



Hewlett Packard
Enterprise

HPE Storage 1/8 G3 Tape Autoloader User and Service Guide

Part Number: 20-STG-18ALG3-UG-ED3

Published: September 2025

Edition: 3

HPE Storage 1/8 G3 Tape Autoloader User and Service Guide

Abstract

This guide provides information on installing, configuring, upgrading, and troubleshooting the tape autoloader. This guide is intended for system administrators and other users who need physical and functional knowledge of the tape autoloader. This guide applies to the 1/8 G3 Tape Autoloader, Product Number: R1R75B. Regulatory model number: LVLDC-0501, Type: 1U.

Part Number: 20-STG-18ALG3-UG-ED3

Published: September 2025

Edition: 3

© Copyright 2006–2025 Hewlett Packard Enterprise Development LP

Notices

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

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

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

Acknowledgments

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

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

Table of contents

- [Notices](#)
- [Acknowledgments](#)
- [Features](#)
 - [Autoloader front panel](#)
 - [Front Panel LEDs](#)
 - [Autoloader back panel](#)
 - [Controller health status indicators](#)
 - [Tape drive back panels](#)
 - [LTO-6 FC tape drive back panels](#)
 - [LTO-7, LTO-8, and LTO-9 FC tape drive back panel](#)
 - [LTO-6 SAS tape drive back panel](#)
 - [LTO-7, LTO-8, and LTO-9 SAS tape drive back panel](#)
 - [Autoloader options](#)
 - [HPE Storage 1/8 Tape Autoloader and MSL Tape Libraries Encryption Kit](#)
 - [Command View TL TapeAssure](#)
 - [LTFS Support](#)
 - [Hardware-based encryption](#)
 - [KMIP-based key servers](#)
 - [Application-managed encryption](#)
- [Installing the tape autoloader](#)
 - [FC connection information](#)
 - [SAS connection information](#)
 - [Location requirements](#)
 - [Preparing the host](#)
 - [Unpacking the shipping container](#)
 - [Attaching the feet](#)
 - [Removing the shipping lock](#)
 - [Installing the autoloader in a rack](#)
 - [Installing the tape drive](#)
 - [Connecting the FC cable](#)
 - [Connecting the SAS cable](#)
 - [Powering on the autoloader](#)
 - [The RMI](#)
 - [Configuring the autoloader network](#)
 - [Network configuration information](#)
 - [Finding the IPv4 IP address obtained through DHCP](#)
 - [Configuring IPv4 networking from the OCP](#)
 - [Setting the date and time](#)
 - [Setting the administrator password](#)

- Configuring the FC interface
- Labeling the tape cartridges
- Verifying the host connection
- Verifying the installation
 - Downloading product firmware
- Configuring additional features
- Tape cartridges and magazines
 - Tape cartridges
 - LTO-9 Media initialization
 - LTO-7 Type M media for LTO-8 drives
 - Recommended practices for using and maintaining tape cartridges
 - Recommended practices for labeling tape cartridges
 - Write-protecting data cartridges
 - Read and write compatibility
 - Supported media
 - Magazines
 - Autoloader slot numbering
- Operating the autoloader
 - Autoloader user interfaces
 - The RMI
 - The autoloader OCP
 - OCP menu
 - Logging in to the autoloader
 - Autoloader users and roles
 - Resetting the RMI administrator password
 - Resetting the RMI administrator password and OCP PIN
 - The autoloader RMI main screen
 - Configuring the autoloader
 - Default and restore defaults settings
 - Configuring the simplest configuration
 - Managing the autoloader configuration
 - Saving the autoloader configuration
 - Restoring the autoloader configuration from a file
 - Resetting the autoloader configuration to the default settings
 - Resetting the list of known drives
 - Managing the autoloader date and time
 - Setting the timezone
 - Setting the date and time format
 - Setting the date and time
 - Enabling SNTP (Simple Network Time Protocol) synchronization
 - Configuring media barcode compatibility checking

- Enabling media barcode compatibility checking
 - Disabling media barcode compatibility checking
- Managing license keys
- Setting RMI Language
- Configuring the RMI timeout
- Configuring the autoloader network settings
- Using the Configuration > Network Management screen
 - SNMP options
 - Adding an SNMP target
 - Editing information for an SNMP target
 - Deleting an SNMP target
 - Clearing all SNMPv3 options
- Configuring remote logging
- Configuring event notification parameters
- Configuring tape drives
 - Configuring barcode handling
- Enabling or disabling mailslots
- Partition wizards
 - Using the basic partition wizard
 - Using the expert partition wizard
 - Deleting a partition using the expert partition wizard
- Encryption configuration
 - Setting the default configuration mode for new partitions
 - Allowing the administrator to configure encryption with the Expert Partition Wizard
 - Setting the encryption mode for a partition
- MSL Encryption Kit configuration
 - Entering the key server token password when using the MSL Encryption Kit
 - Viewing the keys on the key server token when using the MSL Encryption Kit
 - Changing the key server token password when using the MSL Encryption Kit
 - Changing the key server token name when using the MSL Encryption Kit
 - Generating a new write key when using the MSL Encryption Kit
 - Configuring automatic key generation when using the MSL Encryption Kit
 - Backing up the key server token data to a file when using the MSL Encryption Kit
 - Restoring key server token data from a backup file when using the MSL Encryption Kit
 - Configuring the key server token log in behavior when using the MSL Encryption Kit
- Using the KMIP wizard
- Configuring FIPS Support Mode
 - FIPS Support Mode prerequisites
- Secure Mode
 - Disabling Secure Mode for an LTO-6 tape drive
 - Disabling Secure Mode for an LTO-7 or later tape drive

- Configuring local user accounts
 - Configuring user account settings
 - Adding a local user account
 - Setting or modifying a user password
 - Allowing magazine and mailslot access for the “user” user
 - Changing the OCP PIN from the RMI
 - Changing the OCP PIN from the OCP
 - Removing a local user account
- Configuring LDAP user accounts
 - Prerequisites for configuring LDAP user accounts
- Configuring Command View for Tape Libraries integration
- Moving CVTL access to a new Management Station
 - Removing the CVTL Management Station trap destination
- Configuring the autoloader RMI
 - Enabling secure communications
 - Adding a signed certificate for SSL/TLS connections
 - Backing up a custom certificate
 - Restoring a custom certificate
 - Configuring the RMI session timeout
 - Enabling OCP/RMI session locking
 - Restricting RMI access for the administrator and security users
- Secure Manager
 - Enabling Secure Manager
 - Creating an access group when using Secure Manager
 - Changing the name of an access group when using Secure Manager
 - Deleting an access group when using Secure Manager
 - Adding a host to an access group when using Secure Manager
 - Removing a host from an access group when using Secure Manager
 - Configuring device access when using Secure Manager
 - Creating a host when using Secure Manager
 - Changing the name of a host when using Secure Manager
 - Deleting a host when using Secure Manager
- Maintaining the autoloader
 - Performing the system test
 - Performing the slot to slot test
 - Performing the element to element test
 - Performing the position test
 - Performing the wellness test
 - Performing the robotic test
 - Viewing log files
 - Downloading log and trace files

- Managing autoloader firmware
 - Updating autoloader firmware from the RMI
 - Updating autoloader firmware from the OCP
- Updating drive firmware from the RMI
- Updating drive firmware from the OCP
- Downloading a tape drive support ticket
- Downloading an autoloader support ticket
- Rebooting the autoloader
- Rebooting a tape drive
- Clearing drive reservations
- Controlling the UID LED
- Using the LTO-9 New Media Initialization Wizard
 - Initialization estimated times
- Operating the autoloader
 - Storage slots
 - Moving media
 - Opening a Mailslot
 - The mailslot cannot be opened
 - Opening a magazine
 - Opening a magazine from the OCP
 - Cleaning a tape drive
 - The auto cleaning feature
 - Configuring auto cleaning
 - Initiating a drive cleaning operation
 - Rescanning the cartridge inventory
 - Forcing a drive to eject a cartridge
 - Difficulty ejecting a cartridge
- Viewing status information
 - Viewing autoloader and module status
 - Status > Library Status screen parameters
 - Using the cartridge inventory modular view
 - Using list views
 - Using the partition map graphical view
 - Viewing autoloader or partition configuration settings
 - Configuration Status screen parameters
 - Viewing drive status
 - Drive Status configuration settings
 - Viewing network status
 - Network Status screen parameters
 - Command View TL status parameters
 - Viewing encryption status

- Encryption status parameters
- Viewing Secure Manager status
 - Secure Manager status parameters
- Using the OCP
 - LED indicators
 - Home screen
 - OCP buttons
 - The OCP menu structure
 - Logging into the OCP
 - Unlocking the mailslot (Unlock Mailslot)
 - Information/Status
 - Viewing cartridge inventory (Information/Status > Inventory)
 - Viewing autoloader information (Information/Status > Library Status)
 - Viewing drive information (Information/Status > Drive 1 Status)
 - Viewing network Status (Information/Status > Network Status)
 - Configuring the autoloader
 - Resetting the RMI password (Configuration > Users > Reset RMI PW)
 - Configuring IPv4 network settings (Configuration > Network)
 - Configuring network settings (Configuration > Configure Network Settings)
 - Reset to Default Settings (Configuration > Library > Reset to Default Settings)
 - Saving the autoloader configuration (Configuration> Library > Save Config to USB Device)
 - Restoring the autoloader configuration (Configuration> Library > Restore Config from USB)
 - Accessing the operation functions
 - Unlocking magazines (Operation > Magazine Unlock Left or Magazine Unlock Right)
 - Unlocking the Mailslot (Operation > Mailslot Unlock)
 - Accessing the Maintenance functions
 - Saving a Library Support Ticket (Maintenance > Save Lib ticket to USB Device)
 - Saving Library Log Files (Maintenance > Save Lib Logs to USB Device)
 - Upgrade Autoloader firmware (Maintenance > Upgrade Drive from USB device)
 - Save Drive Support Ticket (Maintenance > Save Drv ticket to USB device)
 - Upgrade Drive firmware (Maintenance > Upgrade Drive from USB device)
- Troubleshooting information and procedures
 - The autoloader displays errors
 - Fibre Channel connection problems
 - Detection problems after installing a SAS drive
 - Operation problems
 - Performance problems
 - 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 autoloader
 - Data cartridges
 - Tape drive read or write performance seems slow
- Service and repair
 - Releasing the magazines manually
- The wellness test
 - Running the wellness test
- Error codes
 - Finding autoloader logs on the RMI
 - Generating a report or support ticket from L&TT
 - Downloading a support ticket from the autoloader
 - Viewing a downloaded support ticket
 - Finding error code information on an L&TT support ticket or report
 - Error events
 - Warning events
 - Configuration change events
 - Informational events
- Diagnosing problems with Library & Tape Tools
- Upgrading and servicing the autoloader
 - Possible tools needed
 - Removing and replacing a tape drive
 - Removing and replacing a magazine
 - Removing a magazine using the OCP
 - Releasing magazines using the RMI
 - Releasing the magazine using the manual magazine release
 - Removing and replacing the autoloader controller board
 - Identifying the failed component
 - Saving the autoloader configuration
 - Powering off the Autoloader
 - Preparing to remove the controller board
 - Removing a module controller board
 - Installing the new controller board
 - Completing the autoloader controller replacement
 - Verifying the autoloader controller installation
 - Removing and replacing the chassis
 - Removing the cables, controller, magazines, and tape drive
 - Removing the chassis
 - Unpacking the new chassis
 - Installing the replacement chassis
 - Replacing the autoloader components and cables

- Verifying the chassis replacement
 - Replacing the shipping lock on the old chassis
 - Repackaging the old chassis
- Installation and replacement of the autoloader rack kit
 - Removing the cartridges from tape drives
 - Removing the cartridges from the magazines using the OCP
 - Removing the cartridges from the magazines using the RMI
 - Removing the cartridges from the magazines using the manual release
 - Removing the autoloader feet
 - Powering off the library
 - Removing the library
 - Removing the old rails
 - Removing and storing the shipping lock
 - Securing the rails to the rack
 - Installing the library
- Technical specifications
 - Physical specifications
 - Environmental specifications
 - Electrical specifications
 - Regulatory specifications
 - Regulatory compliance identification numbers
- Electrostatic discharge
 - Preventing electrostatic damage
 - Grounding methods
- Websites
 - Accessing the compatibility matrix
 - HPE Storage autoloader websites
- Support and other resources
 - Accessing Hewlett Packard Enterprise Support
 - HPE product registration
 - Accessing updates
 - Remote support
 - Warranty information
 - Regulatory information
 - Documentation feedback

Notices

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

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

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

Acknowledgments

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

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

Features



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 autoloader.

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

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.

The autoloader provides a compact, high-capacity, low-cost solution for simple, unattended data backup. This unique design houses up to eight tape cartridges in a compact 1U form factor with easy access to tape cartridges through two removable magazines and a configurable mailslot. Each magazine can hold up to four cartridges.

The autoloader supports LTO Ultrium half-height tape drives. For the tape drives now available for the autoloader, see the MSL QuickSpecs at <https://www.hpe.com/support/hpesc>. To verify compatibility, see [Accessing the compatibility matrix](#).

The autoloader is compatible with most operating systems and environments that support the SAS, or Fibre Channel interfaces. However, the autoloader requires either direct support from the operating system or a compatible backup application to take full advantage of its many features.

The autoloader provides two user interfaces:

- **Operator Control Panel (OCP):** From the OCP you can operate the autoloader from the front panel.
- **Remote Management Interface (RMI):** From the RMI you can monitor and control the autoloader from a web browser. You can access most autoloader functions from the RMI.

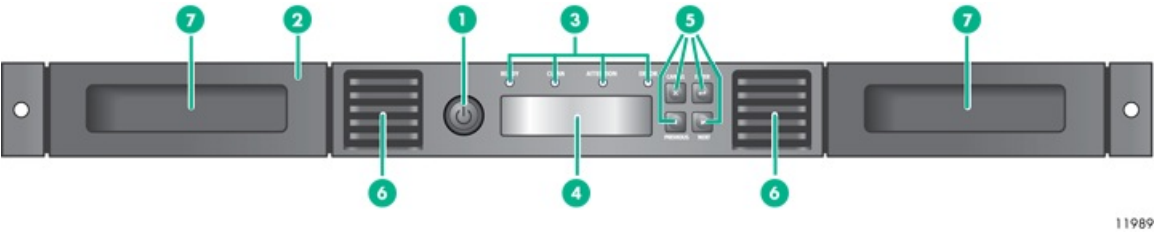
Subtopics

[Autoloader front panel](#)

[Autoloader back panel](#)

[Tape drive back panels](#)

Autoloader front panel



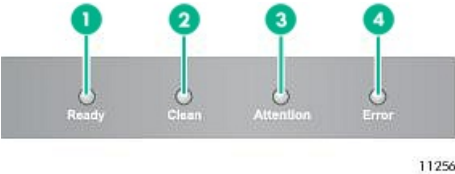
Item Description	
1	Power button
2	Mailslot
3	Front panel LEDs
4	Front panel LCD screen
5	Control buttons
6	Air vents
7	Magazine

Subtopics

Front Panel LEDs

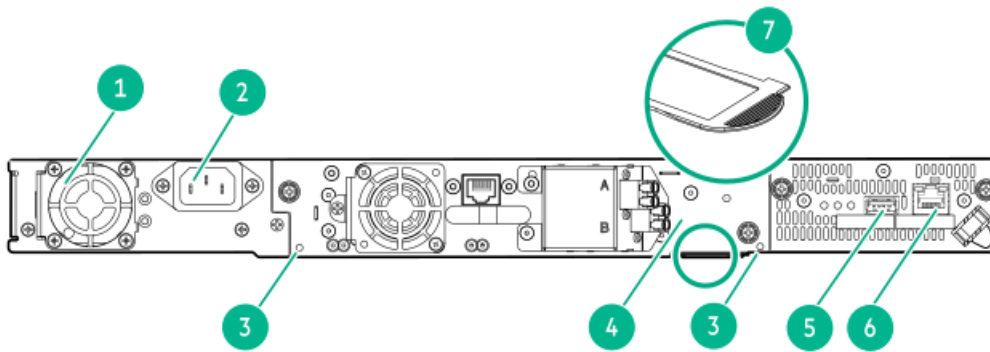
Front Panel LEDs

The Front Panel LEDs indicate system status information.



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

Autoloader back panel



1. Fan	2. Power connector
3. Magazine release hole	4. Tape drive assembly
5. USB port	6. Ethernet port

7. Pull-out tab containing the serial number and other product information

USB ports:

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

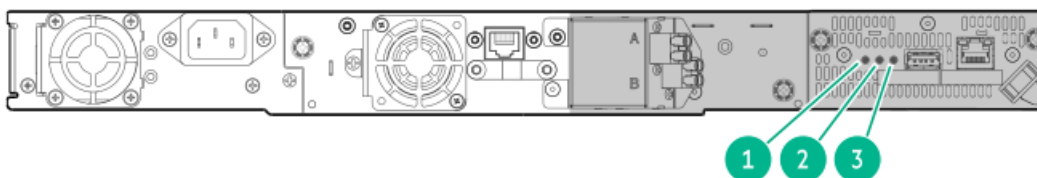
The encryption kit token, which is part of the MSL Encryption Kit, is fully functional in the USB port.

Subtopics

Controller health status indicators

Controller health status indicators

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



Item	Color	Description
1	Blue	Unit identifier (UID).
2	Amber	Error
3	Green	Controller health status LED. <ul style="list-style-type: none"> Pulses on and off in approximately one second cycles during normal operation. Solid green or not illuminated (pulsing) while the autoloader is powered on indicates that the controller is not operating correctly. If the controller health status LED is solid green or not illuminated (pulsing), see the "Operation problems" topic for additional information.

Tape drive back panels

Subtopics

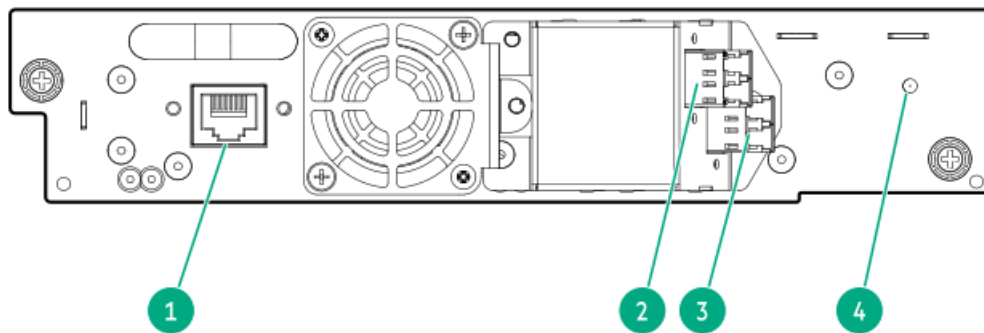
[LTO-6 FC tape drive back panels](#)

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

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

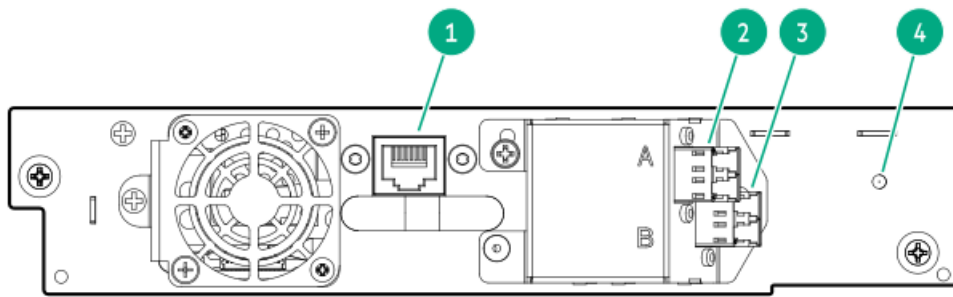
[LTO-7, LTO-8, and LTO-9 SAS tape drive back panel](#)

LTO-6 FC tape drive back panels



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

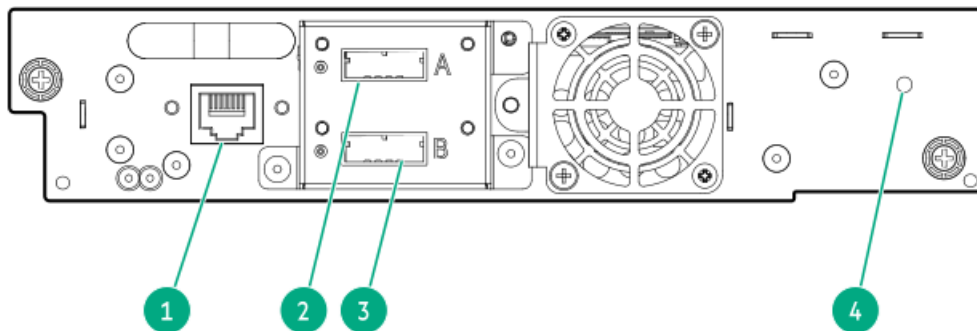
LTO-7, LTO-8, and LTO-9 FC tape drive back panel



Item Description

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

LTO-6 SAS tape drive back panel

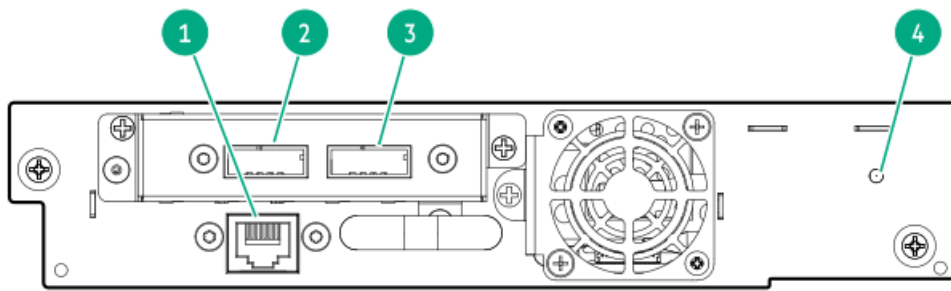


Item Description

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

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

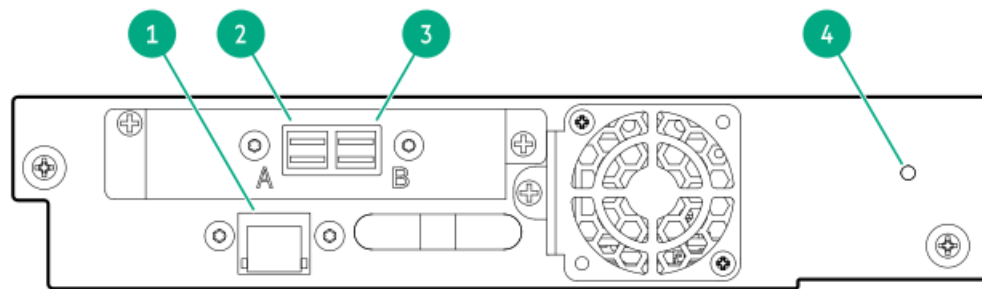
LTO-7 and LTO-8 SAS tape drive back panel



Item Description

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

LTO-9 SAS tape drive back panel



Item Description

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

Autoloader options

Subtopics

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

[Command View TL TapeAssure](#)

[LTFS Support](#)

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

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

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

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

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



IMPORTANT

When encryption is enabled with the encryption kit, the autoloader will not use encryption keys from other sources, such as a key management system or application software. Disable encryption in applications writing to the autoloader 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 HPE Storage Encryption Kit User Guide, which is available from the Hewlett Packard Enterprise Support Center at <https://www.hpe.com/support/hpesc>.

Command View TL TapeAssure

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

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

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

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

LTFS Support

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

Hardware-based encryption

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

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

To use this feature, you need:

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

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

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

Subtopics

[KMIP-based key servers](#)

[Application-managed encryption](#)

KMIP-based key servers

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

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

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

Key managers

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

Operation

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

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

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

Licensing

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

Application-managed encryption

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

**NOTE**

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

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

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

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

**NOTE**

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

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

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

**CAUTION**

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

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

Installing the tape autoloader

Procedure

Plan the autoloader installation.

- [FC connection information](#)
- [SAS connection information](#)
- [Location requirements](#)
- [Preparing the host](#)
- [Unpacking the shipping container](#)
- [Attaching the feet](#)
- [Removing the shipping lock](#)
- [Installing the autoloader in a rack](#)
- [Installing the tape drive](#)
- [Connecting the FC cable](#)
- [Connecting the SAS cable](#)
- [Powering on the autoloader](#)

- [The RMI](#)
- [Configuring the autoloader network](#)
 - [Network configuration information](#)
 - [Finding the IPv4 IP address obtained through DHCP](#)
 - [Configuring IPv4 networking from the OCP](#)
- [Setting the date and time](#)
- [Setting the administrator password](#)
- [Configuring the FC interface](#)
- [Labeling the tape cartridges](#)
- [Verifying the host connection](#)
- [Verifying the installation](#)
 - [Downloading product firmware](#)
- [Configuring additional features](#)

Subtopics

[FC connection information](#)

[SAS connection information](#)

[Location requirements](#)

[Preparing the host](#)

[Unpacking the shipping container](#)

[Attaching the feet](#)

[Removing the shipping lock](#)

[Installing the autoloader in a rack](#)

[Installing the tape drive](#)

[Connecting the FC cable](#)

[Connecting the SAS cable](#)

[Powering on the autoloader](#)

[The RMI](#)

[Configuring the autoloader network](#)

[Setting the date and time](#)

[Setting the administrator password](#)

[Configuring the FC interface](#)

[Labeling the tape cartridges](#)

[Verifying the host connection](#)

[Verifying the installation](#)

[Configuring additional features](#)

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 1. FC drive interface speeds

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

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

feature.

Direct connection

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

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

SAN connection

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

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

Cable requirements

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

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

SAS connection information

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

Table 1. SAS drive interface speeds

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

The autoloader 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 [Accessing the compatibility matrix](#).



CAUTION

Do not connect the autoloader to a SAS RAID controller unless the compatibility matrix shows that the controller is qualified with the autoloader. The server might not be able to boot when the autoloader is connected to an unsupported SAS RAID controller.

**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 or 12 Gb/s data rates. Do not use equalized cables with LTO-6 or later generation tape drives unless these cables are verified for 6 Gb/s or 12 Gb/s data rates.
- For optimal performance, only use cables of the length specified as qualified for your products. If not using the HPE supplied cable and the SAS link is operating at 6 Gb/s the maximum SAS cable length is 6 meters. If operating at 12 Gb/s then the maximum cable length is 4 meters.

Cable requirements

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

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

Connectors

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

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

**CAUTION**

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

Location requirements


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

If you plan to set the autoloader on a table, select a level area large enough to support both edges of the autoloader with access to the host server and a power outlet. You can also set the autoloader on a shelf in the rack. In this case, you must attach the feet during the installation process.

**IMPORTANT**

The autoloader must be mounted in supported rack rails or sit on the enclosed support feet. Placing the autoloader on a surface, such as a tabletop or rack shelf, without the feet applied could result in autoloader errors.

Table 1. Location criteria

Criteria	Definition
Rack requirements	HPE G2 Enterprise Series, Enterprise Series, G2 Advanced Series, Advanced Series, Standard Series, and other HPE square-hole or round-hole racks
Rack space requirements	1U when mounted in the optional rack rails
Operating temperature	10-35° C (50-95° F) for the tape autoloader. Some tape drives have a more limited ambient temperature range and/or have a more limited temperature range when operating at high altitudes. Verify the tape drive operating requirements before installing a tape drive. See Environmental specifications .
Power source	AC power voltage: 100-240 VAC Line frequency: 50-60 Hz Place the autoloader near an AC outlet. The AC power cord is the main AC disconnect device for the autoloader and must be easily accessible at all times.
Weight without media	12 kg (26.45 lb)
Weight with media	13.6 kg (29.98 lb)
Air quality	Place the autoloader 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.
	<div>  CAUTION Chemical contaminant levels in customer environments for Hewlett Packard Enterprise hardware products must not exceed G1 (mild) levels of Group A chemicals at any time as described in the current version of ISA-71.04-2013 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants. </div>
Humidity	20-80 percent relative humidity noncondensing
Clearance	Back: Minimum of 15.4 cm (6 inches) Front: Minimum of 30.8 cm (12 inches) Sides: Minimum of 5.08 cm (2 inches)

**TIP**

Temperature and humidity specifications are more tightly controlled for tape media, tape drives, and tape autoloaders 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.

Preparing the host

Procedure

- If you are not the system administrator of the host computer, check with the system administrator before powering off the computer.
- For an autoloader with SAS drives, confirm availability or install a SAS HBA that supports multiple LUNs.
- For an autoloader with direct-attach Fibre Channel drives, confirm availability or install an FC HBA.
- Verify that multiple LUN support is enabled on the HBA and operating system. See the host computer and HBA documentation for

installation information.

- For an autoloader with Fibre Channel drives connected through a compatible switch, verify that sufficient ports are available.
- Install application software and compatible drivers on the host computer. See the application software manuals for installation and configuration information.
- Install the Library & Tape Tools (L&TT) diagnostic utility to see what devices are connected to the host, verify the installation, upgrade firmware, and aid in troubleshooting.

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

Unpacking the shipping container

Prerequisites



CAUTION

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

Procedure

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



CAUTION

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

5. Carefully remove the foam padding and then the bag from the autoloader.
6. Save the packaging materials for moving or shipping the autoloader in the future.
7. Verify that you received the following components:
 - a. Autoloader
 - b. Ethernet cable
 - c. Six support feet
8. Verify that you have the necessary cables.
 - a. For an FC autoloader, you must provide an FC cable for each FC port you plan to use. See [FC connection information](#).
 - b. For a SAS autoloader, you must provide a SAS cable with the correct connector for your HBA. See [SAS connection information](#).

Attaching the feet

About this task



If you plan to mount the autoloader in a rack, skip this step.



CAUTION

- The autoloader must be supported only under both side edges to operate properly.
- Do not put anything on top of the autoloader. Weight on top of the autoloader can prevent the robotic inside from moving properly.

Procedure

1. Ensure that there are no tape cartridges in the autoloader.

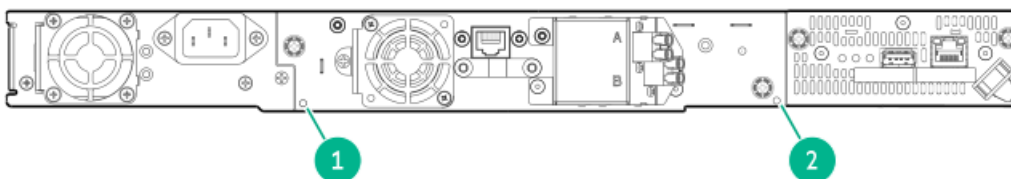


IMPORTANT

The autoloader can be damaged if it is turned over with tape cartridges in the magazines or robot. If the autoloader has been used before and is powered off, use the manual magazine release to remove the cartridges from the autoloader.

- a. If the autoloader is powered on, return all cartridges to the magazines and then power off the autoloader and remove the power cord.
- b. From the back of the autoloader, locate the magazine release holes.

