
 - a. Insert a small flat head screwdriver into the screwdriver relief on the right rear bearing block of the robotic assembly.
 - b. Turn the screwdriver to operate the robotic assembly gear train manually and move the robotic assembly into the next adjacent module.



If the robotic assembly will not move vertically or if moving it into the base module with the screwdriver is not feasible, follow the procedure in **Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is not near the base module or it cannot move vertically.**

4. Repeat steps 2 and 3 until the robotic assembly is in the base module.
5. Lock the robotic assembly; standing at the front of the module, move the blue lever to the left, then away from you, then to the right.
6. Reinstall the bezels previously removed; see **Installing the bezel.**
7. Remove the robotic assembly and spooling mechanism; see **Preparing to remove the robotic assembly and spooling mechanism from the base module.**
8. Install the new robotic assembly and spooling mechanism; see **Installing the robotic assembly and spooling mechanism into the base module.**
9. Slide the base module back into the rack; see **Completing the robotic assembly and spooling mechanism installation.**



Returning the robotic assembly to the base module when the robotic assembly is stopped in an expansion module that is not near the base module or it cannot move vertically

Procedure

1. Remove the left magazine of the base module.

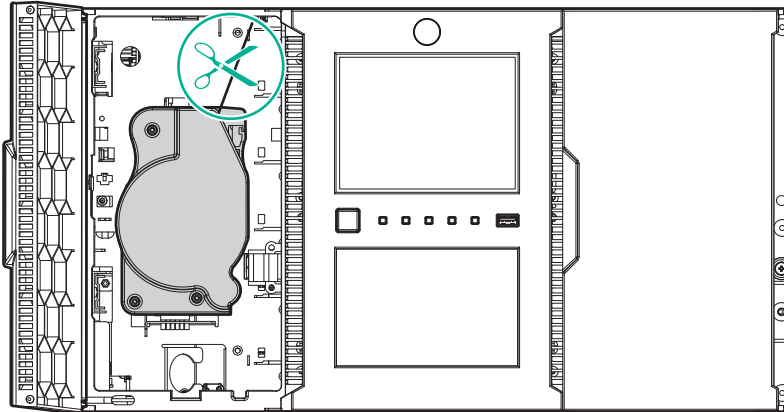
The library should already be powered off. Therefore, you must unlock the magazine using the manual release.

For instructions, see [Removing the magazine](#).

2. Disconnect the power supply cables from all of the modules.
3. Using plastic-handled scissors, reach through the left magazine opening of the base module and carefully cut the spooling cable.

NOTE: Use extreme caution to prevent damaging other parts of the module.

A new spooling cable is provided with the replacement robotic assembly.



4. Extend the expansion module containing the robotic assembly while carefully guiding the free spooling cable.

For instructions, see [Preparing to remove the robotic assembly and spooling mechanism](#). While there may be minor differences, these instructions for a base module will also apply to an expansion module.

5. Remove the robotic assembly from the expansion module using Step 1 through Step 7 in [Removing the robotic assembly and spooling mechanism from the base module](#).

6. Slide the expansion module back into the rack.

For instructions, see [Completing the robotic assembly and spooling mechanism installation](#). While there may be minor differences, these instructions for a base module will also apply to an expansion module.

7. Extend the base module.

For instructions, see [Preparing to remove the robotic assembly and spooling mechanism from the base module](#).

8. Remove the spooling mechanism from the base module using Step 8 through Step 10 in [Removing the robotic assembly and spooling mechanism from the base module](#).



9. Install the new robotic assembly and spooling mechanism; see [Installing the robotic assembly and spooling mechanism into the base module](#).
10. Slide the base module back into the rack; see [Completing the robotic assembly and spooling mechanism installation](#).

Clearing obstructions from the library



WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the tape library.

Read all documentation and procedures before proceeding with magazine extension.

Hazardous moving parts exist inside this product. Do not insert tools nor any portion of your body into the magazine openings.

For proper operation, the robotic assembly must be able to reach the bottom of the library.

Procedure

1. Power off the library by pressing the front power button for 5 seconds and then select the Default Park Location.
The library will park the robotic assembly in the base module behind the OCP.
2. Remove the left magazine from the lowest library module.
For instructions on removing a magazine, see [Unlocking a magazine with the manual release](#).
3. Look into the lowest module and verify that the entire area of the bottom cover is free of any objects that might obstruct the robotic assembly path. Clear any obstructions.
4. Replace the magazines in the magazine slots.
 - a. Position the upper and lower magazine rails onto the alignment rails.
 - b. Push the magazine handle slowly until the magazine release latch snaps into place. The magazine locks into place after it is correctly installed.
5. Power on the library.
The library will perform an initialization and inventory.
6. Verify that no further critical events were generated.
If the library still reports an obstruction, power off the library by pressing the front power button for 5 seconds and then select the **Default Park Location**. Continue checking for tape cartridges that are out of place or have loose labels.
 - Extend and inspect each magazine.
 - Check for cartridges that are not seated properly in the storage or mail slots.
 - Check for loose cartridges.

- Check for loose bar code labels.
- Check for any other objects out of place on the magazine or in the magazine bay.
- Inspect each tape drive for tape cartridges or barcode labels that might block the path of the robotic.
 - Inspect the robotic for loose cartridges or other debris.

7. Power on the library.

The library will perform an initialization and inventory. Verify that no further critical events were generated.

If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event queues.

If the error event reoccurs, check the event log for additional events or event details that provide more specific information.



Library shipping procedures

⚠ WARNING: Each library module weighs 41 kg (90 lb) without media or tape drives and 71.4 kg (157.4 lb) with media (80 cartridges) and six tape drives. When moving the library, to reduce the risk of personal injury or damage to the device:

- Observe local health and safety requirements and guidelines for manual material handling.
- Remove all tapes to reduce the overall weight of the device and to prevent cartridges from falling into the robotic path and damaging the library. Keep the cartridges organized so they can be returned to the same locations.
- Obtain adequate assistance to lift and stabilize the device during installation or removal.

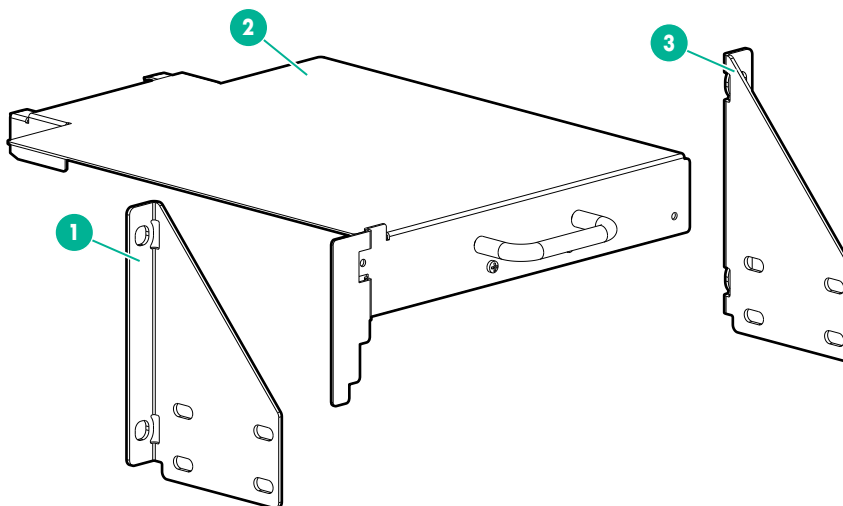
⚠ WARNING: To reduce the risk of personal injury or damage to equipment:

- 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.

⚠ CAUTION: The proper robotic assembly shipping location is only available in firmware versions 4.40 and later. Before shipping a library, upgrade the library firmware if the library is running earlier firmware.

When shipping a library module or library, care must be taken to avoid personal injury and damage to the module or library. The necessary precautions and procedures depend on the library configuration, distance, and mode of travel. Select the procedure that most closely fits your situation.

- Shipping a library that was originally shipped by Hewlett Packard Enterprise in a rack and the original shipping materials are available, including the shock pallet, two module shipping brackets for each module, and in some cases a robotic shipping bracket.



1, 3. Module shipping brackets—two per module

2. Robotic shipping bracket—one per library, depending on library configuration

If the original shock pallet and module shipping brackets are available, all library modules can be shipped with their rack. See **Shipping a library in a rack with the original packaging**.

If the library was originally shipped by Hewlett Packard Enterprise in a rack but the shock pallet and module shipment brackets cannot be located, follow the process for shipping a field-installed library. See **Shipping a library that was field-installed in a square-hole rack**.

- Shipping a library that was field-installed in a square-hole rack. In this case, all library modules will be shipped with their rack. See **Shipping a library that was field-installed in a square-hole rack**.
- Shipping a library that is installed in a round-hole rack. See **Shipping a module outside of a rack**.
- Shipping individual modules. See **Shipping a module outside of a rack**.

When powering off the library from the OCP with 4.40 and later firmware versions, choose the robotic assembly parking location that provides the most protection to the robotic assembly. (On 4.30 and earlier firmware versions, the library returns the robotic assembly to the default parked position when the library is powered off.)

Select the position specified in the shipping procedure.

- **The default parked position**—The default parked position is in the base module behind the OCP.
Choose this position when shipping a library in a rack that has one or more expansion modules installed under the base module and the robotic shipping bracket is available.
- **The shipping position**—The shipping position is near the bottom of the base module. This location can only be used when the base module has a bottom cover properly installed.
Choose this shipping position when the base module is being shipped alone in its normal packaging or when the base module is the bottom module in a rack.



WARNING: If the bottom cover is not properly installed on the base module, the robotic assembly can fall out of the module and be damaged if the module is shipped with the robotic assembly parked in the shipping position.

Shipping a library in a rack with the original packaging

Hewlett Packard Enterprise installs shipping brackets before shipping a library in a rack. The shipping brackets ensure that the library is secure in the rack.

Procedure

1. Locate the module shipping brackets, which might still be mounted on the rear rack columns, and the shock pallet.
If the shipping brackets and shock pallet cannot be located, see **Shipping a library that was field-installed in a square hole rack**.
2. If an expansion module is installed under the base module, also locate the robotic shipping bracket. Continue with this procedure, noting whether the robotic shipping bracket is available or not.
3. Save the library configuration.
For instructions, see **Saving the library configuration**.
4. Remove the data cartridges from the tape drives and magazines.

For instructions, see **Removing the tape cartridges**.

5. Power off the library from the front panel. With firmware versions 4.40 and newer, select the appropriate position for the robotic assembly:

- a. If the robotic shipping bracket is available, select **The default parked position**.

When the library powers off, verify that the robotic assembly is located behind the OCP touch screen.

- b. Otherwise, select the **The shipping position**.

When the library powers off, verify that the robotic assembly is located near the bottom of the base module.

6. Remove the expansion module interconnect cables. Remove all cables that exit the rack, including SAS or FC cables, Ethernet cables, and power cords. Remove any USB devices from the front and rear USB ports.

For instructions, see **Removing the module cables**.

7. Remove the tape drives and place each one in an antistatic bag.

Note the drive locations so the drives can be replaced in the same order and drive bays. The library tracks the drive locations and will issue events for the drives that are not in the expected locations.

Protect the tape drives in the original product packaging or anti-static bubble wrap.

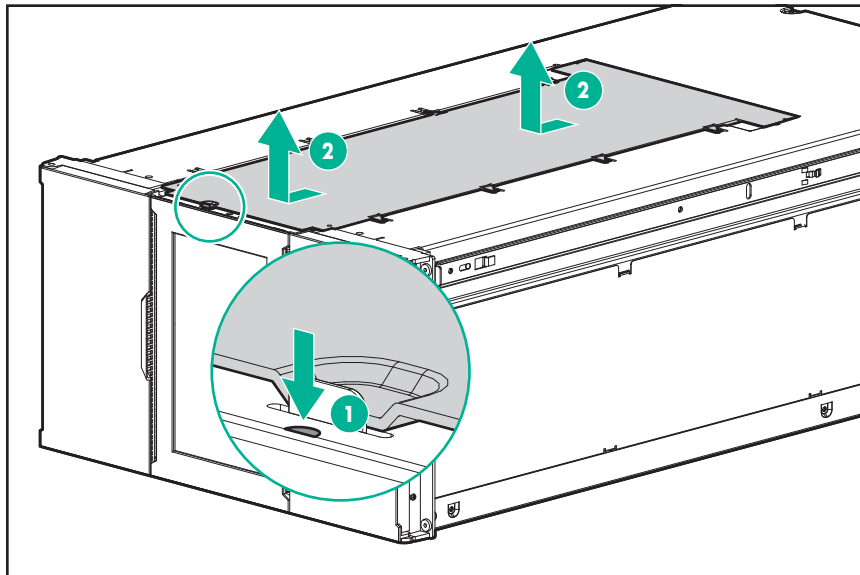
8. If the robotic shipping bracket is not available, the bottom library cover plate must be installed on the bottom of the base module. If one or more expansion modules are installed under the base module, move the bottom cover to the bottom of the base module.

