



Protect data with HPE Storage MSL Vault Partition in MSL3040 & MSL6480 Tape Libraries



Contents

Introduction..... 3

Presenting HPE Storage MSL Vault Partition..... 3

How HPE Storage MSL Vault Partition works..... 4

HPE Storage MSL Vault Partition security 4

HPE Storage MSL Vault Partition in action 4

Configuration and operation 6

Benefits 6

Conclusion 7

Introduction

Ransomware remains a persistent, large-scale threat impacting organizations of every size. To mitigate this risk, there must be clear safeguards for data protection.

HPE Storage Tape MSL Vault Partition provides a cost-effective and highly secure medium for offline data storage. The more isolated the media, the harder it is to attack remotely.

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 good protection, but very advanced threats could exploit backup software commands to load, overwrite, erase, or encrypt media.

The strongest countermeasure is to maintain an offline, fully isolated 'air-gapped' copy. The question is: how can organizations achieve this level of protection when media remains inside the library rather than being physically removed?

Presenting HPE Storage MSL Vault Partition

HPE Storage MSL3040 & MSL6480 Tape Libraries include the ability to create isolated partitions called **MSL Vault Partition**, which are designed to maximize the separation of media that remains operational within the tape library. Media stored in this partition is hidden from applications and cannot be accessed by connected hosts. To access the cartridges, a Security level user with multi-factor authentication (MFA) enabled must explicitly transfer them back into an application partition using the Remote Management Interface (RMI). For an attacker to tamper with tapes in the MSL Vault Partition, they would require extensive knowledge of the environment and need to compromise a Security account using MFA. Enforcing MFA, a standard feature of HPE Storage MSL Tape Library systems with Security level user access, greatly reduces the likelihood of such a scenario.

HPE Storage MSL Vault Partition is supported beginning with the following library firmware versions introduced in 2025.

MSL3040: Version 3370

MSL6480: Version 6.70

The new feature is included at no additional cost with any new MSL3040 or MSL6480 Tape Library. Existing customers can upgrade the library FW to the versions listed above, or later versions, provided the library is still under warranty or is covered by a service package.

This brief explains how the HPE Storage MSL Vault Partition - a built-in feature of the HPE Storage MSL3040 & MSL6480 Tape Libraries - facilitates a secure, air-gapped copy of data that remains in the library, minimizing human error.

How HPE Storage MSL Vault Partitions work

Tape library partitions were designed for multiple applications to share a single physical library. In these application-managed partitions, each application typically has its own dedicated tape drive(s), slots, cartridges, and I/O slots, while sharing the robotics.

The **MSL Vault Partition** creates a secure storage area inside the library that is not assigned to any drive and is completely invisible to applications, making them unaware of its existence and therefore, unable to access it, not even inadvertently. MSL Vault Partitions are configured by administrators with security-level privileges via the RMI, without tape drives assigned to the partition, and are entirely independent of the backup application. The partition can be sized to meet organizational requirements.

HPE Storage MSL Vault Partition security

HPE Storage MSL Vault Partition improves security from various perspectives:

- MSL Vault Partitions cannot be accessed by applications; library management tools enforce this, preventing IT staff from accidentally bringing vaulted media online.
- MSL Vault Partitions contain no tape drives, adding another layer of separation and security by ensuring that cartridges in this partition cannot be loaded into a tape drive.
- Because vaulted cartridges remain inside the library, they are safeguarded from accidental damage or loss.

Administrative controls further enhance configuration security. Only library administrators with Security level access and MFA access enabled can create, modify, delete, or reconfigure Vault Partitions. Standard IT operators have limited privileges. For improved security and authorization controls, HPE Storage MSL tape libraries can integrate with Microsoft Active Directory or other LDAP directory services.

For maximum data protection, HPE Storage MSL Vault Partition technology works in conjunction with standard HPE Storage MSL security features such as tape encryption (via the HPE Storage MSL Encryption Kit or KMIP-supported encryption solution), WORM media, and media security notifications via HPE Command View for Tape Libraries (CVTL) software.

HPE Storage MSL Vault Partition in action

Tapes can be transferred into an MSL Vault Partition either manually through the library management interface or automatically based on policy-driven rules. A typical scenario involves sending any tape exported from a specific application's partition directly into a designated MSL Vault Partition instead of to the I/O slots. The application assumes the media has been physically removed from the tape library, but in fact, the cartridges have been moved into the secure Vault Partition, making them invisible to the rest of the system.