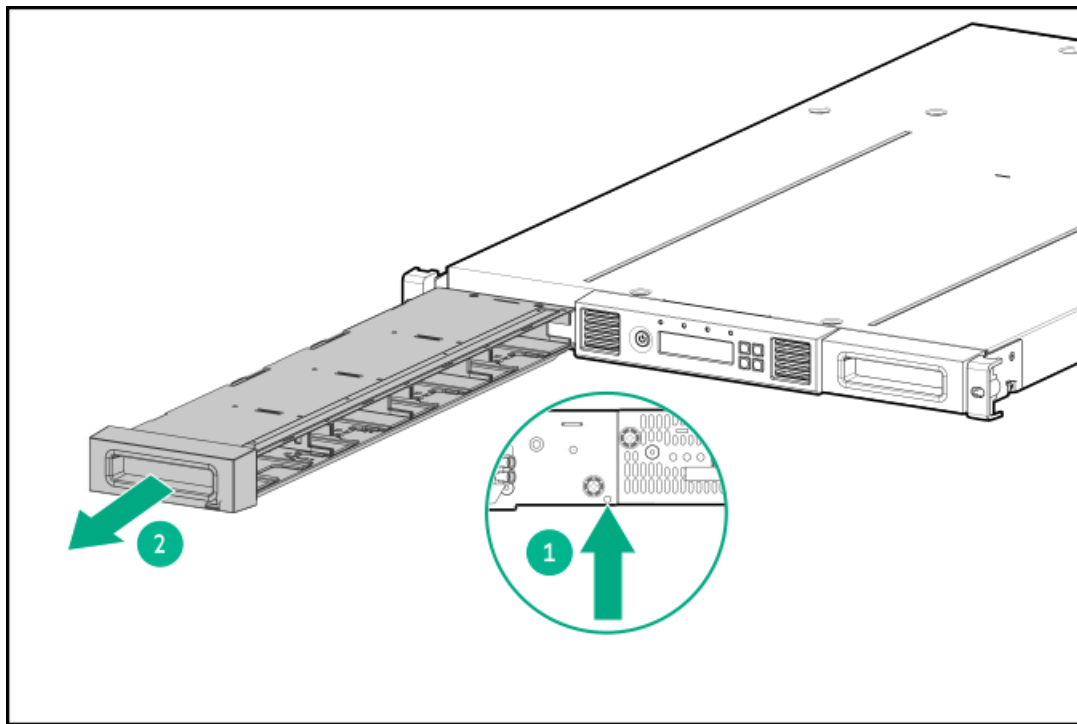
The magazine release holes are located at the bottom corners of the tape drive cover plate. Each hole provides access to a lever that releases the magazine on that side.



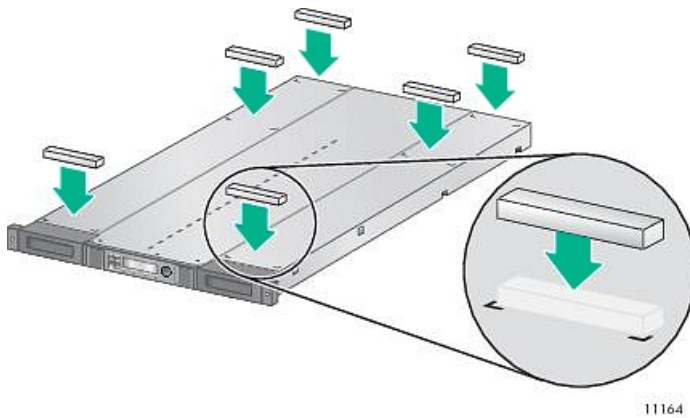
Item Description

- | | |
|---|---------------------------------|
| 1 | Release hole for right magazine |
| 2 | Release hole for left magazine |

- c. Insert a straightened paper clip or small metal pin about 1.5 cm (0.6 inch) into the magazine release hole.



- d. Have another person pull the magazine out of the autoloader and set it aside.
- e. Repeat the process for the other magazine.
2. With another person, gently turn the autoloader over and set it on its top on a smooth clean surface.
3. Locate the six inscribed foot location lines on the bottom of the autoloader.
4. If the autoloader is not new, clean the foot locations with an alcohol wipe or soft cloth lightly moistened with isopropyl alcohol. Do not let alcohol seep into the autoloader.
5. Peel the backing paper off each foot and apply it within a set of foot location lines.



6. With another person, gently turn the autoloader over and set it on its feet.
7. If the magazines were removed earlier, replace them.

Removing the shipping lock

About this task





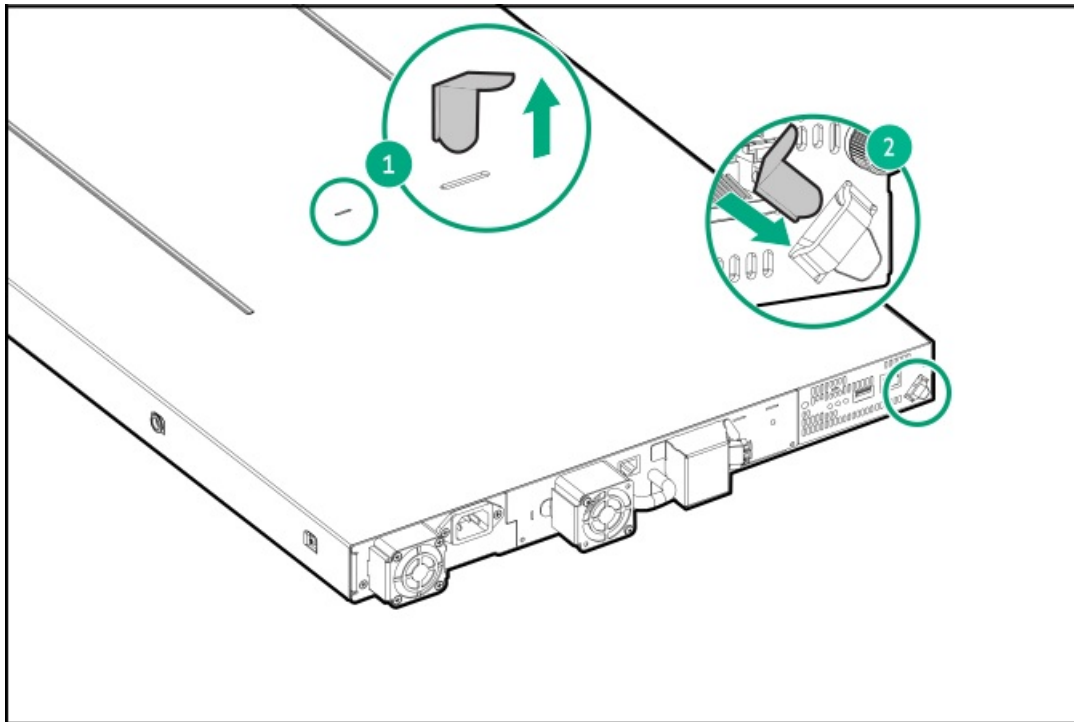
IMPORTANT

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

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

Procedure

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



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

Installing the autoloader in a rack

Prerequisites

#2 and #3 Phillips screwdrivers

Torque driver (optional)

About this task

If the autoloader has support feet, skip this step.



WARNING

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

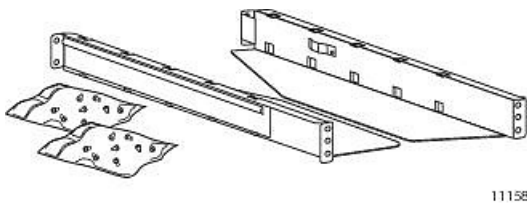
- Extend the leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install the rack stabilizer kit on the rack.
- Extend only one rack component at a time. Racks might become unstable if more than one component is extended.
- Slide or rail mounted equipment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

The autoloader is installed easily into the HPE Standard Series Racks, HPE Enterprise Series Racks, HPE Advanced Series Racks, HPE Rack System/E, and earlier generation HPE 9.5 mm Square-Hole Racks.

Procedure

1. Unpack the rack kit and verify that it includes the following:

- Two rails
- Hardware packets containing M6 screws.



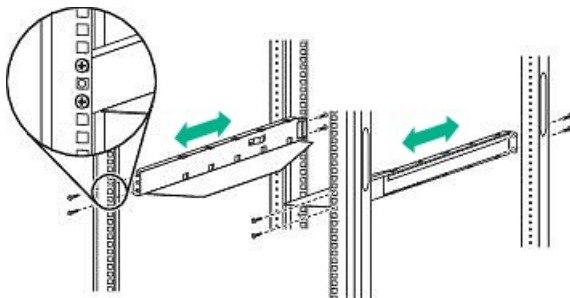
2. Select the hardware packet for your rack.

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

3. Install the rails.

- a. Using the screws from the packet for your rack and a #3 Phillips screwdriver, secure the front of one rail to the front of the rack.

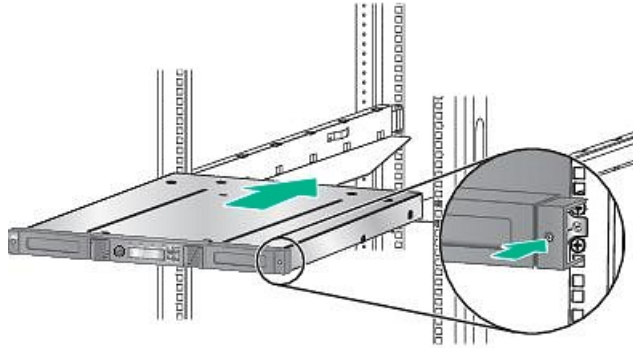
The support platform of each rail is tapered, narrowing towards the rear.



- b. Extend the rail to the depth of the rack and secure the rail to the back of the rack.

- c. Install the other rail.
4. Install the autoloader in the rack.
 - a. Slide the autoloader onto the rails.
 - b. From the front of the autoloader, secure the front bezel to the rack. You can use either a #2 Phillips screw driver or torque driver. Place the tool through the small holes in the mounting bracket. Tighten the captive screws on each side of the autoloader until they are seated.

If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not overtighten. If using a torque driver, the recommended torque is 6 inch pounds or 0.68 N m.



5. Verify that the autoloader is contained within the 1U rack volume.

Installing the tape drive

About this task

If the tape drive is not already installed in the autoloader, install the tape drive before the autoloader is powered on.



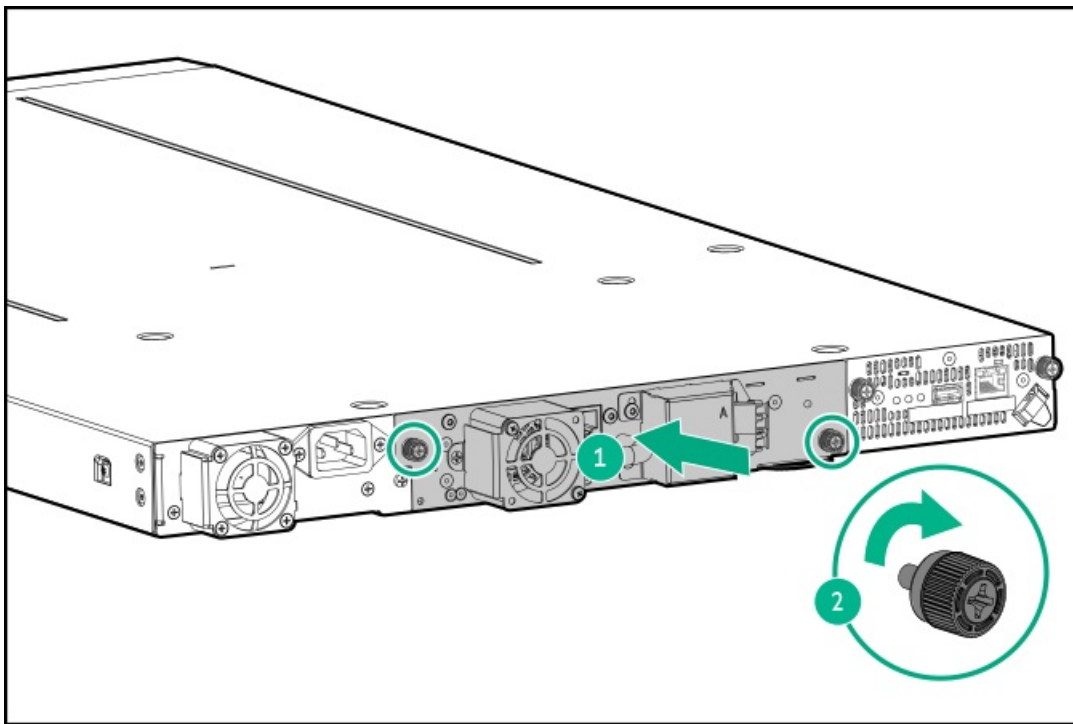
WARNING MOVING PARTS: Only personnel with technical and product safety training (referred to as **users** in this document) may have access to or operate the autoloader.

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

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.

Procedure

1. Holding the tape drive by the handle and supporting it from the bottom, slide the tape drive into the drive bay until it is flush with the back of the autoloader.



2. To secure the tape drive to the chassis, tighten the drive sled mounting screws (the blue captive thumbscrews). You can use either a #2 Phillips screwdriver or a torque driver.
 - If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not overtighten.
 - If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.
 - If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



IMPORTANT

Under certain conditions of external shock and vibration, it has been noted that if the thumbscrews are not tightened, drive performance issues might occur. In that situation, please tighten the thumbscrews to the recommended torque.

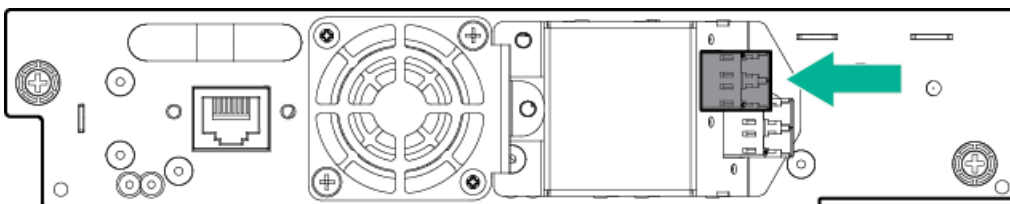
Connecting the FC cable

About this task

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

Procedure

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



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

Connecting the SAS cable

About this task



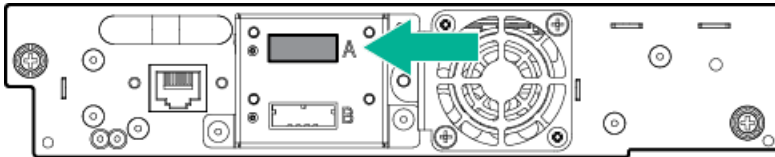
NOTE

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

Procedure

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

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



NOTE

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

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



TIP

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

Powering on the autoloader

About this task



WARNING

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

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

Procedure

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

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

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



NOTE

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

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



NOTE

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

The RMI

About this task

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

Initial configuration steps:

Procedure

1. Log in to the Operator Control Panel (OCP) as Administrator (press any key > Select User: "ADMINISTRATOR" PIN:0000).
2. Verify or change network settings (Configuration > Network >).
3. Set INITIAL RMI Password (Configuration > Users > Reset RMI PW > Select User: "ADMINISTRATOR"). If one person physically installs

the library and a second person will configure the library, share the network settings, and INITIAL RMI Administrator password set.

4. From a browser, log in to the Remote Management Interface (RMI) as the Administrator user. (Use the IP address and the Initial Password set).

After logging in the first time, you will be prompted to set a new password (for password guidelines, see [Configuring user account settings](#)). Then, you will be prompted that the library has no default partition. The library will remain OFFLINE to connected hosts until a valid partition is created.

5. Create a partition using the Basic or Expert Partition Wizard ([Configuration > Partitions > Basic or Expert Wizard](#)).
6. Complete any other configuration details required for your installation from the RMI, including **date/time** settings. With the RMI, you can monitor, configure, and operate most autoloader functions from a web browser. When possible, use the RMI as the primary autoloader interface because it provides access to additional features, includes online help, and is easier to use. However, the RMI is not required to use the autoloader, except to configure advanced features, such as SNMP, IPv6, encryption, and HPE TapeAssure. The only tasks that you cannot do from the RMI are: Use a USB flash drive to save configuration files and support tickets, and download firmware.



NOTE

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

Logging in:

Using the OCP, find the autoloader IP address by Configuring IPv4 networking from the OCP. Open any HTML web browser and enter the autoloader IP address. Select the user, and enter the password.

Click Log In.

Once signed in, click Help in the upper right corner for more information about the fields and information in the RMI.

Status icons:

The green check mark Status OK icon indicates that the autoloader 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 autoloader can still perform most operations.

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

Configuring the autoloader network

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



NOTE

Most IPv4 network configurations are also available through the OCP.

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



NOTE

The autoloader is shipped without an administrator password. You must set the administrator password with the OCP before you can use the RMI administrator functions. Once the administrator password is set, you can access the RMI by providing the administrator password on the login screen.

If you enabled IPv6, you must continue configuring IPv6 from the RMI after setting the administrator password.

Subtopics

[Network configuration information](#)

[Finding the IPv4 IP address obtained through DHCP](#)

[Configuring IPv4 networking from the OCP](#)

Network configuration information

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

Port	Direction	Use
22 (TCP)	Inbound	Service. This port can be disabled by the administrator when the autoloader 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.

Finding the IPv4 IP address obtained through DHCP

Procedure

1. Log into the Operator Control Panel (OCP) as Administrator (press any key > Select User: "ADMINISTRATOR" PIN:0000).
2. From the Home screen, press Next until the display shows **Status/Information** . Press Enter.
3. Press Next until the display shows **Network Information** . Press Enter.
4. The display shows **IPv4 Network Enabled** . Press Enter.
5. Press Next until the display shows the IP address.
6. Press Cancel until the display shows the home screen.

Configuring IPv4 networking from the OCP

About this task

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

Procedure

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

Setting the date and time

Prerequisites

The administrator password.

About this task

The autoloader uses the date and time to record events. When possible, set the date and time during the initial installation process. You can set the timezone, date, and time or configure an NTP (Network Time Protocol) server from the RMI Configuration > System > Date and Time Format.



NOTE

The autoloader time does not automatically adjust for daylight saving time; you must adjust the time manually through the RMI.

Procedure

1. Log in to the RMI as the Administrator user.
2. Navigate to the Configuration > System > Date and Time Format.
3. Set the timezone and time format.
4. Set the date and time manually or configure SNTP.

Setting the administrator password

Setting an administrator password provides access to the administrator functions within the RMI and OCP, and restricts access to administrator functions to only those who know the administrator password.

The OCP and RMI Administrator users have separate login credentials.

Procedure to set the OCP Administrator Password:

The OCP Administrator password is set to 0000 from the factory, but can be changed to any four-digit number. The RMI Administrator password is Null and must be set from the OCP before the RMI can be accessed.

Procedure for changing the OCP Administrator Password

1. Log in to the Operator Control Panel (OCP) as Administrator (press any key > Select User: "ADMINISTRATOR" PIN: 0000).
2. Press Next until the display shows Configuration. Press Enter.
3. Press Next until the display shows Users. Press Enter.
4. Press Next until the display shows Configure PIN. Press Enter.
5. Press Next until the display shows Administrator. Press Enter.
6. Create a new four-digit PIN for the OCP Administrator user using the Next and Prev buttons to select digits. Press Enter to accept the new PIN.

Procedure to set the initial RMI Administrator Password:

1. Log in to the Operator Control Panel (OCP) as Administrator (press any key > Select User: "ADMINISTRATOR" PIN: 0000).
2. Press Next until the display shows Configuration. Press Enter.
3. Press Next until the display shows Users. Press Enter.
4. Press Next until the display shows Reset RMI PW. Press Enter.
5. Press Next until the display shows Administrator. Press Enter.
6. Create a four-digit temporary password for the RMI Administrator user. (If one person physically installs the library and a second person will configure the library, share the network settings and INITIAL RMI Administrator password)
7. From a browser, log in to the Remote Management Interface (RMI) as the Administrator user. After logging in the first time, you will be prompted to set a new password. For password guidelines, see [Configuring user account settings](#).

Configuring the FC interface

About this task

Skip this step if you are replacing a tape drive.

Procedure

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

Drives connected to a SAN

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

Drives connected directly to the host

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

Labeling the tape cartridges

Prerequisites

High-quality preprinted barcode labels with the correct Media ID.

About this task

The autoloader will operate without barcode labels on the cartridges. Using barcode labels in production environments improves inventory time in the autoloader and eases cartridge handling processes outside the autoloader.

Attaching a bar code label to each tape cartridge enables the autoloader and application software to identify the cartridge quickly, which speeds up inventory time. Make using bar code labels on your tapes a practice.



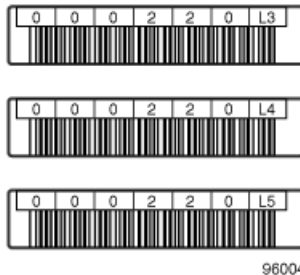
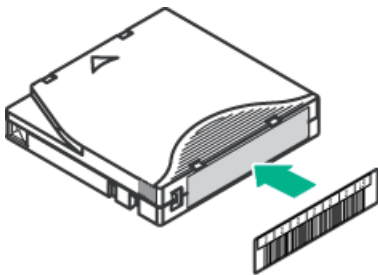
IMPORTANT

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.



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.

Verifying the host connection

Procedure

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

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

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

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

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

This utility verifies that the autoloader is connected and communicating with the host server. It also verifies that the autoloader is functional and provides diagnostic information.

To verify your connections, run Library & Tape Tools Installation Check from the programs menu. L&TT is available without cost at: <https://www.hpe.com/support/tapetoolsoftware>.

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

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

3. For more information on verifying the connection of parallel SCSI devices, consult the operating system documentation.

Verifying the installation

Prerequisites



IMPORTANT

- Do not place anything on the top of the autoloader, the weight may cause errors in the library operation.
- Prevent anything to contact the bottom of the autoloader, contact may cause errors in the library operation.

Procedure

1. Verify that the autoloader and drives have the current firmware revision. The autoloader firmware revision is displayed on the RMI login page, and in the top left corner of the RMI screen if you are logged into the RMI.

From the OCP:

- a. From the Home screen, press Next until the display shows Status/Information. Press Enter.
 - b. Press Next until the display shows Autoloader Information. Press Enter.
 - c. Press Next until the display shows the Firmware Rev. The current installed firmware version is displayed.
 - d. Press Cancel until the display shows the home screen. The drive firmware version is displayed on the RMI Status > Drive Status and the OCP Status > Drive.
2. Determine the current available firmware version. See [Accessing the compatibility matrix](#).
 3. If necessary, update the autoloader firmware from the OCP or RMI Maintenance > Firmware Upgrades > System Firmware.
 4. If necessary, update the drive firmware from the OCP or RMI Maintenance > Firmware Upgrades > Drive Firmware screen.
 5. After configuring the autoloader, 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 Configuration. Having a backup of the autoloader configuration is helpful when recovering from a configuration error or if the autoloader needs a service.
 6. If needed, set the security user password from the Configuration > User Accounts screen. The security user is only needed to access hardware encryption settings.

Subtopics

[Downloading product firmware](#)

Downloading product firmware

Procedure

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



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 and then insert the USB flash drive into one of the library USB ports. You can update firmware from the OCP or the RMI Maintenance > Firmware Upgrades > System Firmware.

Configuring additional features

About this task

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

Procedure

1. Naming the tape autoloader, which is done from the RMI Configuration > Network.
2. Enabling and configuring SNMP network management from the RMI Configuration > Network Management > SNMP. See the HPE Storage Command View TL User Guide for information on configuring SNMP for use with Command View TapeAssure.
3. Setting up an email event notification through the RMI Configuration > Network Management > SMTP.
4. To use the RMI in Japanese, enable the Japanese language option through the RMI Configuration > System > Language.

Tape cartridges and magazines

This chapter explains which media to use with the autoloader, and how to label and write-protect tape cartridges. Careful labeling and handling of the tape cartridges will prolong the life of the tape cartridges and the autoloader.

Subtopics

[Tape cartridges](#)

[Magazines](#)

Tape cartridges

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

WORM data cartridges

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

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

Subtopics

[LTO-9 Media initialization](#)

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

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

[Recommended practices for labeling tape cartridges](#)

[Write-protecting data cartridges](#)

[Read and write compatibility](#)

[Supported media](#)

LTO-9 Media initialization

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

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

LTO-7 Type M media for LTO-8 drives

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



NOTE

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

- Once an LTO-7 cartridge has been initialized to LTO-7 Type M media, the format is irreversible. Do not place an 'M8' 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>.

Recommended practices for using and maintaining tape cartridges



CAUTION

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

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



CAUTION

Use only Ultrium Universal Cleaning Cartridges (UCC).

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

Recommended practices for labeling tape cartridges

The autoloader 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.

Though not recommended, checking Ignore Barcode Media ID in the RMI Configuration > System screen will keep the autoloader from interpreting the bar code Media IDs.

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

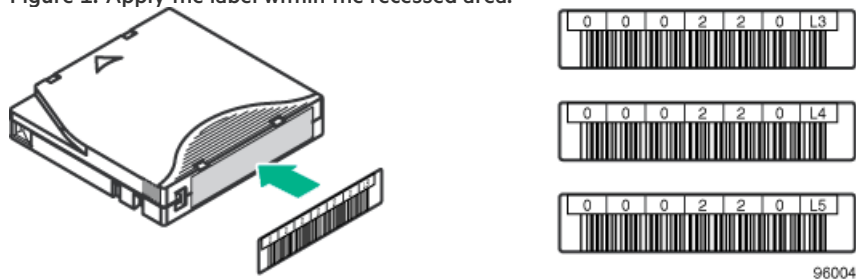
Misusing and misunderstanding bar code technology can result in backup and restore failures. To ensure that your bar code labels meet Hewlett Packard Enterprise quality standards, always purchase them from an approved supplier. Do not print bar code labels yourself. To purchase bar code labels, see the 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 Storage 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.



96004



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.

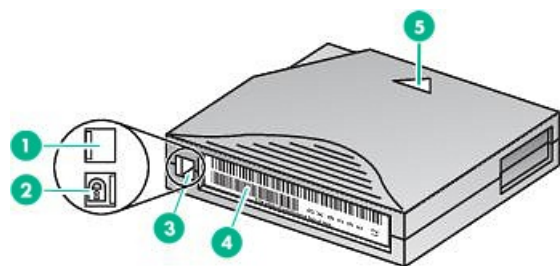
Write-protecting data cartridges

About this task

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

Procedure

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



10454

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

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

Read and write compatibility

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

	LTO-6 drive	LTO-7 drive	LTO-8 drive	LTO-9 drive
LTO-4 media — unencrypted	Read only	Incompatible	Incompatible	Incompatible
LTO-4 media — encrypted	Read only with encryption key	Incompatible	Incompatible	Incompatible
LTO-5 media — unencrypted	Read/Write	Read only	Incompatible	Incompatible
LTO-5 media — encrypted	Read/Write with encryption key	Read only with encryption key	Incompatible	Incompatible
LTO-6 media — unencrypted	Read/Write	Read/Write	Incompatible	Incompatible
LTO-6 media — encrypted	Read/Write with encryption key	Read/Write with encryption key	Incompatible	Incompatible
LTO-7 media — unencrypted	Incompatible	Read/Write	Read/Write	Incompatible
LTO-7 media — encrypted	Incompatible	Read/Write with encryption key	Read/Write with encryption key	Incompatible
LTO-7 Type M media — unencrypted	Incompatible	Incompatible	Read/Write	Incompatible
LTO-7 Type M media — encrypted	Incompatible	Incompatible	Read/Write with encryption key	Incompatible
LTO-8 media — unencrypted	Incompatible	Incompatible	Read/Write	Read/Write
LTO-8 media — encrypted	Incompatible	Incompatible	Read/Write with encryption key	Read/Write with encryption key
LTO-9 media — unencrypted	Incompatible	Incompatible	Incompatible	Read/Write
LTO-9 media — encrypted	Incompatible	Incompatible	Incompatible	Read/Write with encryption key



NOTE

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

Supported media

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

Cleaning cartridge for all supported tape drives

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

LTO-6 data cartridges

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

LTO-7 data cartridges

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

LTO-7 Type M media for LTO-8 drives

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

LTO-8 data cartridges

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

LTO-9 data cartridges

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

Magazines

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

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



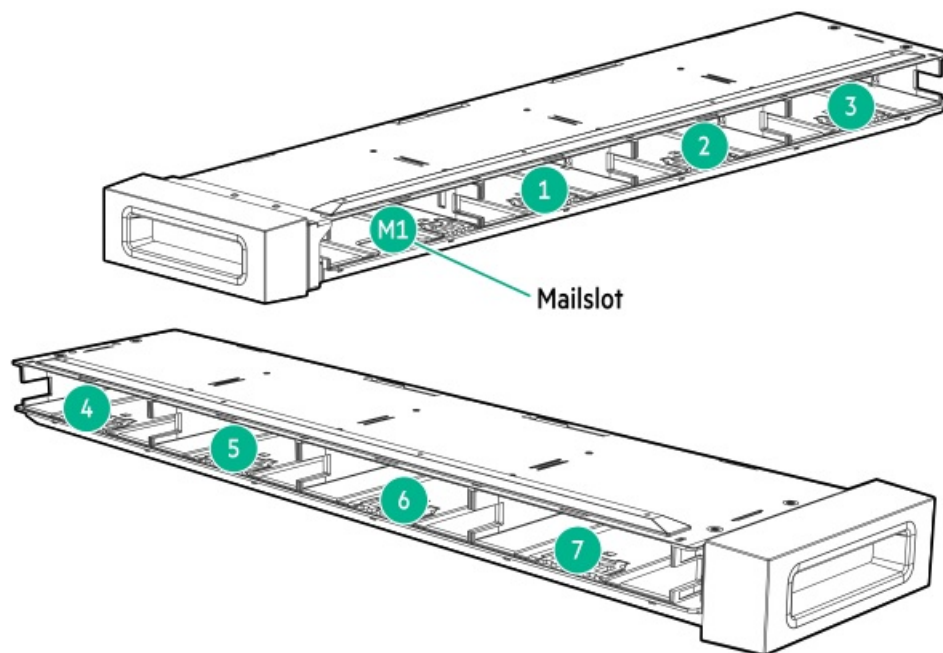
IMPORTANT

To release a magazine manually, see [Releasing the magazines manually](#). However, only use this manual process if the magazine cannot be released using the OCP or the RMI, and the autoloader no longer has power.

Subtopics

[Autoloader slot numbering](#)

Autoloader slot numbering



When the mailslot is disabled, the mailslot (M1) becomes Slot 1, and all other slots are renumbered accordingly.

Operating the autoloader

The autoloader supports the following operation methods:

- **Remote management interface (RMI)**— this interface lets you monitor and control the autoloader from a web page. You can access most autoloader functions from the RMI.
- **Operator control panel (OCP)** — this interface lets you operate the device from the front panel.
- **Host backup software**— You can perform any functions provided by the backup software.



NOTE

Before using the RMI, the autoloader network settings must be configured and the administrator password set.

Subtopics

[Autoloader user interfaces](#)

- [OCP menu](#)
- [Logging in to the autoloader](#)
- [The autoloader RMI main screen](#)
- [Configuring the autoloader](#)
- [Maintaining the autoloader](#)
- [Operating the autoloader](#)
- [Viewing status information](#)
- [Using the OCP](#)

Autoloader user interfaces

The autoloader provides two user interfaces:

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

Subtopics

- [The RMI](#)
- [The autoloader OCP](#)

The RMI

Before using the RMI, you must configure the autoloader network settings and set the INITIAL RMI administrator password with the OCP. You can configure the network settings and set the INITIAL RMI administrator password by following the [instructions](#).




Use the INITIAL RMI administrator password to log in to the RMI the FIRST time as the administrator user. The autoloader will prompt you to set an actual RMI administrator password.