- a. Remove the library cover plate from the bottom of the library.

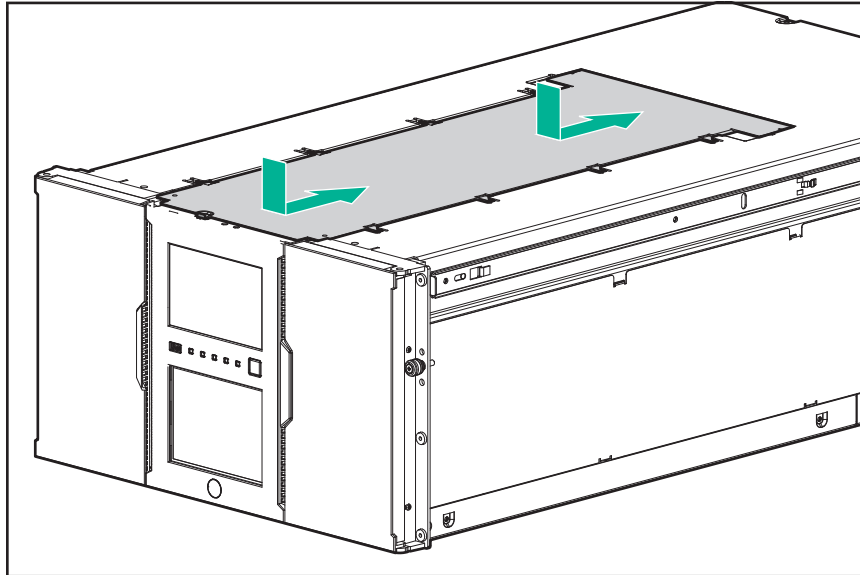
- i. Gain access to the library bottom cover. Options include extending the module from the rack, removing components under the library, or removing the bottom module from the rack. For instructions on removing a module from the rack, see **Removing the empty module from the rack**.

If you removed the bottom module, gently turn it over and place it on a work table.

- ii. Insert a small flathead screwdriver or Torx screwdriver in the hole to retract the spring lock. Slide the cover until it reaches the tool. Remove the tool and continue sliding the cover to the front of the module until all the tabs release.



- III. Remove the cover from the module.
 - IV. If the expansion module is extended from the rack, slide it back into the rack. Secure the expansion module to the rack with the thumbscrews on the front of the module.
- b. Install the cover on the bottom of the base module.
- I. Gain access to the bottom of the base module, if necessary. Options include extending the base module from the rack or removing the base module from the library.
If you removed the base module from the library, gently turn it over and place it on a work table.
 - II. Align all eight tabs on the cover with the slots on the module. Gently push the cover down and then slide it towards the back of the module. The spring lock at the front of the module engages by popping out.



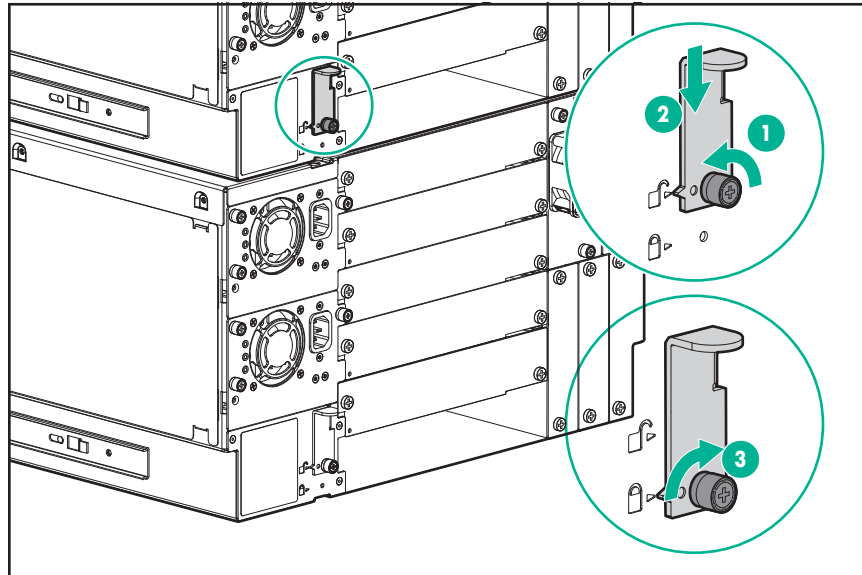
- III. If the base module was extended or removed from the rack, reinstall the base module in the rack and secure it to the rack.
- c. If an expansion module was removed from the rack, reinstall it in the rack and secure it to the rack. For instructions, see **Installing the replacement module into the rack**.
- d. Verify that all alignment mechanisms are locked in their proper positions.
- I. From the front of the library, use your fingers or a #2 Phillips screwdriver to loosen the captive thumbscrews on all modules two full turns.
 - II. From the back of the library, starting with the bottom module and the one above it, align the modules and lock them together. Repeat for each pair of modules.
 - i. Use your fingers to loosen the thumbscrew on the alignment mechanism that will connect the upper module with the lower module.
 - ii. Lower the alignment mechanism. If you encounter resistance, adjust the upper module position. The pin in the alignment mechanism must move easily into the hole in the lower module. When the alignment mechanism is in the locked position, tighten the thumbscrew with your fingers.





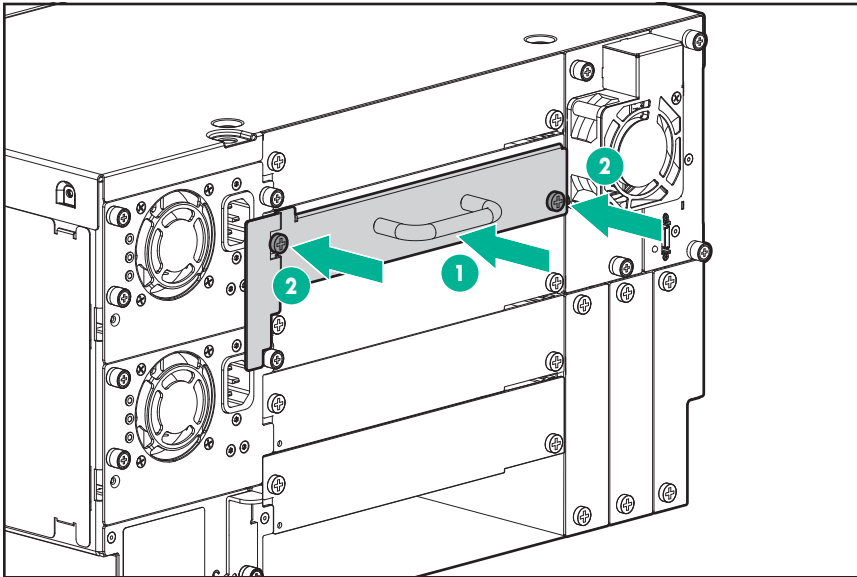
CAUTION: Do not use the alignment mechanism to force the modules into alignment.

The alignment mechanism is designed to hold the modules in position once they are aligned. It is not intended to adjust the module positions.



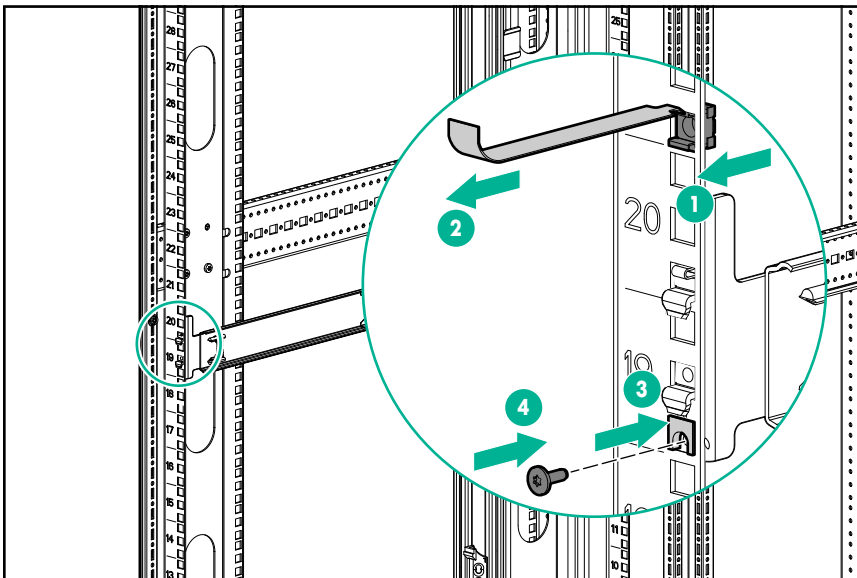
- III. Verify that the lowest module in the library has its alignment mechanism secured in the unlocked position with the thumbscrew.
 - IV. Move to the front of the library. Tighten the captive fasteners on all modules until the fasteners are finger tight. Do not over tighten.
9. If the library has expansion modules **under** the base module and the robotic shipping bracket is available, install the robotic shipping bracket in the second half-height drive bay from the top of the base module.
- a. Remove the drive bay cover from the drive bay, if necessary.
 - b. Look into the open drive bay and verify that the robotic assembly is visible.
 - c. Slide the shipping bracket into the second drive bay from the top until it is fully seated. Secure the bracket with two M3x0.5 6mm screws, which are stored just under the handle on the bracket.





10. Reinstall any available drive bay cover plates over any open drive bays.
11. Reinstall any module shipping brackets on the rear rack columns. Ensure that each module has both module shipping brackets installed.
12. Verify that all retention inserts are properly installed.

If any of the retention inserts are not available, remove the modules from the rack and ship them individually. For instructions, see **Shipping a module outside of a rack**.



13. Move the rack assembly onto the shock pallet and then tighten the rack assembly into place. Cover or wrap the rack with anti-static plastic. If available, install the outer cardboard for protection.

The rack and library are ready for shipment.



Shipping a library that was field-installed in a square-hole rack

Prerequisites



WARNING: Each library module weighs 41 kg (90 lb) without data cartridges or tape drives and 71.4 kg (157.4 lb) with 80 data cartridges and six tape drives.

When moving a library module, to reduce the risk of personal injury or damage to the library: 1) observe local health and safety requirements and guidelines for manual material handling, 2) always remove all cartridges to reduce the overall weight of the module, and 3) obtain adequate assistance to lift and stabilize the module during installation or removal.

Procedure

1. Save the library configuration. For instructions, see [Saving the library configuration](#).
2. Power off the library from the front panel. With firmware versions 4.40 and newer, select **The shipping position**.

When the library powers off, verify that the robotic assembly is located near the bottom of the base module.

3. Remove the expansion module interconnect cables and all cables that exit the rack, including SAS or FC cables, Ethernet cables, and power cords. Remove any USB devices from the front and rear USB ports. For instructions, see [Removing the module cables](#).

4. Remove the tape drives and place each one in an anti-static bag.

Note the drive locations so they can be replaced in the same order and drive bays. The library tracks the drive locations and will issue events if the drives are not in the expected locations.

Protect the tape drives in the original product packaging or anti-static bubble wrap.

5. If the library has expansion modules **below** the base module, move the bottom cover to the bottom of the base module.

