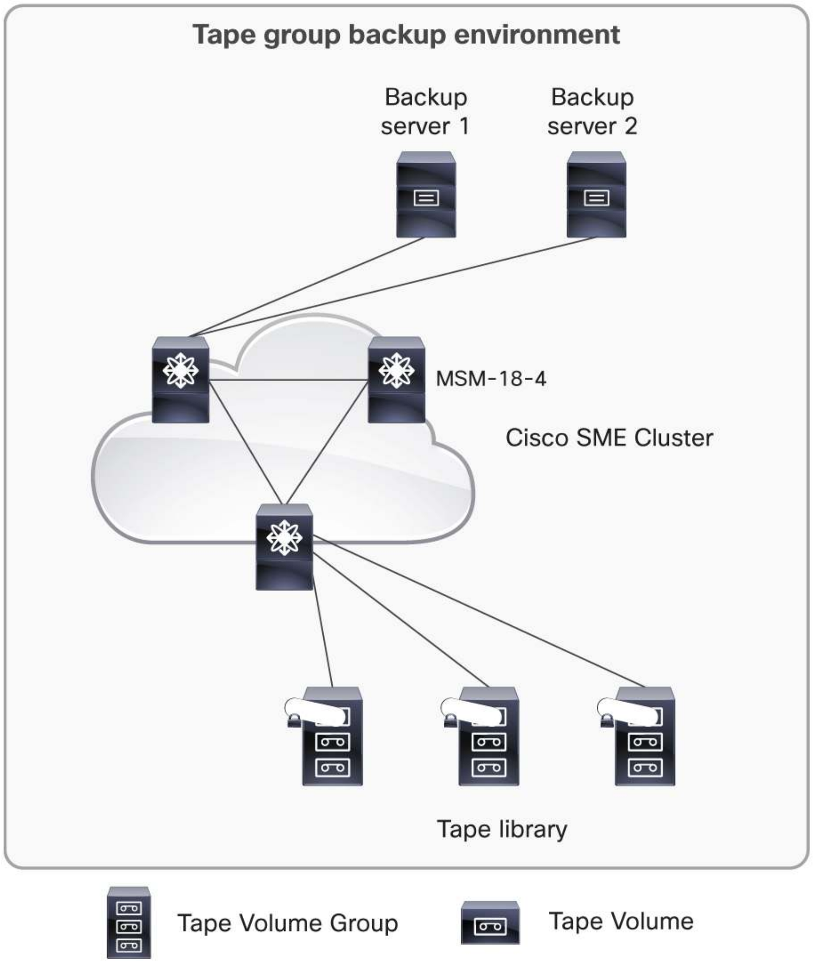
Cisco Storage Media Encryption for Tape

Product Overview

Cisco[®] Storage Media Encryption (SME) protects data at rest on heterogeneous tape drives and virtual tape libraries (VTLs) in a SAN environment using highly secure IEEE Advanced Encryption Standard (AES) algorithms.

Cisco SME hardware and software are fully integrated with the Cisco MDS 9000 Family portfolio. Encryption is performed as a transparent Fibre Channel fabric service, which greatly simplifies the deployment and management of sensitive data on SAN-attached storage devices. Unlike other approaches, Cisco SME requires no downtime to deploy. Cisco SME is built on a system architecture based on Federal Information Processing Standards (FIPS) and offers highly secure, comprehensive key management, with support for offline media recovery (Figure 1).

Figure 1. Cisco SME System



Features and Benefits

Cisco SME provides a complete, integrated solution for encryption of data at rest on heterogeneous tape drives and VTLs. Storage in any virtual SAN (VSAN) can make full use of Cisco SME, providing exceptional flexibility for provisioning this transparent fabric service. Cisco SME requires no SAN reconfiguration or rewiring, eliminating downtime for deployment.

Cisco SME employs clustering technology to enhance reliability and availability, enable automated load-balancing and failover capabilities, and simplify provisioning. To simplify management, this encryption service is provisioned as a single, logical SAN fabric feature rather than as individual switches or modules.

Secure lifecycle key management is included, with essential features such as master key rekey, key archival, key shredding, automatic key replication across data centers, high-availability deployments, and export and import for single- and multiple-site environments. Provisioning and key management for Cisco SME are both integrated into Cisco Data Center Network Manager (DCNM); no additional software is required for management.

Cisco SME includes the following features:

- Rapid, scalable deployment: Cisco SME performance can easily be scaled up by adding more Cisco MDS 9000 Family switches or modules. The innovative Fibre Channel redirect capabilities in the Cisco MDS 9000 SAN-OS and NX-OS Software enable traffic from any switch port to be encrypted without the need to reconfigure or rewire the SAN.
- High availability: Cisco SME services employ clustering technology to create a highly available solution. The cryptographic cluster enhances reliability and availability, enables automated load balancing and failover capabilities, and simplifies provisioning as a single SAN fabric service rather than as individual switches or modules. Additionally, Cisco Key Management Center (KMC) supports 1+1 high-availability deployments.
- High level of security: Cisco SME uses strong, IEEE-compliant AES 256 encryption algorithms to protect data at rest. Advanced Cisco MDS 9000 SAN-OS and NX-OS Software security features, such as Secure Shell (SSH), SSL, RADIUS, and Fibre Channel Security Protocol (FC-SP) provide the foundation for a secure FIPS architecture.
- Comprehensive lifecycle key management: Cisco KMC provides dedicated key management for Cisco SME, with support for single- and multiple-site deployments, including automatic key replication across data centers and high-availability deployments. Cisco KMC provides essential features such as master key rekey, key archival, highly secure export and import and translation for distribution, and key shredding.
- Integrated management: Cisco SME is configured and provisioned using the Cisco MDS 9000 Family command-line interface (CLI) or Cisco DCNM; no additional management software is needed. In addition to consistent management interfaces, Cisco SME supports role-based access control (RBAC) and RADIUS and TACACS+ servers for unified credentials management.