If one person physically installs the autoloader and a second person configures the autoloader using the RMI, share the INITIAL RMI administrator password as appropriate. The RMI administrator password can be reset from the OCP. After resetting the RMI administrator password from the OCP, share the new INITIAL RMI administrator password with the autoloader administrator.

The security user password can be set once by the administrator from the [Configuration > User Accounts](#) screen.

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

Status icons

	The green Status OK icon indicates that the autoloader 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 device can still perform most operations.
	The red X Status Error icon indicates that user intervention is required and that the device is not capable of performing some operations.

The autoloader OCP

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

To power on the autoloader, press the power button. For more information, see [Autoloader Front Panel](#). To power off the library, press the



power button for five seconds and then release it.

OCP menu

Select User
User
Information/Status
Library Status
Drive (x) Status
Network Status
Inventory
Magazine Left Inventory
Magazine Right Inventory
Drive Inventory
Operation
Configuration
Maintenance
Logout
Administrator
Information/Status
Library Status
Drive (x) Status
Network Status
Inventory
Magazine Left Inventory
Magazine Right Inventory
Drive Inventory
Operation
Mailslot Unlock
Magazine Unlock Left
Magazine Unlock Right
Configuration
Network
IPv4 Mode
Static
IPv4 Address
IPv4 Netmask
IPv4 Gateway



	DHCP
Library	
	Reset to Default Settings
	Save Config to USB Device
	Restore Config from USB
Users	
	Reset RMI PW
	Configure PIN
	Disable RMI Restricted Access
Maintenance	
	Save Lib ticket to USB
	Save Lib Logs to USB
	Upgrade Firmware from USB Device
	Save Drv ticket to USB Device
	Select Dump Mode Current Ticket
	Select Dump Mode Health Log
	Upgrade Drive from USB Device
Logout	
Service	
Information/Status	
	Library Status
	Drive (x) Status
	Network Status
	Inventory
	Magazine Left Inventory
	Magazine Right Inventory
	Drive Inventory
Operation	
	Mailslot Unlock
	Magazine Unlock Left
	Magazine Unlock Right
Configuration	
	Network
	IPv4 Mode
	Static
	IPv4 Address



	IPv4 Netmask
	IPv4 Gateway
	DHCP
Library	
	Reset to Default Settings
	Reset to Manufacturing
	Save Config to USB Device
	Restore Config from USB
Users	
	Reset RMI PW
	Configure PIN
	Disable RMI Restricted Access
Maintenance	
	Save Lib ticket to USB
	Save Lib Logs to USB
	Upgrade Firmware from USB Device
	Save Drv ticket to USB Device
	Select Dump Mode Current Ticket
	Select Dump Mode Health Log
	Upgrade Drive from USB Device
Logout	

Logging in to the autoloader

Prerequisites





TIP

By default, the INITIAL RMI administrator password is unset; all the digits are null. Set the INITIAL RMI administrator password from the OCP to access the administrator functions on the RMI. Use the INITIAL RMI administrator password to log in to the RMI the FIRST time as the administrator user. The autoloader will prompt you to set an actual RMI password (for password guidelines, see [Configuring user account settings](#)). If one person physically installs the autoloader and a second person configures the autoloader using the RMI, share the INITIAL RMI administrator password as appropriate. If the RMI administrator password is lost, it can be reset from the OCP. After resetting the RMI administrator password from the OCP, share the new INITIAL RMI administrator password with the autoloader administrator.

The security password can be set once by the administrator, using the [Configuration > User Accounts](#) screen on the RMI. After that, only the security user can modify the security password. The security user is unable to log in to the OCP and can only access the autoloader from the RMI. The security user password cannot be reset without assistance from Hewlett Packard Enterprise Support.

Procedure

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

Subtopics

[Autoloader users and roles](#)

[Resetting the RMI administrator password](#)

[Resetting the RMI administrator password and OCP PIN](#)

Autoloader users and roles

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

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

If the RMI administrator password AND OCP administrator PIN are both lost, see [Resetting the RMI administrator password and OCP PIN](#).

- **Security**—The security user has access to all administrator functionality and can also configure security features and change the security user password.
 - The security password is required to log in as the security user.
 - The administrator user must set the security password the first time.
 - Once the security password is set, only the security user can modify it.
 - If the security password is lost, both the administrator and service passwords are required to change the security password. Changing the security user password requires assistance from Hewlett Packard Enterprise support personnel.
- **Service**—**Access to the service user is by service personnel only.**
 - The service password is set at the factory and is only available to Hewlett Packard Enterprise support personnel.
 - Both the administrator and service passwords are required for a service person to enter the service area.

Resetting the RMI administrator password

About this task

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

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

Procedure

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

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

Resetting the RMI administrator password and OCP PIN

Prerequisites

You can see the autoloader OCP while you contact Hewlett Packard Enterprise support. The temporary administrator password is generated based on the current date and time shown on the OCP and is only good for a limited time.

About this task

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

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

Procedure





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

The autoloader RMI main screen

The autoloader main screen is organized into the following regions:

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

Top banner elements

-  **Home icon:** Returns to the autoloader main screen
- **Lib. Health:** An icon indicating the overall health status of the autoloader
 -  The green check mark **Status OK** icon indicates that all autoloader 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 autoloader 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 autoloader is not capable of performing some operations. To display the event ticket log, click the icon.
- **Status:** The status of the autoloader robotic
 - **Idle:** The autoloader robotic is ready to perform an action.
 - **Moving:** The autoloader robotic is moving a cartridge.
 - **Scanning:** The autoloader robotic is performing an inventory of cartridges.
 - **Offline:** The autoloader robotic has been taken off line by the autoloader.

- Autoloader 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

- Autoloader status: Overall autoloader configuration and status
 - Serial #: The autoloader serial number
 - Hostname: The autoloader hostname
 - Network configuration: The IP version (IPv4 or IPv6) and IP address
 - Firmware: The autoloader firmware version
 - Token: Information about the key server token when using the encryption kit (if installed)
 - CVTL: Status of CVTL configuration system. This overview provides a summary of configuration and health of the autoloader and drive.
- System Status Overview: A summary of configuration and health of the autoloader and drive.
 - System 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 autoloader 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.
 - Drive status: The number of drives installed in the autoloader and the health of the drive.

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

 - A black square indicates that the drive is fully operational and that no user intervention is required.
 - A yellow square indicates that user attention is necessary, but that the drive can still perform most operations.
 - A red square indicates that user intervention is required or the drive is not capable of performing some operations.
 - Magazine slot usage: The number of cartridge slots in use and available.
 - Drive operation status: The current drive activity for the drive.
 - Write: 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.
 - Calib: the drive is initializing a new LTO-9 tape.

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 autoloader can be open at a time.
- **Configuration:** (Administrator user only) Click or tap to configure the autoloader.
- **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.

Configuring the autoloader

About this task

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

Subtopics

[Default and restore defaults settings](#)
[Configuring the simplest configuration](#)
[Managing the autoloader configuration](#)
[Managing the autoloader date and time](#)
[Configuring media barcode compatibility checking](#)
[Managing license keys](#)
[Setting RMI Language](#)
[Configuring the RMI timeout](#)
[Configuring the autoloader network settings](#)
[Using the Configuration > Network Management screen](#)
[Configuring remote logging](#)
[Configuring event notification parameters](#)
[Configuring tape drives](#)
[Enabling or disabling mailslots](#)
[Partition wizards](#)
[Encryption configuration](#)
[MSL Encryption Kit configuration](#)
[Using the KMIP wizard](#)
[Configuring FIPS Support Mode](#)
[Secure Mode](#)
[Configuring local user accounts](#)
[Configuring LDAP user accounts](#)
[Configuring Command View for Tape Libraries integration](#)
[Moving CVTL access to a new Management Station](#)
[Configuring the autoloader RMI](#)
[Secure Manager](#)

Default and restore defaults settings

You can save the configuration settings to a file, restore the settings, or reset the configuration to the default settings. Use the RMI to view or change settings. The following table lists the configuration parameters, with their default settings and whether they are reset to default or saved to a file.

Parameter	Default setting	Reset by Set Defaults	Stored in Saved Config file
Tape drive settings			
FC drive configuration	Automatic speed, auto port type	Yes	Yes
Drive power	Drive powered on	Yes	Yes
Auto clean	Disabled	Yes	
Slots			
Active slots	Maximum possible	Yes	
Reserved slots	0	Yes	Yes
Mailslot configuration	Mailslot disabled	Yes	Yes
Administrator password required for mailslot removal	Enabled	Yes	Yes
Barcode reader settings			
Barcode reader label length	8	Yes	Yes
Barcode reader alignment	Left	Yes	Yes
Ignore barcode Media ID	Disabled	Yes	Yes
Error and event settings			
Event log levels and filter	Continuous trace and all levels and filters active (for HPE Service use only)	Yes	Yes
Error recovery	On	Yes	
E-mail notification	Disabled	Yes, but configurations retained	Yes
Administrator password	Unset	No	Yes
Network settings		No. The network is always enabled and the network addresses are retained.	Yes, including DHCP, DNS, IPv4, and IPv6 addresses
HTTPS	Disabled	Yes	Yes
SNMP	Disabled, but saved addresses do not change	Yes, but saved addresses do not change	Yes
Restricted network access	Enabled	Yes	Yes
Miscellaneous settings			
Date and time	Blank or existing	No	
Encryption and security settings	Disabled	Not applicable	Yes
License Keys	None	No	Yes

Configuring the simplest configuration

About this task

This procedure results in a simple autoloader 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 autoloader network settings need to be modified, see [Configuring the autoloader network](#) and [Setting the administrator password](#).
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 autoloader will prompt you to set an actual RMI password (for password guidelines, see [Configuring user account settings](#)). If one person physically installs the autoloader and a second person accesses the autoloader using the RMI, share the INITIAL RMI administrator password as appropriate.
3. If the autoloader has no partition, you should receive a pop-up warning when you login to the RMI stating **Library has no default partition** . Click the Basic Wizard button. If the pop-up is closed, you can also access the wizard in the RMI by clicking **Configuration** on the RMI home screen. In the right pane, click **Partitions** and then click **Basic Wizard**.
4. In the right pane, click **Partitions** and then click **Basic Wizard**.

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

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

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

Create Partition Scheme

Free Resources That Will Be Used by the Partition Scheme

Slots :

7

Mailslots :

1

Drives :

1

Max. Partitions :

1

Partition Settings

Partition Count (max: 1)

1

Barcode Label Length Reported To Host

8

Barcode Label Alignment Reported To Host

Left

Auto Clean

☐

Encryption Mode

Controlled by Backup Application

Back

Next

Finish

Cancel

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

- The autoloader 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 autoloader resources into partitions. If you accepted the defaults, all the tape drives and mailslots are assigned to a single partition.

7. Click **Finish**.

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

Managing the autoloader configuration

Procedure

- [Saving the autoloader configuration](#)
- [Restoring the autoloader configuration from a file](#)
- [Resetting the autoloader configuration to the default settings](#)
- [Resetting the list of known drives](#)

Subtopics

[Saving the autoloader configuration](#)

[Restoring the autoloader configuration from a file](#)

[Resetting the autoloader configuration to the default settings](#)

[Resetting the list of known drives](#)

Saving the autoloader configuration

About this task

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

Procedure

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

Restoring the autoloader configuration from a file

About this task

From the **Configuration > System > Save/Restore Configuration** you can save the autoloader configuration settings to a file, restore the settings, or reset the autoloader configuration to the default settings. If the autoloader chassis or controller must be replaced, the saved

configuration database will make it easier to recover the autoloader configuration.

Procedure

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

Resetting the autoloader configuration to the default settings

Procedure

From the Configuration > System > Save/Restore Configuration expand the Reset Default Settings section, and then click Reset.

Resetting the list of known drives

About this task

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

Procedure

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

Results



NOTE

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

Managing the autoloader date and time

About this task

The autoloader 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

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

Subtopics

[Setting the timezone](#)

[Setting the date and time format](#)

[Setting the date and time](#)

[Enabling 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 System > Date and Time Format.
2. Expand the Date/Time Format section.
3. Select a time format.
4. Select a date format:

For example, July 30, 2013 is displayed as:

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

5. Click Submit.

Setting the date and time

About this task

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

Procedure

1. Navigate to System > Date and Time Format.

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

Enabling SNTP (Simple Network Time Protocol) synchronization

About this task

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

Procedure

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

Results

Time is synchronized with the SNTP server every eight hours.

Configuring media barcode compatibility checking

About this task

When Barcode Media ID Restriction is enabled, the autoloader 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 autoloader will not move an LTO-9 labeled cartridge into an LTO-8 tape drive.

When disabled, the autoloader will move any data cartridges to any tape drive. If the cartridge is incompatible with the tape drive, the autoloader displays a message.



NOTE

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

Procedure

- [Enabling media barcode compatibility checking](#)
- [Disabling media barcode compatibility checking](#)

Subtopics



Enabling media barcode compatibility checking

Procedure

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

Results



NOTE

Barcode labels are recommended on all cartridges in the autoloader. 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

About this task

When Barcode Media ID Restriction is enabled, the autoloader 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 autoloader will not move an LTO-9 labeled cartridge into an LTO-8 tape drive.

When disabled, the autoloader will move any data cartridges to any tape drive. If the cartridge is incompatible with the tape drive, the autoloader displays a message.



NOTE

With Barcode Media ID Restriction disabled, the autoloader 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 Configuration > System > Media Barcode Compatibility Check.



NOTE

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

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

Managing license keys

About this task

License keys register licensed autoloader 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.

Setting RMI Language

About this task

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

Procedure

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

Configuring the RMI timeout

Procedure

1. Navigate to the Configuration > Web Management. Expand the Session Timeout section.
2. Select one of the available settings from the drop-down menu.

The default is 30 minutes.

3. Click Submit

Configuring the autoloader network settings

About this task



NOTE

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

Procedure

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

To have the autoloader obtain an internet address from a DHCP server, select the DHCP or Stateless method.

5. Click Submit.

Using the Configuration > Network Management screen

Procedure

- [SNMP options](#)
- [Adding an SNMP target](#)
- [Editing information for an SNMP target](#)
- [Deleting an SNMP target](#)
- [Clearing all SNMPv3 options](#)

Subtopics

[SNMP options](#)

[Adding an SNMP target](#)

[Editing information for an SNMP target](#)

[Deleting an SNMP target](#)

[Clearing all SNMPv3 options](#)

SNMP options

The autoloader supports both SNMP configuration and SNMP traps.

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



NOTE

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

- **Community Name:** A string used to match the SNMP management station and autoloader. It must be set to the same name on both the management station and the autoloader. 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.
 - **+Information:** All events are sent as SNMP traps.
- **SNMP Targets:** List of configured SNMP targets.

Addina an SNMP target

About this task

If the autoloader 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.
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 (SNMPv1, SNMPv2, or SNMPv3 unless SNMP is limited to SNMPv3 in the following configuration).
6. Enter the SNMP community string for the target.
7. If any of the targets use SNMPv3, enter the SNMPv3 configurations. These SNMPv3 configuration values require corresponding settings on an SNMPv3-enabled trap receiver.
 - a. Limit all autoloader SNMP communication to SNMPv3: When selected, all SNMP communications must use SNMPv3.



NOTE

If the autoloader 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 autoloader 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.

**NOTE**

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

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

**NOTE**

If the autoloader 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.
 - 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.

**NOTE**

Selecting SNMPv3 does not automatically disable SNMPv1 and SNMPv2.

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

About this task

This feature allows for sending autoloader events to a remote syslog server. The data sent only includes the ticket information generated by autoloader 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 Configuration > Network Management > Remote Logging (rsyslog).
2. Enable remote logging, if necessary, by selecting Remote Logging Enabled.

When Remote Logging Enabled is selected, the autoloader can send events to the configured rsyslog 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.
 - +Information: All events are sent.
4. In Remote Logging Server, enter the remote syslog server hostname, FQDN, or IP address.
5. Configure the Remote Logging Port.

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

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

Configuring event notification parameters

About this task



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

Procedure

1. Navigate to Configuration > Network Management > SMTP.
2. If SMTP is not enabled, click SMTP Enabled.
3. When enabled, the remaining configurations are active.
4. Configure SMTP options:
 - a. Notification Level: The types of events for which the autoloader should send an email:
 - 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: Host name, FQDN, 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 Addresses: The addresses to receive the reported events (for example, firstname.lastname@example.com).
 - f. Mailer Name: The name of the sender of the email.
 - g. Emitter Subject: Subject line for the email message.
 - h. Email Address: Return address to use for the email message.
 - i. Authentication Required: When selected, a user name 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: The password associated with the user name when authentication is required.
5. Click Submit.

A test email will be sent after pressing the submit button, and all future events within the notification level configured will be sent.

Configuring tape drives

Procedure

1. Navigate to the Configuration > Drives > Settings.
2. Modify any of the configurable values.
 - Drive number: The drive currently hosting the SCSI communication for the autoloader is designated with (LUN).



- **Serial number:** The serial number assigned to the tape drive by the autoloader. This serial number is reported to host applications. The serial number cannot be modified.

When a drive is replaced, the autoloader reassigns the serial number and WWN from the drive that was removed to the drive that is installed.

This serial number is not the serial number assigned to the drive by the manufacturer; the serial number assigned by the manufacturer is shown in Manufacturer S/N.

- **LTO generation**
 - LTO 6–Ultrium 6250
 - LTO 7–Ultrium 15000
 - LTO 8–Ultrium 30750
 - LTO 9–Ultrium 45000
- **Drive form factor**
 - HH: half height
- **Drive interface**
 - FC: Fibre Channel
 - SAS: Serial Attached SCSI
- **(Modified):** When present indicates that a setting has been changed. To apply the changes, click **Submit**. To reset all changed fields to their previously saved values, click **Undo**.
- **Pwr:** Indicates whether the drive is 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 autoloader.

- **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, LTO-8, or LTO-9 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.

Subtopics

Configuring barcode handling

Configuring barcode handling

About this task

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.

Enabling or disabling mailslots

About this task

The Configuration \geq Mailslot shows whether the mailslot is enabled or disabled.

Procedure

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

Slots not enabled as mailslots are available as storage slots.

Partition wizards

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

- Each partition must have at least one tape drive which will host the autoloader LUN for the partition. Since the autoloader only supports one tape drive, only one partition can be created.
- 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 autoloader off line.

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. The autoloader can only have a single partition because only one tape drive is supported.

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

- Expert Partition Wizard—You could edit the partition configuration to add or remove autoloader resources.

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

Subtopics

Using the basic partition wizard

About this task

The autoloader 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 > Partitions, select Basic Wizard to start the wizard.

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

2. Click Proceed and then click Next.

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



NOTE

If you want to enable or disable the mailslot, 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 minimum length is 6, the maximum length is 16, and the default is 8.



NOTE

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

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

When initiating a cleaning operation, the autoloader 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 autoloader will use an unexpired cleaning cartridge from an unpartitioned area of the autoloader. When enabling auto cleaning, ensure that each partition has an unexpired cleaning cartridge or place at least one unexpired cleaning cartridge in an area that is not assigned to a partition.

**NOTE**

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

The same LTO Ultrium cleaning cartridges are used for all LTO tape drives. The autoloader 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 displays the proposed allocation of autoloader 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 autoloader will come on line automatically.

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

**TIP**

You can use the Expert Partition Wizard to adjust the allocation of resources after creating the partitions with the Basic Partition Wizard.

Using the expert partition wizard

About this task

**CAUTION**

The autoloader 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 mailslot, Cancel out of the wizard and update the mailslot configuration before configuring partitioning.

Procedure

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

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

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

**NOTE**

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

- b. To reconfigure a partition, click Edit and then click Next.

3. Enter a name for the partition.
4. Select the number of barcode characters reported to the host application.

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



NOTE

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

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

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

6. To enable the auto cleaning feature, select Auto Clean.

When enabled, the autoloader 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 to clean more frequently than earlier generation tape drives. For reliable operation, enable Auto Clean for each partition with an LTO-7 or later generation tape drive and ensure that the partition has a valid cleaning cartridge.

When initiating a cleaning operation, the autoloader 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 autoloader will use an unexpired cleaning cartridge from an unpartitioned area of the autoloader. When enabling auto cleaning, ensure that each partition has an unexpired cleaning cartridge or place at least one unexpired cleaning cartridge in an area that is not assigned to a partition.



NOTE

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

The same LTO Ultrium cleaning cartridges are used for all LTO tape drives. The autoloader 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 autoloader monitors the initiator lists for all the LTO-7 and later generation drives in that partition. If the autoloader detects more than a single host WWNN for a drive, the autoloader generates an LTO7+ Multi-initiator SCSI Conflict Detection warning event. The event lists all 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 autoloader.

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

Importing or exporting cartridges in a partition without an assigned mailslot will require magazine access, which will take the autoloader 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 Drive, select the Active Control Path Drive and click Next.
13. Verify the partition configuration and then click Finish.
14. After the wizard reconfigures the partition, the autoloader will come on line automatically.

Subtopics

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

Deleting a partition using the expert partition wizard

Procedure

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

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



NOTE

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

Encryption configuration

The autoloader supports multiple methods of encryption.

Encryption is configured from the [Configuration > Encryption](#) screen.



NOTE

The autoloader goes offline when the encryption configuration is changed.

Subtopics

[Setting the default configuration mode for new partitions](#)

[Allowing the administrator to configure encryption with the Expert Partition Wizard](#)

[Setting the encryption mode for a partition](#)

Setting the default configuration mode for new partitions

Prerequisites

Logged in to the RMI as the security user

Procedure



1. Navigate to the RMI Configuration > Encryption screen.
2. In the Set Default Encryption Mode for new Partitions , select a mode.
3. To update the setting for all existing partitions, click Apply to all existing partitions .
4. Click Submit.

Allowing the administrator to configure encryption with the Expert Partition Wizard

Prerequisites

Logged in to the RMI as the security user

About this task

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

Procedure

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

Setting the encryption mode for a partition

Prerequisites

Logged in to the RMI as the security user

About this task

Procedure

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

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

3. Click Submit.

MSL Encryption Kit configuration

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

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

Subtopics

[Entering the key server token password when using the MSL Encryption Kit](#)
[Viewing the keys on the key server token when using the MSL Encryption Kit](#)
[Changing the key server token password when using the MSL Encryption Kit](#)
[Changing the key server token name when using the MSL Encryption Kit](#)
[Generating a new write key when using the MSL Encryption Kit](#)
[Configuring automatic key generation when using the MSL Encryption Kit](#)
[Backing up the key server token data to a file when using the MSL Encryption Kit](#)
[Restoring key server token data from a backup file when using the MSL Encryption Kit](#)
[Configuring the key server token log in behavior when using the MSL Encryption Kit](#)

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.

Results





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

About this task

When automatic key generation is enabled, the autoloader will automatically request the key server token to generate a new key periodically, according to the policy you configure. 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.
2. Expand the Key Management section.
3. Check the Enabled box in the Automatic key generation policy section.
4. Set the policy for the new key generation frequency, and the date and time this will occur.



5. Click Submit to apply your selections.

Results



NOTE

A key is not generated when the autoloader time is advanced past a time when a new key would have been generated. If you advance the autoloader 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 autoloader 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.

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

About this task

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

Procedure

1. Navigate to 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.



NOTE

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

5. Click Save.

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

Procedure

1. Navigate to Configuration > Encryption > USB—MSL Encryption Kit.
2. Expand 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. Click Choose File and browse to the location of the key server token backup file on the local computer.
5. Click Restore.

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

About this task

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

Procedure

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

Using the KMIP wizard

Prerequisites

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

About this task

With the Key Management Interoperability Protocol (KMIP) Wizard, you can configure use of KMIP key management servers with the library. For additional information on configuring KMIP servers for use with the library, see the KMIP server documentation.

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

About this task



IMPORTANT

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

Procedure

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

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



NOTE

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

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

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

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

Subtopics

[FIPS Support Mode prerequisites](#)

FIPS Support Mode prerequisites

About this task

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

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

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.

Subtopics

[Disabling Secure Mode for an LTO-6 tape drive](#)

[Disabling Secure Mode for an LTO-7 or later tape drive](#)

Disabling Secure Mode for an LTO-6 tape drive

About this task

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 RMI [Configuration > Drives > Settings](#).
2. Power off the autoloader from the library OCP by holding the power button on the front panel for five seconds.
3. To identify the library that enabled Secure Mode, install the tape drive in any 1/8 G3 Autoloader, MSL2024 G4, MSL3040, or MSL6480 tape library with 4.70 or later firmware version. The serial number of the library that enabled Secure Mode is shown in the RMI [Status > Drive Status](#) for the drive in the common name (CN) field.

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

About this task

LTO-7 and later generation tape drives have separate firmware images that enable or disable Secure Mode when the firmware image is loaded onto the drive.



NOTE

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

Procedure

Download and install the firmware image without Secure Mode.

Configuring local user accounts

Procedure

- [Configuring user account settings](#)
- [Adding a local user account](#)
- [Setting or modifying a user password](#)
- [Allowing magazine and mailslot access for the “user” user](#)
- [Changing the OCP PIN from the RMI](#)
- [Changing the OCP PIN from the OCP](#)
- [Removing a local user account](#)

Subtopics

[Configuring user account settings](#)
[Adding a local user account](#)
[Setting or modifying a user password](#)
[Allowing magazine and mailslot access for the “user” user](#)
[Changing the OCP PIN from the RMI](#)
[Changing the OCP PIN from the OCP](#)
[Removing a local user account](#)

Configuring user account settings

Procedure

1. Navigate to the Configuration > User Accounts > User Accounts Settings.
2. Configure the password rules 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 (!@#\$%^&**O_+=[]\|;:"<>?.,/) - default is 0
 - Maximum number of identical consecutive characters - default is Unlimited
 - Maximum number of failed logins before password is locked - default is 10
 - Maximum number of days before password must be changed - default is Unlimited
 - Minimum number of days before password can be changed - default is unlimited
 - Number of password changes before an old password can be used again - default is 3
 - Maximum number of failed TOTP attempts before login is locked - default is 10
3. Click Submit.

Adding a local user account



About this task

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

Procedure

1. Navigate to the Configuration > User Accounts > Local User Accounts.
2. Click Add User.
3. Enter the user account details.
 - Name - a series of characters and numbers with a minimum length of 1 and maximum length of 32. Allowed characters are a-z, A-Z, and 0-9.
 - Role - User or Administrator.
 - Password - Enter the password, and verify the password.
 - Two-factor authentication - Check the box to enable two-factor authentication for the new user.



NOTE

Only a user with two-factor authentication configured can enable two-factor authentication for a new user. If enabled, the new user will be prompted to set up two-factor authentication with their authenticator on first login.

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. Check the box by Two-factor authentication if you want to enable two-factor authentication for the user.



NOTE

Only a user with two-factor authentication enabled can enable two-factor authentication for another user.

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



NOTE

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

Allowing magazine and mailslot access for the “user” user

About this task

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

Procedure

1. Navigate to the [Configuration > User Accounts > User Account](#) .
2. Expand the Allow Magazine or Mailslot Access by the "User role" section.
 - a. Select the checkbox next to Allow magazine access by the "User role": to enable magazine access.
 - b. Select the checkbox next to Allow mailslot access by the "User role" to enable mailslot access.
3. Click Submit.

Changing the OCP PIN from the RMI

Procedure

1. Navigate to the [Configuration > User Accounts > Local User Accounts](#) screen.
2. In the Modify OCP PINs section, click [Modify OCP PINs](#).
3. Select the user in the Name field.

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

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

The PIN must be a number that contains exactly four digits. For example, "1234".

5. Click [Modify](#).

Changing the OCP PIN from the OCP

Procedure

1. After logging in using the OCP, navigate to the [Configuration > Users > Configure PIN](#).
2. Select the user whose PIN you want to change.
3. Enter the new PIN in the Enter PIN and Verify PIN fields. The PIN must be a number that contains exactly four digits. For example, "1234".
4. Select Yes when asked to change the PIN.

Removing a local user account



Procedure

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



NOTE

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

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

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

DC=Examplegroup,DC=local

- Enter the Attribute Mapping parameters.

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

- c. Click Test Connection to verify the configuration.
- d. When the autoloader successfully connects to the LDAP server, click OK.

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

Subtopics

Prerequisites for configuring LDAP user accounts

Prerequisites for configuring LDAP user accounts

About this task

By default, the autoloader 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 autoloader 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 autoloader administrator.
 3. Base Distinguished Name and Domain.
 4. Distinguished Name for the autoloader administrator. These are the parameters needed to search for potential autoloader 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`. Other LDAP servers may be mapped differently.
 6. If SSL is required for the LDAP server. This field is likely required for newer versions of LDAP servers.
 7. Check for the Global Catalog role on a domain controller by going to `Server Manager -> Tools -> Active Directory Sites and Services`. Expand the `Sites` container until you find the domain controller. Expand the domain controller to show `NTDS Settings`, then right click and select `Properties`. The `Global Catalog` option is on the `Properties` screen.
 8. The Ports can be changed on the LDAP server so verify the correct ports are used in the configuration.

Configuring Command View for Tape Libraries integration

About this task

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



NOTE

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

Procedure

1. Verify that SNMP is enabled.
2. Navigate to the *Configuration > Command View TL Configuration*.
3. Configure the autoloader information.
 - Name— The name of the autoloader to display in CVTL.
 -
 - Serial Number: The serial number of the autoloader. This cannot be modified.
 - Management URL: The URL of the management station, including port. For example, <https://192.0.2.24:8099>.



NOTE

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

4. Product information.
 - Name: Shows the product name. This cannot be modified.
 - Version: autoloader firmware version. This cannot be modified.
5. Configure the contact information.
 - Name: Name of the person to contact about management of the autoloader.
 - Phone: Phone number of the contact person.
 - Email: E-mail address of the contact person.
6. Library REST Interface Enablement.
 - Enable Library REST Interface: Select to allow Command View TL and other applications using the REST interface to communicate with the autoloader over the SSH protocol. Enabling and the REST interface does not enable full SSH access for the console or other uses.
 - Library REST Interface User Name: The user name that the autoloader 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 `cvttl`.
 - Library REST Interface Password: This password must be the same as the REST password configured for this autoloader on the Command View TL management station. The same password is used for all applications using the REST Interface to access this autoloader.
7. Click Submit.

Moving CVTL access to a new Management Station

About this task

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

Procedure

[Removing the CVTL Management Station trap destination.](#)

The autoloader can now be added to a new CVTL Management Station using the Configuring Command View for Tape Libraries integration section.

Subtopics

[Removing the CVTL Management Station trap destination](#)

Removing the CVTL Management Station trap destination

About this task

Follow these steps to remove the CVTL Management Station trap destination:

Procedure

1. On the CVTL Management Station, delete the autoloader being moved or removed from the CVTL Management Station.
2. On the MSL autoloader RMI, on the [Configuration > Command View TL](#) page, ensure that the Management URL is blank. If it is not blank, clear it out, and then click Submit.

Configuring the autoloader RMI

About this task

Configure the autoloader RMI from [Configuration > Web Management](#).