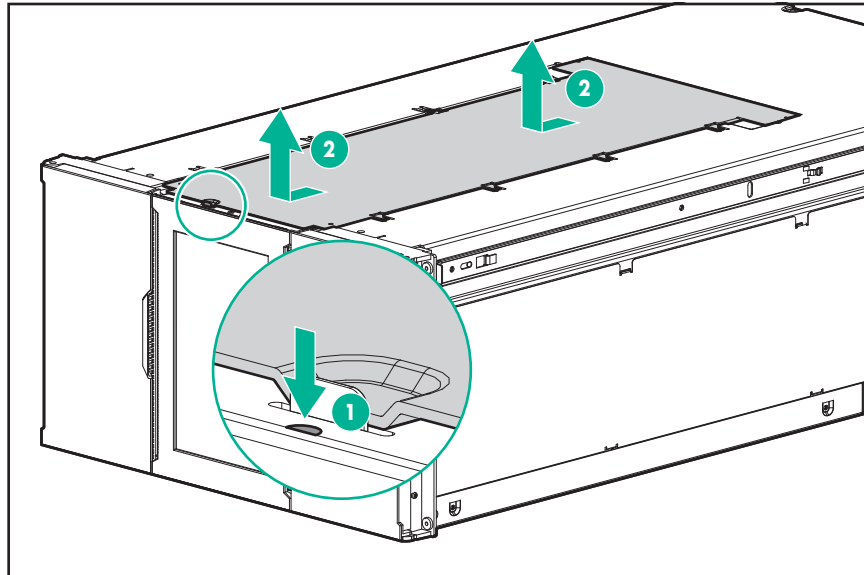
- a. Remove the library cover plate from the bottom of the library.

- I. Gain access to the library bottom cover by extending the module from the rack, removing components below the library, or removing the bottom module from the rack. For instructions on removing a module from the rack, see [Removing the empty module from the rack](#).

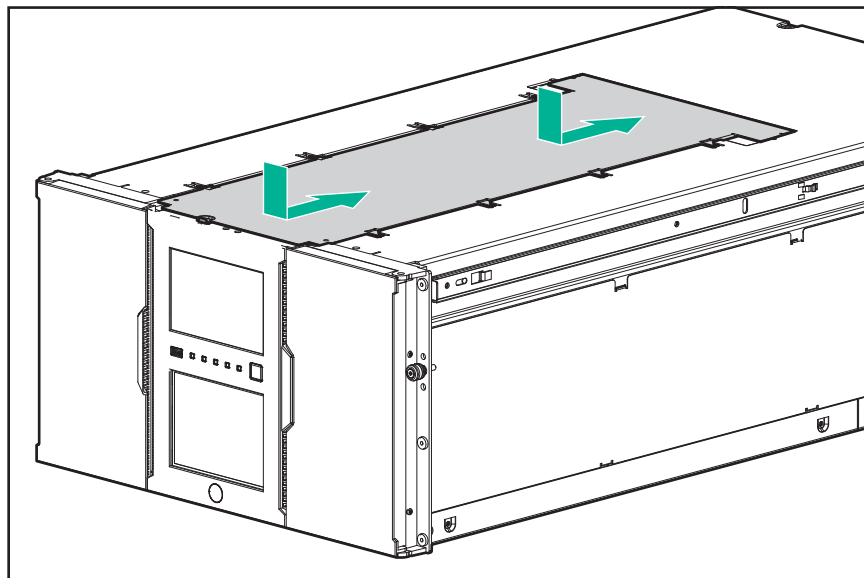
If you removed the bottom module, gently turn it over and place it on a work table.

- II. Insert a small flathead screwdriver or Torx screwdriver into the hole to retract the spring lock, slide the cover until it reaches the tool, remove the tool and continue sliding the cover to the front of the module until all the tabs are released.





- III. Remove the cover from the module.
 - IV. If the expansion module is extended from the rack, slide it back into the rack and secure it to the rack with the thumbscrews on the front of the module.
- b. Install the cover on the bottom of the base module.
- I. Gain access to the bottom of the base module, if necessary, by extending the base module from the rack or removing the base module from the library.
 - II. If you removed the base module from the library, gently turn it over and place it on a work table.
 - III. Align all eight tabs on the cover with the slots on the module, gently push it down, and then slide the cover towards the back of the module until the spring lock at the front of the module engages by popping out.



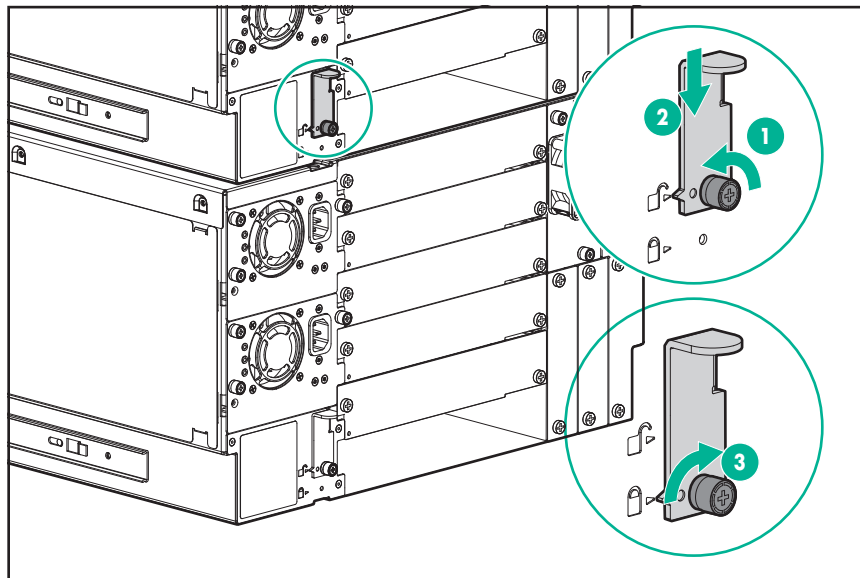
- IV. If the base module was extended or removed from the rack, reinstall the base module in the rack and secure it to the rack. For instructions, see **Installing the replacement module into the rack**.



- c. If an expansion module was removed from the rack, reinstall it in the rack. For instructions, see **Installing the replacement module into the rack**.
- d. If you removed or extended any modules from the library, verify that all of the alignment mechanisms are locked in their proper positions.
 - I. From the front of the library, use your fingers or a #2 Phillips screwdriver to loosen the captive thumbscrews on all of the modules two full turns.
 - II. From the back of the library, starting with the bottom module and the one above it, align the modules and lock them together. Repeat for each pair of modules.
 - i. Use your fingers to loosen the thumbscrew on the alignment mechanism that will connect the upper module with the lower module.
 - ii. Lower the alignment mechanism. If you encounter resistance, adjust the upper module so the pin in the alignment mechanism moves into the hole in the lower module. When the alignment mechanism is in the locked position, tighten the thumbscrew with your fingers.

⚠ CAUTION: Do not use the alignment mechanism to force the modules into alignment.

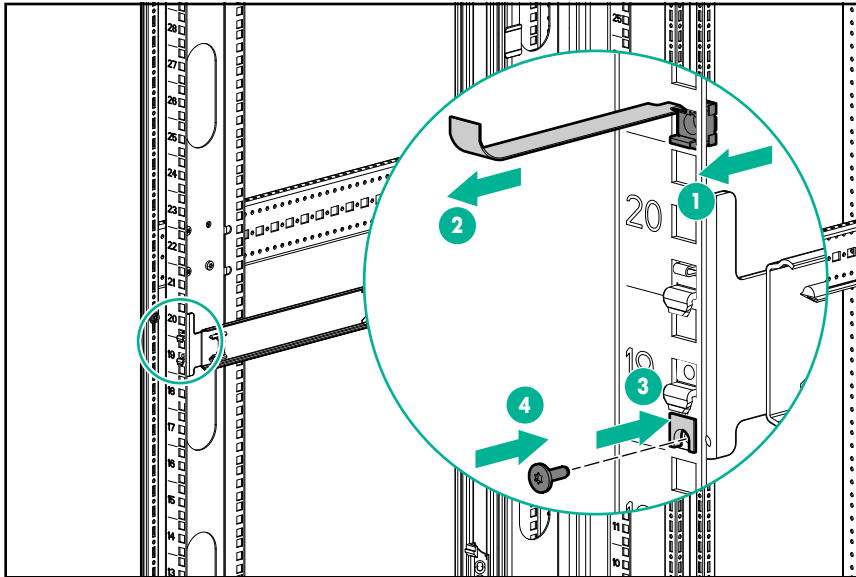
The alignment mechanism is designed to hold the modules in position once they are aligned, but is not intended to adjust the module positions.



- III. Verify that the lowest module in the library has its alignment mechanism secured in the unlocked position with the thumbscrew.
 - IV. From the front of the library, use your fingers or a #2 Phillips screwdriver to tighten the captive fasteners on all of the modules until they are finger tight. Do not over tighten.
6. Reinstall any available drive bay cover plates over any open drive bays.
7. Verify that all retention inserts are properly installed. The retention inserts were shipped with the library in a packet labeled **Retention inserts** and are installed using a T10 Torx driver.

If any of the retention inserts are not available, remove the modules from the rack and ship them individually. For instructions, see **Shipping a module outside of a rack**.





8. Cover or wrap the rack with anti-static plastic. If available, install a layer of cardboard for additional protection.

The rack and library are ready for shipment in a padded van.

Shipping a module outside of a rack

Follow this procedure when shipping one or more modules without their rack. If the library is installed in a round-hole rack, the modules must be removed from the rack and shipped individually.

WARNING: Each library module weighs 41 kg (90 lb) without data cartridges or tape drives and 71.4 kg (157.4 lb) with 80 data cartridges and six tape drives.

When moving a library module, to reduce the risk of personal injury or damage to the library: 1) observe local health and safety requirements and guidelines for manual material handling, 2) always remove all data cartridges to reduce the overall weight of the module, and 3) obtain adequate assistance to lift and stabilize the module during installation or removal.

Procedure

1. Save the library configuration. For instructions, see **Saving the library configuration**.
2. Remove the data cartridges from the tape drives and magazines.
3. Power off the library from the front panel. With firmware versions 4.40 and newer, select **The shipping position**.
When the library powers off, verify that the robotic assembly is located near the bottom of the base module.
4. Remove all cables attached to the modules being shipped. For instructions, see **Removing the module cables**.
5. If the base module is being shipped, remove any USB devices from the front or rear USB ports.
6. Remove the tape drives and place each one in an anti-static bag.

Note the drive locations so they can be replaced in the same order and drive bays. The library tracks the drive locations and will issue events if the drives are not in the expected locations.

Protect the tape drives in the original product packaging or anti-static bubble wrap.

7. Reinstall drive bay cover plates over any open drive bays in the modules being shipped.



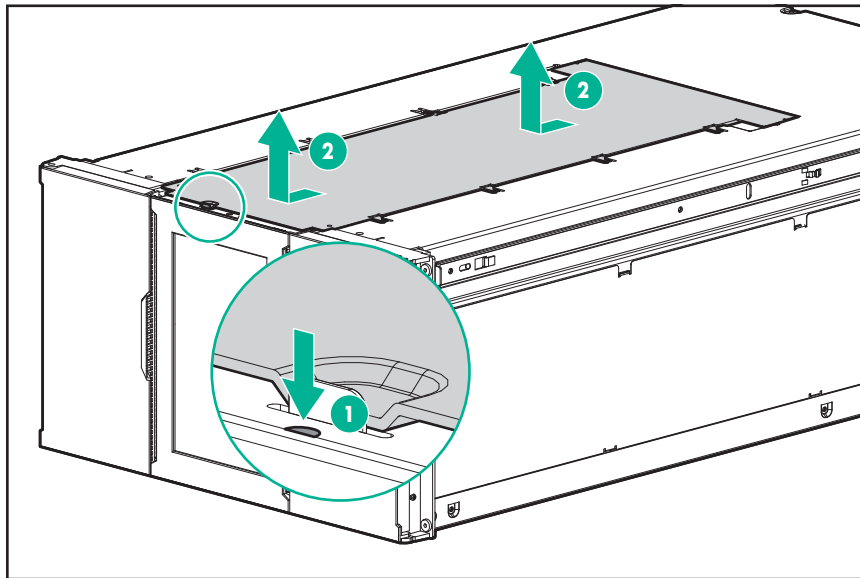
8. Unlock the alignment mechanisms for the modules being shipped.
9. Remove the modules being shipped from the rack. For instructions, see **Removing the empty module from the rack**.
10. If the base module is being shipped, it must have a bottom cover plate installed to avoid damage to the robotic assembly. If the base module does not have a bottom cover plate, remove the bottom cover plate from the lowest expansion module in the library.

