WHITE PAPER

The Quantum Scalar Security Framework:

A Technical White Paper

CONTENTS

Introduction

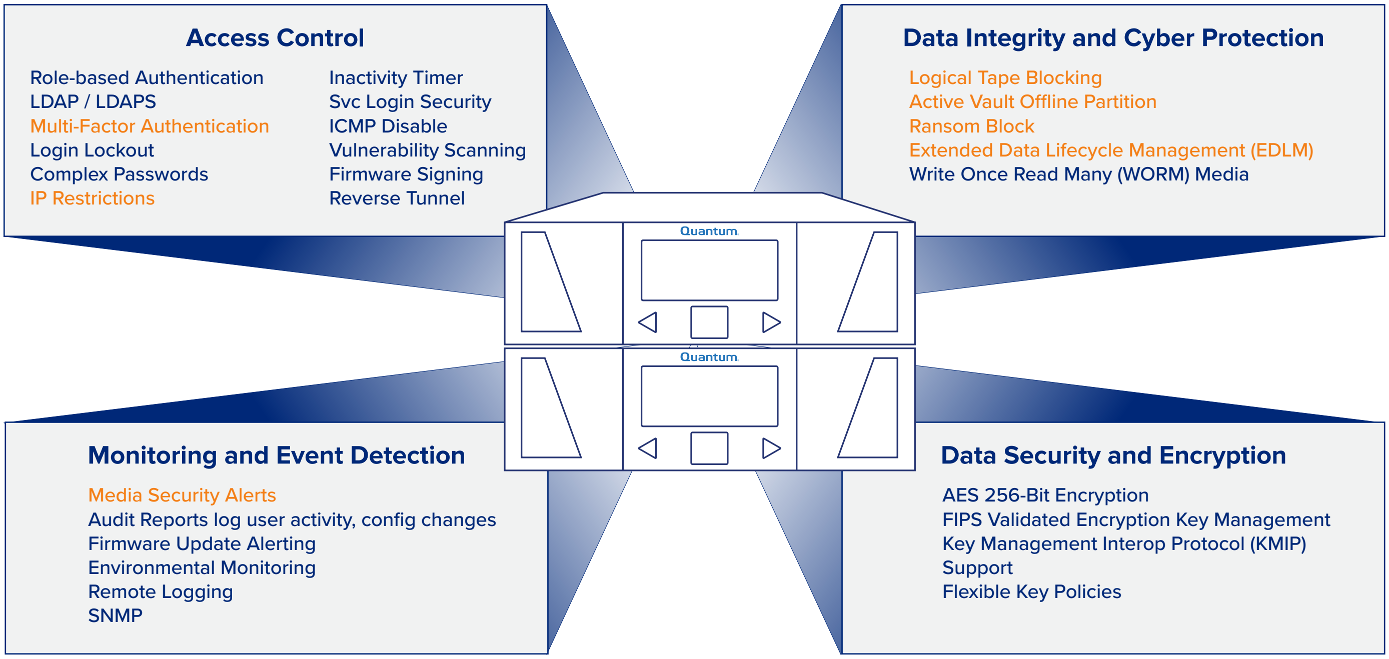
Security isn't something you can buy. It's not a product, or a feature, or any one thing in isolation. Security is better described as an approach, a way of doing things, or even an attitude or state of mind. Security comes from leveraging the right tools and techniques in the right ways at the right times, and from constantly evaluating opportunities to improve security, because adversaries are constantly evaluating ways to get around your defenses.

Quantum Scalar® Tape Libraries are used by everyone from small nonprofits to the world's largest hyperscalers. Organizations rely on them to protect their data, and Quantum takes that responsibility seriously. Scalar libraries are developed with security in mind.

This Tech Brief will provide an overview of the Scalar Security Framework, a combination of tools, features, and methods of operation – many of them unique in the industry – that make Quantum Scalar Tape Libraries the most secure tape storage systems available.

The Scalar Security Framework

The Scalar Security Framework consists of four pillars, each equally critical to achieving and maintaining a secure system. None stands alone, all are interrelated, comprising a layered approach to security. Features in orange below are exclusive to Quantum Scalar Tape Systems. Certain features may not be available in all Scalar library models.



Access Control

Role-based Authentication
LDAP / LDAPS
Multi-Factor Authentication
Login Lockout
Complex Passwords
IP Restrictions
Inactivity Timer
Svc Login Security
ICMP Disable
Vulnerability Scanning
Firmware Signing
Reverse Tunnel

Data Integrity and Cyber Protection

Logical Tape Blocking
Active Vault Offline Partition
Ransom Block
Extended Data Lifecycle Management (EDLM)
Write Once Read Many (WORM) Media

Monitoring and Event Detection

Media Security Alerts
Audit Reports log user activity, config changes
Firmware Update Alerting
Environmental Monitoring
Remote Logging
SNMP

Data Security and Encryption

AES 256-Bit Encryption
FIPS Validated Encryption Key Management
Key Management Interop Protocol (KMIP) Support
Flexible Key Policies

Orange indicates a feature that is unique to Quantum Scalar® Tape Systems.

Access Control

Maintaining data integrity and data security rely upon maintaining the security of the system, which relies on controlling access to administrative interfaces. Robust access control prevents accidental or malicious changes to the system configuration which could weaken data integrity or data security. Quantum Scalar Tape systems provide a comprehensive set of Access Control features as listed in the table below:

Feature	Description
MFA	Multifactor authentication option for library UI login using standard MFA apps
IP Restrictions	Limit which IPv4/v6 addresses may access the library UI
LDAP/LDAPS	User authentication using LDAP directory services, including secure LDAP
Complex Passwords	Support for long (up to 64 character) and complex passwords
Login Lockout	15-min lockout after 5 failed login attempts thwarts brute-force attacks
Inactivity Timer	Users logged out after a configurable period of inactivity
RBAC	Multiple roles and options to limit user access to specific partitions or functions
Svc Login Security	Option to restrict service access to local on-device UI only
Svc Access Window	Set a time-limited window for service personnel access
Svc Access Disable	Option to completely disable service account
Reverse Tunnel	Configurable time-limited reverse tunneling for remote Support access
ICMP Disable	Option to disable ICMP to prevent discovery of library via ‘ping’
Vulnerability Scanning	Every firmware release tested with multiple security scanners. Cloud-Based Analytics (CBA) portal scanned weekly
Firmware Signing	New library firmware is automatically authenticated prior to being installed

Monitoring and Event Detection

Constant monitoring is key to ensuring that the security design of a system is maintained. In addition to damage from attacks, security can be eroded accidentally or unintentionally over time, especially if a system is shared or subject to administration by multiple individuals. Event detection involves detecting and logging important changes to the system, and where applicable, alerting an administrator or other trusted party to the occurrence of an event.

