Technical brief

Securing HPE Storage Tape Libraries with Multifactor Authentication

Contents

Introduction

As ransomware attacks continue to escalate, improving security has become a top priority for businesses of all sizes. Reducing this risk depends on establishing reliable safeguards for sensitive information.

HPE Storage Tape provides a cost-effective and highly secure medium for offline data storage. Layered authentication makes it more difficult for malicious actors to infiltrate the library.

Tape offers an extra layer of security because access requires specialized knowledge and data can only be written sequentially, reducing the risk of misuse or tampering. Cartridges stored in library slots offer some protection, but advanced threats can still exploit backup software commands to load, overwrite, erase, or encrypt media.

Multifactor Authentication (MFA) provides a powerful solution—enabling organizations to enforce strict identity verification before any operations can be executed.

This brief explains how HPE MFA enforces identity verification at multiple layers, ensuring only authorized users can access or modify data in the library, reducing the risk of human error while maintaining secure, controlled operations.

Presenting Multifactor Authentication (MFA) for HPE Storage Tape

MFA creates an additional layer of security by requiring **all** of the following:

— Knowledge of the password.
— Possession of a physical device.
— Registration with an approved authenticator app.

By requiring multiple factors, MFA prevents unauthorized access even if one factor, such as a password, is compromised.

In HPE tape library environments, MFA is applied across three distinct layers—Remote Management Interface, Command View for Tape Libraries (CVTL), and applications (ISV) - each reinforcing the security posture and providing complementary controls to protect offline data from misuse or malicious manipulation.

Remote Management Interface (RMI)

The RMI operates at the firmware level and manages the internal control of the library, including firmware updates, configuration changes, partition management, and hardware health monitoring. By embedding MFA directly within RMI, HPE ensures that only Security administrators can perform high-risk operations.

At this level, RMI protects the device from both accidental misconfiguration and deliberate cyberattacks.

HPE MFA is supported beginning with the following library firmware versions introduced in 2025.

— Autoloader: Version 1000 or later.
— MSL2024.
— MSL3040: Version 3370 or later.
— MSL6480: Version 6.70 or later.
— CVTL: Version 6.6 or later.

The new feature is included at no additional cost with any new tape library. Existing customers can upgrade the MSL3040 and MSL6480 firmware to the versions listed above, or later versions, providing the library is still under warranty or is covered by a service package. The MSL Autoloader and MSL2024 are not field upgradeable.

Command View for Tape Libraries (CVTL)

While RMI enforces access at the device level, CVTL provides an optional, centralized management plane for administrators across multiple libraries. By embedding MFA within CVTL, HPE ensures centralized enforcement of MFA policies, ensuring consistent application of identity verification across an entire library environment.

— CVTL enhances security without interrupting day-to-day library operations.
— HPE MFA for CVTL is supported beginning with Version 6.6 or later.

Application-Level Protection: ISV Software Integration

Independent Software Vendor (ISV) applications—such as backup, archival, and data management software operate independently. While HPE provides secure RMI and CVTL controls, ISVs are independently managed and responsible for their own authentication measures, including MFA, to verify users or systems initiating operations.

How Multifactor Authentication works

Legacy login authentication typically relies on a single factor, such as a password, which can be compromised through phishing, credential theft, or weak password practices. This leaves tape libraries vulnerable to unauthorized access and potential data misuse.

How MFA enhances tape library security

Passwords alone aren't enough to protect today's critical data. MFA adds an extra layer of defense, ensuring that only verified users and systems can access or modify tape library resources. By requiring multiple verification factors, MFA stops unauthorized access and strengthens operational security.

Prevents unauthorized access

MFA requires multiple verification steps before granting access, making it significantly harder for attackers to compromise accounts and execute privileged operations, even if a password is stolen or guessed.

Protects critical operations

By enforcing MFA across firmware (RMI), management (CVTL), and application (ISV) layers, organizations ensure that sensitive tasks—like configuration changes, media movement, or encryption key handling—can only be performed by verified identities.

Enhances compliance and auditability

MFA provides detailed authentication logs that can be integrated into enterprise audit frameworks, supporting regulatory compliance and providing visibility into all access attempts.

Multifactor authentication in action

MFA ensures that only verified users and systems can access tape library resources or perform privileged operations. In HPE environments, MFA operates across three layers—firmware (RMI), management (CVTL), and presumably workflow applications (ISV)—creating a layered approach.

1. Using any authenticator app on their mobile device, the user scans the QR code.
2. Mobile app generates a one-time passcode.
3. Using the one-time passcode generated with their username and password.
4. After user information is verified, access is granted.

For detailed instructions go to:

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

MSL2024: HPE Storage Tape MSL2024 Library User and Service Guide

MSL3040: HPE Storage Tape MSL3040 Library User and Service Guide

MSL6480: HPE Storage Tape MSL6480 Tape Library User and Service Guide

Configuration and operation

This section briefly describes how to set up and use MFA. It is intended only as an overview.

Remote management interface (RMI)

1. The user opens any authenticator app on their mobile device and scans the QR Code generated by the MSL library.

2. Enable MFA and define policy
    a. Turn on MFA in the RMI settings.
    b. Choose the scope:
    c. Apply to all privileged roles, or
    d. Apply to specific roles only.
    e. Set session timeout durations.
    f. Define step-up authentication thresholds for high-risk actions (e.g., firmware updates, partition changes).

3. Enroll authenticators
    a. Register admin tokens or configure Time-based One-Time Passwords (TOTP).
    b. Generate a QR code for TOTP enrollment.
    c. Scan the QR code using an authenticator app.
    d. Validate clock synchronization to ensure TOTP accuracy.

4. Test device actions
    a. Log out and reauthenticate using the test admin account.
    b. Perform a privileged action (e.g., view firmware version or change partition).
    c. Confirm that MFA prompts appear and function correctly.

Benefits of MFA

— Secure (air-gapped) data storage for nearline data cartridges.
— Eliminates the need to manually handle media to move offline.
— Invisible to backup orchestration and archive applications.
— Enables secure offline vaulting for remote lights out environments.
— Reduces the need to expose media to the risk of physical damage or loss during transportation.
— Prevents accidental exposure of media to connected hosts.
— Reduces operator workload and physical overhead.

Conclusion

HPE Storage LTO Ultrium tape technology provides the ultimate last line of defense against ransomware, enabling offline data protection with remote copies of your critical information. Now, with HPE Storage MSL Vault Partition, you can maintain offline data protection for media without ever removing it from the library.

With policy-driven "vaulting," cartridges are automatically moved into an isolated partition inaccessible to applications and the network, which helps reduce human error and eliminates the need for physical media handling—even in unattended data centers. When a restore is needed, an administrator simply returns the tapes to the application partition via the RMI, while built-in safeguards, such as role-based access, MFA, encryption, and WORM media, help prevent tampering.

The optional Data Verification feature in HPE CVTL can be configured to check the health of the media, ensuring that your last-resort copy can be read when it matters. The result is clear: lower cost per TB, less operational overhead, and a resilient, air-gapped layer that keeps your business running and your customers protected, regardless of unforeseen threats.

Learn more at

hpe.com/storage/tape

Visit HPE.com

Chat now

a00155689enw

HEWLETT PACKARD ENTERPRISE

hpe.com