If an expansion module is being shipped and it has a bottom cover plate, remove it from the expansion module so it can remain with the library.

- a. Remove the library cover plate from the bottom of the library.
 - I. Gain access to the library bottom cover by extending the module from the rack, removing components below the library, or removing the bottom module from the rack.

If you removed the bottom module, gently turn it over and place it on a work table.

- II. Insert a small flathead screwdriver or Torx screwdriver into the hole to retract the spring lock, slide the cover until it reaches the tool, remove the tool and continue sliding the cover to the front of the module until all the tabs are released.

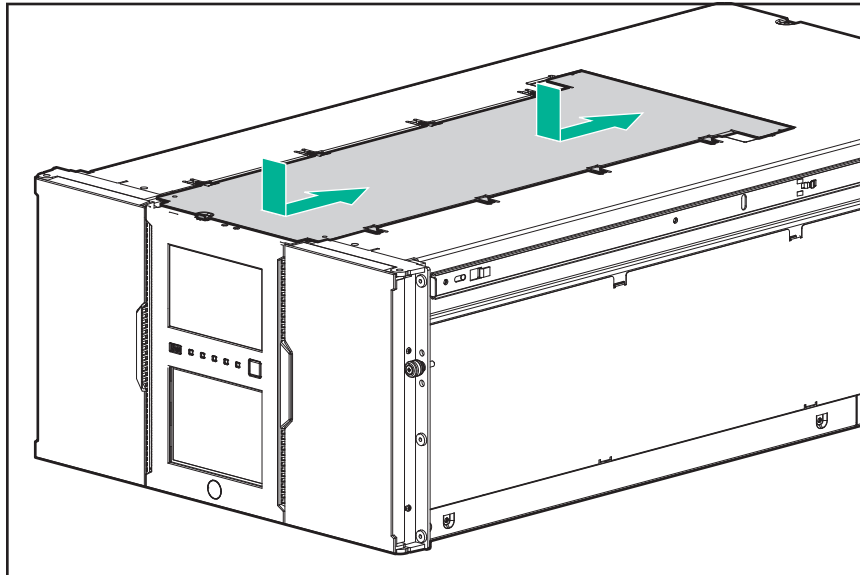


- III. Remove the cover from the module.
 - IV. If the expansion module is extended from the rack and not being shipped, slide it back into the rack and secure it to the rack with the thumbscrews on the front of the module.
- b. If the base module is being shipped, install the library cover plate on the bottom of the base module.

If the base module is remaining in the rack, install the library cover plate on the lowest module in the library.

 - I. Remove the module that will receive the library cover plate from the library, and then gently turn it over and place it on a work table.
 - II. Align all eight tabs on the cover with the slots on the module, gently push it down, and then slide the cover towards the back of the module until the spring lock at the front of the module engages by popping out.





- III. If the module is not being shipped, reinstall it in the rack. For instructions, see **Installing the replacement module into the rack**.

11. If the rack rails are being shipped, remove them from the rack. The rails can be shipped with the module in the original packaging. If the original packaging is not available, ship the rails separately to avoid damage to the module.
12. Cover or wrap the module with anti-static plastic. If available, package the module in its original packaging. If the original packaging is not available, pack the module into an oversized box with bubble wrap or suitable foam.
13. Secure the packaged module to a sturdy pallet.
14. The module is ready for shipment via padded van.



Event codes

Error events

Event code	Message text and description	Details and solution
2000	Failed to move cartridge.	<ol style="list-style-type: none">1. Verify the source and destination elements and retry the move operation.<ul style="list-style-type: none">• If the source is a magazine slot, manually remove and replace the tape cartridge several times to ensure it is not stuck. See <u>Cartridge stuck in storage slot</u>.• If the source is a drive, move the tape cartridge to the magazine slot from the OCP or RMI. See <u>Cartridge stuck in drive</u>.<p>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.</p><p>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.</p>2. Ensure that the library and tape drives are running the latest firmware version.
2002	The initial module discovery (detection of expansion modules) failed.	<ol style="list-style-type: none">1. Verify that all expansion modules are powered on.2. Verify that the expansion interconnect cables installed properly.3. Ensure that the library is running the latest firmware version.

Table Continued



Event code	Message text and description	Details and solution
2003	The library temperature has exceeded the critical limit.	<ol style="list-style-type: none"> <li data-bbox="787 210 1482 283">1. Verify that the chassis fan in each module is present and functioning. <li data-bbox="787 294 1482 367">2. Verify that the drive cover plates are installed in all open drive bays. <li data-bbox="787 378 1482 451">3. Verify that all power supplies are installed and working properly. <li data-bbox="787 462 1482 535">4. Verify that the ambient room temperature is within the specified limits. <li data-bbox="787 546 1482 619">5. Verify that there are no obstructions to airflow through the library. <li data-bbox="787 630 1482 661">6. Ensure that the library is running the latest firmware version.

Table Continued



Event code	Message text and description	Details and solution
2004	Library startup failed	<ol style="list-style-type: none"> 1. If the robotic assembly fails to move through a certain area of the library: <ol style="list-style-type: none"> a. Look through the window in the front panel and see if there are any obstructions. b. Extending one magazine at a time, ensure that all tapes are pushed fully into their slots. 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 a loose, uncontrolled or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u> 2. Verify that all modules have power. 3. Verify that any expansion modules are cabled correctly with the expansion interconnect cables. 4. Verify that the top and bottom cover plates are properly installed on the library. 5. Verify that the module alignment mechanisms at the rear of the library are locked in the proper positions. 6. Power cycle the library. 7. If the robotic assembly moves front to back, but not vertically, the robot shipping lock could be positioned incorrectly. Move the lock to the fully locked position. If the robotic assembly does not unlock the shipping lock after the reboot: <ol style="list-style-type: none"> a. Move the robotic assembly to the base module from the Maintenance > Move Robotic to Base Module screen. See <u>Moving the robotic assembly to the base module.</u> b. Power off the library. c. Remove all cables from the base module and unlock the alignment mechanisms. d. Extend the base module from the rack. e. Ensure that the robot shipping lock is left in the fully locked position

Table Continued



Event code	Message text and description	Details and solution
		<ul style="list-style-type: none"> f. Reassemble in reverse order. g. Power on the library. <p>8. Power off the library and then verify that the robotic assembly is level within the module.</p> <p>If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment.</p> <p>Correct the robotic assembly level if necessary.</p> <p>9. If the error persists, review library events for additional information.</p>
2005	Robotic spooling cable failure	Ensure that the spooling cable is fully seated in the base module and correctly connected to the robotic assembly.
2009	Library test failed due to robotics problem	<ul style="list-style-type: none"> 1. Review the test requirements, address any issues, and then retry the test. 2. Power off the library and then check inside the library for any obstruction that the robotic assembly could hit. <ul style="list-style-type: none"> a. Extending one magazine at a time, 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. d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p>Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u></p> <p>Power on the library.</p> 3. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information.
2010	Library test failed due to spooling mechanism defect	Ensure that the spooling mechanism is fully seated in the base module and installed correctly with the robotic assembly.

Table Continued



Event code	Message text and description	Details and solution
2011	A drive power board has failed. Because of this failure, some drives might be powered off.	<p>Each module has two drive power boards, which are located under the chassis fan. The left drive power board provides power for the upper three half-height tape drive bays in the module. The right drive power board provides power for the lower three half-height tape drive bays in the module. See the event details to determine which drive power board failed.</p> <ol style="list-style-type: none"> 1. Ensure that the drive power boards are fully seated in the module. 2. Reboot or power cycle the library.
2012	Multiple bottom covers detected.	<ul style="list-style-type: none"> • Remove all bottom covers except for the bottom module in the library. • If the library only has one bottom cover, reset the list of known drives and modules. <ol style="list-style-type: none"> 1. Navigate to the Configuration > System > Save/Restore Configuration. 2. Expand the Reset the List of Known Drives and Modules area and then click Reset.
2013	Multiple top covers detected.	<ul style="list-style-type: none"> • Remove all top covers except for the top module in the library. • If the library only has one top cover, reset the list of known drives and modules. <ol style="list-style-type: none"> 1. Navigate to the Configuration > System > Save/Restore Configuration. 2. Expand the Reset the List of Known Drives and Modules area and then click Reset.
2014	Bottom cover is missing.	<p>If the base module cannot detect both a top and bottom cover, the robotic mechanism will not move.</p> <ol style="list-style-type: none"> 1. Install the bottom cover on the bottom module in the library. 2. Check the module interconnect cabling and module power cords. 3. Update the library to 4.90 or newer firmware.

Table Continued



Event code	Message text and description	Details and solution
2015	Top cover is missing	<p>If the base module cannot detect both a top and bottom cover, the robotic mechanism will not move.</p> <ol style="list-style-type: none"> 1. Install the top cover on the top module in the library. 2. Check the module interconnect cabling and module power cords. 3. Update the library to 4.90 or newer firmware.
2016	Module alignment mechanism is not locked properly.	<ol style="list-style-type: none"> 1. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked. (The alignment mechanism in the bottom module must be secured in the unlocked position.) 2. Verify that the library is running firmware version 4.90 or newer.
2017	A communication problem between modules was detected.	<ol style="list-style-type: none"> 1. Ensure that all modules are powered on. 2. Ensure that all module interconnect cables are properly attached. 3. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked.
2021	Database access error.	<p>If this event is seen on a library running 4.70 or earlier firmware versions, the event was generated because of improper error handling. In this case, update the library to 4.90 or newer firmware.</p> <p>If this event is seen on 4.90 or later firmware versions:</p> <ol style="list-style-type: none"> 1. Ensure that the library and tape drives are running latest firmware version. 2. Reboot the library. 3. If the error persists, restore the library configuration. See <u>Restoring the library configuration from a file</u>.
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.	<ol style="list-style-type: none"> 1. Reinsert the removed drive in the same position from which it was removed. Make sure the screws on the drive canister are tight. 2. If the error reoccurs, swap the drives between positions. If the error follows the drive, continue troubleshooting the drive. If the error does not follow the drive, troubleshoot the chassis.
2023	Internal software error.	Reboot the library.

Table Continued

Event code	Message text and description	Details and solution
2024	Exception thrown by application not handled.	An unrecoverable error occurred. Retry the operation and if the error persists reboot the library.
2027	Move failed pulling cartridge from slot.	<ul style="list-style-type: none"> 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. For instructions, see Clearing obstructions from the library.
2028	Move failed inserting cartridge to slot.	

Table Continued



Event code	Message text and description	Details and solution
2029	Initialization failure due to robot front to back positioning error.	<ol style="list-style-type: none"> 1. Power off the library and then check inside library for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Extending one magazine at a time, 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. d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p data-bbox="867 554 1446 646">Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u></p> <p data-bbox="829 688 1040 720">Power on the library.</p> 2. Ensure that all the alignment mechanisms for all modules above the bottom module are engaged and locked. 3. Verify that the rack is level front to back and side to side. 4. If the error event reoccurs, power off the library. For instructions, see <u>Locking or unlocking the robotic assembly manually.</u> Ensure that the robotic assembly is left in the fully locked position. <p data-bbox="829 1020 1040 1052">Power on the library.</p> 5. If the error event reoccurs, power off the library and then verify that the robotic assembly is level within the module. <p data-bbox="829 1150 1455 1243">If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment. Correct the robotic assembly level if necessary.</p> <p data-bbox="829 1262 1040 1293">Power on the library.</p> 6. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. 7. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. 8. If the error event reoccurs, replace the robotics assembly.
2032	Initialization failure due to robot rotation positioning error.	<ol style="list-style-type: none"> 1. Power off the library and then check inside library for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Extending one magazine at a time, ensure that all tapes are pushed fully into their slots. b. Clear any obstructions from the bottom of the library.