Feature	Description
Media Security Alerts	Library alerts on expected and/or unexpected media removal events
Environmental Monitoring	Monitoring and logging of temperature and humidity. Library alerts if values fall outside safe range for media.
Audit Reports	Log all user activity, library configuration changes, and more
Firmware Update Alert	Library alerts operator when updated firmware is available
Remote Logging	Support for sending log events to a remote syslog server
SNMP	Security and health information may be monitored via SNMP

Data Security and Encryption

Maintaining data security involves ensuring that the information stored on the tape media in the library cannot be stolen or viewed by unauthorized parties. Even if individual tapes or the entire library are stolen, data encryption ensures that the information is safe. Robust data security thwarts data breaches, blackmail, and the associated regulatory compliance complications that come with them.

Feature	Description
AES 256-bit Encryption	Support for hardware-based LTO tape encryption – no performance degradation
Encryption Key Management	Support for application-based or centralized SKM or KMIP encryption key management
Flexible Key Policies	Choice of one encryption key per tape, per partition, or per library

Data Integrity and Cyber Protection

Maintaining data integrity means ensuring that data stored in the library has not changed unexpectedly. Unexpected data change can be dramatic, or intentional (on the part of a nefarious actor), such as being encrypted by ransomware. Just as dangerous, and even harder to detect, is data change that's subtle and unintentional, such as those caused by media wear, bit rot, or environmental degradation. Protecting data integrity means safeguarding data from destruction or loss.

Feature	Description
Active Vault	Secure, isolated in-library vault partition not visible to applications or network
Logical Tape Locking	Software-based lock prevents media from leaving the magazine until the magazine is physically removed and re-inserted into the library by an operator.
Ransom Block	Partial eject of magazine puts media physically out of reach of the robot until operator re-inserts the magazine. Media is still visible to the barcode scanner for inventory validation.
Extended Data Lifecycle Mgmt (EDLM)	Monitors data/media health, alerts, and proactively takes action on suspect media.
WORM	Support for hardware-enforced immutability using LTO WORM media

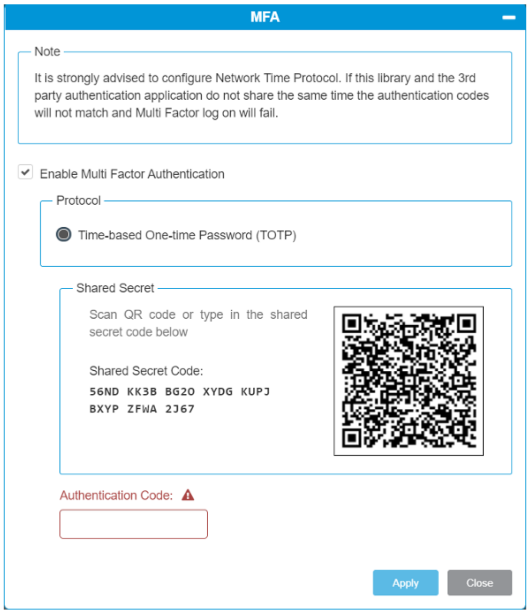
Technical Details

Each of the four pillars is comprised of a set of capabilities and options, some of them extensive. It's not expected or intended that every installation will leverage every capability. The intent is to provide a robust and complete set of options to enable each organization to configure the system to meet their unique needs. A summary of the features in each pillar is provided below. For more details and model-specific configuration information, refer to the user guides in the Quantum Documentation Center at www.quantum.com/documentation.

Access Control

Multifactor Authentication (MFA)

For environments where library administrative access is managed using local (to the library) user accounts, MFA may be enabled. MFA uses standard Time-based One Time Password apps such as Google Authenticator, Microsoft Authenticator, and others. Once enabled, users attempting to log in to the library web UI will be prompted for an authentication code in addition to their username and password. When LDAP is used for authenticating library access, MFA is managed externally to the library.



Note

It is strongly advised to configure Network Time Protocol. If this library and the 3rd party authentication application do not share the same time the authentication codes will not match and Multi Factor log on will fail.

☑ Enable Multi Factor Authentication

Protocol

● Time-based One-time Password (TOTP)

Shared Secret

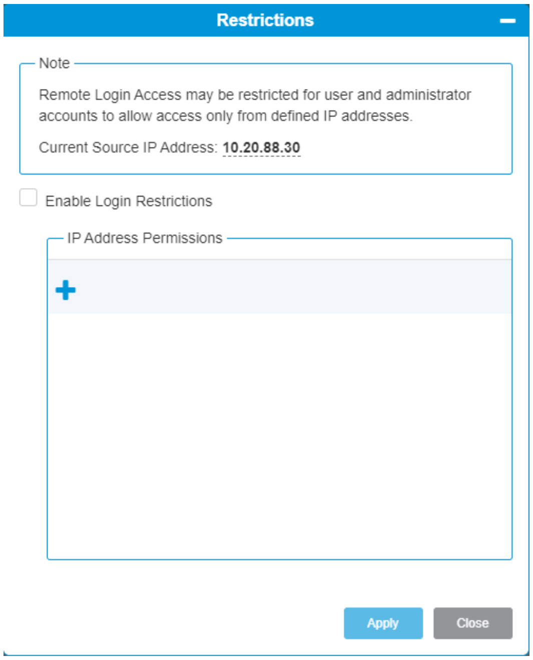
Scan QR code or type in the shared secret code below

Shared Secret Code:
56ND KK3B BG2O XYDG KUPJ
BXYP ZFWA 2J67

Authentication Code:

IP Restrictions

Enabling IP Restrictions ensures that only users whose IP address (v4 or v6) appears on a pre-defined whitelist may access the library remote user interface.