Procedure

- [Enabling secure communications](#)
- [Adding a signed certificate for SSL/TLS connections](#)
- [Backing up a custom certificate](#)
- [Restoring a custom certificate](#)
- [Configuring the RMI session timeout](#)
- [Enabling OCP/RMI session locking](#)
- [Restricting RMI access for the administrator and security users](#)

Subtopics

[Enabling secure communications](#)

[Adding a signed certificate for SSL/TLS connections](#)

[Backing up a custom certificate](#)

[Restoring a custom certificate](#)

[Configuring the RMI session timeout](#)

Enabling secure communications

About this task

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

Procedure

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

Adding a signed certificate for SSL/TLS connections

About this task

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

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

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

Procedure

1. Before starting the wizard, prepare your Certificate Authority to sign the certificate. You will paste the certificate generated by the wizard into a field in the Certificate Authority for signing.
2. To start the wizard click Start Certificate Wizard from the Configuration > Web Management 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 device and organization.
 - b. Click Generate CSR.

The wizard displays the certificate in the lower pane.
 - c. Click Select CSR.
 - d. Use a web browser copy command, such as Ctrl-c to copy the certificate generated by the wizard that is now in your computer copy buffer.
5. Paste the certificate into the appropriate field in your Certificate Authority and then have the Certificate Authority sign the certificate.
6. In the wizard Certificate Signing Request screen, click Next.
7. In the Signed Certificate screen, paste the signed certificate into the Signed Certificate pane and then click Next.
8. On the wizard Finish page, click the Finish button to complete the wizard, apply the changes, and reload the page.
9. To verify that the certificate is being used, open an https connection to the autoloader 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 autoloader will revert to the built-in certificate.

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

Backing up a custom certificate

Procedure

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

Restoring a custom certificate

Procedure

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

Configuring the RMI session timeout

About this task

Procedure

1. Navigate to the Configuration > Web Management screen.
2. In the Session Timeout section, select the length of time before a user is timed out of an RMI session.
3. Click Submit.

Enabling OCP/RMI session locking

About this task

The autoloader 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.
2. Check the box OCP/RMI Session Locking.
3. Click Submit.

Restricting RMI access for the administrator and security users

About this task

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

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

Procedure

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

Secure Manager

Secure Manager is a feature for configuring hosts and drives into access control groups that are managed by the autoloader, 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 autoloader.

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

**NOTE**

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

**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 an autoloader 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. An autoloader and drive device can be in multiple Access Control Groups.

Subtopics

[Enabling Secure Manager](#)

[Creating an access group when using Secure Manager](#)

[Changing the name of an access group when using Secure Manager](#)

[Deleting an access group when using Secure Manager](#)

[Adding a host to an access group when using Secure Manager](#)

[Removing a host from an access group when using Secure Manager](#)

[Configuring device access when using Secure Manager](#)

[Creating a host when using Secure Manager](#)

[Changing the name of a host when using Secure Manager](#)

[Deleting a host when using Secure Manager](#)

Enabling Secure Manager

Procedure

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

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 autoloader 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

About this task



IMPORTANT

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

Procedure

1. Navigate to 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 autoloader

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

Subtopics

[Performing the system test](#)

[Performing the slot to slot test](#)

[Performing the element to element test](#)
[Performing the position test](#)
[Performing the wellness test](#)
[Performing the robotic test](#)
[Viewing log files](#)
[Downloading log and trace files](#)
[Managing autoloader firmware](#)
[Updating drive firmware from the RMI](#)
[Updating drive firmware from the OCP](#)
[Downloading a tape drive support ticket](#)
[Downloading an autoloader support ticket](#)
[Rebooting the autoloader](#)
[Rebooting a tape drive](#)
[Clearing drive reservations](#)
[Controlling the UID LED](#)
[Using the LTO-9 New Media Initialization Wizard](#)

Performing the system test

Prerequisites

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

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

About this task

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

- During each cycle, the autoloader 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 canceled, the autoloader will return the cartridge to its original slot.
- The autoloader will not move cleaning cartridges during the test.
- The test operates over the whole autoloader and does not consider partition configuration.
- During the test, the autoloader is off line.

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



Prerequisites

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

About this task

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

Procedure

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

Performing the element to element test

Prerequisites

- The test requires at least one cartridge in the autoloader.
If moving a cartridge to or from a tape drive, the cartridge must be compatible with the generation of the tape drive.
- One of the selected element locations must be empty and one of the selected element locations must be full.

About this task

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

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

Procedure

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

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

4. Select a location from the Destination Elements list.
5. Select the number of cycles.
6. Click Start Test.

Performing the position test



About this task

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

Procedure

1. Navigate to 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

Prerequisites

- At least one drive must be empty.
- At least one cartridge that is compatible with the empty drive must be in a magazine slot or mailslot.
If moving a cartridge to or from a tape drive, the cartridge must be compatible with the generation of the tape drive.
- One of the selected element locations must be empty and one of the selected element locations must be full.
- All backup operations are stopped.

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

About this task

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

Procedure

1. Navigate to the Maintenance > Autoloader Tests > Wellness Test.
2. Click Start Test.

Performing the robotic test

About this task

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

Procedure

1. Navigate to the Maintenance > Autoloader Tests > Robotic Test.
2. Click Start Test.

Viewing log files

Procedure

1. Navigate to the Maintenance > Logs and Traces > View Logs.



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

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

Downloading log and trace files

About this task



NOTE

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

Procedure

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

Managing autoloader firmware

About this task

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

Procedure

- [Updating autoloader firmware from the RMI](#)
- [Updating autoloader firmware from the OCP](#)

Subtopics

- [Updating autoloader firmware from the RMI](#)
- [Updating autoloader firmware from the OCP](#)

Updating autoloader 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](#).
3. Click Choose File and select the firmware file from the local computer.
4. Once the firmware file is selected, click the Upload button to start the upgrade process.
5. Once the firmware file is uploaded, the RMI will be briefly disconnected while the autoloader updates and reboots. Do not log back into the RMI until the login page displays the new firmware version.

Updating autoloader firmware from the OCP

Procedure

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

Updating drive firmware from the RMI

Procedure

1. In the RMI, navigate to the [Maintenance > Firmware Upgrades > Drive Firmware](#) screen.
2. Select the tape drive.
3. Click Choose File, and then select the firmware file from the local computer.
4. Click Submit.

Results

More information

To see the firmware version currently installed on the drives, navigate to the [Status > Drive Status](#).

Updating drive firmware from the OCP

Procedure

1. Copy the firmware file to a USB flash drive.
2. The autoloader only supports FAT-32 formatted USB flash devices. FAT-32 is the most common flash drive format.
3. Insert the USB thumb drive into the USB port on the back of the autoloader.
4. In the OCP, navigate to the [Maintenance > Upgrade Drive from USB device](#).
5. Select the firmware file.

6. Click Start Upgrade.

Downloading a tape drive support ticket

Procedure

1. Navigate to the Maintenance [_>_](#) Download Support Ticket.
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 type, form factor (half height or full height), and interface type
 - Firmware — The current drive firmware version
 - Serial — The drive serial number
 - Partition — The logical library associated with the tape drive
3. Select the drive.
4. Select the ticket to download.
 - Current Ticket — Pulls and saves a new support ticket from the drive. The Current Ticket contains detailed drive logs and is useful when working on an issue with a service engineer.
 - Last Unload Ticket (LTO-6 and earlier) — Saves the ticket that was pulled automatically after the last cartridge was unloaded from the drive.
 - Health Log (LTO-7 and later) — Pulls and saves a new support ticket with less information than the Current Ticket. The Health Log is faster to download when you only need basic drive health information.
5. Click Save.

Downloading an autoloader support ticket

Procedure

1. Navigate to the Maintenance [_>_](#) Download Support Ticket.
2. Expand the Library Support Ticket area, if necessary, by clicking the down arrow on the left side.
3. Click Save.

Rebooting the autoloader

Procedure

From the Maintenance [_>_](#) System Reboot, click Reboot.

Rebooting a tape drive

Procedure

1. Navigate to the Maintenance [> Drives > Drive](#).
2. Select the drive to be rebooted.
3. Click Submit.

Clearing drive reservations

Prerequisites

- A host is able to connect to a drive or autoloader.
- Commands are rejected with a RESERVATION CONFLICT error or a generic I/O error.

About this task

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

Procedure

1. Navigate to the Maintenance [> Drives > Clear Drive Reservation](#).
2. Select the drive for reservation clearing.
3. Click Submit.

Controlling the UID LED

About this task

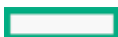
The UID LED is a blue LED on the controller. The UID LED is useful for identifying the autoloader in a data center. The UID LED is controlled by the user.

Procedure

1. Navigate to the Maintenance [> UID LED Control](#).
2. To change the LED status, select the Controller, and click the **Switch LEDs On** or **Switch LEDs Off** button.

Using the LTO-9 New Media Initialization Wizard

About this task





IMPORTANT

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

Procedure

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

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

5. Click Next.
6. Select the drive to be used for initializing the media and click the right arrow. If all the drives are to be used, click **Select All**, then click the right arrow. This will place the drives in the section to the right titled Selected Drives.
7. Click Next.
8. Click Finish to complete the wizard and begin the media initialization process on the selected tapes. The wizard screen will show the progress as the process completes. If you click Exit, you will leave the wizard, but the process will continue and updates will be displayed on the Maintenance > LTO-9 New Media Initialization Wizard page.



NOTE

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

Subtopics

Initialization estimated times

Initialization estimated times

All new LTO-9 tapes require an industry-wide standard initialization process the first time that they are loaded into an LTO-9 drive. It is a one-time process per tape, and is required on all new LTO-9 media from all vendors. For a new autoloader with all new tapes, the time required to run the initialization wizard for 8 tapes with a single LTO-9 drive could take up to 16 hours.

Following are a few things to note:

- Using the LTO-9 initialization wizard is one option to perform the new media initialization on the 1/8 G3 Autoloader. The wizard is designed to help users initialize a batch of new media, with one operation, and not necessarily to initialize an entire autoloader full of new tapes. Another option would be to let each piece of media automatically initialize upon the first load into a drive. Most ISV software is designed to allow for this media initialization time as it is an industry-wide standard. This will add that initialization time (up to 2 hours) to the backup window the first time a new, unused tape cartridge is loaded to a drive by the application. This spreads out the time required to initialize many new tapes by performing the initialization as needed on each tape rather than all at once.

- The 2 hour per tape initialization time is an absolute worst case, and the actual time is often much less.

Operating the autoloader

Click the Operations button on the RMI Home to access the operations features.

Subtopics

[Storage slots](#)

[Moving media](#)

[Opening a Mailslot](#)

[The mailslot cannot be opened](#)

[Opening a magazine](#)

[Opening a magazine from the OCP](#)

[Cleaning a tape drive](#)

[Rescanning the cartridge inventory](#)

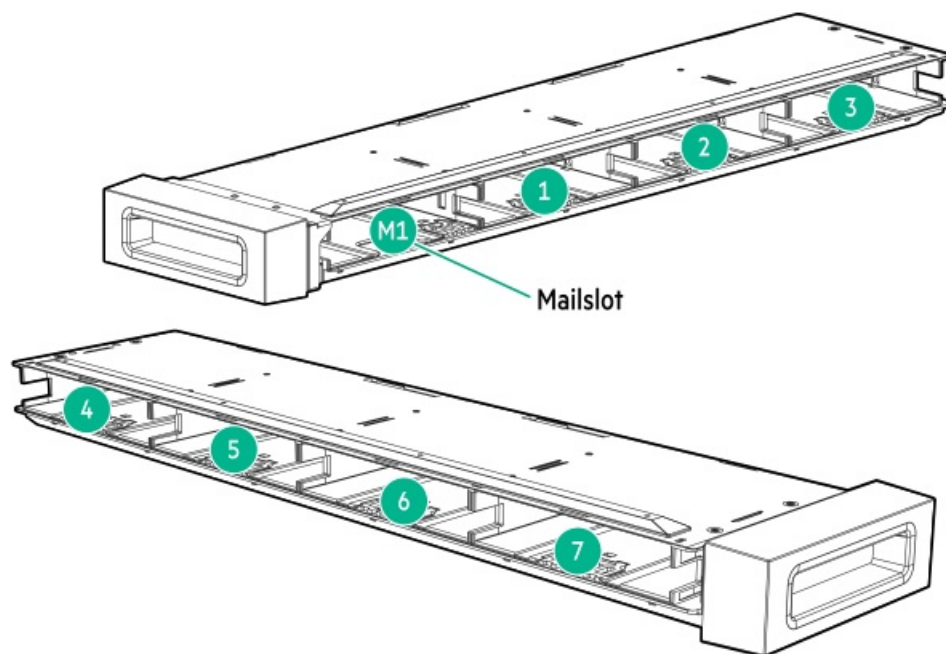
[Forcing a drive to eject a cartridge](#)

Storage slots

Each autoloader has two magazines of storage slots that can be removed from the front of the autoloader. Each magazine has 4 storage slots for tape cartridges.

The following illustration shows the slot numbers for all the slots in the magazines.

The mailslot is in the left magazine. When enabled, the mailslot takes the place of storage slot 1.



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.

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 the barcode label characters in the search area and click Search.

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

4. To perform a different search or display all the available cartridges, click Barcode Filter Off.
5. Select the destination location from Destination Elements.

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

6. Click Submit.

Opening a Mailslot

Procedure

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

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

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

About this task



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 autoloader.

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 the autoloader, the autoloader 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**.
2. Click Open for the magazine.

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

Opening a magazine from the OCP

About this task



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 autoloader.

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. Navigate to the **Operation > Magazine Unlock Left** or **Magazine Unlock Right**.
2. The autoloader will release the lock. A message will be displayed on the OCP indicating the magazine is unlocked.
3. Pull the magazine out of the autoloader.



NOTE

The magazine will relock after 30 seconds.

4. Insert the magazine into the magazine slot.

When reinstalling the magazine, ensure the guides of the magazine are correctly engaged.

Cleaning a tape drive

About this task

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

- [The auto cleaning feature](#)
- [Configuring auto cleaning](#)
- [Initiating a drive cleaning operation](#)

Subtopics

[The auto cleaning feature](#)

[Configuring auto cleaning](#)

[Initiating a drive cleaning operation](#)

The auto cleaning feature

When auto cleaning is enabled, the autoloader must have an unexpired labeled cleaning cartridge loaded. The label must begin with the letters “CLN” for the autoloader 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 autoloader 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 autoloader will choose a cleaning cartridge whose usage count is not available in the cartridge inventory information. If the autoloader knows the usage count for all the cleaning cartridges, the autoloader will choose the one with the highest usage count.

Configuring auto cleaning

About this task

You can configure auto cleaning with the basic or expert partition wizards. When auto cleaning is enabled, the autoloader 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.

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.
2. Click Rescan.

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

Forcing a drive to eject a cartridge

About this task

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

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

Procedure

1. Navigate to the Operation > Force Drive Media Eject.
2. Select the drive in the Source Elements list.
3. Select the destination in the Destination Elements list.
4. Click Submit.

Subtopics

Difficulty ejecting a cartridge

Difficulty ejecting a cartridge

Symptom

A drive has difficulty ejecting a cartridge.

Cause

This problem is usually caused by bad or damaged media.

Action

Remove the cartridge from the media pool,



Viewing status information

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

Subtopics

[Viewing autoloader and module status](#)

[Viewing autoloader or partition configuration settings](#)

[Viewing drive status](#)

[Viewing network status](#)

[Command View TL status parameters](#)

[Viewing encryption status](#)

[Viewing Secure Manager status](#)

Viewing autoloader and module status

Procedure

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

Subtopics

[Status > Library Status screen parameters](#)

[Using the cartridge inventory modular view](#)

[Using list views](#)

[Using the partition map graphical view](#)

Status > Library Status screen parameters

Library information

- **Vendor** - Vendor ID of the SCSI Inquiry string
- **Product ID** - Product ID of the SCSI Inquiry string
- **Serial Number** - Autoloader serial number
- **Base Firmware Revision**
- **Base Controller Revision**
- **Robotic Hardware Revision**
- **Robotic Firmware Revision** - Version of the currently installed robotic assembly firmware. The robotic assembly firmware is bundled and installed with the autoloader firmware.
- **Barcode Reader Hardware Revision**
- **Barcode Reader Firmware Revision** - Version of the currently installed barcode reader firmware. The barcode reader firmware is bundled and installed with the autoloader firmware.

Library status

- **Library Status**

- Idle—The autoloader robotic is ready to perform an action.
- Moving—The autoloader robotic is moving a cartridge.
- Scanning—The autoloader robotic is performing an inventory of cartridges.
- Offline—The autoloader robotic has been taken off line by the autoloader.
- **Total Power On Time**—Total time that the autoloader has been powered on since it was manufactured
- **Cartridge in Transport**—When applicable, displays the barcode label of the cartridge currently in the robotic assembly
- **Odometer**—Robotic assembly move count
- **Left Magazine Status**—The lock status of the left magazine
- **Right Magazine Status**—The lock status of the left magazine
- **Mailslot Status**—The lock status of the mailslot
- **Shipping Lock**—The shipping lock status

Using the cartridge inventory modular view

Procedure

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

Using list views

About this task

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

Procedure

1. Navigate to one of the list views.
 - To see the elements organized by module, navigate to the **Status > Cartridge Inventory > List View**.
 - To see the elements organized by logical autoloader or partition, navigate to the **Status > Partition Map > List View**.
2. In the Inventory List, you could see:
 - **Slot #**—The slot number in the form `<module>.<slot>`, where `module` is the module number and `slot` is the slot number.
 - **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.

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.

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

Viewing autoloader or partition configuration settings

About this task



NOTE

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

Procedure

Navigate to the Status > Partition Map > Configuration Status.

The autoloader displays the current configuration settings for the partition.

Subtopics

[Configuration Status screen parameters](#)

Configuration Status screen parameters

- Partition Number—The partition number assigned by the autoloader.
- Partition Name—The partition name assigned with one of the partition wizards.
- Partition S/N—The partition serial number assigned by the autoloader.
- 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 autoloader will report 123456 . If alignment is right, the autoloader will report 345678 .
- Auto Clean—Indicates whether autoloader-managed cleaning is enabled or disabled.
- Key Manager Type—The type of encryption key manager configured for use with the partition.
- FIPS Support Mode—Indicates whether FIPS support mode is enabled or disabled.
- Active Control Path Drive —The tape drive that hosts the LUN for the partition.
- LTO-7+ Multi-initiator SCSI Conflict Detection —Indicates whether LTO-7+ Multi-Initiator SCSI Conflict Detection is enabled or disabled.

Viewing drive status

Procedure

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

Subtopics

Drive Status configuration settings

Drive Status configuration settings

- Drive number—Drives are numbered starting with one from the bottom of the autoloader up. The drive currently hosting the SCSI communication for the autoloader is designated with (LUN).
- Serial number— The serial number assigned to the tape drive by the autoloader. This serial number is reported to host applications.
- LTO generation
 - LTO 6—Ultrium 6250
 - LTO 7—Ultrium 15000
 - LTO 8—Ultrium 30750
 - LTO 9—Ultrium 45000
- Drive form factor
 - HH—Half height
- 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 explanation 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.
 - **Encrypt**—The drive is writing encrypted data.
- **Power on status**—Indicates whether the drive is powered on or off.
- **Firmware**—The version of firmware currently installed on the drive
- **Powered**—On or Off
- **Vendor**—The Vendor ID of the SCSI Inquiry string
- **Personality**—A service engineer might request this information.
- **Firmware**—Current Firmware version of drive
- **Manufacturer S/N**—The serial number assigned to the drive when it was manufactured. Use this serial number when working with service.

Powered- Current power status

- **WWNN**—Worldwide unique number for the drive. The autoloader assigns WWNNs to the drive bays. If a tape drive is replaced, the WWNN is reassigned to the replacement drive.
- **Temperature**—Internal temperature reported by the drive. The normal temperature range varies depending on the type 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.

- **Partition**—Partition to which the drive is assigned.
 - **Encryption**—Indicates the type of encryption the drive is configured for.
 - **Cartridge**—Information about the cartridge, if any, currently in the drive.
- IP Address—IP address of the drive Ethernet port. The drive ethernet port is not used when installed in an autoloader.
- **Media Removal**—Whether the media can be removed from the drive or not. Many host applications prevent media removal while accessing the cartridge in the tape drive.
 - **Data Compression**—Indicates whether the drive is using data compression.
 - **Cooling Fan Status**—When the drive cooling fan is operating correctly, the status will be Active.
 - **Product ID**—The product ID portion of the SCSI inquiry string.
 - **Firmware Type**—For LTO-7 and later drives, indicates whether Normal or Secure Mode firmware is loaded on the drive.
 - **Manufacturer S/N**—The serial number assigned to the drive when it was manufactured. Use this serial number when working with service.
 - **WWNN**—Worldwide unique number for the drive. The autoloader 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.
- Fibre Channel Fabric Log-in Name (LTO-6 only)
- Port configuration—Drive port status
 - WWPN—Displays the worldwide port name, a unique identifier for each interface.
 - Speed—Displays the current interface speed.
 - Port Type
 - Automatic (FC only)
 - Loop—Enables selection of the Addressing Mode.
 - Fabric (N/F)
 - Interface—The status of the port connection.
 - N-Port ID—Logical port identifier for the FC drive port (FC only).
 - Fibre Channel Fabric Log-in Name (LTO-6 only) (FC only).
- Secure Mode—Indicates whether the drive is running in Secure Mode.

Viewing network status

Procedure

In the Status > Network you can see the status of the autoloader networking.

Subtopics

[Network Status screen parameters](#)

Network Status screen parameters

- Host Name—Autoloader hostname
- Domain Name—Autoloader Domain Name
- Protocol—IPv4 and/or IPv6
- MAC Address— A unique identifier for the autoloader controller network interface
- Link Status—Enabled or disabled
- Link Speed—Speed of the Ethernet connection to the autoloader
- Duplex—Enabled or disabled

IPv4 settings

- DHCP—When Enabled, the autoloader requests an IP address from a DHCP server each time the autoloader is powered on.
- Address—IP address in use by the autoloader. If DHCP is enabled, this address is obtained from the DHCP server. When DHCP is not enabled, the address was configured.



- Netmask—The network mask of the autoloader controller used when DHCP is not enabled.
- Gateway—The gateway used when DHCP is not enabled.
- DNS 1— Address of the first DNS server
- DNS 2— Address of a secondary DNS server (if applicable)

IPv6 settings

- Stateless Addressing—When Enabled, the autoloader will generate an address for itself based on the routing information obtained from a router advertisement and the MAC address. The autoloader can manage up to five global addresses at the same time, which can be assigned from different routers.
- Static Addressing—When Enabled, the autoloader 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—Autoloader name displayed in Command View TL
- Serial Number—Autoloader serial number reported to Command View TL.
- Management URL—Management station URL, including port. For example: https://192.0.2.24:8099.

Product information

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

Contact information

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

Viewing encryption status

Procedure

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

Subtopics

Encryption status parameters

Encryption status parameters

- USB—MSL Encryption Kit—Status of the key server token.
- KMIP—Status of the connection to the KMIP server.

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

Viewing Secure Manager status

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

Subtopics

Secure Manager status parameters

Secure Manager status parameters

Hosts

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

Drives

- Drive number—The drive number assigned by the autoloader. Drives are numbered starting with one from the bottom of the autoloader up.
- LTO generation
 - LTO6—Ultrium 6250
 - LTO7—Ultrium 15000
 - LTO8—Ultrium 30750
 - LTO9—Ultrium 45000
- Form factor
 - HH—Half height
- Drive interface
 - FC—Fibre Channel
 - SAS—Serial Attached SCSI
- Serial#—The serial number assigned to the tape drive by the autoloader.
- Partition—Autoloader 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.

Using the OCP

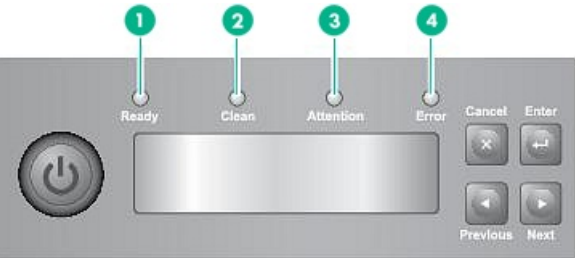
The OCP on the front of the autoloader includes a 2-line by 16-character green backlit liquid crystal display (LCD), four function keys, and four LEDs. This panel provides everything that you need to monitor the autoloader status and control some functions.

Subtopics

- [LED indicators](#)
- [Home screen](#)
- [OCP buttons](#)
- [The OCP menu structure](#)
- [Unlocking the mailslot \(Unlock Mailslot\)](#)
- [Information/Status](#)
- [Configuring the autoloader](#)
- [Accessing the operation functions](#)
- [Accessing the Maintenance functions](#)

LED indicators

The operator panel includes four LEDs that provide a summary of the autoloader status.



11159

Item	Label	Color	Description
1	Ready	Green	Illuminated when power is on. Blinking during tape drive or robotics activity.
2	Clean	Amber	Illuminated when a cleaning cartridge should be used.
3	Attention	Amber	Illuminated if the device has detected a condition that requires attention.
4	Error	Amber	Illuminated if an unrecoverable error occurs. A corresponding error message displays on the LCD screen. You might need to cycle power the autoloader to clear the Error LED.

Home screen

The first line of the Home screen displays the device product name. The second line displays a brief status message.

Figure 1. Home screen

Drive status definitions

Status	Definition
IDLE	Drive has a tape inserted, but there is no activity
RD	Drive is reading
FWD	Drive is forwarding
WR	Drive is writing
LD	Drive is loading a tape
ULD	Drive is unloading a tape
CLN	Drive is cleaning
RWD	Drive is rewinding
SEEK	Drive is seeking
MOV	Performing a tape move or tape exchange operation
ERASE	Drive is erasing a tape
CAL	Drive is calibrating
TEST	Performing a test
UPGR	Performing a firmware upgrade operation
DCR	Decrypting
ENC	Encrypting

OCP buttons

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



10763

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

The OCP menu structure

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

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

From the menu, use the **Previous** and **Next** keys to cycle through the menus, press **Enter** to see the first option in the menu, or press **Cancel** to return to the Home screen.

From an option, use the **Previous** and **Next** keys to cycle through the options in the menu, press **Enter** to select the option, or press **Cancel** to return to the menu list.

Select User	
User	
Information/Status	
Library Status	
Drive (x) Status	
Network Status	
Inventory	
	Magazine Left Inventory
	Magazine Right Inventory
	Drive Inventory
Operation	
Configuration	
Maintenance	
Logout	
Administrator	
Information/Status	
Library Status	
Drive (x) Status	
Network Status	
Inventory	
	Magazine Left Inventory
	Magazine Right Inventory
	Drive Inventory
Operation	
	Mailslot Unlock
	Magazine Unlock Left
	Magazine Unlock Right
Configuration	
	Network
	IPv4 Mode
	Static
	IPv4 Address
	IPv4 Netmask
	IPv4 Gateway
	DHCP
	Library

	Reset to Default Settings
	Save Config to USB Device
	Restore Config from USB
Users	
	Reset RMI PW
	Configure PIN
	Disable RMI Restricted Access
Maintenance	
	Save Lib ticket to USB
	Save Lib Logs to USB
	Upgrade Firmware from USB Device
	Save Drv ticket to USB Device
	Select Dump Mode Current Ticket
	Select Dump Mode Health Log
	Upgrade Drive from USB Device
Logout	
Service	
Information/Status	
	Library Status
	Drive (x) Status
	Network Status
	Inventory
	Magazine Left Inventory
	Magazine Right Inventory
	Drive Inventory
Operation	
	Mailslot Unlock
	Magazine Unlock Left
	Magazine Unlock Right
Configuration	
	Network
	IPv4 Mode
	Static
	IPv4 Address
	IPv4 Netmask
	IPv4 Gateway

DHCP
Library
Reset to Default Settings
Reset to Manufacturing
Save Config to USB Device
Restore Config from USB
Users
Reset RMI PW
Configure PIN
Disable RMI Restricted Access
Maintenance
Save Lib ticket to USB
Save Lib Logs to USB
Upgrade Firmware from USB Device
Save Drv ticket to USB Device
Select Dump Mode Current Ticket
Select Dump Mode Health Log
Upgrade Drive from USB Device
Logout

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

Subtopics

[Logging into the OCP](#)

Logging into the OCP

About this task



TIP

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

Procedure

1. Press any key on the OCP, then Select the user to log in as at the Select User: prompt.



2. When prompted for the PIN, press **Next** to scroll to the first number of the PIN and press **Enter**. The number you selected is replaced with an asterisk (*), and the cursor proceeds to the next text box. Repeat this until you have entered all four numbers. After the last number has been entered, you will be logged in.
3. Press **Next**, **Prev**, **Enter**, and **Cancel** to navigate the menus and options.

Unlocking the mailslot (Unlock Mailslot)

About this task

The mailslot in the left magazine is used only with host system software that supports this feature. The mailslot feature allows you to insert or remove a single tape without removing the entire magazine. The benefit of using a mailslot is that the device will not inventory the rest of the slots in the magazine so the device can return to service sooner. The mailslot is in the left magazine.



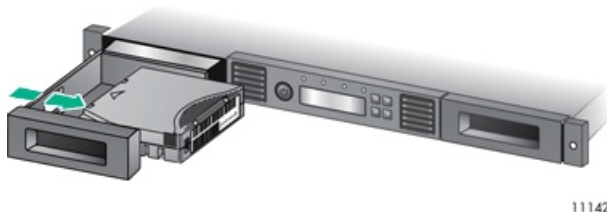
NOTE

The Unlock Mailslot menu is only displayed when the mailslot is enabled.

Procedure

1. Login to the OCP as Administrator, then press **Next** until the screen displays **Operation**. Press **Enter** to select.
2. The autoloader will unlock the mailslot. Once the display reads mailslot unlocked, pull the mailslot out to access the tape.
3. The autoloader will unlock the mailslot.
4. The mailslot ejects automatically. Pull the mailslot out to access the tape.
5. Remove the tape cartridge from the mailslot and insert a different tape cartridge.
6. Push the mailslot back into the autoloader.

Figure 1. Removing a tape from the mailslot



Information/Status

The Information/Status menu provides access to the following status options:

- [Library Status](#)
- [Drive 1 Status](#)
- [Network Status](#)
- [Inventory](#)

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

4. Press **Enter** to select.

Subtopics

[Viewing cartridge inventory \(Information/Status > Inventory\)](#)

[Viewing autoloader information \(Information/Status > Library Status\)](#)

[Viewing drive information \(Information/Status > Drive 1 Status\)](#)

[Viewing network Status \(Information/Status > Network Status\)](#)

Viewing cartridge inventory (Information/Status > Inventory)

About this task

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

- Full (tapes without bar code labels)
- Bar code identification from the tape
- Empty

The autoloader has the following inventory locations:

- Left magazine
- Right magazine
- Drive

Each location provides tape status information:

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



NOTE

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

Procedure

To view the tape inventory:

1. Login to the OCP as Administrator or User, then press **Previous** or **Next** until the screen displays **Information/Status**. Press **Enter** to select.
2. Press **Previous** or **Next** until the screen displays **Inventory**. Press **Enter** to select.
3. Use **Previous** or **Next** to select from the following inventory locations:
 - Magazine Inventory Left — includes the mailslot
 - Magazine Inventory Right
 - Drive (s) Inventory

Viewing autoloader information (Information/Status > Library Status)

Procedure

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

select.

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

Viewing drive information (Information/Status > Drive 1 Status)

Procedure

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

- Firmware Version
- Vendor ID
- Product ID
- LTO Generation
- Interface Type
- Serial Number

Viewing network Status (Information/Status > Network Status)

Procedure

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

Configuring the autoloader

About this task

Configure the autoloader from the Configuration menu.