Table Continued



Event code	Message text and description	Details and solution
2033	Initialization failure due to robot vertical positioning error.	<ul style="list-style-type: none"> <li data-bbox="829 212 1360 239">c. Clear any loose tape cartridge from the elevator. <li data-bbox="829 258 1430 321">d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p data-bbox="867 340 1442 430">Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library</u>.</p> <p data-bbox="829 478 1040 506">Power on the library.</p> <ul style="list-style-type: none"> <li data-bbox="792 525 1422 588">2. If the error event reoccurs, power off the library and then verify that the robotic assembly is level within the module. <p data-bbox="829 606 1430 697">If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment, correct if necessary.</p> <p data-bbox="829 716 1040 743">Power on the library.</p> <ul style="list-style-type: none"> <li data-bbox="792 762 1455 888">3. If the error event reoccurs, power off the library. For instructions, see <u>Locking or unlocking the robotic assembly manually</u>. Ensure that the robotic assembly is left in the fully locked position. <p data-bbox="829 907 1040 934">Power on the library.</p> <ul style="list-style-type: none"> <li data-bbox="792 953 1455 1016">4. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. <li data-bbox="792 1035 1471 1140">5. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. <li data-bbox="792 1159 1414 1186">6. If the error event reoccurs, replace the robotics assembly.
2034	Cable to spooling mechanism has failed during initialization.	Ensure that the spooling mechanism is fully seated in the base module and installed correctly with the robotic assembly.

Table Continued



Event code	Message text and description	Details and solution
2035	Initialization failure due to robot gripper positioning error.	<ol style="list-style-type: none"> 1. Power off the library and then check inside library for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Extending one magazine at a time, 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. 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. For instructions, see <u>Clearing obstructions from the library.</u> <p>Power on the library.</p> 2. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. 3. Power cycle the library and then retry the operation.
2036	Unintended termination of application process.	Power cycle the library and then retry the operation.
2037	Robotics firmware version upgrade failed.	
2038	Lost connection to module.	<ul style="list-style-type: none"> • Ensure that all modules are powered on. • Ensure that all module interconnect cables are properly installed. • Reboot the library.
2039	Cartridge left in robot gripper, unable to be moved to any open location.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Check for additional events that might provide an indication of the reason for the failure. 2. Retry the wellness test.

Table Continued



Event code	Message text and description	Details and solution
2041	Wellness test failed because unit lock failed.	<p>Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked.</p> <p>(The alignment mechanism in the bottom module must be secured in the unlocked position.)</p>
2042	Wellness test failed because top cover is missing.	If the base module cannot detect both a top and bottom cover, the robot will not move.
2043	Wellness test failed because bottom cover is missing.	<ol style="list-style-type: none"> 1. Verify that both the top and bottom covers are properly installed. 2. Verify that the module interconnect cables are properly connected. 3. Verify that all modules are powered on.
2044	Wellness test failed because drive power board failed.	<p>Each module has two drive power boards, which are located under the chassis fan. The left drive power board provides power for the upper three half-height tape drive bays in the module. The right drive power board provides power for the lower three half-height tape drive bays in the module. See the event details to determine which drive power board failed.</p> <ol style="list-style-type: none"> 1. Power off the library. 2. Ensure that the drive power boards are fully seated in the module. 3. Reboot or power cycle the library.
2045	Wellness test failed because move media test failed.	<ol style="list-style-type: none"> 1. Verify that at least one unloaded drive and one data cartridge compatible with that unloaded drive are installed in the library. If no drives are unloaded or no compatible cartridge is found, the test will fail and this error event will be generated. 2. Unload all tape drives and then rerun the test. 3. Check for obstructions between the robotic assembly and magazines. 4. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked. 5. Verified that the rack is level front to front and back to back. 6. Power off the library. Verify that the robotics assembly is not stuck in the lock mechanism. Move the robotics assembly away from the locking mechanism. For instructions, see <u>Locking or unlocking the robotic assembly manually</u>. Ensure that the robotic assembly is left in the fully locked position. <p>Power on the library.</p>

Table Continued



Event code	Message text and description	Details and solution
2046	Wellness test failed because drive communication test failed.	<ol style="list-style-type: none"> 1. Power off the library. Remove and then reinstall the tape drive to ensure the drive is fully seated. Power on the library. 2. Verify that the drive is running the most recent firmware version. 3. Use the RMI to pull a drive support ticket and check the device analysis section. L&TT must be installed to view a support ticket.
2047	Wellness test failed because the barcode scanning test failed.	<ol style="list-style-type: none"> 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. For instructions, see Clearing obstructions from the library.
2048	Wellness test failed because unlocking the right magazine failed.	<ol style="list-style-type: none"> 1. Ensure that all magazines are fully inserted. 2. Reboot the library and then retry the test.
2049	Wellness test failed because unlocking the left magazine failed.	
2050	Wellness test failed because unlocking the mailslot bank failed.	

Table Continued



Event code	Message text and description	Details and solution
2051	Wellness test failed because the robotic test failed.	<ol style="list-style-type: none"> 1. Check for obstructions in the path of the robotic assembly, such as a cartridge sticking out of a magazine. 2. Ensure that the alignment mechanisms for all modules above the bottom module are engaged and locked. 3. Verify that the rack is level front to back and side to side. 4. Reboot the library and check the event logs for any errors. 5. If the robotic assembly moves front to back, but not vertically, the robot shipping lock could be positioned incorrectly. Move the shipping lock to the fully locked position. If the robotic assembly does not unlock the shipping lock after the reboot: <ol style="list-style-type: none"> a. Move the robotic assembly to the base module from the Maintenance > Move Robotic to Base Module screen. See <u>Moving the robotic assembly to the base module</u>. b. Power off the library. c. Remove all cables from the base module and unlock the alignment mechanisms. d. Extend the base module from the rack. e. Ensure that the robot shipping lock is left in the fully locked position. f. Reassemble in reverse order. g. Power on the library. 6. Ensure that the spooling cable is fully seated in the base module and correctly connected to the robotic assembly.
2052	An open magazine was detected in one or more modules and as a result the system was taken offline.	<ol style="list-style-type: none"> 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. Verify that the library is running firmware version 4.90 or newer.
2053	An open top cover was detected and as a result the system was taken offline.	<ol style="list-style-type: none"> 1. Ensure that the top cover is inserted completely and properly locked. 2. Verify that no items are sitting on top of the library. 3. Do not remove the top cover while the library is powered on. 4. Verify that the library is running firmware version 4.90 or newer.

Table Continued



Event code	Message text and description	Details and solution
2054	An open bottom cover was detected and as a result the system was taken offline.	<ol style="list-style-type: none"> 1. Ensure that the bottom cover is inserted completely and properly locked. 2. Do not remove the bottom cover while the library is powered on. 3. Verify that the library is running firmware version 4.90 or newer.
2055	An open unit lock was detected and as a result the system was taken offline.	<ol style="list-style-type: none"> 1. Ensure that all alignment mechanisms between modules are properly locked. 2. Do not open the alignment mechanism locks while the library is operating and the robot is moving. 3. Verify that the library is running firmware version 4.90 or newer.
2056	Initialization failure due to picker push pull positioning error.	Check 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.
2057	Robotics shipping lock in incorrect position.	<ol style="list-style-type: none"> 1. Ensure that both the top and bottom covers are installed and then reboot the library. 2. If the error event reoccurs, power off the library. For instructions, see Locking or unlocking the robotic assembly manually. Ensure that the robotic assembly is left in the fully locked position. Power on the library. 3. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information.

Table Continued



Event code	Message text and description	Details and solution
2061	Move failed pulling cartridge from drive.	<ol style="list-style-type: none"> 1. Verify that the drive is completely seated in the library and that all the thumb screws are tightened. 2. Check for loose bar code 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 into drive.	<ol style="list-style-type: none"> 1. Verify that the drive is completely seated in the library and that all the thumb screws are tightened. 2. Check 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. If the cartridge still cannot be moved with the OCP, power cycle the drive and then retry the move. If the cartridge still cannot be moved to the drive, power cycle the library, and then retry the move. 4. Ensure that the library and tape drives are running the latest firmware version.

Table Continued



Event code	Message text and description	Details and solution
2063	Move failed positioning picker in front of drive.	<ol style="list-style-type: none"> 1. Check the event log for additional events or event detail that provide more specific information. 2. Power off the library and then check inside the library for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Extending one magazine at a time, 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. d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p>Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u></p> <p>Power on the library.</p> 3. If the error event reoccurs, power off the library and then verify that the robotic assembly is level within the module. <p>If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment.</p> <p>Power on the library,</p>
2064	Library test failed with critical error.	<ol style="list-style-type: none"> 1. Check for additional events that might provide an indication of the reason for the failure. 2. Verify that the minimum requirements are met for the test and then retry the test. 3. To verify robotic movement, perform a slot-to-slot or element-to-element test.
2065	Library startup process failed because of robotics initialization issue.	<ol style="list-style-type: none"> 1. Power off the library and then check inside library for any obstruction the robotic assembly may be hitting. <ul style="list-style-type: none"> • Extending one magazine at a time, 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. • Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p>Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u></p>

Table Continued



Event code	Message text and description	Details and solution
2066	Library startup process failed during inventory scan.	<p>Power on the library.</p> <ol style="list-style-type: none"> <li data-bbox="787 252 1482 420">2. If the error event reoccurs, power off the library and then verify that the robotic assembly is level within the module. If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment, correct if necessary. Power on the library. <li data-bbox="787 483 1482 619">3. If the error event reoccurs, power off the library. For instructions, see Locking or unlocking the robotic assembly manually. Ensure that the robotic assembly is left in the fully locked position. Power on the library. <li data-bbox="787 693 1482 756">4. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. <li data-bbox="787 777 1482 871">5. If the issue is corrected, continue with the next debugging step or return the library to normal operation and clear the event codes. <li data-bbox="787 892 1482 924">6. If the error event reoccurs, replace the robotics assembly.
2067	For safety reasons, the robot movement was halted in place.	The library detected a physical opening in the library and stopped movement of the robotic assembly.
2068	An emergency stop condition was detected in one or more modules and prevented the robotic from initialization.	<ul style="list-style-type: none"> <li data-bbox="787 1060 1482 1186">• 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. <li data-bbox="787 1207 1482 1302">• Ensure that the top and bottom covers are properly installed and locked. Do not unlock or remove the covers while the library is powered on. <li data-bbox="787 1323 1482 1417">• Ensure that all alignment mechanisms between modules are properly locked. Do not open the alignment mechanism locks while the library is operating and the robot is moving. <li data-bbox="787 1438 1482 1470">• Ensure that all modules are powered on. <li data-bbox="787 1491 1482 1554">• Ensure that all module interconnect cables are properly attached.

Table Continued



Event code	Message text and description	Details and solution
2069	Initialization failure due to barcode reader error.	<ul style="list-style-type: none"> • Check the event log for additional events that provide more specific information. • Run the robotic test. • Verify that all cartridges have high-quality proper barcode labels and that the labels are properly applied. • 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.	<ol style="list-style-type: none"> 1. Power off the library and then check inside library for any obstruction the robotic assembly may be hitting. <ul style="list-style-type: none"> a. Extending one magazine at a time, 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. d. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p style="margin-left: 20px;">Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library</u>.</p> <p style="margin-left: 20px;">Power on the library.</p> 2. If the error event reoccurs, power off the library and then verify that the robotic assembly is level within the module. <p style="margin-left: 20px;">If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment, correct if necessary.</p> <p style="margin-left: 20px;">Power on the library.</p> 3. If the error event reoccurs, power off the library. For instructions, see <u>Locking or unlocking the robotic assembly manually</u>. Ensure that the robotic assembly is left in the fully locked position. <p style="margin-left: 20px;">Power on the library.</p> 4. If the error event reoccurs, check the event log for additional events or event detail 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 robotics assembly.

Table Continued



Event code	Message text and description	Details and solution
2071	Cartridge on picker when trying to scan.	<ul style="list-style-type: none"> • Check the event log for additional events that provide more specific information. • Ensure that the library has an open storage slot or mailslot. • If a cartridge is in the robotic assembly, remove it manually. • Inspect the cartridge for damage. Ensure that the cartridge is properly labeled and that the label is in good condition. • Ensure that all the tape drives are fully inserted into the library. • Ensure that each drive is secured with both thumbscrews. • Run the element-to-element test specifying the same elements and media that caused the event. • Run the slot-to-slot test.
2072	Top cover detected at an incorrect position.	<ul style="list-style-type: none"> • Ensure that the top and bottom covers are properly installed and locked.
2073	Bottom cover detected at an incorrect position.	<ul style="list-style-type: none"> • Ensure that all alignment mechanisms between modules are properly locked. • Ensure that all modules are powered on and that all module interconnect cables are properly attached.
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.	
2076	I2C bus signals invalid.	<ol style="list-style-type: none"> 1. Remove all tape drives from the affected module and then reboot the library. If the problem persists, the cause is likely to be in the module. 2. Reinstall one drive after another, rebooting after each one. 3. If the problem comes back, the cause could be in the drive that was most recently added or in the drive slot. 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. 4. If the problem appears to be with the tape drive, use the RMI to pull a drive support ticket and check the device analysis section. L&TT must be installed to view a support ticket.