Note

Remote Login Access may be restricted for user and administrator accounts to allow access only from defined IP addresses.

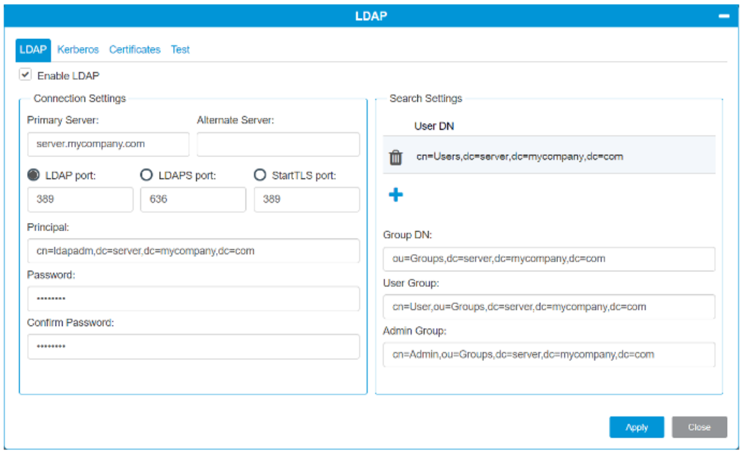
Current Source IP Address: 10.20.88.30

□ Enable Login Restrictions

IP Address Permissions

Lightweight Directory Access Protocol (LDAP/LDAPS)

To enable more efficient, secure, enterprise-wide management of credentials, Scalar libraries support common LDAP directory services, including Microsoft Active Directory, NetIQ (formerly Novell) eDirectory, OpenLDAP, etc. For additional security, secure LDAP (LDAPS) may be enabled by installing appropriate certificates onto the library.



☑ Enable LDAP

Connection Settings

Primary Server: server.mycompany.com

Alternate Server:

● LDAP port: 389 ○ LDAPS port: 636 ○ StartTLS port: 389

Principal: cn=ldapadm,dc=server,dc=mycompany,dc=com

Password: ********

Confirm Password: ********

Search Settings

User DN

cn=Users,dc=server,dc=mycompany,dc=com

Group DN: ou=Groups,dc=server,dc=mycompany,dc=com

User Group: cn=User,ou=Groups,dc=server,dc=mycompany,dc=com

Admin Group: cn=Admin,ou=Groups,dc=server,dc=mycompany,dc=com

Complex Passwords

To encourage the use of strong passwords, Scalar libraries require all passwords used to access the UI to be at least 8, and up to 64 characters long. Passwords may include any printable characters except the back tick (`) and the tilde (~).

Login Lockout

If a library user fails to successfully log in five times within a span of five minutes, their account is locked out for 15 minutes. This greatly reduces the likelihood of a successful brute-force attack against a library admin account, especially if long and complex passwords are used.

Inactivity Timer

All library users are logged out automatically after a configurable duration of inactivity, from 5 minutes to 24 hours. The default timeout period is 30 minutes, and shorter times provide greater security.

Role-Based Access Control (RBAC)

Users of the library UI are configured as either users or administrators. Users can initiate library actions, but not change configuration. In a multi-partition library, each user may be restricted as to the specific partitions they are able to access and control. This facilitates tighter security when multiple applications or application domains with different administrators are sharing a single library.

Service Login Security

The Service user login (used by Quantum technicians for troubleshooting and repair) may be restricted to only be accepted when the user is onsite and physically plugged into the library service port. Local service logins are controlled by the Service Access Window, and service users are automatically logged out after four hours of inactivity.

Service Access Window

The Service Access Window feature enables administrators to define a period that a service user may connect to a library via remote or local connection. When the time window closes, service access is disabled. This enables administrators to accommodate necessary service without the need to remember to disable the service account when maintenance is complete.

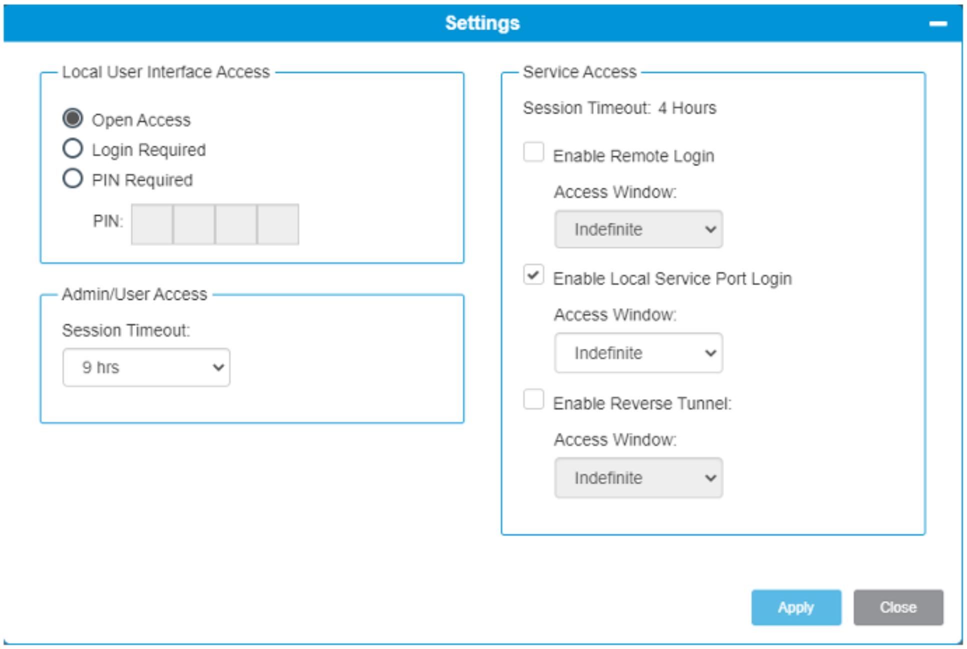
Service Access Disable

By default, both local and remote Service user access to Scalar libraries is disabled. Local and remote Service access may be enabled separately or together, or both may remain disabled.

Reverse Tunnel

Secure remote access for Quantum service and support personnel is secured via a reverse tunneling process. Reverse tunneling does not require any special firewall rules or network configuration, as it is initiated outbound from the library to the Quantum Cloud-Based Analytics (CBA) portal, never inbound.