Procedure

1. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Configuration**.
2. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays your selected function.
 - [Resetting the RMI password \(Configuration > Users > Reset RMI PW\)](#)
 - [Configuring IPv4 network settings \(Configuration > Network\)](#)
 - [Configuring network settings \(Configuration > Configure Network Settings\)](#)
 - [Reset to Default Settings \(Configuration > Library > Reset to Default Settings\)](#)
 - [Saving the autoloader configuration \(Configuration > Library > Save Config to USB Device\)](#)
 - [Restoring the autoloader configuration \(Configuration > Library > Restore Config from USB\)](#)



4. Press **Enter** to select.

Subtopics

[Resetting the RMI password \(Configuration > Users > Reset RMI PW\)](#)

[Configuring IPv4 network settings \(Configuration > Network\)](#)

[Configuring network settings \(Configuration > Configure Network Settings\)](#)

[Reset to Default Settings \(Configuration > Library > Reset to Default Settings\)](#)

[Saving the autoloader configuration \(Configuration> Library > Save Config to USB Device\)](#)

[Restoring the autoloader configuration \(Configuration> Library > Restore Config from USB\)](#)

Resetting the RMI password (Configuration > Users > Reset RMI PW)

About this task

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

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

Resetting the RMI administrator password and OCP PIN.

Procedure

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

Configuring IPv4 network settings (Configuration > Network)

About this task

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

Procedure

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

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

Configuring network settings (Configuration > Configure Network Settings)

Procedure

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

Reset to Default Settings (Configuration > Library > Reset to Default Settings)

About this task

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

The following settings are not reset:

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

Procedure

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

Saving the autoloader configuration (Configuration> Library > Save Config to USB Device)

About this task

Use this option to save the configuration settings to a USB flash drive.

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



NOTE

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

Procedure

1. Insert the USB flash drive in the USB port on the back of the autoloader.
2. Login to the OCP as Administrator, then press **Previous** or **Next** until the screen displays **Configuration**. Press **Enter** to select.
3. Press **Previous** or **Next** until the screen displays **Library**. Press **Enter** to select.
4. Press **Previous** or **Next** until the screen displays **Save Config to USB Device**. Press **Enter** to save.
5. When the save operation is completed, remove the USB flash drive from the USB port.

Restoring the autoloader configuration (Configuration > Library > Restore Config from USB)

About this task

Use this option to restore the configuration settings from a USB flash drive.

Procedure

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

Accessing the operation functions

About this task

The Operations menu provides access to the following functions:

- Unlocking magazines (Operation > Magazine Unlock Left or Magazine Unlock Right)
- Unlocking the Mailslot (Operation > Mailslot Unlock)

Procedure

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

Subtopics

[Unlocking magazines \(Operation > Magazine Unlock Left or Magazine Unlock Right\)](#)

[Unlocking the Mailslot \(Operation > Mailslot Unlock\)](#)

Unlocking magazines (Operation > Magazine Unlock Left or Magazine Unlock Right)

Procedure

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

Unlocking the Mailslot (Operation > Mailslot Unlock)

Procedure

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

Accessing the Maintenance functions

About this task

The Maintenance menu provides access to the following functions:

- [Saving a Library Support Ticket \(Maintenance > Save Lib ticket to USB\)](#)
- [Saving Library Log Files \(Maintenance > Save Lib Logs to USB\)](#)
- [Upgrade Autoloader firmware \(Maintenance > Upgrade Firmware from USB Device\)](#)
- [Save Drive Support Ticket \(Maintenance > Save Drv ticket to USB device\)](#)

Procedure

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

2. Press **Previous** or **Next** until the screen displays your selected function. Press **Enter** to select.

Subtopics

[Saving a Library Support Ticket \(Maintenance > Save Lib ticket to USB Device\)](#)

[Saving Library Log Files \(Maintenance > Save Lib Logs to USB Device\)](#)

[Upgrade Autoloader firmware \(Maintenance > Upgrade Drive from USB device\)](#)

[Save Drive Support Ticket \(Maintenance > Save Drv ticket to USB device\)](#)

[Upgrade Drive firmware \(Maintenance > Upgrade Drive from USB device\)](#)

Saving a Library Support Ticket (Maintenance > Save Lib ticket to USB Device)

About this task

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

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

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

Procedure

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

Saving Library Log Files (Maintenance > Save Lib Logs to USB Device)

About this task

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

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

Procedure

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

Upgrade Autoloader firmware (Maintenance > Upgrade Drive from USB device)



About this task

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

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

Procedure

1. Download current autoloader firmware from the Hewlett Packard Enterprise support website at <https://www.hpe.com/support/storage>.
2. Copy the firmware onto the USB flash drive.



TIP

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

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

Save Drive Support Ticket (Maintenance > Save Drv ticket to USB device)

About this task

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

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

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

Procedure

1. Insert the USB flash drive in the USB port on the back of the autoloader.
2. Login to the OCP as Administrator, then press Previous or Next until the screen displays Maintenance. Press Enter to select.
3. Press Previous or Next until the screen displays Save Drv Ticket to USB Device. Press Enter to select.
4. Press Enter when the display shows Select Drive Drive 1.
5. Press Previous or Next to select either Current Ticket or Health Log when the display reads Select Dump Mode. Press Enter.



NOTE

The Current Ticket will contain more information, and is more useful for troubleshooting drive issues.

6. Press Enter when the display shows Are you Sure? Yes.
7. Once the ticket has been saved, the display will read Save Successful. Press any button to return to the menu.

8. Remove the USB flash drive from the USB port.

Upgrade Drive firmware (Maintenance > Upgrade Drive from USB device)

About this task

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

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

Procedure

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



TIP

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

3. Insert the USB flash drive in the USB port on the back of the autoloader.
4. Login to the OCP as Administrator, then press Previous or Next until the screen displays Maintenance. Press Enter to select.
5. Press Previous or Next until the screen displays Upgrade Drive from USB Device. Press Enter to select.
6. Press Enter when the display shows Select Drive Drive 1.
7. Press Previous or Next until the screen displays the filename of the drive firmware file on the USB drive. Press Enter to select the firmware file.
8. Press Enter when the display shows Are you Sure? Yes.
9. Once the firmware file has been updated, the drive will reset and the Ready light on the autoloader will be on.
10. Remove the USB flash drive from the USB port.

Troubleshooting information and procedures



CAUTION

Shipping Lock: The shipping lock must be removed for the robotics to operate properly. The autoloader displays a robot move error if the shipping lock is not removed (see [Removing the shipping lock](#)).

Subtopics

[The autoloader displays errors](#)

[Fibre Channel connection problems](#)

[Detection problems after installing a SAS drive](#)

[Operation problems](#)

[Performance problems](#)

[Service and repair](#)

[The wellness test](#)

[Error codes](#)

[Diagnosing problems with Library & Tape Tools](#)

The autoloader displays errors

Symptom

The autoloader displays autoloader errors and the autoloader edges are not properly supported.

Cause

The autoloader is not properly supported.

Action

- Ensure that the autoloader is installed in a rack using the optional Rack Kit.
- Ensure that the autoloader is sitting on a level surface on the included plastic feet.



CAUTION

Operating the autoloader without one of these kits or the feet could result in autoloader errors.

Placing any weight on top of the autoloader cover might cause errors.

Fibre Channel connection problems

Use the Status screen to check the link connection for your tape drive.

If the screen shows Logged Out:

- Check that the Fibre speed is set to Automatic (on the RMI) or Auto Detect (on the OCP), or that the correct fibre speed is selected. If you are unsure of the speed of the HBA or switch that the autoloader is connected to, try Automatic (on the RMI) or Auto Detect (on the OCP).
- Check that the correct port type, fabric, or loop, is selected. Loop requires additional configuration. If you are unsure of the correct port type, try Automatic (on the RMI) or Auto Detect (on the OCP).

If the screen shows No Link, the Speed Status is – and the Link LED on the back of the drive is off:

- The speed is probably set incorrectly. Try setting the speed to Automatic (on the RMI interface) or Auto Detect (on the OCP).
- If there are still issues, change the port type to Auto Detect.

If the screen shows No Light:

- The cable is not plugged in correctly. Check that it is connected correctly to Port A of the tape drive.
- The cable is damaged. FC cables are delicate. If the cable has been bent or twisted sharply, it might be broken and must be replaced.

If the screen shows ALPA Conflict:

- There might be a conflict with the ALPA address on Loop ports. Select Soft for the Loop mode to allow the system to select an available address each time the tape drive connects to the FC fabric. If your server configuration does not support changing addresses, try using the Hard Auto-Select option for the Loop mode. This allows the system to select an available address when it first connects, and then retain that address for future connections.

Detection problems after installing a SAS drive



Problems encountered after installation are often caused by improper SAS cable connections, application software configuration errors, or an incorrectly configured operating system. If the application software or operating system does not communicate with the autoloader or drive after installation, determine the extent of the detection problem:

- Does the application software detect the tape drive?
- Does the application software detect the autoloader?
- Does the operating system detect the tape drive?
- Does the operating system detect the autoloader?
- Does the operating system detect the autoloader, but list it as a generic device?

Based on the extent of the detection problem, check the following:

- If neither the application software nor operating system detects the tape drive, or they do not detect both the tape drive and the autoloader:
 - Verify that all SAS cables are securely connected on both ends. If the mini-SAS connectors that connect to the tape drive and some HBAs will not plug in, check the key. The mini-SAS connector on the tape drive is keyed at location four, which is the standard location for end devices. If the connector on the cable is keyed in a different location, the connector not plug-in and the cable probably will not work.
 - Check the length and integrity of your SAS cabling. For reliable operation, do not use a SAS cable longer than 6 meters. Do not use a cable adapter or converters between the HBA and the autoloader.
 - Check the SAS connectors for damage or debris.
 - Verify that your HBA is supported by the host computer and qualified with the autoloader. For current HBA compatibility information, see the compatibility matrix at [Accessing the compatibility matrix](#).
 - Verify that your HBA has the latest firmware.
- If the application software or operating system detects the tape drive, but not the autoloader:
 - Verify that multiple LUN support is enabled on the HBA. The device uses two Logical Unit Numbers (LUNs) to control the tape drive (LUN 0) and robotic (LUN 1). The device requires an HBA with multiple LUN support and 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 autoloader.



NOTE

Many RAID or array controllers do not provide multiple LUN support.

- If the application software or operating system does not detect any devices on the HBA:
 - Verify that the SAS host adapter is installed correctly. See the manual that came with your host adapter for installation and troubleshooting instructions. Pay particular attention to any steps describing configuration settings. Ensure that the host adapter is properly seated in the motherboard slot and the operating system correctly detects the host adapter.
 - Verify that the proper device driver is installed for the SAS host adapter.
- If the autoloader is detected by the operating system, but not by the application software:
 - See the documentation included with your backup application for instructions on how to verify proper installation. Some backup software packages require an additional module to communicate with the robotics.
- If the autoloader is detected by the operating system, but is listed as an unknown or generic device:
 - Make sure that the proper device driver, if applicable, is installed for the device. Check your software provider website for the latest drivers and patches.



NOTE

Many backup applications use their own drivers. Before installing a driver, make sure that it is not in conflict with the application software.

If you continue to have problems with a SAS autoloader, check the following:

- Ensure that the device is compatible with the SAS host adapter and backup application you plan to use. For a list of compatible SAS host bus adapters and application software, check with your SAS host adapter manufacturer, backup application vendor, or the compatibility matrix at [Accessing the compatibility matrix](#).
- Verify that your HBA is supported by the host computer and qualified with the autoloader. For current HBA compatibility information, see the compatibility matrix at [Accessing the compatibility matrix](#).
- Ensure that you are using a compatible, high-quality cable. See the product QuickSpecs for a list of supported cables.

Operation problems

Power problems

Problem	Solution
Device does not power on.	<ol style="list-style-type: none">1. Check all power cord connections.2. Make sure that the power button on the front panel has been pressed, and the green READY LED is illuminated.3. Make sure that the outlet has power. Try another working outlet.4. Replace the power cord.
No display messages appear.	<ol style="list-style-type: none">1. Make sure that the power cord is connected.2. Make sure that the power button on the front panel has been pressed, and the green READY LED is illuminated.3. Power cycle the device.4. If the display is still blank but the device seems to be powered on, try to get the device status or error information from the RMI.

Failure/attention indications displayed on the front panel

Problem	Solution
"!" in operator panel inventory display.	Export the data cartridge marked with an ! in the inventory. The cartridge is either damaged, incompatible with the drive, or the wrong type for the attempted operation.
The LCD displays an error code.	Look up the error code, try to resolve the failure, and power cycle the device (see Error codes).

Controller health status

Problem	Solution
Controller health status LED is solid green or not illuminated (pulsing).	To determine if the controller is faulty, power cycle the autoloader. When operating normally, the LED pulses on and off in cycles of approximately one second. If, after power cycling the autoloader, the LED remains solid green or is not illuminated (pulsing), review the logs for error codes and details. In the RMI, navigate to Maintenance > Logs and Traces > View Logs. For assistance with error codes and next steps, contact HPE Support.

Tape movement problems

Problem

Tape stuck in drive.

Solution

Try the following steps, in this order, to remove the stuck tape.



NOTE

The tape drive must rewind the tape before ejecting it. This can take as long as five minutes, depending on how much tape must be rewound. Once the tape is rewound, the eject cycle will take fewer than 16 seconds.

The **READY** light flashes while the tape rewinds. Wait for the tape to finish rewinding before attempting another operation.

1. Attempt to unload the tape from your backup software.
2. Shut down the backup software and stop the operating system's removable storage services. From the OCP, attempt to unload or move the tape to a slot.
3. Power down the unit, disconnect the cable from the drive, power up the unit, and wait until the tape drive is idle or ready. From the OCP, attempt to unload or move the tape to a slot.
4. From the OCP, attempt a force eject or emergency unload operation.



IMPORTANT

Inspect the tape cartridge that was stuck. Damage or misplaced labels on the cartridge could have caused the load/unload failure. Discard any tape cartridge found to have issues.

Tape stuck in storage slot.

To remove a stuck tape from a storage slot:

If the OCP or the RMI is still operational:

1. Move the tapes from the drives to the magazines using the **Move Tape** command.
2. Use the magazine removal process to release the magazine and remove it from the device. First try removing the magazine from the OCP and RMI. If neither one of these processes works, see [Releasing the magazines manually](#).
3. Manually remove the cartridge from the magazine by inserting a finger in the hole at the back of the magazine. Some tapes need to be inserted and removed several times to condition them for free movement in and out of the magazine.

Media problems

Problem	Solution
Cleaning or data cartridge incompatible with drive.	Make sure that you are using data and cleaning cartridges that are compatible with the drive and model of your device (see Tape cartridges) and that you are using the correct cartridge type for the operation. The device automatically unloads incompatible cartridges, the Attention LED flashes, and an exclamation point (!) displays in the inventory display for the indicated slot number. Export the media to clear the state.

Cannot write to or read from tape.




- Make sure that the cartridge is not a WORM cartridge that has already been used.
- Make sure that the cartridge is write enabled (move the write-protect switch to the enabled position).
- Make sure that the data cartridge is compatible with the drive model. (See [Read and write compatibility](#).)
- Make sure that you are using an Ultrium cartridge that has not been degaussed. **Do not degauss Ultrium cartridges!**
- Make sure that the cartridge has not been exposed to harsh environmental or electrical conditions and is not physically damaged in any way.
- Many backup applications do not read or write to cartridges that were created using a different backup application. In this case, you might have to perform an erase, format, or label operation on the cartridge.
- Make sure that you understand any data protection or overwrite protection schemes that your backup application might be using, which could prevent you from writing to a given cartridge.
- Retry the operation with a different, known good tape.
- Clean the tape drive.

SAS Tape drive not detected

Problem	Solution
Device not detected	<ul style="list-style-type: none"> • Check that the HBA supports multiple LUNs and this feature is enabled. If not, only the tape drive will be detected. • Power on the device before powering on the host computer. • Make sure that the autoloader does not have the drive off line and that the autoloader is not running a test. • Check that the device is fully powered up and is not in an error state.

Attention LED is illuminated

Problem	Solution
---------	----------

Problem	Solution
Both the Attention and Cleaning LEDs are lit.	<p>This is caused by a dirty drive that cannot read a tape and marks the tape invalid.</p> <ol style="list-style-type: none"> 1. View the inventory with the RMI. Note the slots that have tapes marked with  . 2. Remove any magazines that contain tapes marked with  . 3. Remove the tapes that were marked with  . 4. Inspect each removed tape for damage, check that the tape is compatible with the drive, and ensure that it is not past its usage life. See Tape cartridges. Discard any tapes that are damaged or past their usage life. Do not use cartridges that are incompatible with the tape drive. 5. Reload the magazines with tapes that have passed inspection and new tapes to replace cartridges that did not pass inspection. 6. Replace the magazines. 7. Clean the tape drive.
A particular cartridge sets off the cleaning light.	Check the cartridge for contamination by loose debris.
A cartridge recently imported from a different environment is causing issues.	Media that is moved from one environment to another can cause issues until it has acclimated to the new conditions. A cartridge should be acclimated for at least 24 hours before being used, particularly if it has been stored at a substantially different temperature or level of humidity than the device.
The Attention LED is lit but the Cleaning LED is not lit after a cartridge load.	<p>The autoloader was unable to complete the requested operation with the selected tape cartridge.</p> <ul style="list-style-type: none"> • Use only cartridges that are compatible with the drive type (see Tape cartridges) . • Use the correct type of cartridges for the operation. For example, use a cleaning cartridge for cleaning. • Make sure that you are using an Ultrium Universal cleaning cartridge (see Tape cartridges) .
The Cleaning LED is lit after using a cleaning cartridge.	The cleaning cartridge is expired. A cleaning cartridge will expire after 50 cleaning cycles.
A particular cartridge sets off the Attention LED and possibly the Cleaning LED.	<p>If the Media Attention LED is cleared and the drive has been cleaned, and then immediately redisplay each time a particular cartridge is reloaded, that cartridge should be suspected as being defective.</p> <ul style="list-style-type: none"> • If this occurs, export the cartridge and load a known good cartridge. In some cases, a cartridge can be worn out, have a defective Cartridge Memory, or have been formatted as a Firmware Upgrade Cartridge. • Any cartridge that is suspected of being defective or contaminated should NOT be reused in any drive. • If the bad cartridge is a cleaning cartridge, it might be expired.

Inventory problems

Problem	Solution
The inventory labels the cartridge Full instead of showing its bar code	<ul style="list-style-type: none"> • Verify that the label is a Hewlett Packard Enterprise label. The bar code reader might not be able to read other labels. • Verify that the label is properly applied. See Labeling the tape cartridges. • Verify that the label is not soiled.
The inventory process takes a long time	Apply high-quality Hewlett Packard Enterprise labels to all tape cartridges. During the inventory process, the bar code reader attempts to read the bar code on the cartridge or the bar code on the back of the storage slot until it identifies the cartridge or determines that the slot is empty. The reader can usually identify a properly labeled cartridge the first time, while determining that an unlabeled cartridge is in a storage slot can take four times as long.

RMI network connection issues

Problem	Solution
Cannot connect to the remote management interface (RMI)	<ul style="list-style-type: none"> • Verify that the device is connected to the LAN with a CAT 5E, 6, or 6E Ethernet cable. • Verify that the link LED on the RJ45 (LAN) connector is lit when the device is powered up. If the LED is not lit, the device is not communicating with the LAN. See your network administrator for help. • Verify that the device has been configured with a valid static network address or DHCP has been enabled so the device can obtain a network address. If using DHCP, write down the device network address from the OCP Information menu. If the device did not obtain a valid address via DHCP, verify that the DHCP server is up and the device has network access to it. If necessary, set a static network address instead. • Enter the device IP address into the address bar of a web browser connected to the same LAN as the device. If the RMI web page does not display, ping the device IP address. If the ping fails, verify that the device has a valid network address and that there are no firewalls or other obstructions to network traffic between the computer with the web browser and the device. See your network administrator for help.

Cleaning problems

Problem	Solution
Cannot load the cleaning cartridge.	<ul style="list-style-type: none"> • Make sure that you are using an Ultrium Universal cleaning cartridge (see Tape cartridges). • Make sure that the cleaning cartridge has not expired. A cleaning cartridge will expire after 50 cleaning cycles. • Ensure that the cleaning cartridge has a cleaning cartridge label installed. For more information on labeling tape cartridges, see Labeling the tape cartridges. • Power cycle the autoloader.

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 autoloader, 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 autoloader](#)
- [Data cartridges](#)
- [Tape drive read or write performance seems slow](#)

You can use the L&TT system performance test to assess the performance of simulated backup and restore operations. For information on downloading and using L&TT, see [Diagnosing problems with Library & Tape Tools](#).

Subtopics

[Average file size](#)

[File storage system](#)

[Connection from the backup server to the disk array](#)

[Backup/archive server](#)

[Backup/archive software and method](#)

[Connection from the archive/backup host server to the autoloader](#)

[Data cartridges](#)

[Tape drive read or write performance seems slow](#)

Average file size

The hard drive must seek to the position of a file before it can start reading. The more time the disks are seeking to files, the lower the performance. Therefore, if the average file size is small, the read performance will be lower.

To determine the average file size, divide the size of the backup by the number of files.

If the average file size is small (64 KB or less), consider using a sequential, image, or block backup method that backs up the whole hard drive or LUN image instead of individual files. The trade-off for using one of these methods is that you might only be able to restore the entire image instead of individual files.



NOTE

File fragmentation will also cause excessive drive seeking, which lowers performance, so ensure that files are regularly defragmented.

File storage system

The file storage system determines the organization of the files on the disks. Using RAID controllers to spread files over multiple disks can improve performance because some disks can be seeking while others are reading. Storing files on a single non-RAID disk results in the slowest performance while storing files on a high-end disk array results in the fastest performance.

Converting standalone disks to RAID can improve performance.

Ensure that the file systems being backed up have no or minimal fragmentation.

Connection from the backup server to the disk array

The connection between the host server and the disks determines how much data can be transferred from the disks to the host computer at 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 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 while also running the backup or archive software and any other processes.

Check the RAM and processor usage during a backup operation. If they are operating at capacity, adding RAM or processor capability can improve performance.

Backup/archive software and method

Each backup method has its own impact on performance, depending on how well it can keep data streaming to the tape drive. In most cases, native applications do not have the features required to maximize performance for LTO tape drives. Hewlett Packard Enterprise recommends using a full-featured backup or archive application with this autoloader.

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 autoloader

For the best performance, the connection from the host server to the autoloader 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 autoloader 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 autoloader is not properly secured to the rack, vibration may cause slow read or write performance. Vibration could come from the cooling fan or external sources.

Action

1. To ensure that the tape drives are securely tightened to the chassis, tighten the drive sled mounting screws (the blue captive thumbscrews). You can use either a #2 Phillips screwdriver or a torque driver.
 - If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not overtighten.
 - If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.
 - If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



IMPORTANT

Under certain conditions of external shock and vibration, it has been noted that if the thumbscrews are not tightened, drive performance issues might occur. In that situation, please tighten the thumbscrews to the recommended torque.

2. Ensure that the chassis is securely tightened to the rack.

From the front of the autoloader, use either a #2 Phillips screwdriver or a torque driver to tighten the captive fasteners

If using a #2 Phillips screwdriver, tighten the captive fasteners until a low initial threshold torque achieves a snug tight condition. Do not overtighten. If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.

3. If the autoloader is not mounted in a rack, verify that it is sitting on a stable, non-vibrating surface.

Service and repair

Subtopics

[Releasing the magazines manually](#)

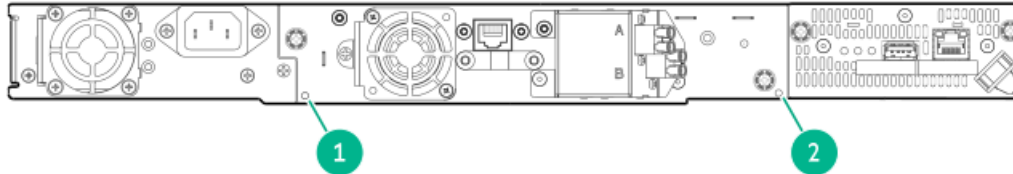
Releasing the magazines manually

About this task

Only use this manual process if the magazine cannot be released using the OCP or RMI, and the device no longer has power.

Procedure

1. If the autoloader is powered on, return all cartridges to the magazines with the RMI Operation > Move Media.
2. Unplug the power cord from the autoloader.
3. From the back of the autoloader, find the access holes for the right and left magazines.

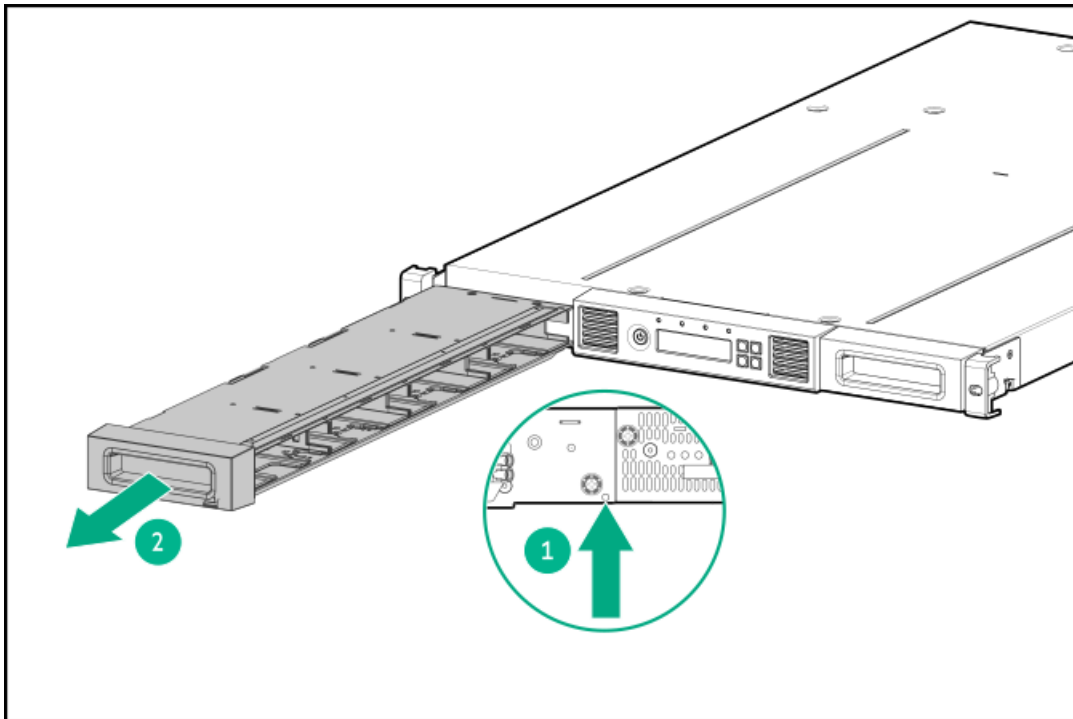


Item Description

- | | |
|---|------------------------------------|
| 1 | Right magazine release access hole |
| 2 | Left magazine release access hole |

The magazine release is a small latch.

4. Insert the end of a small metal pin or straightened paper clip into the magazine access hole at the back of the autoloader about 1.5 cm (0.6 inch), while another person grasps the magazine on that side and pulls it out of the front of the autoloader.



Item Description

- | | |
|---|---|
| 1 | Push a paper clip into the access hole. |
| 2 | Pull the magazine out of the front of the autoloader. |



IMPORTANT

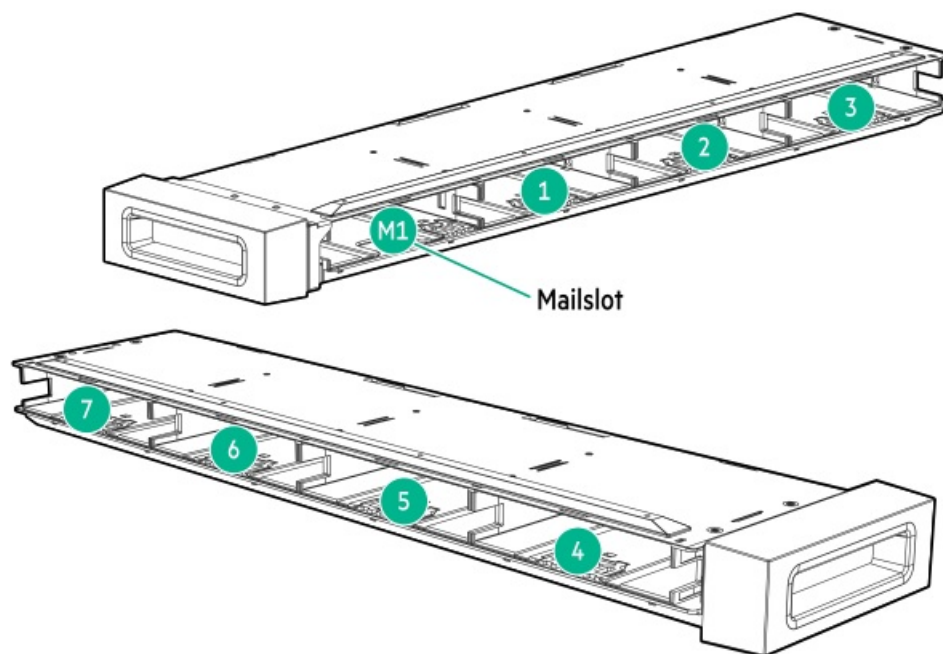
Do not force the pin once you encounter resistance. Doing so can damage the device.

5. Repeat step 3 for the other magazine if necessary.
6. If other tapes are still in the library, for example loose on the robotic or loose on the bottom of the library, attempt to remove them through the magazine openings. If you were unable to remove the magazines, power cycle the library and attempt removal again.

The wellness test

The wellness test exercises all autoloader and tape drive hardware, except the external connections, and is useful for verifying that an autoloader is working correctly.

The Wellness Test requires at least one enabled and functional drive and one cartridge with barcode label in the library. For more information, see the online help. For a quick test execution, it is recommended to have one functional drive and compatible data cartridges in the corner slots of the library.



IMPORTANT

The autoloader will remove any tape cartridge from the tape drive and go offline when running the Wellness test. Verify that any applications using the autoloader are completed before starting the wellness test.

Subtopics

Running the wellness test

Running the wellness test

Prerequisites

- At least one drive must be empty.

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

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

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

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

About this task

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

Procedure

1. Navigate to the Maintenance > Autoloader Tests > Wellness Test.
2. Click Start Test.

Error codes

If an error occurs during operation, the device stops the current operation and displays an error code on the LCD screen.

To check the overall operation of the device, run the wellness test from the OCP. The wellness test exercises all robotic movements and checks the status of the electrical components and communication.

If the error persists, contact support personnel.

There are three ways to obtain logs from the device:

- On the OCP
- On the RMI
- On an L&TT support ticket or report

For more information on Saving Logs and Tickets from the OCP using a USB drive, see [Saving a Library Support Ticket](#) and [Saving Library Logs Files](#).

