



Overview

Cisco® Storage Media Encryption (SME) secures data stored on tape drives and virtual tape libraries (VTLs) in a SAN environment using secure IEEE-standard Advanced Encryption Standard (AES) 256-bit algorithms. Cisco SME is built on Federal Information Processing Standards (FIPS) system architecture and offers secure, comprehensive key management, with support for offline media recovery.

Cisco SME uses cryptographic engines on the Cisco MDS 9222i Multiservice Modular Switch (MMS), MDS 9000 18/4-Port Multiservice Module (MSM), and MDS 9000 16-Port Storage Services Node (SSN), each providing enough throughput to sustain continuous streaming to multiple tape drives. Each Cisco MDS 9000 16-Port Storage Services Node provides encryption throughput that is four times that provided by the Cisco MDS 9222i and MDS 9000 18/4-Port Multiservice Module. Multiple encryption engines can be deployed in a Fibre Channel fabric to easily scale performance, enable load balancing, and increase availability.

Cisco SME hardware and software integration with the Cisco MDS 9000 Family facilitates deployment and management of sensitive data on SAN attached storage devices. Unlike competitive offerings, Cisco SME requires little downtime to deploy. The Cisco MDS 9000 18/4-Port Multiservice Modules and MDS 9000 16-Port Storage Services Nodes are hot swappable, so they can be installed while an existing SAN is in use. No rewiring or SAN configuration changes are required, and encryption provisioning can be performed without shutting down applications.

The enterprise-class capabilities that Cisco SME provides are integrated transparently as a fabric service, rather than by a separate hardware appliance. Fibre Channel redirect capabilities in Cisco MDS 9000 Family fabrics enable traffic from any port to be routed through an encryption engine without SAN reconfiguration. Traffic between hosts and tape devices in any virtual SAN (VSAN) can make full use of Cisco SME services such as encryption, compression, load-balancing, and clustering capabilities for failover.

Cisco SME integrates transparently with Cisco Fabric Manager software and with Cisco MDS 9000 NX-OS Software advanced security features such as role-based access control (RBAC) at the VSAN level. Through this integration at multiple levels, including physical, network protocol and services, management software, and security features, Cisco SME simplifies encryption of SAN attached storage devices (Figure 1).

Figure 1. Cisco Storage Media Encryption



Features and Benefits

- **Exceptional flexibility and scalability:** Cisco SME is available for both the Cisco MDS 9200 Series Multilayer Switches and Cisco MDS 9500 Series Multilayer Directors. Encryption services can be scaled up simply by adding Cisco MDS 9222i fabric switches, MDS 9000 18/4-Port Multiservice Modules, or MDS 9000 16-Port Storage Services Nodes to new or existing configurations. Cisco SME software manages the encryption engines collectively, allowing administrators to focus on tasks such as provision encryption and to manage keys without the need to be concerned about the physical partitioning. Automated load balancing and failover for encryption and compression fabric services facilitate scalable performance and simplified management.
- **Reduced downtime for deployment:** Alternative solutions providing encryption for SAN attached storage devices require downtime or significant network degradation for rewiring of the SAN to insert them, plus downtime to change the SAN and storage device configuration. In contrast, the Cisco MDS 9000 Family switching modules can be inserted without disruption, and traffic can be redirected through the encryption engines without the need to rewire the SAN or reconfigure any devices, eliminating most sources of downtime for deployment.



- **Load balancing:** The Cisco MDS 9000 NX-OS Software allows partitioning of a single physical SAN into multiple VSANs, creating separate, isolated environments to improve Fibre Channel SAN scalability, availability, manageability, and network security. Cisco SME can encrypt traffic from any VSAN in a physical fabric. The consolidated services provided by Cisco SME greatly simplify provisioning and performance management. Competitive solutions require separate physical connections to different VSANs, complicating installation and load-balancing performance across entire physical fabrics.
- **Comprehensive security:** The encryption capabilities that Cisco SME provides significantly expand the Cisco MDS 9000 Family Fibre Channel SAN security offering. Cisco SME uses strong, IEEE-compliant AES-256 encryption algorithms to protect data at rest. Cisco MDS 9000 NX-OS Software security features such as Secure Shell (SSH), SSL, RADIUS, Fibre Channel Security Protocol (FC-SP), and Secure File Transfer Protocol (SFTP) provide the foundation for the secure FIPS architecture of Cisco SME.
- **Advanced key management:** Cisco SME offers secure, comprehensive key management, with provisions for master keys to reside in smart cards. Storage media keys reside in clear text only within the crypto boundary on the switch module. For flexibility, Cisco SME can provide either a unique media key for each tape or for each tape volume group. Tape keys can also be stored on the tapes. Media keys are encrypted before storage or transport to the Cisco Key Management Center (KMC). Integrated key management services are available with media key archival, recovery, distribution, and shredding. Cisco KMC accommodates single- and multiple-site environments, including automatic key replication across data centers and high-availability deployments. Keys and management traffic are transported securely using the SSH, and HTTPS protocols.
- **Simplified provisioning:** Cisco MDS 9000 Family switches and Cisco SME are both managed with the same software, command-line interface (CLI), and Cisco Fabric Manager; no new management software is needed. In addition to consistent interfaces, Cisco SME supports RBAC; authentication, authorization, and accounting (AAA) servers; and VSAN-based access control for unified credentials management.

Cisco SME Features

- Offers strong AES-256 encryption of heterogeneous tape devices and VTLs
- Integrates as a transparent Fibre Channel fabric service within Cisco MDS 9500 Series and MDS 9200 Series
- Provides VSAN-independent encryption and compression services
- Load-balances traffic automatically within each fabric
- Through Cisco KMC, offers comprehensive lifecycle management for encryption keys
- Provides clustering support for highly available key management and fabric services
- Through software-only decryption, enables media recovery without the need for Cisco MDS 9000 Family hardware
- Uses smart cards to provide secure master key storage
- Meets Common Criteria (CC) EAL-3 with a Cisco MDS 9000 Family security assurance tested solution
- Provides a hardware and software architecture designed to meet FIPS requirements
- Supports all Cisco MDS 9000 NX-OS Software advanced and basic security features, such as RBAC
- Provides management through Cisco MDS 9000 NX-OS Software CLI and Cisco Fabric Manager
- For product specifications, check the Cisco Storage Media Encryption Datasheet at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps8502/product_data_sheet0900aecd8068ed59.html

Ordering Information

For ordering information, check the Cisco Storage Media Encryption Datasheet at http://www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps6028/ps8502/product_data_sheet0900aecd8068ed59.html.

For More Information

For more information about Cisco Storage Media Encryption, visit <http://www.cisco.com/en/US/products/hw/ps4159/index.html> or contact your local account representative.