To initiate a reverse tunnel, the library administrator first sets an access window period for the tunnel to be in effect and enables the tunnel in the library Web GUI. The library then makes a reverse service tunnel request via the CBA portal. The library administrator must then approve the request in the CBA portal. Once approved, Quantum Service may make secured connections to the library using the CBA infrastructure during the specified access window. When the access window expires, all service connections are closed.



Settings

Local User Interface Access

● Open Access
○ Login Required
○ PIN Required

PIN:

Admin/User Access

Session Timeout: 9 hrs

Service Access

Session Timeout: 4 Hours

□ Enable Remote Login

Access Window: Indefinite

☑ Enable Local Service Port Login

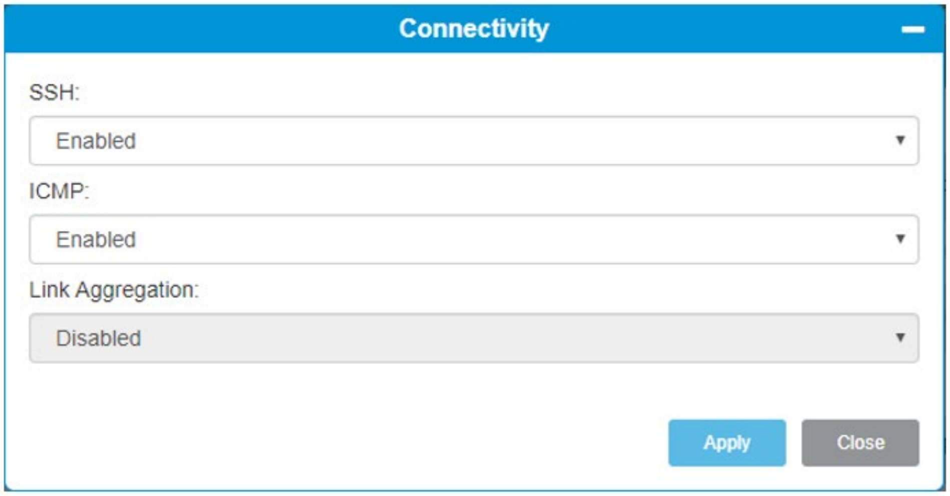
Access Window: Indefinite

□ Enable Reverse Tunnel:

Access Window: Indefinite

ICMP Disable

Once cyber attackers breach a network by establishing access, they attempt to move laterally to discover and map the servers and other resources that are present. The ubiquitous ‘ping’ utility is used to determine live IP addresses. Disabling the ICMP protocol on a Scalar library makes it invisible to ‘ping’ discovery.



Connectivity

SSH: Enabled

ICMP: Enabled

Link Aggregation: Disabled

Vulnerability Scanning

The cybersecurity threat landscape is constantly evolving. To ensure that Scalar library firmware is secure, every revision of firmware is tested with multiple commercial security scanners, and any issues are remediated before release.

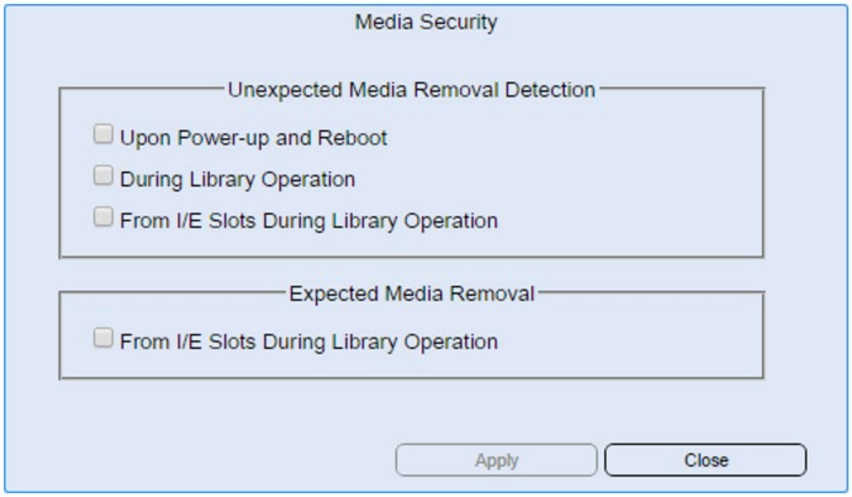
Firmware Signing

It would take a very determined attacker to try to bypass Scalar library security by loading custom firmware, but it could in theory be attempted. Any such attacker will be severely disappointed to find that official Quantum firmware is cryptographically signed, and Scalar libraries will reject any firmware that is not authentic.

Monitoring and Event Detection

Media Security Alerts

Security breaches and data leaks are usually perpetrated remotely – but not always. Insiders can walk out with storage media containing confidential information, and innocent errors in handling can cause tapes to be lost, causing problems for regulatory compliance. Scalar Media Security Alerts notify the administrator when media is removed – either expectedly or unexpectedly – from the library.



Unexpected Media Removal Detection

□ Upon Power-up and Reboot

□ During Library Operation

□ From I/E Slots During Library Operation

Expected Media Removal

□ From I/E Slots During Library Operation

Four types of alerts may be configured, alone or in combination, as shown in the image above.

1. Selecting '*Upon Power-up and Reboot*' will send an alert on boot if the media inventory does not match the inventory recorded at shutdown.

2. Selecting '*During Library Operation*' will send an alert if media is removed by an operator during library operation, not in conjunction with an application export command. For example, if an operator were to open the front door of a Scalar i6000 library and remove tapes, this alert would occur.

3. Selecting '*From I/E Slots During Library Operation*' will send an alert if media placed by an operator into the import/export slots is later removed before it can be imported into the library.

4. One expected media removal alert may be configured, which will alert the administrator any time media is removed from the library I/E slots due to an export request from an application or the library UI.

Environmental Monitoring

One key to maximizing the life of data stored on tape is to store media under appropriate environmental conditions. Usually in a data center this is not a problem, but air conditioning systems can become unreliable, overloaded, fail intermittently, or be improperly programmed, resulting in room temperature or humidity values going out of bounds. Scalar libraries contain multiple temperature and humidity sensors with configurable upper and lower thresholds for alerting. When values drift outside the proscribed ranges, the administrator is alerted.