Subtopics

[Finding autoloader logs on the RMI](#)

[Generating a report or support ticket from L&TT](#)

[Downloading a support ticket from the autoloader](#)

[Viewing a downloaded support ticket](#)

[Finding error code information on an L&TT support ticket or report](#)

[Error events](#)

[Warning events](#)

[Configuration change events](#)

[Informational events](#)

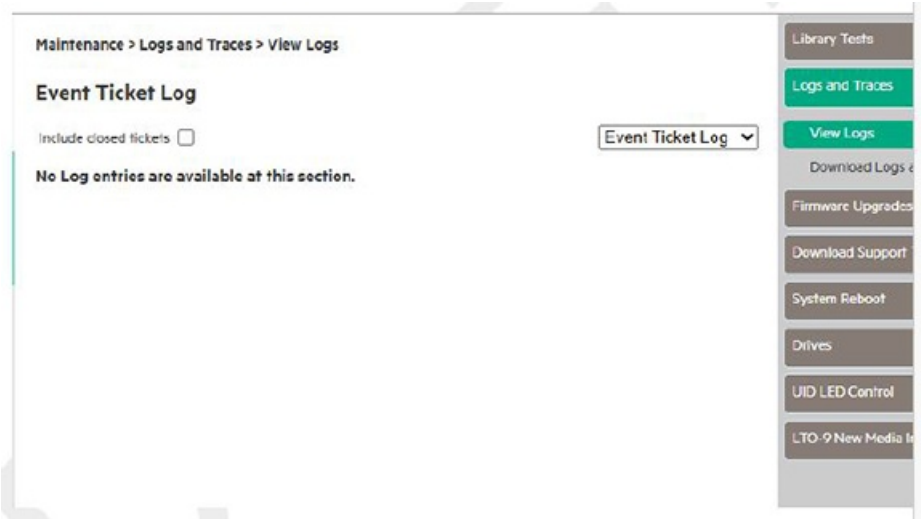
Finding autoloader logs on the RMI

You can view or save logs on the RMI Maintenance > Logs and Traces. The available logs are: Event Ticket Log, Information Log, Configuration Log, or Show All.

The log entries are displayed in order of most recent to oldest. Log entries will have the Time of the Event, the Event code, and a Description of the Event. Clicking on an individual event will show more details.



A Library support ticket can also be saved from the autoloader RMI from the Maintenance > Download Support Ticket > Library Support Ticket. See [Downloading an autoloader support ticket](#).



Generating a report or support ticket from L&TT

Procedure

1. In the L&TT By Product or By Connection tab, select the device from the device list.
2. Click the Health button on the main toolbar to generate and display a standard report, or click the Support button on the main toolbar to display the Support screen for additional report or support ticket options.

Downloading a support ticket from the autoloader

About this task



TIP

Each support ticket downloaded from the RMI will only contain information for the autoloader itself or one drive. To capture all support information, download a ticket from the autoloader 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

- From the RMI Support > Support ticket screen, click Download.
- Insert a USB flash drive into the USB port on the rear panel and then from the OCP, select Download support ticket to USB.

Viewing a downloaded support ticket

Procedure

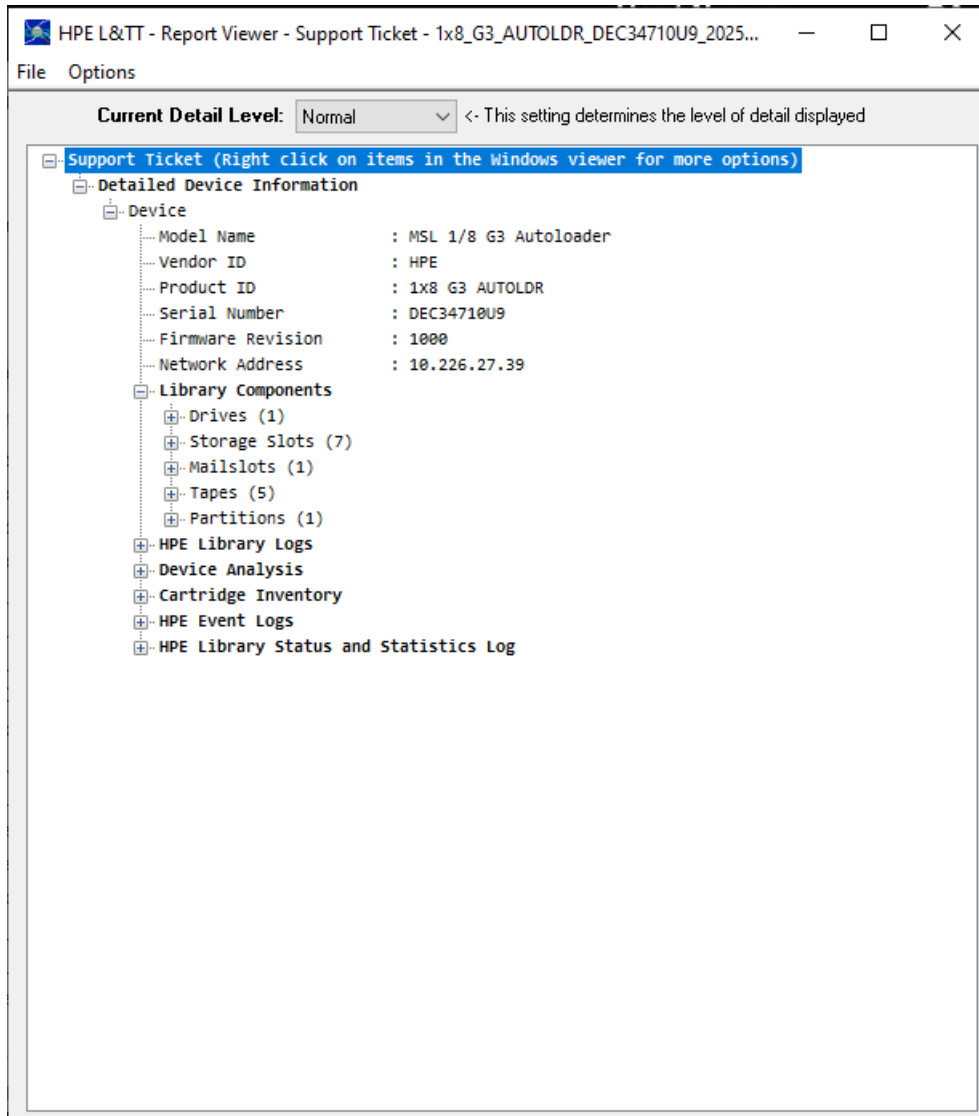
1. From the L&TT File menu, select Load Support Ticket.

2. Select the support ticket file in the browser.

Finding error code information on an L&TT support ticket or report

An L&TT support ticket or report contains detailed information about the device configuration, along with errors and warnings. The support ticket and report contain the same information. The report is easier to read, but must be generated and read on the host computer. The support ticket can be downloaded from the device and then viewed on any computer with L&TT installed.

The top of the support ticket contains basic configuration information about the autoloader.



Expand HP Event Logs to see events divided into three categories:

- Events in the last 24 hours
- Events in the last 31 days
- Events older than 31 days

Set the Current Detail Level to see additional types of events:

- Normal will only show critical events or hard errors.
- More details will also show warning and configuration events.
- Everything shows all events.

Critical events are designated with a STOP sign icon. Expand an event for more information.

The time stamp is in the format hours : minutes : seconds. The hours are in 24-hour clock format.

The date is in the format year/month/day.

The type of event:

- **Crit**—error events
- **Warn**—warning events
- **Config**—configuration events
- **Info**—informational events


The event ID is the number on the header line. It uniquely maps to an error code. For error codes, see [Event codes](#).

The text description in the header is the simple text description of the event.


- The time stamp is in the format hours : minutes : seconds. The hours are in 24-hour clock format. For example, in this case 14 is 2 p.m.
- The date is in the format year/month/day.
- The event ID is the number on the header line, 0x006E in this example. It uniquely maps to an error code.
- HE designates a hard error. The STOP sign icon and the word Crit before the event ID also indicate a hard error.
- The text description in the header (“robotic controller error” in this example) is the simple text description of the main error code.
- The main error code (0x83) is displayed in parentheses as the Global error code. The text after the main error code (Robotic controller generic problem in this example) is the text description for the error code.
- The error sub-code (0x02) is displayed in parentheses as the Module error code. The text after the error sub-code (Robotic: connection to slave robotic failed in this example) is name of the component followed by the text description of the error sub-code.
- The Current command provides information for factory use only.

Error events

Event code	Message text and description	Details and solution
2000	Failed to move cartridge.	<div><div>1. Verify the source and destination elements and retry the move operation.</div><div><div><div>• If the source is a magazine slot, manually remove and replace the tape cartridge several times to ensure that it is not stuck.</div><div>• If the source is a drive, move the tape cartridge to the magazine slot from the OCP or RMI.</div></div><div><div>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 OperationForce Drive Media Eject.</div><div>If the cartridge still cannot be moved from the drive, power cycle the library and then retry the move. If the move is not successful, attempt a force drive media eject from the OperationForce Drive Media Eject.</div></div></div><div>2. Ensure that the autoloader and tape drives are running the latest firmware version.</div></div>

Event code	Message text and description	Details and solution
2003	The Autoloader temperature has exceeded the critical limit.	<ol style="list-style-type: none"> 1. Verify that the power supply fan is functioning. 2. Verify that the drive cover plates are installed in all open drive bays. 3. Verify that the ambient room temperature is within the specified limits. 4. Verify that there are no obstructions to airflow through the autoloader. 5. Ensure that the autoloader is running the latest firmware version.
2004	Autoloader startup failed	<div>  IMPORTANT Verify that the shipping lock is removed. </div> <ol style="list-style-type: none"> 1. Power off the autoloader and then check inside autoloader for any obstruction that the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Clear any loose tape cartridge from the elevator. c. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. Power on the autoloader. d. When reinstalling the magazines, ensure the magazine guides at the top and bottom are correctly engaged. Ensure that the magazine is fully inserted into the autoloader. 2. If the error event reoccurs, ensure that AC power is connected. Using power supply LEDs and controller LEDs, verify that each component is powered on and functioning correctly. 3. Verify that the module alignment mechanisms at the rear of the autoloader are locked in the proper positions. 4. Power cycle the autoloader. 5. If the error event reoccurs, power off the autoloader. Power on the autoloader. 6. If the error event reoccurs, power off the autoloader. If the autoloader was recently moved, the assembly could be out of alignment, correct if necessary. Power on the autoloader. 7. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 8. If the sue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes.

Event code	Message text and description	Details and solution
2009	Autoloader test failed due to robotics problem	<ol style="list-style-type: none"> 1. Review the test requirements, address any issues, and then retry the test. 2. Power off the autoloader and then check inside the autoloader for any obstruction that the robotic assembly could hit. <ol style="list-style-type: none"> a. Clear any obstructions from the bottom of the autoloader. Remove all magazines and ensure that all tapes are pushed fully into their slots. b. Clear any loose tape cartridge from the elevator. c. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. d. When reinstalling the magazines, ensure magazine guides at the bottom are correctly engaged. Ensure that the magazine is the fully inserted into the autoloader. Power on the autoloader. 3. If the error event reoccurs, power off the autoloader. 4. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. <p>If the error event reoccurs, check the event log for additional events or event details that provide more specific information.</p>
2021	Database access error.	<ol style="list-style-type: none"> 1. Ensure that the autoloader and tape drives are running latest firmware version. 2. Power cycle the autoloader. 3. If the error persists, restore the autoloader configuration.
2022	Drive has been hot removed while in active status as LUN master. Tape drives must be powered off before removing them from the autoloader.	<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.
2023	Internal software error.	Power cycle the autoloader.
2024	Exception thrown by application not handled.	<p>An unrecoverable error occurred. Retry the operation and if the error persists power cycle the autoloader.</p> <p>If the error reoccurs, update the library firmware.</p>
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 autoloader. • If the source is a magazine slot, manually remove and replace the tape cartridge several times to ensure that it is not stuck.
2028	Move failed inserting cartridge to slot.	

Event code	Message text and description	Details and solution
2029	Initialization failure due to robot front to back positioning error.	<div>  NOTE If the cartridge still cannot be moved, power cycle the autoloader and then retry that the robotic assembly move. </div> <ol style="list-style-type: none"> Power off the autoloader and then check inside autoloader for any obstruction that may be hitting. If the cartridge still cannot be moved, power cycle the autoloader and then retry the move. <ol style="list-style-type: none"> Remove all magazines and ensure that all tapes are pushed fully into their slots. Clear any obstructions from the bottom of the autoloader. Clear any loose tape cartridge from the elevator. Confirm that the robotics shipping lock is removed. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. Ensure that the magazine is the fully inserted into the autoloader. Power on the autoloader. Verify that the autoloader level front to back and side to side. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. If the error event reoccurs, replace the chassis assembly.
2032	Initialization failure due to robot rotation positioning error. Confirm that the robotics shipping lock is removed.	<ol style="list-style-type: none"> Power off the autoloader and then check inside autoloader for any obstruction that may be hitting. <ol style="list-style-type: none"> Remove all magazines and ensure that all tapes are pushed fully into their slots. Clear any obstructions from the bottom of the autoloader. Remove all magazines and ensure that all tapes are pushed fully into their slots. Clear any loose tape cartridge from the elevator. Confirm that the robotics shipping lock is removed. Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. When reinstalling the magazines, ensure the magazine guides at bottom are correctly engaged. Ensure that magazine is fully inserted into the autoloader. When reinstalling the magazines, ensure magazine guides at the bottom are correctly engaged. Ensure that the magazine is inserted into the autoloader.

Event code	Message text and description	Details and solution
2033	Initialization failure due to robot vertical positioning error.	<p>Power on the autoloader.</p> <ol style="list-style-type: none"> 2. Verify that the autoloader is the level front to back and side to side. Power on the autoloader. 3. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. 4. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the robotic assembly event codes. 5. If the error event reoccurs, replace the chassis assembly.
2035	Initialization failure due to robot gripper positioning error.	<ol style="list-style-type: none"> 1. Power off the autoloader and then check inside autoloader for any obstruction that may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. b. Clear any obstructions from the bottom of the autoloader. Remove all magazines and ensure that all tapes are pushed fully into their slots. 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 appropriate magazine storage slots.</p> e. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. Ensure that the magazine is the fully inserted into the autoloader. <p>Power on the autoloader.</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 autoloader and then retry the operation.
2036	Unintended termination of application process.	Power cycle the autoloader and then retry the operation.

Event code	Message text and description	Details and solution
2037	Robotics firmware version upgrade failed.	
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 autoloader to open slots if necessary. 2. Power cycle the autoloader. 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.
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 that the robotic assembly autoloader. If no drives are unloaded or no compatible cartridge is found, the test will fail and the error event will be generated. 2. Unload all tape drives and then rerun the test. 3. Power off the autoloader and then check inside autoloader for any obstruction that may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Clear any obstructions from the bottom of the autoloader. 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. Power on the autoloader. 4. Verified that the autoloader is level front to back and side to side. 5. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 6. If issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes.
2046	Wellness test failed because drive communication test failed.	<ol style="list-style-type: none"> 1. Power off the autoloader. Remove and then reinstall the tape drive to ensure that the drive is the fully seated. Power on the autoloader. 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.
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 autoloader.

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. Verify that the autoloader is level front to back and side to side. 2. Power off the autoloader and then check inside library for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Confirm that the robotics shipping lock is removed. c. Clear any obstructions from the bottom of the autoloader. 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. Power on the autoloader. 3. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 4. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 5. If the error event reoccurs, replace the autoloader controller.
2052	An open magazine was detected and as a result that the system was taken offline.	<ol style="list-style-type: none"> 1. Ensure that all magazines are inserted completely into the autoloader and properly locked. Do not open magazines using the emergency release while the autoloader is operating and the robot is moving.
2056	Initialization failures 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.
2061	Move failed pulling cartridge from drive.	<ol style="list-style-type: none"> 1. Verify that the drive is seated in the autoloader 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 \geq Force Drive Media Eject screen. If the cartridge still cannot be moved from the drive, power cycle the autoloader, and then retry the move. If the move is not successful, attempt a force drive media eject from the Operation \geq Force Drive Media Eject screen. 4. Ensure that the autoloader and tape drives are running the latest firmware version.

Event code	Message text and description	Details and solution
2062	Move failed inserting cartridge into drive.	<ol style="list-style-type: none"> 1. Verify that the drive is seated in the autoloader 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 autoloader, 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 autoloader and tape drives are running the latest firmware version. If the move is not successful, attempt a force drive media eject from the Operation > Force Drive Media Eject screen.
2063	Move failed positioning picker in front of drive.	<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 autoloader and then check inside the autoloader for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. b. Clear any obstructions from the bottom of autoloader. Remove all magazines and ensure that all tapes are pushed fully into their slots. 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. e. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. Ensure that the magazine is the fully inserted into the autoloader. Power on the autoloader. 3. If the error event reoccurs, power off the autoloader and then verify that the autoloader is level within the rack. Power on the autoloader.
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. 4. Update the library to the latest firmware.

Event code	Message text and description	Details and solution
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.
2066	Autoloader startup process failed during inventory scan.	<ul style="list-style-type: none"> • Remove all magazines and ensure that all tapes are pushed fully into their slots. • Clear any obstructions from the bottom of the autoloader. Remove all magazines and ensure that all tapes are pushed fully into their slots. • Clear any loose tape cartridge from the elevator. • Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. <p>Return loose or uncontrolled tape cartridges to appropriate magazine storage slots.</p> <ul style="list-style-type: none"> • When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. Ensure that the magazine is the fully inserted into the autoloader. <p>Power on the autoloader.</p> <ol style="list-style-type: none"> 2. If the error event reoccurs, power off the autoloader and then verify that the autoloader is level within the rack. <p>If the autoloader was recently moved the assembly could be out of alignment, correct if necessary.</p> <p>Power on the autoloader.</p> <ol style="list-style-type: none"> 3. Power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. Remove all magazines and ensure that all tapes are pushed fully into their slots. <ul style="list-style-type: none"> • Clear any obstructions from the bottom of the autoloader. • Clear any loose tape cartridge from the elevator. Verify that all tape cartridges have high-quality proper barcode labels and that the labels are properly applied. • Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. • When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. Ensure that the magazine is fully inserted into the autoloader. <p>Power on the autoloader.</p> <ol style="list-style-type: none"> 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 autoloader to normal operation and clear the event codes. 6. If the error event reoccurs, replace the autoloader controller.

Event code	Message text and description	Details and solution
2067	For safety reasons, the robot movement was halted in place.	<p>The autoloader detected a physical opening in the autoloader and stopped movement of the robotic assembly.</p> <ul style="list-style-type: none"> • Ensure that all magazines are inserted completely into the autoloader and properly locked. Do not open magazines using the emergency release while the autoloader is operating and the robot is moving. • Ensure that the AC power is connected. Using both power supply LEDs and controller LEDs, verify that everything is powered and functional.
2069	Initialization failure due to barcode reader error.	<ul style="list-style-type: none"> • Check the event log for additional events that provide more specific information. • Run the robotic test. • Power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. Remove all magazines and ensure that all tapes are pushed fully into their slots. <ul style="list-style-type: none"> ◦ Clear any obstructions from the bottom of the autoloader. ◦ Clear any loose tape cartridge from the elevator. <p>Verify that all cartridges have high-quality proper barcode labels and that the labels are properly applied.</p> ◦ 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.</p> <p>Power on the autoloader.</p> <ul style="list-style-type: none"> • Verify that the autoloader is running the latest firmware version. If not, update the autoloader firmware. • Power cycle the autoloader and see if the issue persists.

Event code	Message text and description	Details and solution
2070	Inventory scan failed because of elevator axis problem.	<ol style="list-style-type: none"> 1. Power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. b. Clear any obstructions from the bottom of the autoloader. c. Clear any loose tape cartridge from the elevator. d. Verify that all cartridges have high-quality proper barcode labels and that the labels are properly applied. 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. f. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. Ensure that the magazine is fully inserted into the autoloader. <p>Power on the autoloader.</p> 2. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. 3. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 4. If the error event reoccurs, replace the autoloader controller.
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 autoloader 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 autoloader. • 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.
2074	The autoloader startup failed due to a GPIO error.	Power cycle the autoloader.
2075	The autoloader startup failed due to an error when trying to open the robotics serial port.	Verify that the autoloader is running the latest firmware version. If not, update the autoloader firmware.

Event code	Message text and description	Details and solution
2076	I2C bus signals invalid.	<ol style="list-style-type: none"> 1. Remove all tape drives from the affected chassis and then power on the autoloader. If the problem persists, the cause is likely to be in the chassis. Power off the autoloader. 2. Reinstall the drive. Power on the autoloader. 3. If the problem comes back, the cause could be in the drive. If possible, try a different drive in the drive slot and then try the suspect drive in a different slot to see which part is causing the problem. 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.
2079	Could not upgrade barcode reader firmware.	<ol style="list-style-type: none"> 1. Power cycle the autoloader. 2. If the error persists, see if the event log shows events related to the spooling mechanism or robotic assembly. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information.
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 autoloader. It is likely on top of the robotic assembly or on the bottom of the autoloader. 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 autoloader. 3. Inspect the cartridge for signs of physical damage, and if so, discard it from the media pool.
2082	Drive with Secure Mode enabled has been hot removed while in active status as LUN master.	<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. The drive can now be safely removed.
2087	Error accessing the backplane flash memory.	Power cycle the autoloader.
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 autoloader. Power on the autoloader. 2. If the error event reoccurs, replace the autoloader controller.

Event code	Message text and description	Details and solution
2094	An emergency stop condition was detected 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 are completely inserted and properly locked. • Insert all open magazines before powering on the autoloader. • Ensure that the autoloader is powered.
2095	Inventory scan failed because of robotic positioning problem	<ol style="list-style-type: none"> 1. Power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. Remove all magazines and ensure that all tapes are pushed fully into their slots. <ul style="list-style-type: none"> • Clear any obstructions from the bottom of the autoloader. • Clear any loose tape cartridge from the elevator. Verify that all tape cartridges have high-quality proper barcode labels and that the labels are properly applied. • Check the tape drives for a loose, uncontrolled, or stuck tape cartridge. Return loose or uncontrolled tape cartridges to the appropriate magazine storage slots. Power on the autoloader. 2. If the error event reoccurs, check the event log for additional events or event detail that provide more specific information. 3. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 4. If the error event reoccurs, replace the autoloader controller.
2096	Initializing a communication interface on the autoloader controller failed	<p>Power cycle the autoloader.</p> <p>If the error persists replace the library controller.</p>

Event code	Message text and description	Details and solution
2097	Robotics re-initialization failed	<ol style="list-style-type: none"> 1. Verify that the autoloader is running the latest firmware version. 2. If the error event reoccurs, power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Clear any obstructions from the bottom of the autoloader. 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. Power on the autoloader. 3. If the error event reoccurs, power off the autoloader, and verify that the autoloader is level within the rack. Power on the autoloader. 4. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 5. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 6. If the error event reoccurs, replace the autoloader controller.

Event code	Message text and description	Details and solution
2100	Robotic move to requested position failed	<ol style="list-style-type: none"> 1. Power off the autoloader. Confirm that the shipping lock is removed. Power on the autoloader. 2. If the error event reoccurs, power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Clear any obstructions from the bottom of the autoloader. 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 Clearing obstructions from the library. Power on the autoloader. 3. If the error event reoccurs, power off the autoloader, and verify that the autoloader is level within the rack. Power on the autoloader. 4. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 5. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 6. If the error event reoccurs, replace the autoloader controller.

Event code	Message text and description	Details and solution
2105	Robotic initialization failed due to horizontal positioning problem	<ol style="list-style-type: none"> 1. Power off the autoloader. Confirm that the shipping lock is removed. Power on the autoloader. 2. If the error event reoccurs, power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Clear any obstructions from the bottom of the autoloader. 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 Clearing obstructions from the library. Power on the autoloader. 3. If the error event reoccurs, power off the autoloader, and verify that the autoloader is level within the rack. Power on the autoloader. 4. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 5. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 6. If the error event reoccurs, replace the autoloader controller.

Event code	Message text and description	Details and solution
2106	An elevator block was detected and as a result the system was taken offline	<ol style="list-style-type: none"> 1. Power off the autoloader and then check inside autoloader for any obstruction the robotic assembly may be hitting. <ol style="list-style-type: none"> a. Remove all magazines and ensure that all tapes are pushed fully into their slots. When reinstalling the magazines, ensure the magazine guides at the bottom are correctly engaged. b. Clear any obstructions from the bottom of the autoloader. 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 Clearing obstructions from the library. Power on the autoloader. 2. If the error event reoccurs, power off the autoloader, and verify that the autoloader is level within the rack. Power on the autoloader. 3. If the error event reoccurs, check the event log for additional events or event details that provide more specific information. 4. If the issue is corrected, continue with the next debugging step or return the autoloader to normal operation and clear the event codes. 5. If the error event reoccurs, replace the autoloader controller.

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.

Event code	Message and description	Details and solution
4002	A drive sent a clean request.	<ol style="list-style-type: none"> 1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. Check events occurring at the same time for drive and/or tape cartridge interactions. Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information. If a second know good drive is available, check the suspect tape cartridges in this drive. Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty. 5. If you have not already done so, consider setting up auto clean in each library partition. For more information about auto cleaning, see Configuring Auto Cleaning. Make sure that at least one unexpired cleaning cartridge is physically located in each partition.
4003	The drive configuration failed.	<ol style="list-style-type: none"> 1. Power off the library. Remove and then reinstall the tape drive to ensure that the drive is fully seated. Power on the library. Retry the operation. 2. If the drive installed is a different LTO generation than the drive previously installed, reset the list of known drives 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.

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 that 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. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. Check events occurring at the same time for drive and/or tape cartridge interactions. Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information. If a second know good drive is available, check the suspect tape cartridges in this drive. Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.
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.

Event code	Message and description	Details and solution
4007	Cartridge error.	<ol style="list-style-type: none"> 1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. Remove the tape cartridge and inspect it for damage. If damaged, remove the cartridge from use. 2. Assuming the original cartridge is not damaged, retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. <p>Check events occurring at the same time for drive and/or tape cartridge interactions. Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information.</p> <p>If a second know good drive is available, check the suspect tape cartridges in this drive.</p> <p>Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.</p>
4008	Cleaning cartridge expired.	Discard the cleaning cartridge and retry the cleaning operation with a new unexpired 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.
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. <p>Only install drives that are supported by the library.</p> <ol style="list-style-type: none"> 4. Power on the library.

Event code	Message and description	Details and solution
4012	Move cartridge operation failed due to drive or media issue.	<ol style="list-style-type: none"> 1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. <p>Check events occurring at the same time for drive and/or tape cartridge interactions.</p> <p>Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information.</p> <p>If a second know good drive is available, check the suspect tape cartridges in this drive.</p> <p>Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.</p>
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.
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, and the green light on. <ul style="list-style-type: none"> • If the white light is on or off, verify that the power cords are properly plugged in. • If the green LED is off, replace the power supply.
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.


Event code	Message and description	Details and solution
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. 2. Ensure that the drive is in a healthy state and does not have a cartridge.
4019	General drive firmware bundle upgrade failure.	<ol style="list-style-type: none"> 3. Retry the operation. 4. Power cycle the library and retry the operation.
4020	Database has been reset due to a problem that prevented the library from powering up.	Restore previously saved configuration data. If you do not have a saved configuration file, reconfigure the library.
4021	Drive has been hot removed while in active status as data transfer device.	<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. 3. Power on the library.
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.	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.

Event code	Message and description	Details and solution
4030	Move cartridge operation failed due to media error.	<ol style="list-style-type: none"> 1. Power cycle the drive. Remove the tape cartridge and inspect it for damage. If damaged, remove the cartridge from use. Make sure that the destination drive does not already have a tape cartridge loaded. If the drive has a tape cartridge loaded, make sure that the backup application is finished using the drive, then see event code 2061 Details and Solution. 2. Assuming the original cartridge is not damaged, retry the operation with the same drive and tape cartridge combination. If the problem persists, retry the operation with a different tape cartridge in the same drive. 3. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. Check events occurring at the same time for drive and/or tape cartridge interactions. Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information. <p>If a second know good drive is available, check the suspect tape cartridges in this drive. Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty.</p>
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.	<p>Advanced path failover, ADPF and ACPF, are only supported on LTO-6 tape drives.</p> <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.
4039	The drive configuration failed because of unsupported ACPF features selected.	Use the Partition Wizard to update the partition and drive configuration.
4040	Data path failover occurred.	Check the cabling and all network components between the affected drive and host computer.
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.

Event code	Message and description	Details and solution
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.
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.	
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.	
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.

Event code	Message and description	Details and solution
4063	KMIP configuration invalid.	Use the KMIP configuration wizard to verify the KMIP configuration.
4064	KMIP feature is not licensed.	Disable the KMIP feature or install the necessary license.
4065	A tape alert event was reported by a drive.	<ol style="list-style-type: none"> 1. Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. 2. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. 3. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. 4. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. Check events occurring at the same time for drive and/or tape cartridge interactions. Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information. If a second know good drive is available, check the suspect tape cartridges in this drive. Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty. 5. Verify that the ambient temperature and humidity is within specification for the specific drive generations installed.
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.
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.

Event code	Message and description	Details and solution
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.</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.	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.
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.	1. Verify that all magazines are fully inserted in the library.
4078	Unlocking the left magazine failed.	2. Power cycle the library and then retry the operation.
4079	Unlocking the mailslot failed.	<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.


Event code	Message and description	Details and solution
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.
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. <div data-bbox="915 1423 1481 1587">  <p>NOTE If this warning displays and you are not using DHCP for your environment, disregard the message.</p> </div>
4094	Drive interface I/O error.	Reboot the library to reinitialize the hardware and device drivers.
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.

Event code	Message and description	Details and solution
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.
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 Disabling Secure Mode for an LTO-6 tape drive .
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 Disabling Secure Mode for an LTO-6 tape drive .
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.
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.

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.	<p>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.</p> <div>  NOTE The drive primary ports are offline and the drive status reports FIPS not supported. </div>
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.	<p>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.</p> <p>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.</p>
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.
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 that the library has tape media installed.
4123	No empty slot available for slot to slot test.	Verify that the library has at least one empty tape slot, remove one or more tapes if necessary.
4124	Drive or media statistics could not be retrieved when unloading the tape.	<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.

Event code	Message and description	Details and solution
4125	Potential conflict: Tape drive has been accessed by multiple initiators.	<ol style="list-style-type: none"> 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. 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
4141	Drive requires cleaning.	<ol style="list-style-type: none"> Clean the drive using an unexpired cleaning cartridge. Power cycle the drive. Retry the operation with the same drive and tape cartridge combination. If the problem persists, clean the drive again using an unexpired cleaning cartridge. Retry the operation with a different tape cartridge in the same drive. If the problem reoccurs with the original tape cartridge, but not the different tape cartridge, remove the original cartridge from use. If the problem reoccurs with both tape cartridges, the drive may be faulty or more than one tape cartridge maybe causing issues. Check events occurring at the same time for drive and/or tape cartridge interactions. Using L&TT, run a drive assessment test. Use the RMI to pull a drive support ticket. Use L&TT to view the support ticket and check the device analysis section for more information. If a second know good drive is available, check the suspect tape cartridges in this drive. Based on the information contained in the drive support ticket and the results gathered using the know good drive, determine whether multiple tape cartridges are faulty or if the drive is faulty. If you have not already done so, consider setting up auto clean in each library partition. For more information about auto cleaning, see Configuring Auto Cleaning. Make sure that at least one unexpired cleaning cartridge is physically located in each partition.
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.

Event code	Message and description	Details and solution
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.
4152	The selected port on the target machine is not open, the connection is refused.	Verify that the server application is running on the target machine and the firewall is not blocking the selected port. Contact your IT Personnel to verify the port settings.
4153	The authentication on server side fails, because the client certificate cannot be trusted.	Use a client certificate, which is signed by a trusted Certification Authority (CA) or manually select the untrusted certificate on server side and trust it (not available on all servers).
4154	The target machine could not be reached, no network connection possible.	Verify the following: <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 that the entered host name is correct. Verify the DNS address in the network settings. Contact your IT personnel for the verification of the entered data.
4159	The TLS server certificate could not be verified as a valid and trusted certificate.	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.