Note:

When multiple applications share the library, each application can have its own Vault Partition.

For detailed instructions go to [Partition Wizards | HPE Storage MSL3040 Tape Library User and Service Guide](#)

Saving time and reducing risk—Off-site Tape Storage vs. On-site Tape Storage with HPE Storage MSL Vault Partition

Off-site vault storage:

- The operator sends a command to export tapes using the application.
- The operator removes tapes from the library's I/O slots.
- The operator transports cartridges to secure storage.

On-site vault storage with HPE Storage MSL Vault Partition:

- The operator sends a command to export tapes using the application.
- A policy-based rule is followed, and the robot automatically transfers tapes into the secure MSL Vault Partition.

The MSL Vault Partition requires no extra steps or operator intervention. IT teams can securely replicate cartridge removal without physically handling media - even when the library is located in a remote, fully automated 'lights-out' data center with no on-site staff. Note: MSL Vault Partition may offer additional protection from a ransomware attack, it will not protect against a data center disaster such as flooding or fire.

Off-site vault retrieval for access:

- The operator recovers tape cartridges from secure storage.
- The operator inserts cartridges into the library's I/O slots.
- The operator imports media using the designated application.

On-site vault retrieval for access with HPE Storage MSL Vault Partition:

- Operators with Security level access and MFA-enabled use the RMI to move tapes from the MSL Vault Partition back to the application vault partition.
- The robot relocates the media, and the application is notified when data is available for access.

HPE Storage MSL Vault Partition and HPE CVTL Data Verification

The most reliable way to confirm that offline data remains readable is to test it. But cartridges that are manually vaulted and left on a shelf are rarely tested - it's simply too cumbersome.

Monitor the health of your media automatically

To address this, HPE offers a licensed feature within HPE Command View for Tape (CVTL) Libraries called Data Verification. Data Verification works by utilizing tape library hardware and CVTL to carry out a background read operation on infrequently accessed tapes, verifying data integrity and media health without disrupting host applications or backup operations.

For CVTL Data Verification to work, tapes must first be moved from an MSL Vault Partition back into an application partition.

Configuration and operation

This section briefly describes how to set up and use HPE Storage MSL Vault Partitions. It is intended only as an overview. For further details, refer to the user guide for [MSL3040 User and Service Guide](#) and [MSL6480 User and Service Guide](#).

Logical partitioning and library control

HPE Storage MSL Vault Partitions are created by designating a range of slots within the physical library. A configuration wizard is available in the library RMI to configure an MSL Vault Partition. Slots are assigned in groups of 5 to the MSL Vault Partition, and “Auto Move to Vault Partition” can be enabled. Any partition can be edited in the future to add or remove slots, including MSL Vault Partitions. Changing the size of a partition may require reconfiguration of the ISV to properly identify the new setup.

Cartridges in the MSL Vault Partition are not visible to the ISV. If ISVs report “destination element full” errors when attempting to export tapes, it may be due to the MSL Vault Partition being full when “Auto Move to Vault Partition” is enabled. Check the library RMI for Vault Full errors, and remove tapes from the Vault or increase its size.

The RMI will also issue a warning when the vault is nearly full. A cartridge can only be retrieved by an administrator with Security level access and MFA configured, logged into the RMI.

ISV policy integration

Most ISVs can be configured to “export” media if the library has configured import/export slots (mailslots). When a MSL Vault Partition is created/edited, you can configure “Auto Move to Vault Partition” for mailslots assigned to a specific user MSL Vault Partition. If this is enabled, any tape that the application “exports” to the mailslot (expecting a user to open the mailslot and remove the media) is automatically moved into the MSL Vault Partition if an empty slot is available there.

Tapes moved into the MSL Vault Partition are segregated from ISV-controlled partitions, making them invisible to the ISV. Because tapes are invisible to the ISV, it cannot export media.

Benefits of the HPE Storage MSL Vault Partition

- 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 MSL Tape Libraries provide the ultimate last line of defense against ransomware, enabling offline data protection with remote copies of your critical information. Now, with HPE Storage Tape 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 MSL Vault 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 CVTL can be configured to check the media’s health, ensuring 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](https://hpe.com)

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Active Directory and Microsoft 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.

a00155511enw

HEWLETT PACKARD ENTERPRISE

hpe.com