To aid in system troubleshooting, current library temperature and humidity values are reported as standard data within every RAS (reliability, availability, serviceability) ticket issued by a Scalar library, and reports may be run showing the environmental values over time. The reports can be extremely valuable for detecting conditions such as incorrect programming that turns down or disables data center A/C on weekends, or cooling equipment struggling to cope with increased demand or seasonal load fluctuation.

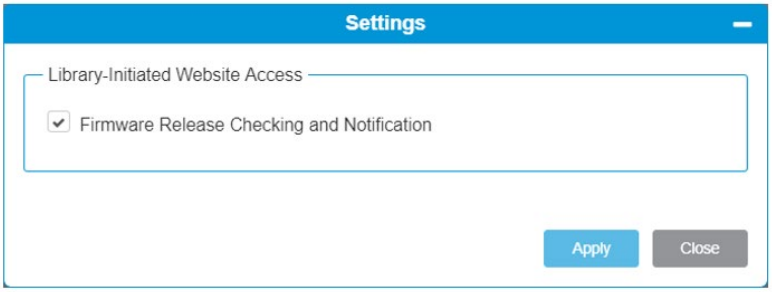
Audit Reports

Scalar libraries log a lot of data. Data about library operations, the environment the library is operating in, interactions with administrators, users, and applications. Data about media, and data about tape drives. Data about features, capacity, usage, and more. A wide range of reports are available to display this collected information in ways that make it easy for administrators to spot trends or anomalies, including activity that may indicate unwanted activity or security breaches. The table below lists some of the reports that are relevant to system and data security. All reports may be automatically generated and sent to administrators on a schedule.

Feature	Description
Cross-Partition Media Move	Shows which tape cartridges have moved from one partition to another.
EDLM Scan Test	Shows which media was tested when, with which scan type, and the scan results. Shows whether media is healthy, suspect, or failed.
EKM Media Status	Provides encryption status for all media currently present in the library.
EKM Partition Activity	Provides partition encryption summaries, including historic information about when library managed encryption was enabled or disabled on a partition.
Library Configuration Record	Shows historical library configuration change activity.
Login Activity	Provides login and command request history for every administrator and user account. This report details who logged in, when, and how, and captures command operations and command attempts, providing a library login audit trail.
Media Integrity Analysis	Heat map of tape drives vs. cartridges helps visualize whether problems (as determined by tape alerts) are caused by problematic drives, media, or both.
Media Security	Shows which tape cartridges have been removed from the library, either expectedly (properly exported) or unexpectedly.
Temperature/Humidity	Graphs system temperature and humidity over a specified period.

Firmware Update Alert

Quantum periodically releases updated firmware for Scalar libraries. Updated firmware may include feature enhancements, security enhancements, and bug fixes. If ‘Firmware Release Checking and Notification’ is enabled, the library will periodically check with Quantum to see if a newer release is available. Updates are not downloaded or applied automatically – the administrator is simply alerted to the presence of updated firmware so they may determine if an upgrade is warranted.



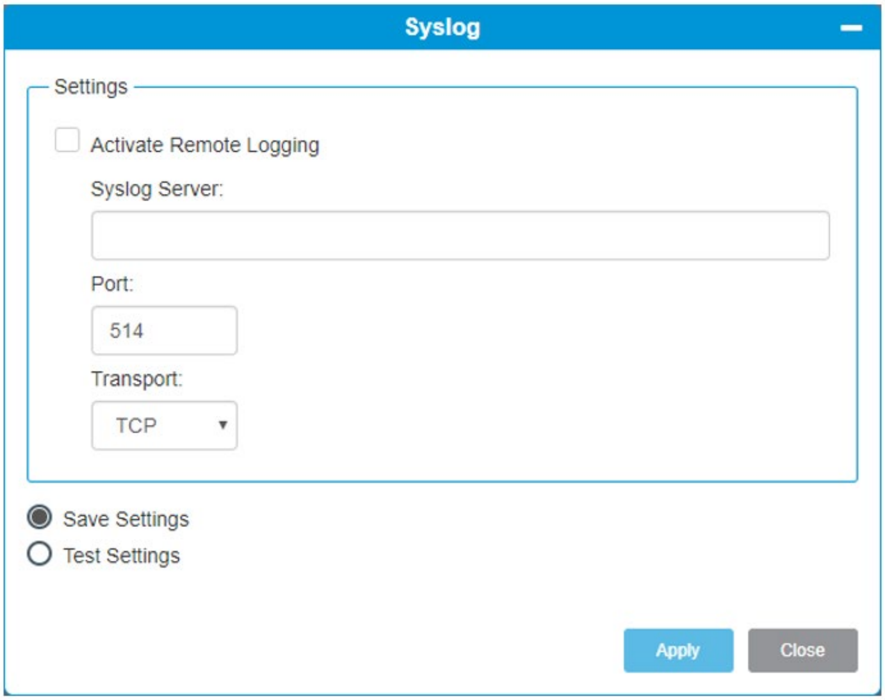
Settings

Library-Initiated Website Access

☑ Firmware Release Checking and Notification

Remote Logging

It is standard procedure for cyber attackers to attempt to cover their tracks by modifying or deleting system logs. Sending log events to a remote server can thwart this tactic. Scalar libraries can be configured to send log events to a standard syslog server using TCP or UDP protocol, with a configurable port number.



Syslog

Settings

□ Activate Remote Logging

Syslog Server:

Port: 514

Transport: TCP

● Save Settings

○ Test Settings

Simple Network Management Protocol (SNMP)

SNMP has long been a popular standard for remote management and monitoring of data center infrastructure. Scalar libraries support SNMP v1, v2c, and v3, including SMIv2 compliance. This enables integration with all common infrastructure monitoring frameworks. MIBs (Management Information Bases) are hosted on the libraries, and may be downloaded directly. Trap notifications may be individually configured so that only items of interest trigger notifications.