Event code	Message and description	Details and solution
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.
4176	Failed to send CVTL ticket	<p>Library is unable to send support tickets to the CVTL server. Check the CVTL configuration of the library. Verify that the CVTL server is online and accessible on the network.</p>

Configuration change events

Event code	Message and description
8000	The configuration of a drive changed.
8001	The drive was added or removed from the system.
8002	A partition was added/removed or changed.
8003	A mailslot bank was enabled/disabled.
8004	Drive firmware changed due to firmware upgrade.
8005	The configuration of hostname/domain name has changed.
8006	The email configuration settings have been changed.
8007	The configuration of a date/time format changed.
8009	The timezone configuration has changed.
8011	The network settings have changed.
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	<p>Level of media generation checking has changed.</p> <p>LTO generation media checking has been enabled or disabled by the user.</p>
8016	Library reset default settings invoked by user. The library settings have been reset to their default values.
8017	Library firmware changed. The firmware process was initiated by a user.
8018	The Unlabeled Media Support configuration has changed.
8019	Robotics firmware version upgraded.
8020	A new key was created automatically. A new security token key was created through the Encryption Kit automatic key generation mode.
8021	Secure Manager status changed.

Event code	Message and description
8022	RMI/OCP Timeout configuration changed.
8024	Mailslot / Magazine access control configuration changed.
8026	Robotics assembly change detected. The robotics assembly has been replaced.
8029	The SNMP configuration changed.
8030	An SNMP target has been added.
8031	An SNMP target has been deleted.
8032	The SNMPv3 settings changed.
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.
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.
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.
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.
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.

Event code	Message
9027	Library test stopped by user.
9028	Configuration backup to base module was successful.
9029	Configuration restore operation from base module was successful.
9031	Library health status changed to status "OK".
9032	Library health status changed to status "Warning".
9033	Library health status changed to status "Critical".
9035	New library chassis detected. The library detected a new expansion module.
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.
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. 2. Power cycle the library. 3. Retry the operation.
9047	MSL Encryption Kit backup has been initiated
9048	MSL Encryption Kit restore has been initiated.
9049	MSL Encryption Kit partial backup has been initiated.
9050	More than five invalid MSL Encryption Kit PIN attempts.
9051	MSL Encryption Kit key server token contains keys that have not been backed up.
9052	MSL Encryption Kit key server token is full. Adding or generation new keys is prohibited.
9053	MSL Encryption Kit key provided.
9055	MSL Encryption Kit key server token not present.
9056	MSL Encryption Kit key server token was inserted.
9057	MSL Encryption Kit key server token was removed.
9060	One or multiple configured DNS servers are not responding.
9061	A user account has been locked due to too many invalid login attempts on RMI.
9062	Invalid password used for login.
9064	Backup of certificate created.
9065	Certificate has been restored.

Event code	Message
9071	MSL Encryption Kit has been password set automatically.

Diagnosing problems with Library & Tape Tools

About this task

With Library & Tape Tools installed on the host server you can:

- Identify all SAS and FC devices connected to your system.
- View detailed configuration, identification, inventory, and drive information for the device.
- Easily update device and drive firmware.
- Run advanced diagnostic tests, including connectivity, read/write, media validation, and testing the functionality of the device.
- View device and drive error logs.
- Generate a detailed support ticket that can be e-mailed or faxed to your support representative for analysis.

The Library & Tape Tools diagnostic provides an intuitive graphical user interface with integrated context-sensitive help. It can be downloaded free of charge from <https://www.hpe.com/support/TapeTools>.

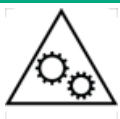
Procedure

1. Run L&TT on the host server.

You can install L&TT on the host server, or run it from a CD-ROM or USB flash drive on the host server.

2. Pull a support ticket for the device.
3. Look at the device analysis results for additional information about the device operation.

Upgrading and servicing the autoloader



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 autoloader.

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

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

A discharge of static electricity can damage static-sensitive devices or microcircuitry. Proper packaging and grounding techniques are necessary precautions to prevent damage.

To prevent electrostatic damage, observe the following precautions:

- Transport products in static-safe containers such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free stations.
- Cover the device with approved static-dissipating material. Provide a wrist strap connected to the work surface and properly grounded tools and equipment.
- Keep the work area free of nonconducting materials, such as ordinary plastic assembly aids and foam packing.
- Make sure that you are always properly grounded when touching a static-sensitive component or assembly.
- Avoid touching pins, leads, or circuitry.
- Use conductive field service tools.



WARNING

The autoloader weighs 12 kg (26.45 lb) without media and 13.6 kg (29.98 lb) with media (eight cartridges). When moving the autoloader, to reduce the risk of personal injury or damage to the autoloader: 1) observe local health and safety requirements and guidelines for manual material handling, 2) always remove all tapes to reduce the overall weight of the autoloader, and 3) obtain adequate assistance to lift and stabilize the autoloader during installation or removal.



WARNING

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

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- Extend only one rack component at a time. If more than one component is extended, a rack can become unstable.



CAUTION

Before moving the autoloader, remove all media. During a move, the cartridges could come out of the storage slots and damage the autoloader.

Subtopics

[Possible tools needed](#)

[Removing and replacing a tape drive](#)

[Removing and replacing a magazine](#)

[Removing and replacing the autoloader controller board](#)

[Removing and replacing the chassis](#)

[Installation and replacement of the autoloader rack kit](#)

Possible tools needed



To service the autoloader, you might need one or more of the following tools:

- Flat-blade screwdrivers (large and small)
- Short-handle #1 Phillips screwdriver
- #2 and #3 Phillips screwdrivers
- Torque driver
- Ground strap
- Paper clip or pin (for manual magazine removal)
- Library and Tape Tools (L&TT) diagnostic software



NOTE

You can use the L&TT diagnostic utility to perform diagnostic functions for the autoloader. L&TT is a diagnostic tool designed to aid in the installation and maintenance of tape storage products. L&TT includes several features designed for use by both storage customers and trained service personnel.

Hewlett Packard Enterprise updates L&TT periodically with new diagnostic features and device support. When using L&TT for troubleshooting, download and update to the current version. You can verify that you are using the latest version and download L&TT without cost from the L&TT website: <https://www.hpe.com/support/TapeTools>

Removing and replacing a tape drive

About this task

Remove and replace the tape drive from the back of the autoloader.

Procedure

1. Using the RMI, unload any tape cartridge from the tape drive, if present.
2. Power off the drive from the RMI. See, [Configuring tape drives](#).
3. Make sure that the LED on the tape drive is off.



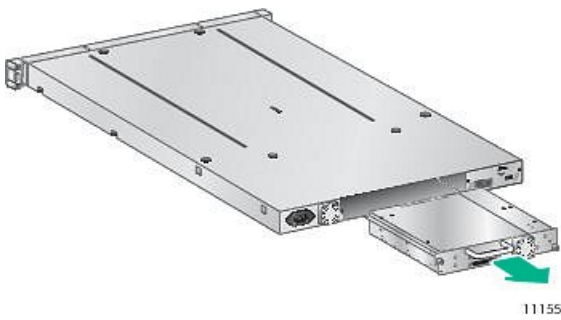
11190

4. Remove the cables from the tape drive being removed.
5. Loosen the blue captive thumbscrews on the drive.



10798

6. To remove the tape drive from the autoloader, pull straight back on the tape drive handle.

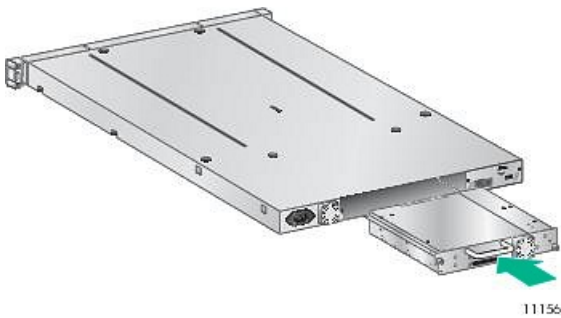


7. Before installing the new drive, inspect the connectors on the tape drive. Ensure that the connectors are intact, free of any foreign objects, and have no cracks or deformed or bent contacts.
8. Holding the tape drive by the handle and supporting it from the bottom, slide it into the drive bay until it is flush with the back of the autoloader.



CAUTION

Push in on the tape drive handle while supporting the bottom of the tape drive. Stop pushing when the tape drive is properly seated. If this procedure is not followed, the connector pins can be damaged.



9. To secure the tape drive to the chassis, tighten the drive sled mounting screws (the blue captive thumbscrews). You can use either a #2 Phillips screwdriver or a torque driver.
 - If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not overtighten.
 - If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.
 - If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



IMPORTANT

Under certain conditions of external shock and vibration, it has been noted that if the thumbscrews are not tightened, drive performance issues might occur. In that situation, please tighten the thumbscrews to the recommended torque.

10. Attach the cables, if necessary, that you removed from the old tape drive.
11. Power on the tape drive.
12. If necessary, upgrade the autoloader and drive firmware using L&TT, the RMI, or a USB flash drive.

Removing and replacing a magazine

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

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



IMPORTANT

To release a magazine manually, see [Releasing the magazines manually](#). However, only use this manual process if the magazine cannot be released using the OCP or the RMI, and the device no longer has power.

Subtopics

[Removing a magazine using the OCP](#)

[Releasing magazines using the RMI](#)

[Releasing the magazine using the manual magazine release](#)

Removing a magazine using the OCP

Prerequisites

Administrator password



IMPORTANT

When removing a magazine using the OCP, once a magazine is removed, the robot cannot perform any other operation.

Procedure

1. Log in to the Operator Control Panel (OCP) as Administrator:
 - a. Press any key.
 - b. Select User: "ADMINISTRATOR", and press Enter.
 - c. Enter the PIN using the Previous, Next, and Enter buttons.
2. Click Next until the screen displays Operation.
 - a. Press Enter.
 - b. Press Next to display Magazine Unlock Right or Magazine Unlock Left.
 - c. Press Enter to release the desired magazine.

The screen displays Magazine Unlocked for 30s.

3. Pull the unlocked magazine out of the library.
4. Remove the tape cartridges from the magazine, noting their locations so each can be replaced in the proper slot.
5. Install the tape cartridges into the replacement magazine in the same slots that they were removed from.

The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

Releasing magazines using the RMI

Prerequisites





IMPORTANT

When removing a magazine using the RMI, once a magazine is removed, the robot cannot perform any other operation.

Procedure

1. Log in to the RMI as the administrator user.
2. Navigate to Operation > Open Magazine.
3. Use the Open button to release each magazine. When a magazine is unlocked, the OCP displays Magazine unlocked.
4. Pull the unlocked magazine out of the library.
5. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot.
6. Install the tape cartridges into the replacement magazine in the same slots that they were removed from.
7. When the OCP screen displays Magazine Removed, slide the replacement magazine completely into the library.

The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

Releasing the magazine using the manual magazine release

About this task

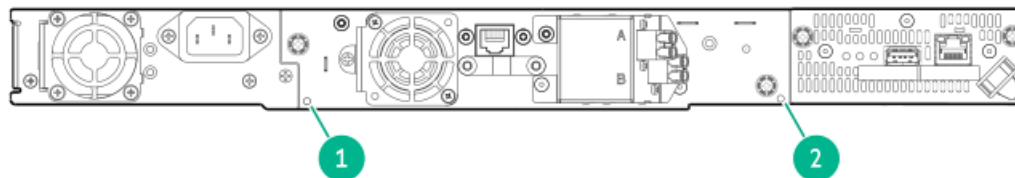


IMPORTANT

Only use this manual process if the magazine cannot be released using the OCP or the RMI and the device no longer has power.

Procedure

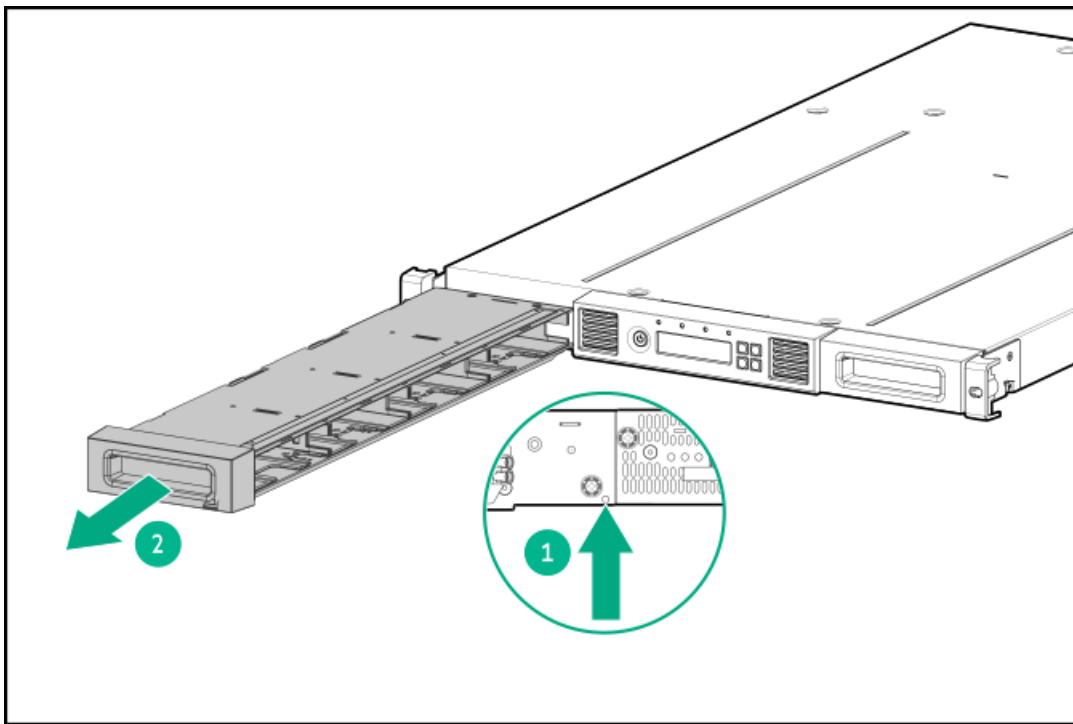
1. From the back of the autoloader, locate the magazine release hole associated with the magazine being released. The magazine release latches are accessed from the magazine release holes on the bottom tape drive plate.



Item Description

- | Item | Description |
|------|---------------------------------|
| 1 | Release hole for right magazine |
| 2 | Release hole for left magazine |

2. Insert a straightened paper clip or small metal pin about 1.5 cm (0.6 inch) into the magazine release hole. Have another person pull out the magazine out of the autoloader and set it aside.



Item Description

- 1 Insert a pin into access hole.
- 2 Release and remove the magazine.



IMPORTANT

Do not force the pin once you encounter resistance. Doing so can damage the autoloader.

3. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot.
4. Install the tape cartridges into the replacement magazine in the same slots that they were removed from.
5. Install the replacement magazine into the autoloader.

Removing and replacing the autoloader controller board

Prerequisites

Tools required: #2 Phillips screwdriver

Procedure

- [Identifying the failed component](#)
- [Saving the autoloader configuration](#)
- [Powering off the Autoloader](#)
- [Preparing to remove the controller board](#)
- [Removing a module controller board](#)
- [Installing the new controller board](#)

- [Completing the autoloader controller replacement](#)
- [Verifying the autoloader controller installation](#)

Subtopics

[Identifying the failed component](#)

[Saving the autoloader configuration](#)

[Powering off the Autoloader](#)

[Preparing to remove the controller board](#)

[Removing a module controller board](#)

[Installing the new controller board](#)

[Completing the autoloader controller replacement](#)

[Verifying the autoloader controller installation](#)

Identifying the failed component

Procedure

1. Check the RMI Maintenance > Logs and Traces > View Logs to get details of the errors and help identifying.
2. Activate the UID LED from the RMI Maintenance > UID LED Control.

Activating the UID LEDs makes it easier to locate the autoloader from the back of the rack.

Saving the autoloader configuration

From the RMI Configuration > System > Save/Restore Configuration screen you can save the autoloader configuration settings to a file, restore the settings, or reset the autoloader configuration to the default settings. The saved configuration database will make it easier to recover the autoloader configuration in the case of a controller replacement.

Procedure (RMI)

1. Navigate to the Configuration > System > Save/Restore Configuration.
2. Click Save. As a result, the Save Configuration process starts and once the file is ready, press Download to save the file to the system you are running the browser on.

Procedure (OCP)

1. Insert the USB flash drive in the USB port on the back of the autoloader.
2. Login to the OCP as Administrator, then press Previous or Next until the screen displays Configuration. Press Enter to select.
3. Press Previous or Next until the screen displays Library. Press Enter.
4. Press Previous or Next until the screen displays Save Config to USB Device. Press Enter to save.
5. When the save operation is completed, remove the USB flash drive from the USB port.

Powering off the Autoloader

Procedure

1. Verify that all host processes are idle.

2. From the front panel, depress the power button and hold it for 5 seconds.
3. If the autoloader does not perform a soft shutdown, depress and hold the power button for 10 seconds.

Preparing to remove the controller board

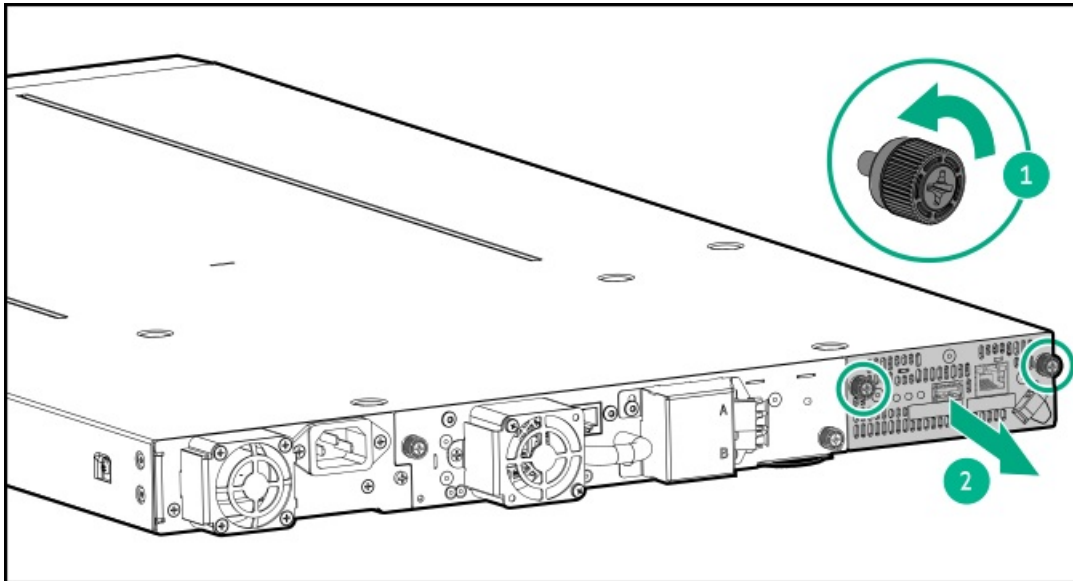
Procedure

1. Unplug the AC power cable from the autoloader.
2. Remove the Ethernet cables, and the USB device from the failed controller board, if present.

Removing a module controller board

Procedure

1. Loosen the two blue captive thumbscrews on the controller board.

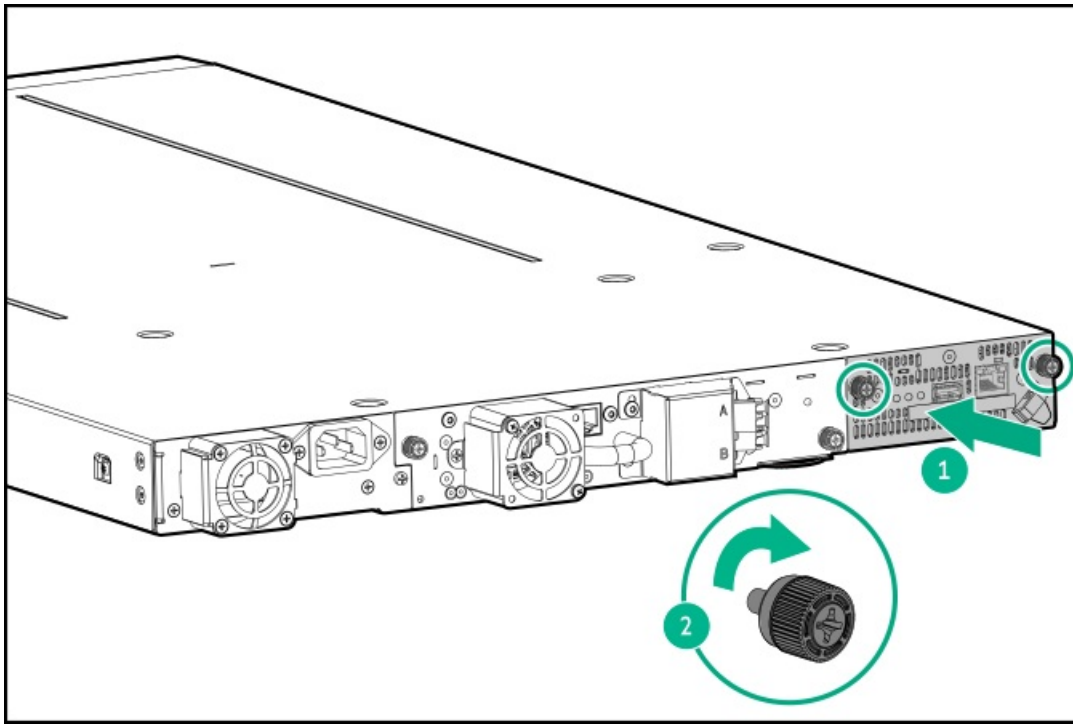


2. Using the thumbscrews, slowly remove the controller board from the autoloader.

Installing the new controller board

Procedure

1. Position the new controller board in the alignment rails.



2. Slide the controller board into the autoloader until firmly seated.
3. Tighten the two thumbscrews with your fingers or a Phillips #2 screwdriver until they are finger tight. Do not over tighten.

Completing the autoloader controller replacement

Procedure

1. If necessary, connect the Ethernet cable and insert the USB device if one was removed.
2. Replace the AC power cord for the autoloader.

Verifying the autoloader controller installation

Procedure

1. Power on the autoloader.
2. Check the overall autoloader status from the RMI [Status > Library Status](#) or on the OCP from the [Information/Status > Library Status](#).
3. Using the RMI, check for events; the event that indicated the controller was faulty should be cleared.
4. Upgrade the firmware if necessary.

After replacing the controller, the firmware version will be the firmware version shipped on the replacement controller. The firmware version shipped on the replacement controller might be earlier than the firmware running on the autoloader before the replacement. In this case, update the autoloader firmware to the version previously installed on the autoloader or the available firmware version.

To find the version of firmware installed on the autoloader, check the upper left corner of the RMI or the [Information/Status > Library Status](#) screen on the OCP. Update the firmware from the RMI [Maintenance > Firmware Upgrades > System Firmware](#).

5. Verify that the autoloader configuration is correct from the RMI [Status > Partition Map > Configuration Status](#) screen.

If the autoloader configuration is incorrect after replacing the controller, restore the previous settings from the RMI [Configuration > System > Save/Restore Configuration](#) or the OCP [Configuration > Library > Restore Config](#) from USB, or reconfigure the autoloader.

If using the MSL Encryption Kit, you might need to enter the token password in the RMI [Configuration > Encryption](#) while logged into the RMI as the Security User.

6. If the UID LED is still illuminated, deactivate it using the RMI [Maintenance > UID LED Control](#).
7. Resume host applications.

Removing and replacing the chassis

Prerequisites

If the autoloader is being managed by Command View for Tape Libraries (CVTL), remove the library from the managed library list in the CVTL Management Station **before** you power off the chassis that is being replaced. After the chassis is replaced, see [Configuring Command View for Tape Libraries integration](#) to add the autoloader back to CVTL.

About this task

The procedure in this topic is a high-level process overview. You must complete the procedures in the subtopics that follow this topic to fully complete the chassis removal and replacement.



WARNING

The autoloader weighs 12 kg (26.45 lb) without media and 13.6 kg (29.98 lb) with media (eight cartridges). When moving the autoloader, to reduce the risk of personal injury or damage to the autoloader:

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



WARNING

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

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



CAUTION

Discharge of static electricity can damage static-sensitive devices or microcircuitry. Proper packaging and grounding techniques are necessary precautions to prevent damage.

To prevent electrostatic damage, observe the following precautions:

- Transport products in static-safe containers such as conductive tubes, bags, or boxes.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free stations.
- Cover the device with approved static-dissipating material. Provide a wrist strap connected to the work surface and properly grounded tools and equipment.
- Keep the work area free of nonconducting materials, such as ordinary plastic assembly aids and foam packing.
- Make sure that you are always properly grounded when touching a static-sensitive component or assembly.
- Avoid touching pins, leads, or circuitry.
- Use conductive field service tools.

Procedure

1. Record the configuration settings.

If the OCP or RMI works, save the configuration settings to the USB flash drive from the OCP or to a file from the RMI. You might need these settings to re-configure the autoloader after replacing the chassis.

2. Remove the tape cartridge from the tape drive using the RMI.



CAUTION

If you cannot remove the tape cartridge from the tape drive, handle the tape drive gently during the rest of the procedure to avoid damaging the tape and losing data.

3. If necessary, remove the USB thumb drive or MSL encryption kit from the controller.
4. Remove the cables, controller, magazines, and tape drive.
5. Remove the chassis from the rack.
6. Unpack the new chassis.
7. Install the replacement chassis.
8. Replace the controller, tape drive, magazines, and cables.
9. Verify the chassis replacement.
10. Replace the shipping lock on the old chassis (the chassis that will be returned).
11. Repackage the old chassis (the chassis that will be returned).

Subtopics

[Removing the cables, controller, magazines, and tape drive](#)

[Removing the chassis](#)

[Unpacking the new chassis](#)

[Installing the replacement chassis](#)

[Replacing the autoloader components and cables](#)

[Verifying the chassis replacement](#)

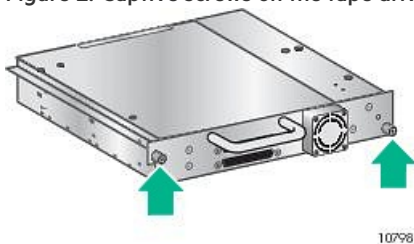
[Replacing the shipping lock on the old chassis](#)

Removing the cables, controller, magazines, and tape drive

Procedure

1. If the OCP or RMI is operational, remove the magazines using the RMI or OCP. For more information, see [Removing the magazines using the RMI or OCP](#).
2. Power off the autoloader. See [Power off the autoloader](#).
3. After powering off the autoloader, look through the shipping lock slot in the top cover. Confirm that the robotic shipping lock slot is immediately below and in vertical alignment with the top cover shipping lock slot. If not and if possible, power cycle the autoloader and recheck the alignment of the two slots.
4. If necessary, remove the USB thumb drive or MSL encryption kit from the controller.
5. Remove the controller and place the controller on a static-safe surface.
6. Remove the power cord and other cables from the autoloader.
7. If the magazines have not been removed, remove the magazines from the autoloader using the manual process (see [Releasing the magazines manually](#)).
8. Loosen the blue captive thumbscrews on the drive.

Figure 1. Captive screws on the tape drive



9. While supporting the bottom of the tape drive, pull straight back on the tape drive handle to remove the tape drive from the autoloader. Place the drive on a static-safe surface.

Removing the chassis

Prerequisites

#2 Phillips screwdriver

About this task



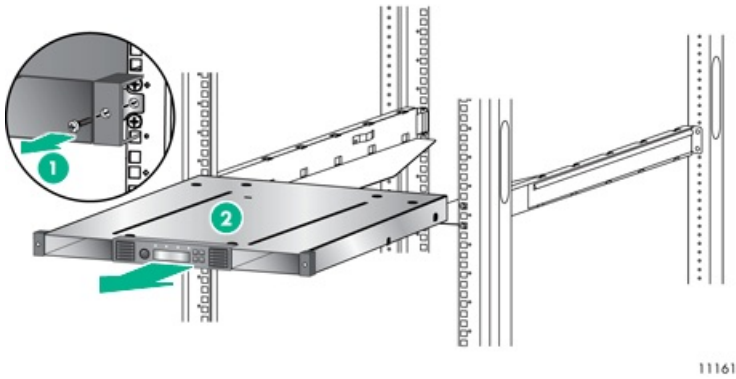
CAUTION

Lift the autoloader from the side edges. Lifting the autoloader from the magazine or tape drive openings can damage the autoloader.

Procedure

1. Obtain adequate assistance to lift and stabilize the autoloader during removal and replacement.
2. If the autoloader is mounted in a rack, from the front of the autoloader:

- a. Loosen the screws inside the left and right front bezel (these screws are captive and cannot be removed).
- b. Slide the autoloader out of the rack using assistance.



Unpacking the new chassis

Procedure

1. Remove the new chassis from the packaging materials and place it on a sturdy table.



NOTE

Save the packaging materials to return the old chassis.

2. Verify alignment of the robotic shipping lock slot.

Look through the shipping lock slot in the top cover. The robotic shipping lock slot is immediately below and in vertical alignment with the top cover shipping lock slot. The alignment of these two slots should be identical in the returned chassis.

Installing the replacement chassis

About this task

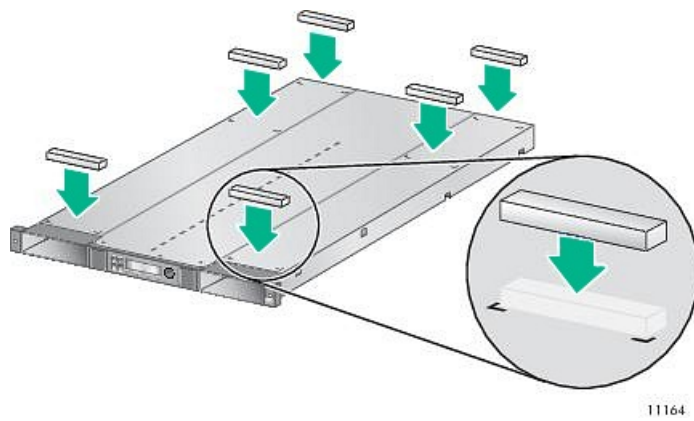


CAUTION

Lift the autoloader from the side edges. Lifting the autoloader from the magazine or tape drive openings can damage the autoloader.

Procedure

1. If the autoloader is not installed in a rack and sits directly on a flat surface, attach the feet. If the autoloader is installed in a rack, skip this step.
 - a. Locate the six support feet that were shipped with the chassis.
 - b. With another person, gently turn the chassis over and set it on its back.
 - c. Locate the six inscribed foot location lines.
 - d. Peel the backing paper off each foot and apply it within a set of foot location lines.