Table Continued



Event code	Message text and description	Details and solution
2077	Failed to store calibration data to chassis.	Power cycle the library.
2078	The library firmware currently installed does not support the installed robotics assembly type.	The installed robotics assembly has an alternate motor encoder implementation, which is not supported by the installed library firmware. Update the library to 4.80 or newer firmware.
2079	Could not upgrade barcode reader firmware.	<ol style="list-style-type: none"> 1. Power cycle the library. 2. If the error persists, see if the event log shows events related to the spooling mechanism or robotic assembly.
2080	Cartridge lost while inserting it into slot or drive.	<p>A data or cleaning cartridge came loose from the robotic assembly while the cartridge was being inserted into a magazine slot or tape drive.</p> <ol style="list-style-type: none"> 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.
2081	I2C port expander read write error	<p>While this error persists, the base module is not able to communicate with any of the attached expansion modules.</p> <ol style="list-style-type: none"> 1. Verify that all the modules are powered on and that the module interconnect cables are properly connected. 2. Reboot the library to see if the error persists. 3. If the error persists, power off the library and then reseal the base module controller. 4. If the error continues to persist, replace the base module controller.
2082	Drive with Secure Mode enabled has been hot removed while in active status as LUN master.	<p>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.</p> <ol style="list-style-type: none"> 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. <p>The drive can now be safely removed.</p>

Table Continued

Event code	Message text and description	Details and solution
2083	The drive power board is not compatible with this library and does not match the installed power supply.	The library supports different drive power board and power supply revisions. Replace the drive power board or power supplies in the module to have a consistent set of components.
2084	Lost connection to module, possibly due to abnormal network activity.	<ol style="list-style-type: none"> 1. Ensure that all modules are powered on. 2. Verify that all module interconnect cables are properly installed. 3. If this event is seen on multiple modules, ensure that the network that the base module is connected to is not experiencing broadcast storms or other abnormal activity. 4. Reboot or power cycle the library to rediscover the modules.
2085	Communication failure to the base module controller board I2C port expander component.	<p>While this error persists, the base module is not able to discover any of the attached expansion modules.</p> <ol style="list-style-type: none"> 1. Reboot the library to see if the error persists. 2. If the error persists, power off the library and then reseal the base module controller. 3. If the error continues to persist, replace the base module controller.
2086	Communication failure to the expansion module controller board I2C port expander component.	<p>While this error persists, the base module is not able to discover any of the attached expansion modules.</p> <ol style="list-style-type: none"> 1. Reboot the library. 2. If the error persists, power off the library and then reseal the expansion module controller. 3. If the error continues to persist, replace the expansion module controller.
2087	Error accessing the backplane flash memory.	Reboot the library.

Table Continued



Event code	Message text and description	Details and solution
2088	Failure moving to the lowest vertical position of the library, check for obstructions on the bottom cover.	<p>For proper operation, the robotic assembly must be able to reach the bottom of the library.</p> <ol style="list-style-type: none"> 1. Power off the library by pressing the front power button for 5 seconds and then select the Default Park location. 2. Remove the left magazine from the lowest library module and verify that the entire bottom cover is free of objects that might obstruct the robotic assembly path. 3. After clearing any obstructions, replace the magazine and then power on the library. The library will perform its power-on sequence and inventory. 4. Verify that no further critical events were generated.
2090	Wellness test failed because incompatible drive power board detected	Remove incompatible Drive Power Board. Only install Drive Power Boards that are compatible with the library.

Table Continued



Event code	Message text and description	Details and solution
2092	Locking the Robotics Assembly has failed during Power Down process	<p>In normal operation, the library returns the robotic assembly to its home position in the base module, behind the OCP, and sets the lock holding the robotic position when the library is powered off.</p> <p>This event code will be reported if the robotics was NOT able to lock the mechanism during the NEXT POWER ON process. Meaning after a repair is completed the NEXT power on cycle may throw the same error code even though the repair might have been successful. Therefore TWO library power cycles will be required after each repair attempt to determine whether the repair was successful.</p> <ol style="list-style-type: none"> 1. Verify that the library is running the latest firmware version. 2. If the library is running the latest firmware version, power cycle the library. 3. If the error event reoccurs, power off the library, ensure that the robotic assembly is left in the fully locked position. See <u>Locking or unlocking the robotic assembly manually.</u> Power on the library. If the error event reoccurs, after the power-on self test is complete, power cycle the library, AGAIN. 4. If the error event reoccurs, power off the library, check inside library for any obstruction the robotic assembly may be hitting. Extending one magazine at a time, 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. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u> Power on the library. If the error event reoccurs, after the power-on self test is complete, power cycle the library, AGAIN. 5. If the error event reoccurs, check the event log for additional events or event detail that provides 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. 7. If the error event reoccurs, replace the robotics assembly.

Table Continued



Event code	Message text and description	Details and solution
2093	Communication to Robotic Controller could not be established	<p>This event is generated when during startup the communication to the robotics controller could not be established and has failed.</p> <ol style="list-style-type: none"> 1. Power off the library, ensure that the spooling mechanism is fully seated in the base module and properly connected to the robotic assembly. Power on the library. 2. If the error event reoccurs, replace the robotics assembly.
2094	An emergency stop condition was detected in one or more modules and prevented the robotic from running the inventory scan	<p>This event is generated in case an emergency stop condition occurred during inventory scan</p> <ul style="list-style-type: none"> • Ensure that all magazines, top or bottom covers and unit locks are completely inserted and properly locked. • Insert all open magazines and install all necessary covers and unit locks before powering on the library. • Ensure that all modules are powered and have the interconnection cable properly attached.
2101	Inventory scan failed	<p>Power off the library and then check inside library for any obstruction in the horizontal path of the robotic assembly.</p> <ul style="list-style-type: none"> • Extending one magazine at a time, ensure that all tapes are pushed fully into their slots. • Clear away any internal cables that might be in the way. • Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p>Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library.</u></p> <p>Power on the library.</p>

Table Continued



Event code	Message text and description	Details and solution
2102	Inventory scan failed because of a slider axis problem	<p>Power off the library and then check inside library for any obstruction to horizontal movement of the robotic assembly.</p> <ul style="list-style-type: none"> • Extending one magazine at a time, ensure that all tapes are pushed fully into their slots. • Clear away any internal cables that might be in the way. • Clear any obstructions from the bottom of the library. • Clear any loose tape cartridge from the elevator. • Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p>Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. For instructions, see <u>Clearing obstructions from the library</u>.</p> <p>Power on the library.</p>
2103	Incorrect stack assembly, too many expansion modules below main library	Ensure that not more than three expansion modules are mounted and connected below or above the base module.
2104	Incorrect stack assembly, too many expansion modules above main library	Ensure that no more than three expansion modules are mounted and connected below or above the base module.

Warning events

Event code	Message and description	Details and solution
4000	A reported drive canister fan speed is too slow.	Ensure that there are no obstructions to the drive fans.
4002	A drive sent a clean request.	Clean the drive with an approved cleaning cartridge.
4003	The drive configuration failed.	<ol style="list-style-type: none"> 1. Power off the library. Remove and then reinstall the tape drive to ensure 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 and modules from the RMI Configuration > System page. 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.

Table Continued



Event code	Message and description	Details and solution
4004	The drive status request failed.	<ol style="list-style-type: none"> 1. Power off the library. Remove and then reinstall the tape drive to ensure the drive is fully seated. Power on the library. Retry the operation. 2. If the problem persists, reset the drive from the RMI Configuration > Drives page. 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.	<ol style="list-style-type: none"> 1. Power cycle the drive and then verify whether the drive reports the same TapeAlert. 2. 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.
4006	A drive temperature reported is above the threshold.	<ol style="list-style-type: none"> 1. Verify that the drive fan is spinning and not obstructed. 2. Verify that the ambient temperature is within specification. 3. Verify that the drive cover plates are installed in all open drive bays. The drive cover plates are required for proper airflow within the library.
4007	Cartridge error.	<ol style="list-style-type: none"> 1. Remove the cartridge and inspect it for damage. 2. Retry the operation with another cartridge.
4008	Cleaning cartridge expired.	Discard the cleaning cartridge and retry the cleaning operation with a new cleaning cartridge.
4009	Firmware upgrade of one or multiple expansion modules failed.	<p>The base module must be able to communicate with a powered on and connected expansion module to perform the upgrade.</p> <ol style="list-style-type: none"> 1. Reseat the expansion module controller. 2. Check the module interconnect cable and power connections. 3. Retry the firmware upgrade.

Table Continued



Event code	Message and description	Details and solution
4010	Drive is not compatible with this library.	<ol style="list-style-type: none"> 1. Power off the library. 2. Remove the incompatible drive. 3. Install a compatible drive. Only install drives that are supported by the library. For instructions, see <u>Installing or replacing a tape drive.</u> 4. Power on the library.
4012	Move cartridge operation failed due to drive or media issue.	<ol style="list-style-type: none"> 1. Check events occurring at the same time for drive or media problems. 2. Retry the operation with the same source and destination. If the problem persists, retry the operation with a different cartridge in the same drive 3. If the problem follows the media, remove the cartridge from use. 4. If the problem follows the drive, 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.
4014	Library test failed due to a drive issue.	<ol style="list-style-type: none"> 1. Verify the test parameters and then retry the test. 2. Check 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.

Table Continued



Event code	Message and description	Details and solution
4015	Power supply has failed. Redundancy is not available.	<ol style="list-style-type: none"> 1. Verify that each module has two power supplies installed. 2. Ensure that all power supplies are installed properly. 3. Verify that all power sources are supplying power that is within the product requirements. 4. Verify that all power supplies have the white LED on, the amber LED off and the green light on. <ul style="list-style-type: none"> • If the white light is on, verify that the power cords are properly plugged in. • If the amber LED is on, replace that power supply. 5. Verify that the library is running firmware version 4.90 or newer.
4016	Backup configuration data to base module failed.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Verify that the firmware file is correct for the drive.
4019	General drive firmware bundle upgrade failure.	<ol style="list-style-type: none"> 2. Ensure that the drive is in a healthy state and does not have a cartridge. 3. 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.

Table Continued



Event code	Message and description	Details and solution
4021	Drive has been hot removed while in active status as data transfer device.	<p>Drives must be powered off before removing them from the library.</p> <ol style="list-style-type: none"> 1. Power off the library. 2. Reinstall the removed tape drive in the same position from which it was removed. <p>For instructions, see <u>Installing or replacing a tape drive</u>.</p> <ol style="list-style-type: none"> 3. Power on the library.
4022	A full-height drive in incorrect boundary location.	<p>Full-height drives will only operate in the top, bottom, or middle pair of half-height drive bays. Reinstall the tape drive in an acceptable location.</p>
4025	Library test failed due to a cartridge error.	<ol style="list-style-type: none"> 1. Remove the cartridge and inspect it for damage. 2. 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.	<ol style="list-style-type: none"> 1. Verify that the LTO generation on the barcode label media ID matches the LTO generation of the data cartridge. 2. Remove cartridges that are incompatible with the drives in the library.
4029	Incompatible media move operation blocked by media barcode ID check.	<p>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.</p>
4030	Move cartridge operation failed due to media error.	<p>Remove the cartridge and inspect it for damage. If the operation fails again, retry the operation with another cartridge.</p>
4032	Connection to the ESKM failed.	<ol style="list-style-type: none"> 1. Verify that the configured IP addresses and/or hostnames are correct. 2. Verify the username and password configured to log in to the ESKM server. 3. Verify that all necessary SSL certificates have been configured. 4. Verify that the ESKM server is reachable within the network.