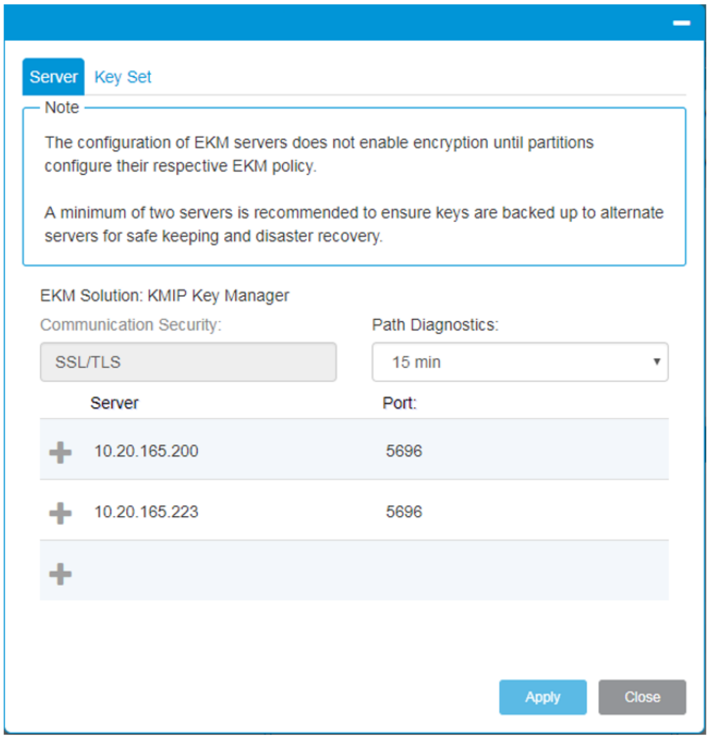
Data Security and Encryption

Data Encryption

Introduced with the fourth generation of LTO tape technology, onboard data encryption has been available since 2007. The encryption is performed in hardware and is situated in the data path after the data compression operation. For these reasons enabling encryption does not negatively impact performance or capacity, as is the case with approaches that encrypt data prior to sending it to tape. All Quantum Scalar tape libraries support LTO Encryption.

Encryption Key Management (EKM)

Encrypting data requires encryption keys. The management of encryption keys is vital, since losing the key is tantamount to losing the data encrypted with that key. All Quantum Scalar tape libraries support both application-managed keys and external key managers such as those conforming to the OASIS KMIP specification.



Note

The configuration of EKM servers does not enable encryption until partitions configure their respective EKM policy.

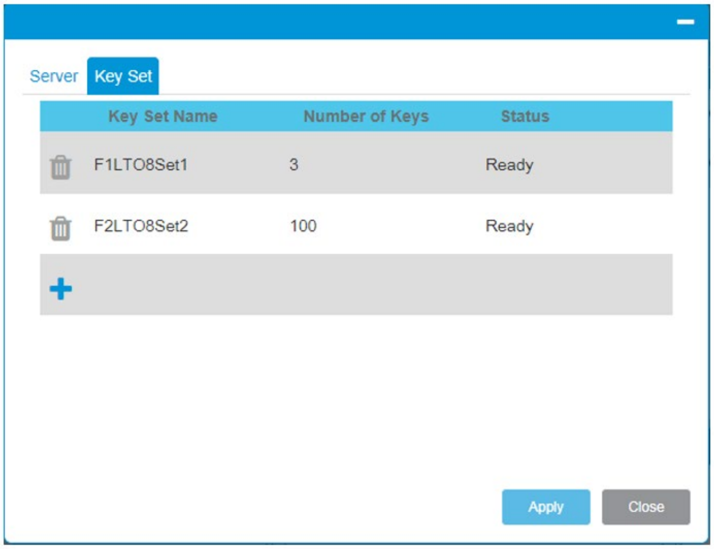
A minimum of two servers is recommended to ensure keys are backed up to alternate servers for safe keeping and disaster recovery.

EKM Solution: KMIP Key Manager

Communication Security: SSL/TLS

Path Diagnostics: 15 min

Server	Port:
10.20.165.200	5696
10.20.165.223	5696



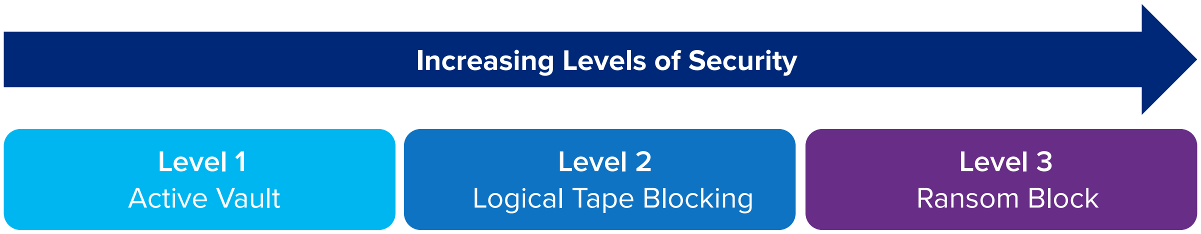
Key Set Name	Number of Keys	Status
F1LTO8Set1	3	Ready
F2LTO8Set2	100	Ready

Flexible Key Policies

The more data that is encrypted with a particular encryption key, the more data is at risk if that key is compromised. Managing more encryption keys can be more challenging but is correspondingly more secure. Scalar libraries provide a range of key policies to enable each organization to choose the right balance of security and convenience. At the most granular level, one unique key may be used per tape. Alternatively, one key may be assigned to each library partition (one partition often corresponds to one application), or one key may be used for an entire library.

Data Integrity and Cyber Protection

When it comes to data integrity and cyber-protection, Quantum Scalar tape systems offer three specific features that provide increasing levels of security for protecting data stored on tape. These features are listed below, shown in increasing levels of security.