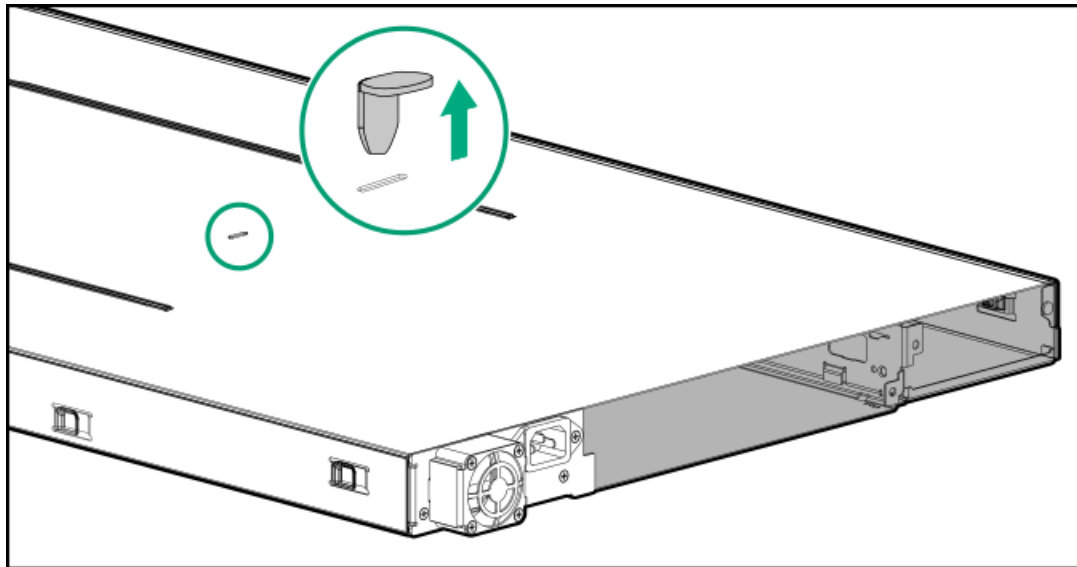


11164

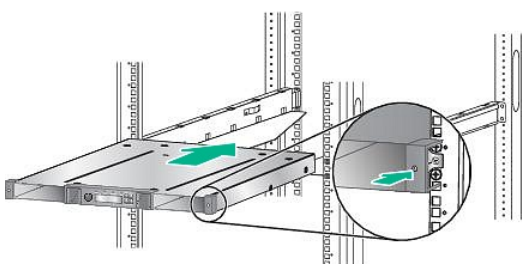
- e. With another person, gently turn the chassis over and set it on its feet.
2. From the new (replacement) chassis, remove and save the shipping lock.

The shipping lock prevents the robotic transport mechanism from moving during shipment. The shipping lock must be removed before powering on the autoloader. The shipping lock is held in place with a piece of tape and is located in the top center of the new (replacement) chassis.

- a. Locate the tape and lock at the top of the chassis.



- b. Remove the tape, then remove the lock. Set the removed lock aside so it can be used to stabilize the robotic transport mechanism in the original chassis (the chassis that will be returned).
3. Mount the autoloader in a rack if it does not have the rubber support feet attached. If the rubber support feet are attached, skip this step.
 - a. With assistance, slide the autoloader onto the metal rails that are already in position in the rack.
 - b. From the front of the autoloader, secure the front bezel to the rack using a #2 Phillips screw driver placed through the small holes in the mounting bracket to tighten the captive screws on each side of the autoloader.



11157

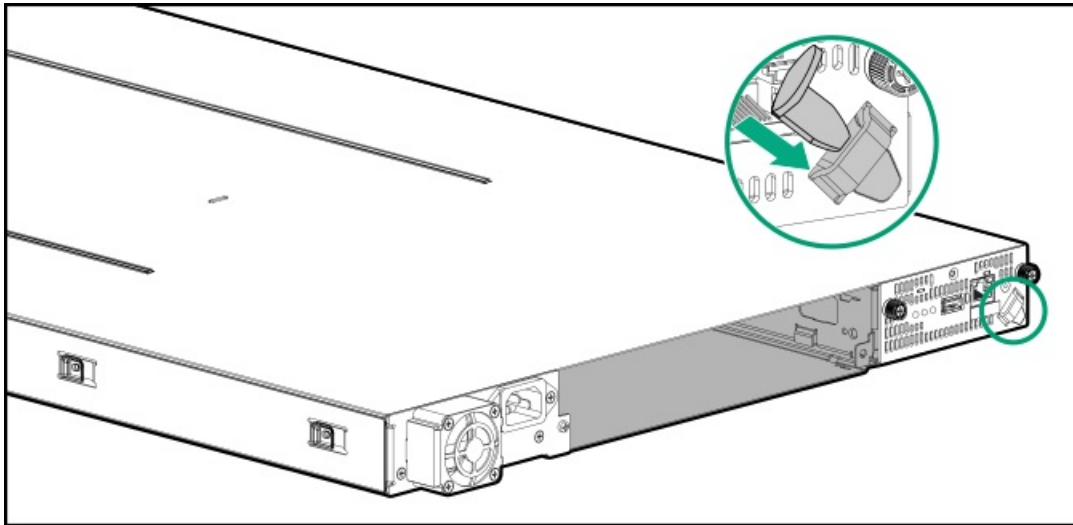
Replacing the autoloader components and cables

About this task

Replace the autoloader 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 magazines.
2. Replace the controller. If a lock is stored on the back panel of the old chassis (the chassis that was removed), move the lock to the replacement chassis and store it in the location shown.



3. Replace the tape drive.

To secure the tape drive to the chassis, tighten the drive sled mounting screws (the blue captive thumbscrews). You can use either a #2 Phillips screwdriver or a torque driver.

- If using a screwdriver, tighten the thumbscrews until a low initial threshold torque achieves a snug tight condition. Do not overtighten.
- If using a torque driver, tighten to a recommended torque of 6 inch pounds or 0.68 N m.
- If the thumbscrews cannot be tightened, verify that the tape drive is aligned properly.



IMPORTANT

Under certain conditions of external shock and vibration, it has been noted that if the thumbscrews are not tightened, drive performance issues might occur. In that situation, please tighten the thumbscrews to the recommended torque.

4. Reattach any SAS, FC, and Ethernet cables removed earlier.
5. Reinsert the USB device if you removed it earlier.
6. Reattach the power cord.

Verifying the chassis replacement

About this task

This topic describes the steps to verify the status and configuration of the autoloader after chassis replacement.

Another aspect of replacement is the serial number, which is stored electronically in the chassis and in the controller and physically on the chassis pull-out tab. The replacement chassis will have a different serial number from the original chassis. However, when the existing controller is placed in the new chassis and the chassis is powered on, the controller updates the serial number electronically in the chassis. Electronically, the serial number matches the original serial number and all library data, support tickets, warranty data, and any licenses tied to the original serial number remain valid. Be aware that because the serial number on the chassis pull-out tab is physically printed, it will **not** match the electronic serial number. The mismatch does not affect ongoing service. HPE retains records of replacements and the autoloader will continue to be identified by the electronic serial number.

Procedure

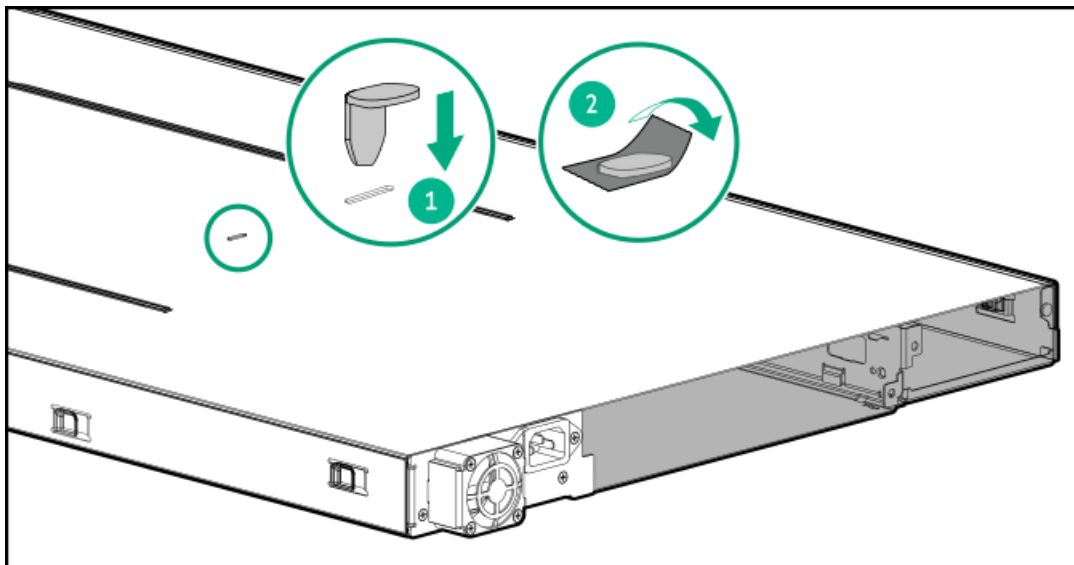
1. Power on the autoloader.
2. Check the overall autoloader status from the RMI. Navigate to **Status > Autoloader**.
3. Verify that the configuration settings are correct. If necessary [restore the settings from a file](#), or saved settings, or re-enter them using the RMI or OCP.
 - a. If the autoloader has licensed features, verify that the license information was retained and then re-enable the feature.
 - 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.
4. If using the MSL Encryption Kit, re-enter the token password. Using the RMI confirms that the administrator user can access the autoloader.
5. Resume host applications.

Replacing the shipping lock on the old chassis

Procedure

1. Locate the shipping lock that was set aside from the replacement chassis.
2. Place the shipping lock in the shipping position on top of the old chassis (callout 1).
3. Tape the shipping lock to the chassis to keep it in place during shipping (callout 2).

Results



Repackaging the old chassis

Procedure

1. Place the box from the replacement chassis on a sturdy surface. Slide the bottom foam piece into the box.



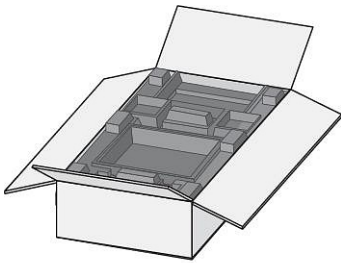
2. If a thin layer of protective foam was included in the replacement shipment, rewrap the chassis in the foam to prevent cosmetic damage. Lower the chassis in the box.



3. Place the top piece of foam on top of the chassis.



4. The top piece of foam should be level with the top of the box.



11699

Installation and replacement of the autoloader rack kit

- When installing a new HPE Storage 1/8 G3 Tape Autoloader, start with **Removing and storing the shipping lock**.
- When replacing the rack rails on a tape autoloader that might contain tape cartridges or has support feet attached, it is a best practice to allow the backup application to complete and return the tape cartridges to the storage slots. After the backup application has completed, start with **Removing the cartridges from tape drives**.

You will need the following for this procedure:

- #2 and a #3 Phillips screwdriver for this procedure.
- Alcohol wipe or soft cloth and isopropyl alcohol if the autoloader currently has support feet attached.



WARNING

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

- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- In multiple-rack installations, secure the racks together.
- Extend only one rack component at a time. Racks may become unstable if more than one component is extended.



WARNING

The autoloader weighs 12 kg (26.45 lb) without media and 13.6 kg (29.98 lb) with media (8 cartridges). When moving the autoloader, to reduce the risk of personal injury or damage to the autoloader,

- Observe local health and safety requirements and guidelines for manual material handling.
- Always remove all tapes to reduce the overall weight of the autoloader and to avoid internal damage to the autoloader.
- Obtain adequate assistance to lift and stabilize the autoloader during installation or removal.

Subtopics

[Removing the cartridges from tape drives](#)

[Removing the cartridges from the magazines using the OCP](#)

[Removing the cartridges from the magazines using the RMI](#)

[Removing the cartridges from the magazines using the manual release](#)

[Removing the autoloader feet](#)

[Powering off the library](#)

[Removing the library](#)

[Removing the old rails](#)

[Removing and storing the shipping lock](#)

[Securing the rails to the rack](#)

[Installing the library](#)

Removing the cartridges from tape drives

About this task

If tape cartridges are installed in the library, do the following to avoid damaging the tape cartridge or tape drive during the procedure.

Procedure

1. Using the remote management interface (RMI), navigate to the **Operations > Move Media** screen to move tape cartridges from the tape drives to storage slots or mailslots.
2. Proceed to remove all tape cartridges from the library using the remote management interface (RMI) or the OCP.

Removing the cartridges from the magazines using the OCP

About this task



IMPORTANT

When possible, unlock the magazines using the OCP or RMI. However, if the OCP or RMI process fails or a magazine needs to be removed when the power is off, you can release the magazines manually. See [Removing the cartridges from the magazines using the manual release](#).

Procedure

1. Log in to the Operator Control Panel (OCP) as Administrator:
 - a. Press any key.

- b. Select User: "ADMINISTRATOR", and press Enter.
 - c. Enter the PIN using the Previous, Next, and Enter buttons.
2. Click Next until the screen displays **Operation**.
 - a. Press Enter.
 - b. Press Next to display **Magazine Unlock Right** or **Magazine Unlock Left**.
 - c. Press Enter to release the desired magazine.

The screen displays **Magazine Unlocked for 30s**.

3. Pull the unlocked magazine out of the library.
4. Remove the tape cartridges from the magazine, noting their locations so each can be replaced in the proper slot.
5. When the screen displays **Magazine Removed**, slide the magazine completely into the library.

The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

6. Repeat this procedure to remove the tape cartridges from the other magazine.



IMPORTANT

When removing a magazine using the OCP, once a magazine is removed, the robot cannot perform any other operation. The removed magazine must be reinserted to allow removal of the other magazine.

Removing the cartridges from the magazines using the RMI

About this task



IMPORTANT

When possible, unlock the magazines using the OCP or RMI. However, if the OCP or RMI process fails or a magazine needs to be removed when the power is off, you can release the magazines manually.

Procedure

1. Navigate to **Operation > Open Magazine**.
2. Use the Open button to release each magazine.

When a magazine is unlocked, the OCP displays **Magazine unlocked**.
3. Pull the unlocked magazine out of the library.
4. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot.
5. When the OCP screen displays **Magazine Removed**, slide the magazine completely into the library.



IMPORTANT

When removing a magazine using the RMI, once a magazine is removed, the robot cannot perform any other operation. The removed magazine must be reinserted to allow removal of the other magazine.

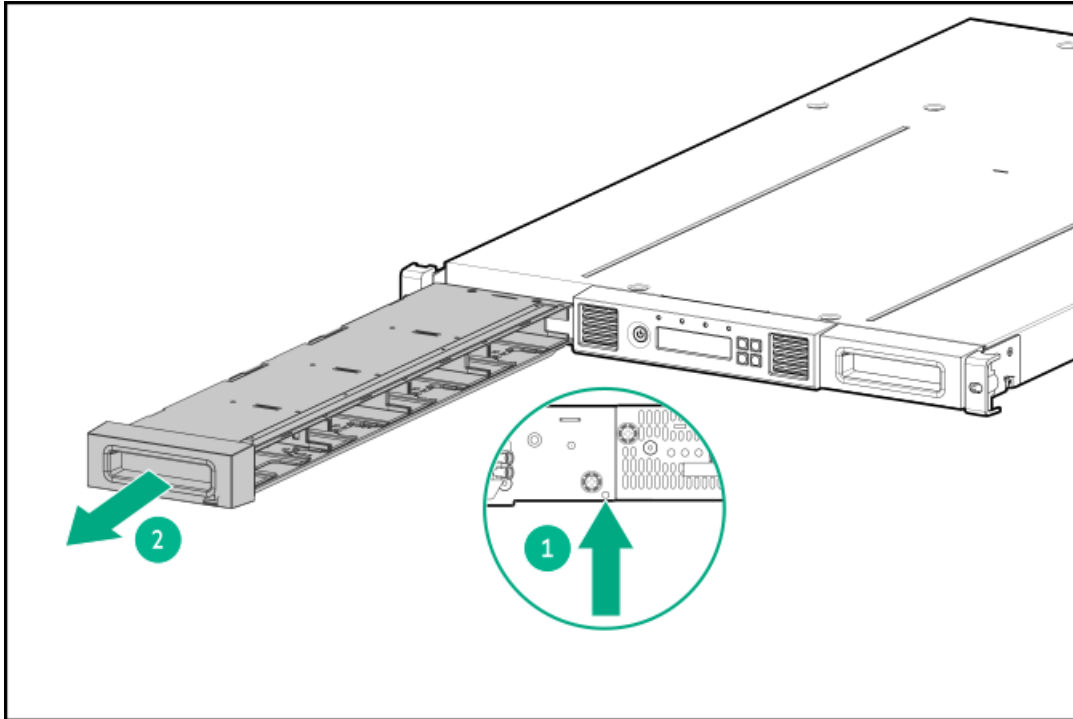
The magazine locks into place once it is correctly installed and then the library inventories the magazine. The Ready LED blinks while the library inventories the magazine and then stops when the operation is complete.

6. Repeat this procedure to remove the tape cartridges from the other magazine.

Removing the cartridges from the magazines using the manual release

Procedure

1. Insert a small metal pin or straightened paper clip about 1.5 cm (0.6 inch) into one of the release holes on the back of the library, while another person grasps the magazines from the released side and removes them from the library.



IMPORTANT

Do not force the pin once you encounter resistance. Doing so can damage the library.

2. Remove the tape cartridges from the magazine, noting the locations so each can be replaced in the proper slot, then reinsert the magazines into the library. The magazines will lock into place once it is correctly installed.
3. Repeat this step to remove the magazines from the other side.

Removing the autoloader feet

About this task

Skip this step if the autoloader does not have support feet.

The feet must be removed for correct robotic operation in a rack and to allow the autoloader to be securely installed in the rack within its 1U rack volume.

Procedure

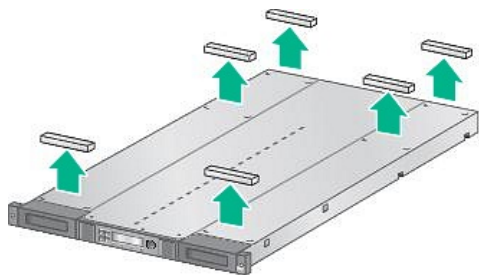
1. Disconnect any cords or cables attached to the autoloader.
2. Remove the shipping lock from its storage location on the back panel.

3. Gently turn the autoloader over and set it on its top on a clean smooth surface.
4. Peel off the support feet.



TIP

If a foot is difficult to remove, loosen it by gently pushing on a corner, and then gradually rolling the foot off the surface.



11300

5. Remove any adhesive residue using an alcohol wipe or soft cloth lightly moistened with isopropyl alcohol. Do not let alcohol seep into the autoloader.
6. Gently turn the autoloader right side up.
7. Return the shipping lock to its storage location on the back panel.

Powering off the library

Procedure

1. From the front panel, press and hold the power button for five seconds.
2. Detach the power cords and all other cables from the back of the library.

Removing the library

About this task



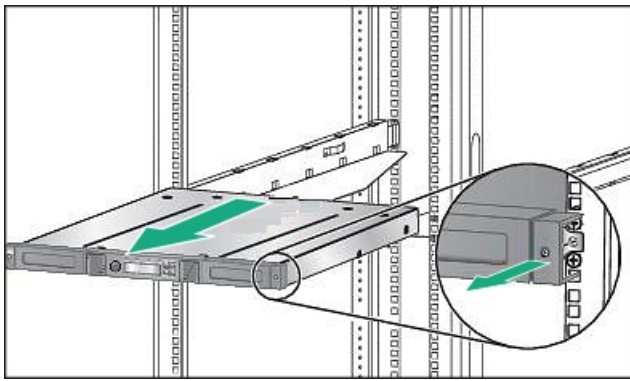
CAUTION

When lifting the library, hold it under its side edges. Lifting it from the drive or magazine openings can damage the chassis and cause errors.

Procedure

1. With a #2 Phillips screwdriver, loosen the captive screws on the front bezel. The autoloader has one screw on each side.





2. With assistance, slide the library out of the rack.

Removing the old rails

With a #3 Phillips screwdriver, remove the screws holding the rails to the rack.

Removing and storing the shipping lock

About this task



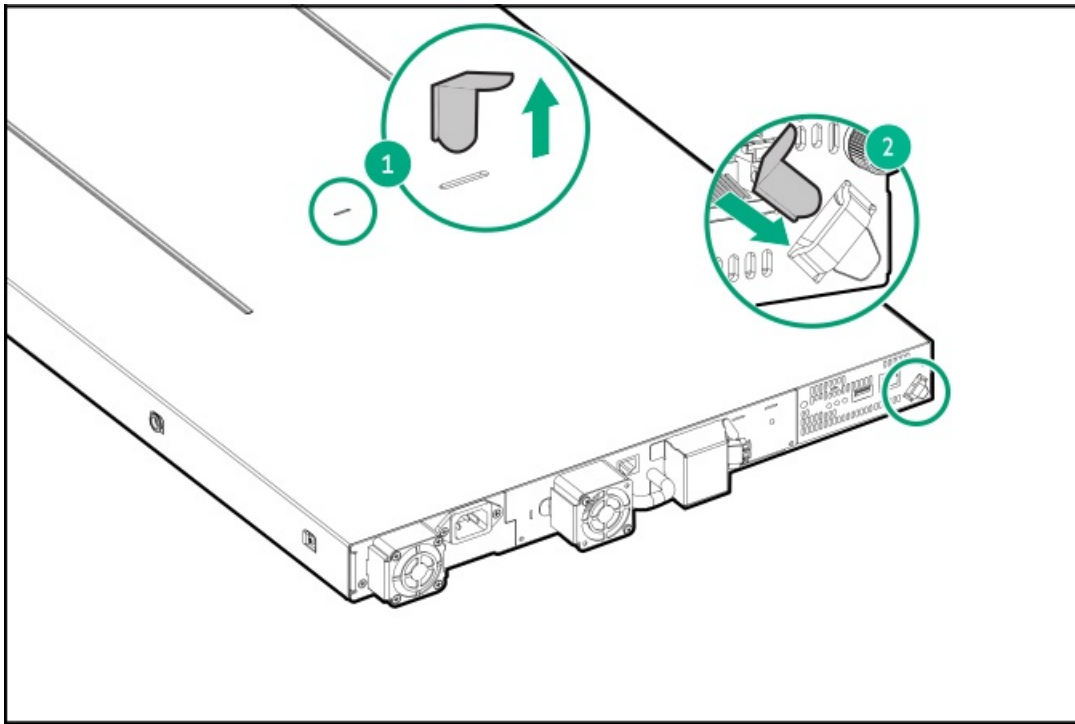
NOTE

The shipping lock is normally removed when the autoloader is first unpacked. If this is not an initial installation, the shipping lock might have already been removed and stored.

Procedure

1. Locate the tape holding the shipping lock at the top of the autoloader. Remove the tape.
2. Remove the lock.
3. Store the lock in the pocket on the back panel.

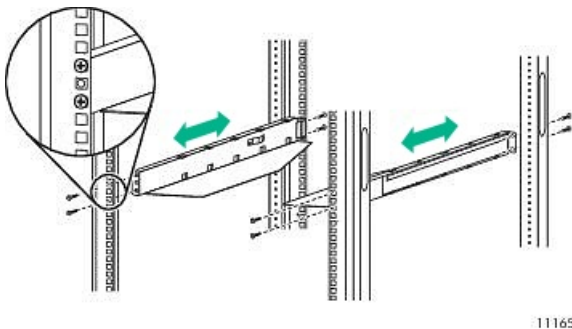
Results



Securing the rails to the rack

Procedure

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



11165

2. Extend the rail and then use two screws to secure the other end of the rail to the rear rack column.
3. Repeat steps 1 and 2 to secure the other rail.

Installing the library

About this task

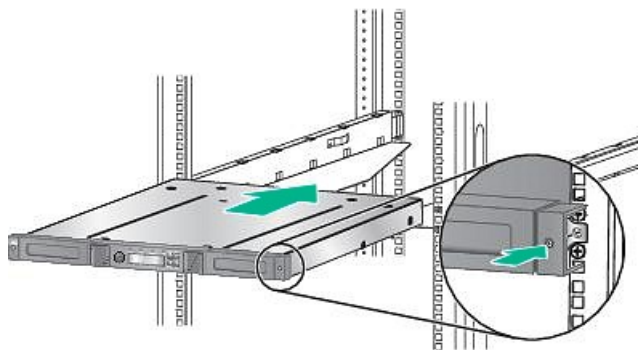


CAUTION

When lifting the library, hold it under its side edges. Lifting it from the drive or magazine openings can damage the chassis and cause errors.

Procedure

- 1. Slide the library onto the rails.
- 2. From the front of the library, secure the front bezel to the rack using a #2 Phillips screw driver placed through the small holes in the mounting bracket. Tighten the captive screws on each side of the library until seated.



- 3. Load the cartridges into the magazines if necessary.
- 4. Slide the magazines into the library if necessary.
- 5. Attach or reattach the cables.
- 6. Power on the library.

Technical specifications

Autoloader capacity

Characteristic	Value
Form factor	1U
Maximum cartridge slots	8
Mailslots	0, 1
Maximum tape drives	1

Supported interfaces

LTO generation	Interface
LTO-6, LTO-7, LTO-8, LTO-9	Fibre Channel, SAS

Subtopics

- [Physical specifications](#)
- [Environmental specifications](#)
- [Electrical specifications](#)
- [Regulatory specifications](#)
- [Regulatory compliance identification numbers](#)

Physical specifications



Characteristics	Product alone (without media) Packaged (Shipped)	
Height	44 mm (1.73 inches)	250 mm (9.84 inches)
Width	482 mm (18.98 inches)	580 mm (22.83 inches)
Depth	809 mm (31.85 inches)	990 mm (38.98 inches)
Weight	12 kg (26.45 pounds)	13.6 kg (29.98 pounds)

Environmental specifications

Characteristic	Specification		
	LTO-9	LTO-7 and LTO-8	LTO-6
Temperature			
Operating (Recommended)	15°C to 25°C	20°C to 25°C	
Operating (Allowable)	15°C to 32°C. Derate 1°C/ 300m above 900m.	10°C to 35°C up to 3000m and 10°C to 30°C above 3000m and up to 4000m.	10° to 35°C
Non-operating	-30° to 60° C	-30° to 60° C	-30° to 60° C
Maximum rate of change	5° C per hour	10° C per hour	10° C per hour
Humidity			
Operating (Recommended)	20% to 50% RH (non-condensing)	20% to 50% RH (non-condensing)	
Operating (Allowable)	20% to 80% RH (non-condensing, 22°C dew point maximum)	20% to 80% RH (non-condensing, max wet bulb temperature = 26°C)	20% to 80% RH (non-condensing, max wet bulb temperature = 26°C)
Non-operating	10% to 90% RH (non-condensing)	10% to 90% RH (non-condensing)	10% to 95% RH (non-condensing)
Miscellaneous			
Altitude	3048 meters	4000 meters (see Operating temperatures)	4000 meters
Dust concentration	ISO 14644-1 Class 8	ISO 14644 -1 Class 8	Less than 200 microgram / cubic meter

Electrical specifications

Power —80 Watts (max)

Input Requirements— 100 - 240V AC, 1100 - 550mA, 50/60Hz

USB port—USB 2.0

Ethernet port—10BASE-T_e, 100BASE-TX, 1000BASE-T are supported

Regulatory specifications

Product safety test conditions

Characteristic	Tested condition or value
Equipment mobility	Stationary (rack-mount or desk-top)
Connection to the mains	Pluggable — Type A
Operating condition	Continuous
Access location	Operator accessible
Over voltage category (OVC)	OVC II
Mains supply tolerance (%) or absolute mains supply values	-10%, +10%
Tested for IT power systems	No
IT testing, phase-phase voltage (V)	N/A
Class of equipment	Class I
Considered current rating (A)	20 A (branch circuit protection)
Pollution degree (PD)	PD 2
IP protection class	IPX0
Altitude during operation (m)	Max 5000
Altitude of test laboratory (m)	38
Mass of equipment (kg)	Max 25 kg
Manufacturer's Declared Ambient (°C)	40 °C



NOTE

The product safety test conditions might differ from the product specification limits.

Regulatory compliance identification numbers

For the purpose of regulatory compliance certifications and identification, each product is assigned a unique regulatory model number. The regulatory model number can be found on the product nameplate label, along with all required approval markings and information. When requesting compliance information for the product, always see this regulatory model number. The regulatory model number is not the marketing name or model number of the product.

The Regulatory Compliance label is on the bottom of the autoloader. To view this information from the back of the autoloader, tilt the autoloader up until the label is visible.

Product-specific information:

Regulatory model number: LVLDC-0501, Type: 1U

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>

Electrostatic discharge

To prevent damaging the system, be aware of and follow precautions when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

Subtopics

[Preventing electrostatic damage](#)

[Grounding methods](#)

Preventing electrostatic damage

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly. See the next section.

Grounding methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm (± 10 percent) resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have your authorized reseller install the part.



NOTE

For more information on static electricity, or assistance with product installation, contact your authorized reseller.

Websites



General websites

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

<https://www.hpe.com/storage/spock>

Technical papers and analyst reports

<https://www.hpe.com/us/en/resource-library>

For additional websites, see [Support and other resources](#).

Subtopics

[Accessing the compatibility matrix](#)

[HPE Storage autoloader websites](#)

Accessing the compatibility matrix

Procedure

1. Go to <https://www.hpe.com/Storage/TapeCompatibilityMatrix>.
2. On the Welcome to SPOCK page, click Sign in/Register.
3. Log in with your existing HPE account or create an account.
4. From the SPOCK home page, expand the plus sign (+) next to Explore HPE Storage Tape Solutions.
5. Click HPE Storage Tape Solutions Documents, and then select the compatibility matrix.

HPE Storage autoloader websites

For more information on Storage products, see <https://www.hpe.com/storage/msl>.

For product information about Command View for Tape Libraries, see <https://www.hpe.com/storage/cvttl>.

To download Command View for Tape Libraries, see <https://www.hpe.com/support/cvttl>.

For more information about TapeAssure Advanced, see <https://www.hpe.com/storage/tapeassure>.

For more information about Data Verification, see <https://www.hpe.com/storage/dataverification>.

Download HPE Library & Tape Tools without charge from <https://www.hpe.com/support/TapeTools>.

Support and other resources

Subtopics

[Accessing Hewlett Packard Enterprise Support](#)

[HPE product registration](#)

[Accessing updates](#)

[Remote support](#)

[Warranty information](#)

[Regulatory information](#)

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

<https://www.hpe.com/info/assistance>

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

<https://www.hpe.com/support/hpesc>

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see <https://www.hpe.com/info/add-products-contracts>.

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

Hewlett Packard Enterprise Support Center

<https://www.hpe.com/support/hpesc>

My HPE Software Center

<https://www.hpe.com/software/hpesoftwarecenter>

- To subscribe to eNewsletters and alerts:

<https://www.hpe.com/support/e-updates>

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the [Hewlett Packard Enterprise Support Center More Information on Access to Support Materials](#) page:

<https://www.hpe.com/support/AccessToSupportMaterials>



IMPORTANT

Access to some updates might require product entitlement when accessed through the [Hewlett Packard Enterprise Support Center](#). You must have an [HPE Account](#) set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

<https://www.hpe.com/services/getconnected>

HPE Tech Care Service

<https://www.hpe.com/services/techcare>

HPE Complete Care Service

<https://www.hpe.com/services/completecure>

Warranty information

To view the warranty information for your product, see the [warranty check tool](#).

Regulatory information

To view the regulatory information for your product, view the [Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products](#), available at the Hewlett Packard Enterprise Support Center:

<https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

<https://www.hpe.com/info/reach>

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

<https://www.hpe.com/info/ecodata>

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

<https://www.hpe.com/info/environment>

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (<https://www.hpe.com/support/hpesc>) to send any errors, suggestions, or comments. This process captures all document information.