Table Continued



Event code	Message and description	Details and solution
4033	Unsupported key generation (keygen) policy.	<ol style="list-style-type: none"> 1. Check the network connection and ESKM server configuration for the specified partition. 2. After ensuring that all partitions have the same KeyGenPolicy, rerun the Expert Partitioning wizard for the specified partition. 3. From the Status > Security screen, verify that all drives and partitions are configured correctly for encryption. <p>Example ESKM server KeyGenPolicy for a three-partition library: SER1020633_LL01 KT SER1020633_LL02 KT SER1020633_LL03 KT</p>
4034	Key not found on ESKM server.	Verify that the requested key is available on the ESKM server. Check the ESKM server logs for additional details.
4035	Key creation on ESKM server failed.	Check the ESKM server logs for additional details about why key creation failed.
4036	ESKM configuration invalid.	Use the ESKM configuration wizard to verify the ESKM configuration.
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.
4039	The drive configuration failed because of unsupported ACPF features selected.	<ul style="list-style-type: none"> • If the drive is an LTO-6 drive, verify that the drive 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.
4040	Data path failover occurred.	Check the cabling and all network components between the affected drive and host computer.

Table Continued



Event code	Message and description	Details and solution
4041	Wellness test failed because power supply redundancy test failed.	<ul style="list-style-type: none"> • Ensure that all power supplies are installed properly. • Ensure that each power supply is connected to a valid AC power source. • Verify that all power supplies have the white LED on, the amber LED off, and the green light on. <ul style="list-style-type: none"> ◦ If the white light is on, verify that the power cords are properly plugged in. ◦ If the amber LED is on, replace that power supply.
4042	ESKM feature not licensed.	Disable ESKM or install the necessary ESKM license.
4043	Control path failover occurred.	<p>This event applies to Advanced Control Path Failover.</p> <p>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.</p> <p>Check the cabling and all network components between the affected drive and host computer.</p>
4044	One of the library tests failed because a source element or destination element is not accessible.	<p>The library either could not find the source cartridge or the destination element was unexpectedly full. This error can happen if a cartridge in the destination element has an unreadable barcode label.</p> <ol style="list-style-type: none"> 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 proper barcode label.

Table Continued



Event code	Message and description	Details and solution
4045	Drive is offline because no ESKM key generation policy available.	<ol style="list-style-type: none"> 1. Check the network connection and ESKM server configuration for the specified partition. 2. After ensuring that all partitions have the same KeyGenPolicy, rerun the Expert Partitioning wizard for the specified partition. 3. From the Status > Security screen, verify that all drives and partitions are configured correctly for encryption. Test connectivity using the Connectivity Check button. <p>Example ESKM server KeyGenPolicy for a three-partition library:</p> <pre>SER1020633_LL01 KT SER1020633_LL02 KT SER1020633_LL03 KT</pre>
4046	The drive configuration failed because of missing DPF license.	Disable path failover or install the necessary failover license.
4047	The drive configuration failed because of missing CPF license.	
4048	The drive configuration failed because of unsupported BDPF feature selected.	Disable basic path failover for this drive or replace the drive with one supporting this feature.
4049	The drive configuration failed because of unsupported BCPF feature selected.	
4050	Basic datapath failover occurred.	Check cabling and all network components between the affected drive and host computer.
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.	
4053	Manual control path failover from active to passive drive failed; partition may be disconnected from host.	Check cabling and all network components between the affected drive and host computer.
4054	Chassis fan failed	<p>Check the event details to see which chassis fan failed.</p> <p>Verify that the chassis fan is spinning and there are no obstructions in the fan.</p>

Table Continued



Event code	Message and description	Details and solution
4056	Failed to copy settings from active to passive drive in basic control path failover.	The partition no longer has a passive drive that is available for control path failover. Reconfigure the partition so that at least one drive in the partition is available for control path failover.
4057	Passive control path drive not available for control path failover.	Verify that the configured control path failover drive is present, powered on, and ready to accept the control path.
4058	Disabling active control path drive caused failover to passive one.	If the failover is 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.
4059	A drive that does not support encryption is configured in a partition with encryption enabled.	A drive that does not support encryption is configured as part of a partition with encryption enabled. The library has taken the drive offline. Replace the drive with an LTO-4 or later generation drive or disable encryption for the partition.
4060	Connection to the KMIP server failed.	<ol style="list-style-type: none"> 1. Verify the username and password configured to log in to the 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 hostnames are correct.
4061	Key not found on KMIP server.	Verify that the requested key is available on the KMIP server. Check the KMIP server logs for additional details.
4062	Key creation on KMIP server failed.	Check the KMIP server logs for additional details about why key creation failed.
4063	KMIP configuration invalid.	Use the KMIP configuration wizard to verify the KMIP configuration.
4064	KMIP feature is not licensed.	Disable the KMIP feature or install the necessary license.
4065	A tape alert event was reported by a drive.	Check event details for additional information.
4066	Automatic control path failover by disabling LUN drive failed; partition may be disconnected from host.	Check 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.

Table Continued



Event code	Message and description	Details and solution
4069	Configuring the drive default map ID was not possible.	Ensure that the drive is powered on, is communicating with the library, and has current firmware. If this error persists, disable Secure Manager for the library and re-enable it. Secure Manager is only supported on LTO-4 and later generation FC drives.
4070	Key not found on ESKM server and key not available on MSL Encryption Kit token.	Verify that the requested key is either available on the key server or that the key server token containing the requested key is inserted and logged in.
4071	Power supply fan failed.	Verify that the power supply fan is spinning and ensure that there are no obstructions in the fan.
4072	No cleaning cartridge in partition available for auto cleaning.	<p>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.</p> <p>The cleaning cartridge label must begin with the letters “CLN” for the library to recognize it as a cleaning cartridge. For more information about auto cleaning, see Configuring auto cleaning.</p> <ol style="list-style-type: none"> 1. 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. 2. Perform a load and unload on any drives that need cleaning to initiate autocleaning.
4073	Medium source element empty.	<ol style="list-style-type: none"> 1. Visually inspect the source slot and then rescan inventory.
4074	Medium source element empty.	<ol style="list-style-type: none"> 2. Verify that the cartridge has a valid and readable barcode label. 3. Rescan the inventory from the backup application.

Table Continued



Event code	Message and description	Details and solution
4075	Cartridge lost while extracting it from the slot/drive.	<ol style="list-style-type: none"> 1. Inspect the source element and ensure that there are not 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.	<ol style="list-style-type: none"> 1. Verify that all magazines are fully inserted in the library.
4078	Unlocking the left magazine failed.	<ol style="list-style-type: none"> 2. Power cycle the library and then retry the operation.
4079	Unlocking the mailslot failed.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.
4082	Magazine release motor initialization failure.	<ol style="list-style-type: none"> 1. Verify that all magazines are fully inserted in the library. 2. Power cycle the library and then retry the operation. 3. If the problem persists, power off the library and then release the magazine manually. 4. Check for obstructions or damage near the magazines.

Table Continued



Event code	Message and description	Details and solution
4083	Library not properly calibrated. Lack of calibration might cause media movement failures.	<ol style="list-style-type: none"> 1. Verify that the library is running the most recent firmware version. 2. Power cycle the library. The library initiates the calibration operation during power-on. If the calibration operation does not begin during the power-on or the error persists, initiate the auto calibrate operation from the Maintenance > Auto Calibration RMI screen. <p>For more information about auto calibration, see Calibrating the library.</p> <hr/> <p>NOTE: The Auto Calibration routine can take up to 15 minutes per module. The library will be offline to hosts while the routine is running.</p>
4084	Failed reading logged in hosts table.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Check for additional events that might provide an indication of the reason for the failure. 2. Check 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.	<ol style="list-style-type: none"> 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.
4088	Library not properly calibrated. This might cause media movement failures.	Some chassis calibration data does not match the installed robotic assembly.

Table Continued

Event code	Message and description	Details and solution
4089	Auto calibration of one or more modules failed. Library not properly calibrated. Lack of calibration might cause media movement failures.	<ol style="list-style-type: none"> 1. Verify that the library is running the current firmware version. 2. Power cycle the library. The library initiates the calibration operation during power-on. If the calibration operation does not begin during the power-on or the error persists, initiate the auto calibrate operation from the Maintenance > Auto Calibration RMI screen.
4090	Auto calibration of one or more modules failed. Library not properly calibrated. Lack of calibration might cause media movement failures.	
4091	Auto calibration of one or more modules failed. Library not properly calibrated. Lack of calibration might cause media movement failures.	<p>For more information about auto calibration, see Calibrating the library.</p> <p>NOTE: The Auto Calibration routine can take up to 15 minutes per module. The library will be offline to hosts while the routine is running.</p>
4092	Installed robotic does not support auto calibration.	<p>This warning event is generated when newer library firmware attempts to auto calibrate some robotic assembly types. If there are no related move events, this warning can be ignored.</p> <ol style="list-style-type: none"> 1. Check for additional events that occurred at the same time. If there are no additional events, this warning can be ignored. 2. If there are associated move events, run the slot to slot test. 3. Verify that the robotic assembly is level within the module. If the module was recently moved or the robotic assembly replaced, the assembly could be out of alignment. 4. If the library continues having move failures, contact service.
4093	Could not obtain an IP address from a DHCP server.	<ol style="list-style-type: none"> 1. Check the network configuration settings from the Status > Network screen. 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 from the Configuration > Network screen or unplugging the network cable and then plugging it in after a few seconds.
4094	Drive interface I/O error.	Reboot the library to reinitialize the hardware and device drivers.

Table Continued

Event code	Message and description	Details and solution
4095	Library test failed. Not enough valid cartridges available for testing.	<ol style="list-style-type: none"> 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.
4096	Chassis fan will not be operational if no drive power board is installed in the right drive power board slot.	Install the drive power board in the correct drive power board slot and then connect the chassis fan.
4097	Drive port configured to NPIV but failed to negotiate with Fibre Channel switch.	<ol style="list-style-type: none"> 1. Verify that the FC switch supports NPIV and that this option is enabled for the port connected to the tape drive. 2. If the problem persists, disconnect and reconnect the cable after changing the FC switch NPIV configuration. 3. If your infrastructure cannot support NPIV, disable basic control path failover.
4098	System time synchronization through SNTP failed.	<ol style="list-style-type: none"> 1. Verify that the SNTP server address in the Configuration > System > Date and Time Format screen is valid. 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.
4100	Drive with FIPS Secure Mode enabled has been hot removed while in active status as data transfer device.	LTO-6 tape drives with FIPS Secure Mode enabled must be powered off before removing them from the library. For additional information and instructions, see Disabling Secure Mode for an LTO-6 tape drive .
4101	The drive configuration failed. FIPS Secure Mode is not supported.	<ol style="list-style-type: none"> 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 partition FIPS Support Mode settings are correct.

Table Continued



Event code	Message and description	Details and solution
4103	The drive configuration failed during disabling FIPS secure mode for the tape drive.	An LTO-6 drive probably had Secure Mode enabled in a library and then the drive was removed without first powering off the drive. For additional information and instructions, see <u>Disabling Secure Mode for an LTO-6 tape drive.</u>
4104	Drive configuration failed because of missing ESKM connection.	The drive timed out while trying to retrieve the encryption policy from the ESKM server. If the drive is configured for ESKM encryption, see the corresponding warning events that describe any encryption server connection errors.
4105	Drive configuration failed during enabling FIPS Secure Mode for the tape drive.	An LTO-6 drive probably had Secure Mode enabled in a library and then the drive was removed without first powering off the drive. For additional information and instructions, see <u>Disabling Secure Mode for an LTO-6 tape drive.</u>
4106	The drive configuration failed while enabling FIPS Secure Mode for the tape drive.	Rerun the FIPS Support Mode wizard to generate certificates or disable FIPS Support Mode. For additional information and instructions, see <u>Configuring FIPS Support Mode .</u>
4107	The key generation encryption policy on the ESKM server changed.	To ensure that the drive encryption configuration is updated appropriately for the new key generation policy setting, run the Expert Partition Wizard for the specified partition. For additional information and instructions, see <u>Using the expert partition wizard.</u> If any of the partitions have FIPS Support Mode enabled, also run the FIPS Support Mode wizard. For additional information and instructions, see <u>Configuring FIPS Support Mode.</u>
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 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.