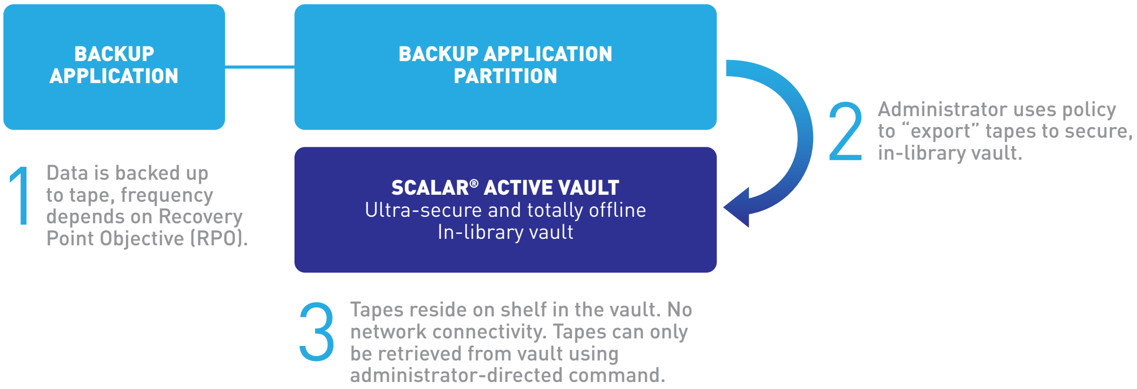
Administrator moves tapes to a secure, isolated in-library Active Vault partition not visible to any application or network.

Administrator initiates Logical Tape Blocking, which prevents robots from moving tapes via software locking.

Administrator initiates Ransom Block, which ejects magazine to create a physical barrier.

Active Vault

This feature enables tapes to be moved into a secure, isolated in-library vault partition that has no network connectivity and is not visible to any application or network. This feature could be considered "level 1" security, though there is still some risk of data compromise in the unlikely event that the tape library is hacked. Active Vault works with any application and provides an additional layer of security for media without exposing them to the environmental dangers inherent in manually handling tapes or removing them from the library.


BACKUP APPLICATION
BACKUP APPLICATION PARTITION
SCALAR® ACTIVE VAULT
Ultra-secure and totally offline
In-library vault

1 Data is backed up to tape, frequency depends on Recovery Point Objective (RPO).

2 Administrator uses policy to "export" tapes to secure, in-library vault.

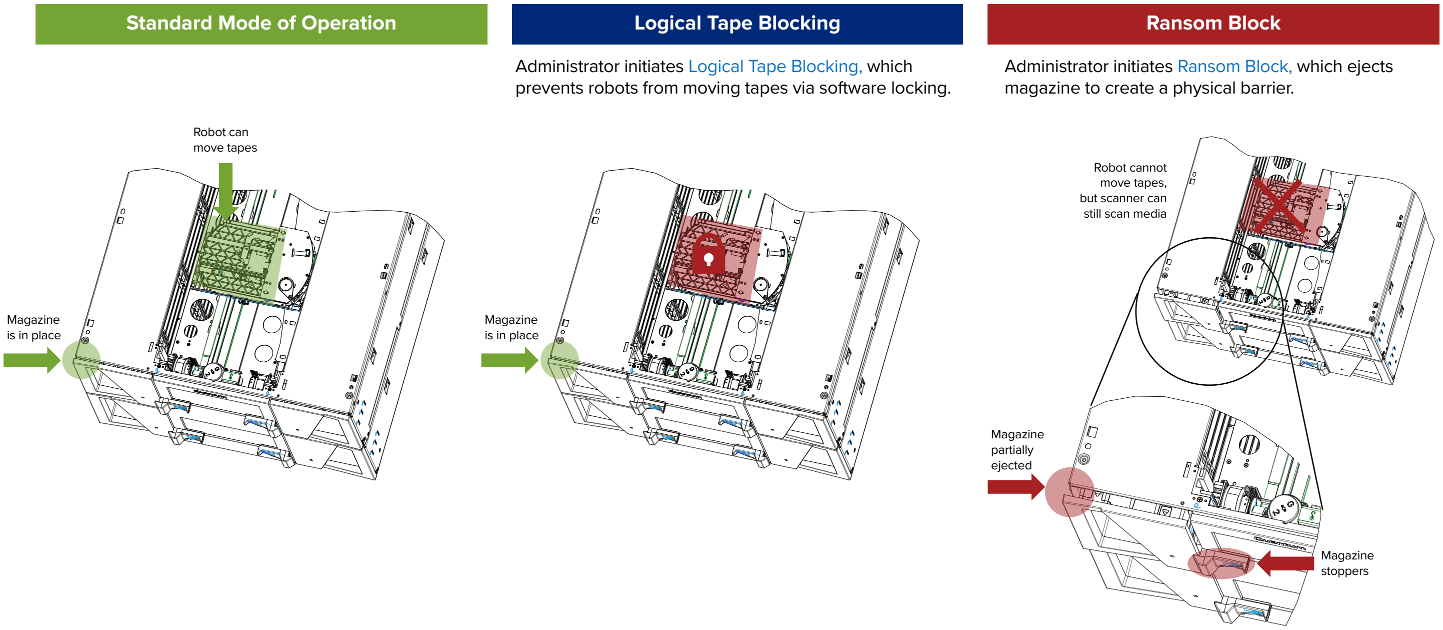
3 Tapes reside on shelf in the vault. No network connectivity. Tapes can only be retrieved from vault using administrator-directed command.

Logical Tape Blocking

Logical Tape Blocking is a logical policy-based block that's placed on a tape magazine. When a tape is moved into a covered magazine, Logical Tape Blocking denies future requests to move that tape elsewhere, such as into a drive. To allow blocked tapes to be accessed again, the magazine must be ejected from the library and then re-inserted, operations which require the operator to be physically present at the library. Tape Block may be enabled remotely but can only be disabled using the local library operator panel, again requiring physical presence in the data center. Logical Tape Blocking may be used on its own but is ideally used with Active Vault and Ransom Block to provide the best security.

Ransom Block

Quantum Scalar® Ransom Block employs a simple and unique concept to create a physical barrier between data stored on tapes and the network connected tape library.



Standard Mode of Operation

Logical Tape Blocking

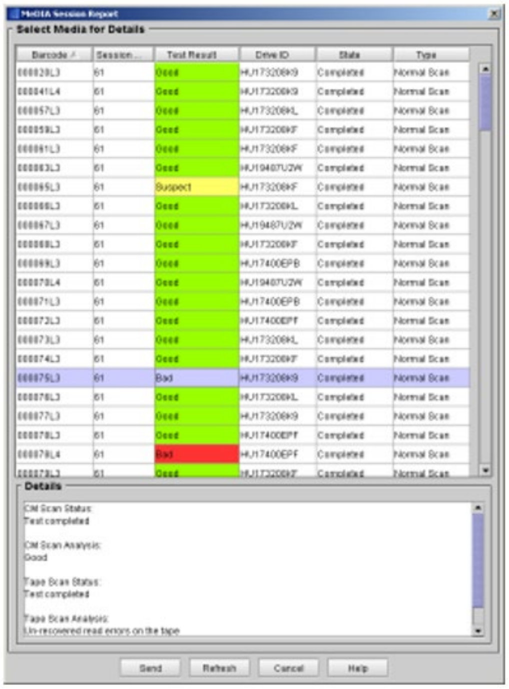
Administrator initiates Logical Tape Blocking, which prevents robots from moving tapes via software locking.

