



> Thales Encryption Key Manager for Storage

KEY BENEFITS

- > Automates and centralizes lifecycle encryption key management
- > Lowers the risk of security breaches with a hardened appliance approach
- > Accelerates deployment by enabling pre-qualified partner encryption devices
- > Simplifies audits and policy compliance through federated device management
- > Reduces administrative time and cost with a consistent storage key manager
- > Meets storage continuity and data retention goals with increased reliability

Your information is at risk

Storage managers are under pressure to protect sensitive information and support regulatory mandates that reduce risk. The consequences of data loss can be devastating, including costly penalties, remediation expenses and damaged business reputation. While storage encryption is a well-proven method to control exposure of data at rest, storage managers must decide how best to deploy and manage encryption across a diverse storage environment.

Networked storage devices, such as tape libraries, disk arrays and SAN switches, now include embedded encryption capabilities. However, without a reliable key manager, the cost and complexity of deploying and managing encryption can delay adoption. When planning a storage security strategy, storage managers must ensure that encryption does not impact business continuity or data access. A systematic and simplified approach is needed to automate key lifecycle management, while ensuring long-term protection of cryptographic keys.

>> Thales Encryption Key Manager for Storage

Simplified storage encryption using a hardened appliance key manager

Thales Encryption Manager for Storage is a standards-based, FIPS-designed key manager that enables organizations to confidently manage cryptographic keys across multiple classes of encrypting storage devices. The appliance supports standards-based protocols as well as legacy interoperability with leading storage products. The key manager appliance centralizes administration for consistent key lifecycle management and auditing of encryption controls, while ensuring that business continuity and data recovery requirements are met. Pre-qualified, native support for industry-leading storage products and encryption devices delivers a comprehensive, integrated solution that grows with your enterprise storage needs.

Confidently deploy and manage encryption to prevent data loss

Key manager reliability when recovering keys is a top priority to control data access with confidence. With Thales Encryption Manager for Storage, security architects can accelerate the adoption of encryption devices with pre-qualified integration that simplifies deployment.

- > **Certified device integration** – Tested and validated solutions from Thales and storage encryption partners allow for accelerated setup and deployment.
- > **Extensible** – A storage vendor-neutral approach allows new storage encryption devices to be certified and integrated quickly as new industry standards and products become available.

Meet data continuity and retention requirements

Your business expects continuous access to data. The performance-optimized key manager appliance safeguards keys long-term by using a redundant hardware design to maintain access to sensitive data.

- > **Redundant, FIPS-designed hardware** – The security-hardened, high-performance key manager appliance is designed with redundant components, including hot-swappable fans and power supply units to minimize the risk of downtime.



- > **Key backup** – The key manager ensures access to data with backups to offsite data centers.
- > **Synchronized key replication** – Automated archiving of keys by clients to multiple key managers, failover deployment and pre-generated key pool options all help to provide high-availability.

Achieve compliance and audit goals

To comply with an ever-increasing number of data protection mandates, the key manager enforces security policy and maintains logs within secure audit facilities, which is critical for reporting integrity.

- > **Key sharing policy** – End-to-end key lifecycle management is provided via logical domains and key groups with rules for key manager sharing.
- > **A single point for auditing** – Routine and ad hoc reporting are simplified with an auditor role and a centralized repository for administrative, system and key lifecycle activities.
- > **Event alerting and export** – System functions are logged, with the ability to notify through email, SNMP, and syslog, and to securely export audit logs for controls attestation.

Reduce cost of managing encryption with a unified approach

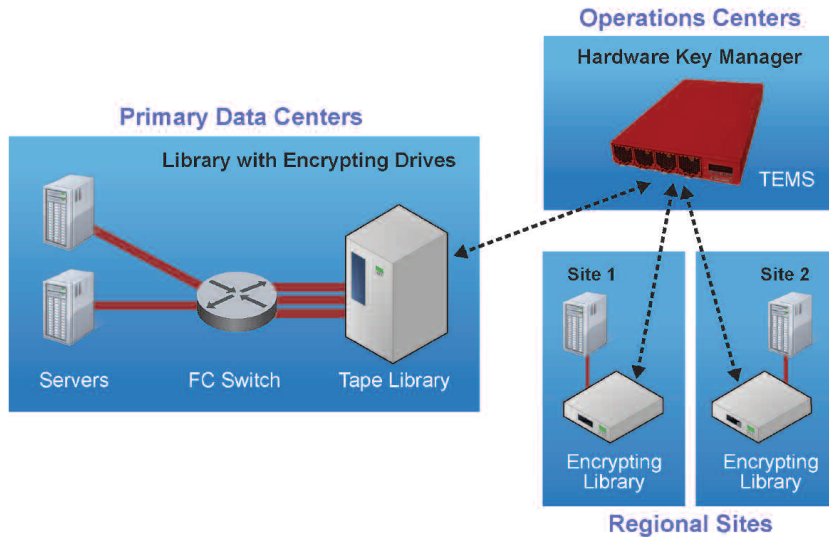
The appliance key manager simplifies routine maintenance by enabling standards of due care, freeing administrator time and reducing cost through a single solution based around best practices.

- > **Single key manager** – Storage, compliance, and security teams manage encryption from a single, central console which reduces the need for additional single-purpose key managers.

>> Thales Encryption Key Manager for Storage

> **Role-based access controls** – Pre-defined entitlements, two-factor authentication, two-person rules, and System Key split knowledge maintain separation of duties and provide accountability.

> **Current and legacy device protocols** – Standards-based and proprietary interfaces offer flexibility that extends current investments for future encryption device support.



Dimensions and Weight	2U standard rack units. Height 3.47 in. (8.81cm), width 17.19 in. (43.66 cm), depth 30 in. (76.20 cm). 41 lbs (18.6 kg) without the rack mounting kit.
Input Voltage	100 to 240 VAC (autosensing); input line frequency nominally 50 to 60 Hz; total power consumption 250 W
Temperature	Operating temperature 10 to 40° C (50 to 104° F); operating humidity 5% to 85% non-condensing at 40° C (104° F); operating altitude 0 to 6562 feet (2 km) above sea level Non-operating shock 20 G, 11 ms duration, square wave Non-operating vibration 10 G, 5 to 500 to 5 Hz @ 1 octave intervals
Shock	Operating shock 5 G, 11 ms duration, half sine; operating vibration 5 G, 5 to 500 to 5 Hz at 1 octave intervals; non-operating temperature -30° to 65° C (-22° to 149° F); non-operating humidity 95% RH maximum; non-operating altitude 0 to 47 250 feet (12 km) above sea level
Airflow	Airflow volume 300 ft ³ (8.5 m ³) per minute; airflow direction Intake from front, exhaust to rear
Replaceable Components	Hot-swappable redundant fans and power supply units
Interfaces	Serial RJ-45 console port for command line interface (setup only) 10/100BaseT Ethernet ports to the LAN Smart card reader (ISO 7816 compliant) for system key and configuration backup Web graphical user interface for role-based administration
Certified Encryption Devices	Brocade Encryption Switch and FS8-18 blades TKLM-compatible IBM storage devices (TS-series tape and DS8000-series disk)

Thales - Security Solutions & Services