Table Continued



Event code	Message and description	Details and solution
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 tape drive. NOTE: The drive primary ports are offline and the drive status reports FIPS not supported.
4110	Drive disabled due to an incompatible Drive Power Board	Remove incompatible Drive Power Board. Only install Drive Power Boards that are compatible with the library.
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 into an LTO-7 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 tape drive.
4112	Move cartridge failed due to cartridge not seating properly.	<ol style="list-style-type: none"> 1. Look for surrounding 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.	Retry the operation. If the problem persists, verify that the library is running the latest released firmware version.
4121	No compatible media available for system test.	Verify 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 the library has tape media installed.

Table Continued

Event code	Message and description	Details and solution
4123	No empty slot available for slot to slot test.	Verify 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.	<ol style="list-style-type: none"> 1. Check 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.	<ol style="list-style-type: none"> 1. View the list of host WWNN addresses listed in the event text. <ul style="list-style-type: none"> • 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.
4129	Media removal prevented by drive	Check backup application how to allow media removal from drive. If unsuccessful try Force Drive Media Eject option in operations menu.
4130	Wellness test failed because drive not finally initialized	Wait until drive initialization completed and run test again
4134	Not all slots successfully scanned	<p>The inventory scan failed to detect the status of all affected slots.</p> <ul style="list-style-type: none"> • Rescan the inventory from RMI. If problem persists, replace the spooling mechanism. • Verify that the barcode labels are properly applied and in good condition. • See the event logs for additional events that could indicate a cause.
4145	Key not available on MSL Encryption Kit token	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.
4147	Type M cartridge without a Type M barcode detected.	Replace cartridge barcode label by correct version.

Table Continued



Event code	Message and description	Details and solution
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 can not 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • The IP settings (IP Address, Gateway and Netmask) and confirm them with your IT personnel. • The Firewall settings on the target machine are correct.
4156	The TLS connection could not be established because of Handshake errors during certificate exchange.	Verify the following: <ul style="list-style-type: none"> • 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 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.

Table Continued



Event code	Message and description	Details and solution
4159	The TLS server certificate could not be verified as a valid and trusted certificate.	Check 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.
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.
4174	KMIP CA certificate failure	<p>The CA certificate could not be verified as a valid and trusted certificate.</p> <ul style="list-style-type: none"> • Verify that the correct CA certificate was used. • Verify that the CA certificate on the encryption server is current.

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.
8008	The system language setting changed.
8009	The timezone configuration has changed.
8010	A new partition was added.
8011	The network settings have changed.

Table Continued



Event code Message and description

8012	All expansion modules upgraded. The firmware for all expansion modules has been upgraded.
8013	The NTP time synchronization configuration has changed.
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. See Default and restore defaults settings .
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.
8023	MSL Encryption Kit/ESKM migration configuration changed.
8024	Mailslot / Magazine access control configuration changed.
8025	Mailslot / Magazine automatic re-lock duration changed.
8026	Robotics assembly change detected. The robotics assembly has been replaced.
8027	Power board has been exchanged. A drive power board has been exchanged or added.
8028	Power supply has changed. A power supply has been moved within the library or 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.

Table Continued



Event code	Message and description
8033	The OCP module has been 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.
8035	Chassis calibration data has been changed.
8036	New chassis detected. One of the modules has been replaced.
8037	Chassis has been removed. One of the expansion modules has been removed from the library.
8038	New hardware component first time detected in this library and added to system configuration. The library detected a new replaceable hardware component, such as a power supply, power board, or chassis fan, and has started monitoring the new component. Removing the component will create an alert and set the library in warning status.
8039	Hardware autodetection status reset to default values.
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.
8046	Logout prevention configuration changed.
8047	FIPS Secure Mode configuration changed.
8056	Command View TL configuration changed.
8059	A hardware component of the library has been replaced.
8060	New Expansion Controller detected.
8061	New Base Library Controller detected.
8062	Auto calibration successfully finished.
8064	Password rules configuration changed.

Table Continued



Event code	Message and description
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.

Informational events

Event code	Message
9000	A tape alert flag was reported by a drive.
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.

Table Continued



Event code	Message
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.
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.
9030	An incompatible MSL Encryption Token was inserted.
9031	Library health status changed to status "OK".
9032	Library health status changed to status "Warning".
9033	Library health status changed to status "Critical".
9034	New system controller detected. The library detected a new module controller
9035	New library chassis detected. The library detected a new expansion module.
9036	Key on key server created.
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. In case of an error, one or more warning events will be generated.
9044	Key from MSL encryption token migrated.

Table Continued



Event code	Message
9045	Library configuration data failed to duplicate onto the base module. <ol style="list-style-type: none"> 1. Attempt to save the library configuration from the Configuration > System, Save/Restore Configuration screen. If additional information, see <u>Saving the library configuration</u>. 2. Power cycle the library. 3. Retry the operation.
9046	The chassis fan speed could not be determined. This is not a critical event. This fan provides enhanced cooling for unusually high temperature environments. The chassis fan can be removed without interrupting the library operation. Remove the chassis fan, check for any obstructions in the fan, and reinsert it. If the chassis fan event persists after it is removed and reinserted, the fan should be replaced when convenient.
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.
9054	Not at BOT without read.
9055	MSL Encryption Kit key server token not present.
9056	MSL Encryption Kit key server token was inserted.
9057	MSL Encryption Kit key server token was removed.
9058	Power supply fan failed.
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.
9071	MSL Encryption Kit has been password set automatically.



Technical specifications

Physical specifications

Table 12: Physical specifications

Characteristic	Product alone	Packaged
Height	268 mm	615 mm
Width	475 mm	800 mm
Depth	892 mm	1200 mm
Weight	Base module: 41.0 kg Expansion module: 36.50 kg	Base module: 54.5 kg Expansion module: 50.0 kg

Each module is shipped on a wooden pallet. For storage purposes, pallets may be stacked three high.

Environmental specifications

Table 13: Environmental specifications

Characteristic	Specification	
	LTO-7 and LTO-8	LTO-5 and LTO-6
Temperature		
Operating	10° to 35° C up to 3000m 10° to 30° C above 3000m and up to 4000m	10° to 35° C
Storage	-30° to 60° C	
Temperature shock immunity — maximum rate of change	10° C per hour	
Miscellaneous		
Dust concentration	ISO 14644 -1 Class 8	less than 200 microgram / cubic meter
Altitude	4000 meters (see operating temperature)	4000 meters

Table Continued



Characteristic	Specification	
	LTO-7 and LTO-8	LTO-5 and LTO-6
Humidity		
Operating	20% to 80% RH (noncondensing, max wet bulb temperature = 26C)	
Nonoperating	10% to 90% RH noncondensing	10% to 95% RH noncondensing

Electrical specifications

Table 14: Electrical specifications

Characteristic	Specification
Current	5.0—3.5 A
Voltage	100—240 V 50/60 Hz
Power	350 W

Regulatory specifications

Table 15: Product safety test conditions

Characteristic	Tested condition or value
Equipment mobility	Stationary—rack mount
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%, +6%
Tested for IT power systems	No
IT testing, phase-phase voltage (V)	N/A

Table Continued



Characteristic	Tested condition or value
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 2000
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, this product has been 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 this product, always refer to this regulatory model number. The regulatory model number is not the marketing name or model number of the product.

The Regulatory Compliance label is located 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-1101-CM (Control module) and LVLDC-1101-EM (Expansion module)

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/Safety-Compliance-EnterpriseProducts>

Manufacturer: Hewlett Packard Enterprise Company, Palo Alto, California

Manufacturer's representative: ZAO Hewlett-Packard A.O.



Default and restore defaults settings

Table 16: Default settings

Parameter	Default setting	Reset to default?
Users and passwords		
Administrator login	User: administrator	No
	Password: null	
Security login	User: security	No
	Password: security	
User login	User: user	
	Password: null	
Network configuration (eth0)		
DHCP	Enabled	
Host name	Blank	
IP address	(obtain from DHCP)	
Subnet mask	(obtain from DHCP)	
Default gateway	(obtain from DHCP)	
Network configuration		
IPv4	Enabled	No
DHCPv4	Enabled	No
IPv6	Disabled	No
Static V6	Disabled	No
Stateless V6	Disabled	No
DNS configuration	Blank	No
Network access services		
Primary network interface (eth0)	Enabled	
SSH	Disabled	
SSL	Disabled	
Slots		
Mailslots	Disabled	Yes

Table Continued



Parameter	Default setting	Reset to default?
Administrator password required for mailslot removal	Enabled	Yes
Reserved slots	0	Yes
Partitions	Disabled (no partitions)	Yes
Date and Time		
NTP/SNTP setting	Disabled	Disabled with configuration retained
Date	Blank or existing	
Time	Blank or existing	
Time zone	GMT	
E-mail notifications (SMTP)	Disabled	Disabled with configuration retained
SNMP/SMI-S		
SNMP v1, v2, v3	Disabled	Disabled with configuration retained
SCSI defaults		
Library product ID—INQUIRY product ID string (Std Inquiry page)	MSL6480	
Library vendor ID—INQUIRY vendor ID string (Std Inquiry page)	HP	
Library product ID—INQUIRY product ID string (INQ page CC)	MSL6480	
Library vendor ID—INQUIRY vendor ID string (INQ page CC)	HP	
SCSI element addressing	Starting element addresses in decimal: <ul style="list-style-type: none"> Slot: 1001 Picker: NA Drives: 1 I/E slots: 101 Values in hex: <ul style="list-style-type: none"> Slot: 0x3E9 Picker: NA Drives: 0x1 I/E slots: 0x65 	Yes

Table Continued



Parameter	Default setting	Reset to default?
Miscellaneous settings		
Return drive serial numbers to host	Enabled	
Return barcodes to host (RES SCSI data)	Enabled	
Barcode format and length returned to host	8 digits, left justified	Yes
Language settings	English	Yes
Auto unload (library controlled unload)	Enabled	
Log tracing	Continuous, all levels selected	Yes
Ignore barcode media ID	Disabled	Yes
All licensed features	Disabled	Disabled, configuration retained where possible
Licenses	Not applicable	Not deleted
OCP		
Barcode format displayed on OCP	8 digits, left justified	Yes
OCP contrast		No
Screen saver		Yes
Drive defaults		
Drive speed and topology setting	Auto speed/Fabric	Yes
Drive hosting the library LUN	Drive 1 or the lowest numbered existing drive	Yes
Drive power	All drives powered on	Yes
Auto clean	Disabled	Yes
PLR for both drives and library	Disabled	Yes, Command View TL receiver IP cleared



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.

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 authorized reseller install the part.

NOTE:

For more information on static electricity, or assistance with product installation, contact your authorized reseller.



Websites

General websites

Hewlett Packard Enterprise Information Library

<https://www.hpe.com/info/EIL>

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

<https://www.hpe.com/storage/spock>

Storage white papers and analyst reports

<https://www.hpe.com/storage/whitepapers>

For additional websites, see [Support and other resources](#).

HPE StoreEver library websites

For more information on StoreEver products, see <https://www.hpe.com/storage/msl>.

For the most current list of supported devices, see the StoreEver Support Matrix at <https://www.hpe.com/storage/StoreEverSupportMatrix>.

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

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

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>

Hewlett Packard Enterprise Support Center: Software downloads

<https://www.hpe.com/support/downloads>

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 Passport 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 will initiate a fast and accurate resolution based on your product's service level. 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.

Remote support and Proactive Care information

HPE Get Connected

<https://www.hpe.com/services/getconnected>

HPE Proactive Care services

<https://www.hpe.com/services/proactivecare>

HPE Datacenter Care services

<https://www.hpe.com/services/datacentercare>

HPE Proactive Care service: Supported products list

<https://www.hpe.com/services/proactivecaresupportedproducts>

HPE Proactive Care advanced service: Supported products list

<https://www.hpe.com/services/proactivecareadvancedsupportedproducts>

Proactive Care customer information

Proactive Care central

<https://www.hpe.com/services/proactivecarecentral>

Proactive Care service activation

<https://www.hpe.com/services/proactivecarecentralgetstarted>

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

<https://www.hpe.com/support/ProLiantServers-Warranties>

HPE Enterprise and Cloudline Servers

<https://www.hpe.com/support/EnterpriseServers-Warranties>

HPE Storage Products

<https://www.hpe.com/support/Storage-Warranties>

HPE Networking Products

<https://www.hpe.com/support/Networking-Warranties>

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, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