Additional features and benefits are presented in Table 1.

Table 1. Additional Features and Benefits

Feature	Benefit
VSAN independence	Traffic on any VSAN can fully use Cisco SME encryption capabilities, providing outstanding flexibility for provisioning and load balancing.
Data compression	To increase the utilization of tape media, Cisco SME provides an option to compress tape data before encrypting it.

Feature	Benefit
Smart cards	For increased operating security, smart cards are offered to protect master keys, facilitate master key escrow, and help prevent unauthorized cryptographic cluster formation and key recovery.
Investment protection	In addition to supporting heterogeneous storage devices, the multipurpose hardware used by Cisco SME supports Cisco MDS 9000 Family storage network services and applications, providing solid investment protection.

Product Specifications

Table 2 lists the product specifications for the Cisco SME.

Table 2. Product Specifications

Item	Specification
Product compatibility	• Cisco MDS 9500 Series Multilayer Directors and MDS 9200 Series Multilayer Switches • Cisco MDS 9000 18/4-Port Multiservice Module (MSM) and MDS 9000 16-Port Storage Services Node (SSN) line cards
Software compatibility	For tape drive encryption: • Cisco MDS 9000 SAN-OS Software 3.3(1c) or later and NX-OS 4.1(3a) or later • Cisco Fabric Manager 3.3(1c) or later and NX-OS 4.1(3a) or later
Protocols	• Simple Network Management Protocol (SNMP) Version 3 • SSH Version 2 • SSL and HTTPS • RADIUS and TACACS+ authentication protocols • RSA
Encryption algorithms	• RSA • AES-256
Approvals and compliance	• Payment Card Industry (PCI) Data Security Standard (DSS) 2.0 compliant

System Requirements

Cisco DCNM is used to provision and manage encryption keys for Cisco SME. The Cisco DCNM data sheet lists the system requirements. Table 3 provides a summary of the requirements.

Table 3. System Requirements

Item	Requirement
Encryption type	AES-256
Encryption strength	256 bits
Encryption targets	All major storage media: tape drives and VTLs
Compression	4-to-1 for tape
Key complexity	256-bit length and generated by random-number generator (PCS DSS 2.0 compliant)
Key management	Cisco KMC generates, tracks, and manages the keys
Host and application protection	Host and device authentication
Others	Hardware-based encryption, crypto shred for key deletion, RBAC, and rekey
Security	Smartcards for key store and quorum for recovery
High availability	Clustering architecture supporting load balancing and resiliency for crypto engines and 1+1 Cisco KMC for key management redundancy

Ordering Information

Table 4 lists product ordering information for Cisco SME licenses and components.

Cisco SME also requires Cisco MDS 9000 Family hardware modules or switches that support this feature. The following hardware includes encryption units suitable for Cisco SME:

- Cisco MDS 9222i Multiservice Modular Switch (MMS)
- Cisco MDS 9000 18/4-Port MSM
- Cisco MDS 9000 16-Port SSN
- Cisco DCNM for SAN Advanced Edition is required to run Cisco KMC. A single Cisco KMC can support a multisite deployment. Two instances provide 1+1 high availability.
- The web client (supported by Cisco DCNM for SAN Advanced Edition) provides the Cisco SME provisioning wizard. At least one instance of Cisco DCNM for SAN Advanced Edition is thus required.

For more information about ordering hardware and about Cisco DCNM requirements, see the Cisco MDS 9000 Family product literature at http://www.cisco.com/en/US/products/hw/ps4159/ps4358/index.html.

Table 4. Ordering Information

Description	Part Number
Storage Media Encryption package for one MSM-18/4 in the Cisco MDS 9500 Series	M9500SME1MK9
Storage Media Encryption package for one MSM-18/4 in the Cisco MDS 9200 Series	M9200SME1MK9
Storage Media Encryption package for one service engine on SSN-16 in the Cisco MDS 9500 Series	M95SMESSNK9=
Storage Media Encryption package for one service engine on SSN-16 in the Cisco MDS 9200 Series	M92SMESSNK9=
Storage Media Encryption package for Cisco MDS 9222i MMS fixed slot	M9200SME1FK9
Smart card reader for Cisco SME	DS-SCR-K9=
Smart card for Cisco SME	DS-SC-K9=
DCNM for SAN Advanced Edition for MDS 9500	DCNM-SAN-M95-K9
DCNM for SAN Advanced Edition for MDS 9200	DCNM-SAN-M92-K9

Note: Cisco MDS 9000 Series Switches do not need Cisco Fabric Manager Server license packages to provision Cisco SME or to use the associated key management capabilities.

To place an order, visit the Cisco Ordering homepage. To download software, visit the Cisco Software Center.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services helps you protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Advanced Services.

Using the Cisco Lifecycle Services approach, Cisco and its partners provide a broad portfolio of end-to-end services and support that can help increase your network's business value and return on investment (ROI). This approach defines the minimum set of activities needed, by technology and by network complexity, to help you successfully deploy and operate Cisco technologies and optimize their performance throughout the lifecycle of your network.

For More Information

Go to http://www.cisco.com/en/US/products/ps8502/index.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-414371-08 04/13