Ransom Block

Administrator initiates Ransom Block, which ejects magazine to create a physical barrier.

Robot can move tapes
Magazine is in place
Magazine is in place
Robot cannot move tapes, but scanner can still scan media
Magazine partially ejected
Magazine stoppers

Tapes stored in the library sit in a magazine. Quantum's patent-pending design partially ejects the magazine so the tapes cannot be picked by the robot until an operator physically re-inserts the magazine. Because the magazine is only partially ejected, the barcode scanner on the robot can still scan the tape barcodes, so that system administrators can perform periodic audits of the tape system to ensure tapes are still present.



Barcode	Session...	Test Result	Drive ID	State	Type
000020L3	61	Good	HUJ173208K9	Completed	Normal Scan
000041L4	61	Good	HUJ173208K9	Completed	Normal Scan
000057L3	61	Good	HUJ173208KL	Completed	Normal Scan
000059L3	61	Good	HUJ173208KF	Completed	Normal Scan
000061L3	61	Good	HUJ173208KF	Completed	Normal Scan
000063L3	61	Good	HUJ19407U2W	Completed	Normal Scan
000065L3	61	Suspect	HUJ173208KF	Completed	Normal Scan
000066L3	61	Good	HUJ173208KL	Completed	Normal Scan
000067L3	61	Good	HUJ19487U2W	Completed	Normal Scan
000068L3	61	Good	HUJ173208KF	Completed	Normal Scan
000069L3	61	Good	HUJ17400EPB	Completed	Normal Scan
000070L4	61	Good	HUJ19407U2W	Completed	Normal Scan
000071L3	61	Good	HUJ17400EPB	Completed	Normal Scan
000072L3	61	Good	HUJ17400EPF	Completed	Normal Scan
000073L3	61	Good	HUJ173208KL	Completed	Normal Scan
000074L3	61	Good	HUJ173208KF	Completed	Normal Scan
000075L3	61	Bad	HUJ173208K9	Completed	Normal Scan
000076L3	61	Good	HUJ173208KL	Completed	Normal Scan
000077L3	61	Good	HUJ173208K9	Completed	Normal Scan
000078L3	61	Good	HUJ17400EPF	Completed	Normal Scan
000079L4	61	Bad	HUJ17400EPF	Completed	Normal Scan
000079L3	61	Good	HUJ173208KF	Completed	Normal Scan

Details

CM Scan Status:
Test completed

CM Scan Analysis:
Good

Tape Scan Status:
Test completed

Tape Scan Analysis:
Un-recovered read errors on the tape

The tapes are inaccessible until an operator, who must have physical access to the tape library, re-inserts the magazine. Tape systems can be stored in secure data centers that require badged access.

Extended Data Lifecycle Management (EDLM)

Not all threats are personal – some are environmental. Tape media is subject to wear and degradation from use, improper temperature and humidity in storage or transport, contamination, physical abuse, and human error. Traditionally, organizations discover that media is unreadable at the worst possible time – when they need access to the data it contains.

EDLM enables proactive, flexible, scheduled, policy-based, multi-level testing of tape readability, to ensure that when the data is needed, it's available. Administrators are warned about tapes that are becoming unreliable in time to copy the data to fresh media. Some applications, such as Quantum StorNext®, can even migrate data onto fresh media automatically based on EDLM alerts. To ensure accuracy, media testing is done with special drives that cannot be used for regular library operations. Because it's not possible to connect these drives to the network, EDLM may be used in concert with Active Vault, to ensure that the condition of vaulted media is always known.

Write Once Read Many (WORM)

LTO tape has been capable of WORM operation since the release of the third generation (LTO-3). WORM operation requires the use of special media and is managed and enforced through a combination of hardware characteristics and firmware code. LTO WORM very secure and has been validated to comply with SEC rule 17a-4(f) and similar regulations that require storage that is non-rewritable, non-erasable, and unalterable. For organizations in regulated industries that require compliant storage, LTO WORM is by far the lowest cost and most scalable option. All Quantum Scalar libraries support LTO WORM.

Scalar Security Framework Feature Summary

Feature	Data Integrity	Data Security	Access Control	Event Detection
Active Vault	X			
Tape Block	X			
Ransom Block	X			
EDLM	X			
WORM	X			
Encryption		X		
EKM		X		
Key Policy		X		
Multifactor Authentication			X	
IP Restrictions			X	
LDAP/LDAPS			X	
Complex Passwords			X	
Login Lockout			X	
Inactivity Timer			X	
RBAC			X	
Svc Login Security			X	
Svc Access Window			X	
Svc Access Disable			X	
Reverse Tunnel			X	
ICMP Disable			X	
Vulnerability Scanning			X	
Firmware Signing			X	
Media Security Alerts			X	
Environmental Monitoring			X	
Audit Reports				X
Firmware Update Alert				X
Remote Logging				X
SNMP				X

Conclusion

Quantum takes the security of our customer's data seriously, as evidenced by the thorough approach to security represented by the Scalar Security Framework. For more information on any of the items discussed in this document, consult the product documentation at www.quantum.com/documentation.

Quantum®

Quantum technology, software, and services provide the solutions that today's organizations need to make video and other unstructured data smarter – so their data works for them and not the other way around. With over 40 years of innovation, Quantum's end-to-end platform is uniquely equipped to orchestrate, protect, and enrich data across its lifecycle, providing enhanced intelligence and actionable insights. Leading organizations in cloud services, entertainment, government, research, education, transportation, and enterprise IT trust Quantum to bring their data to life, because data makes life better, safer, and smarter. Quantum is listed on Nasdaq (QMCO) and the Russell 2000® Index. For more information visit www.quantum.com.

www.quantum.com | 800-677-6268