Cisco Storage Media Encryption Key Management

What You Will Learn

The Cisco® Storage Media Encryption (SME) solution enables hardware compression and encryption on the network before data is written to a tape device.

With the introduction of the Cisco MDS 9222i Multiservice Modular Switch and of the Cisco MDS 9000 18/4-Port Multiservice Module line card providing encryption services, the Cisco SME solution provides a distributed, highly scalable, and secure network based on the Cisco MDS 9000 family of switches and directors. It offers centralized administration and key management, simplifying the deployment and management of the solution. This document describes the Cisco SME key management architecture and options.

Data Security Landscape

In the past, only a small number of organizations adopted some of the available tape encryption technologies. Data on tape was considered relatively safe, and the risk involved was not enough to justify the additional cost, slower performance, and additional operation procedures.

Recently, new conditions have caused the risks associated with tape data loss to be seen as much more critical:

- More stringent privacy regulations: Private data stored in electronic form is subject to privacy laws such as the European Union (EU) Directive on Privacy and Electronic Communication (2002), and the Japanese Bill to Protect Personal Data (2001). A growing number of U.S. states have privacy regulations in place, and several bills were introduced in the U.S. Congress in 2005. The Visa and MasterCard Payment Card Industry Data Security Standards (PCI DSS) and the Japan Bank Association's Data Protection Support standards are more examples of data privacy demands on technologies.
- Public disclosure of data breaches: The California Database Breach Act (California Senate Bill [SB] 1386, 2003) requires that any data breach involving the private data of a California citizen be announced to the public. As a consequence, most data breaches associated with lost or stolen clear-text tapes require organizations to alert customers, provide credit monitoring, and perform damage control, and potential losses may be millions of U.S. dollars.
- Long-term data retention requirements: Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Securities and Exchange Commission (SEC) Rule 17a-4 demand long-term retention of records. Tape is often used for data archiving, and tape encryption can be used to keep the data confidential and tamper-proof.

Tape encryption is now widely regarded as a necessity. In addition, new technology options are making implementation of a solution that secures data on tape less costly in term of capital expenses and maintenance.

Although tape encryption can be seen as an insurance policy for dealing with the threat of lost or stolen tapes, this technology must be integrated into the security procedures of the tape-based business processes, and this objective must be achieved without creating too much operational overhead. Tape-based business procedures that pose requirements on the key management infrastructure include:

- Data sharing, which requires the sharing of encryption keys among business partners
- Data archiving, which requires a key lifecycle solution built for long-term storage of encrypted data
- Disaster recovery, which requires encrypted data to be decrypted at a secondary site after a disaster, making tape encryption operations such as key management, backup, and restoration part of the disaster planning and business-continuity process

The Cisco SME solution, integrated into a SAN based on the Cisco MDS 9000 family of switches and directors, is capable of compressing and encrypting the data being copied on tape while respecting all the requirements mentioned here. In addition, the actual cryptographic processing is performed in a distributed and scalable fashion on high-speed secure processors, and key management and administration are centralized for operational efficiency.

Cisco SME Overview

Cisco SME is a service that enables the secure storage of data that resides on the tapes in a SAN environment.

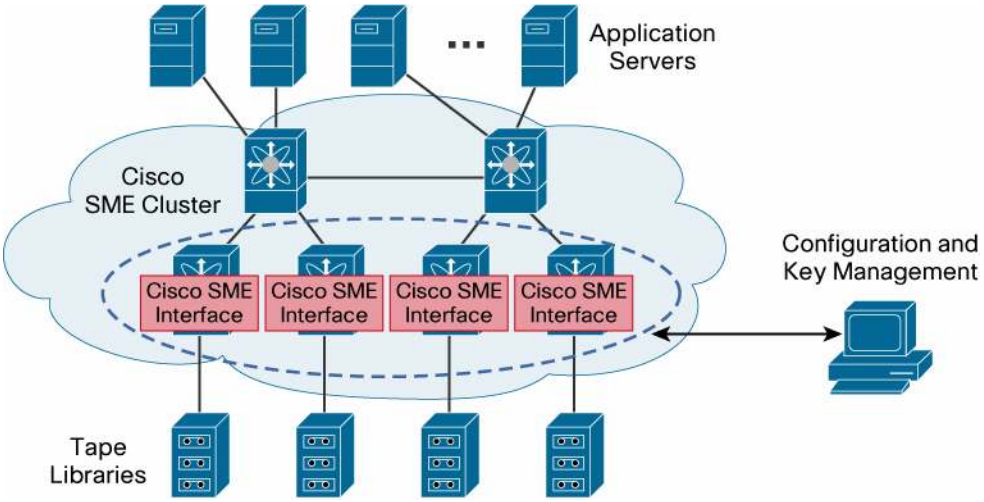
Cisco SME Hardware Components

The Cisco SME service is executed by security processing engines, known as Cisco SME interfaces. Each Cisco MDS 9000 18/4-Port Multiservice Module or Cisco MDS 9222i switch (without the optional line card) has a single Cisco SME interface. The Cisco SME interfaces are distributed in the various Cisco MDS 9000 family modular switches and directors in the fabric.

The Cisco SME interface can intercept the traffic generated by a host to a tape and encrypt it before it reaches the target. Similarly, the interface intercepts the traffic generated by a target to be routed to a host and decrypts it before forwarding it to the host. The capability of a Cisco MDS 9000 family switch or director to selectively reroute a specific flow of data to a Cisco SME interface located anywhere in the fabric is called Fibre Channel redirect.

Within a single physical fabric, the Cisco SME cluster helps ensure high availability of the Cisco SME service. The Cisco SME cluster is a collection of one or more nodes and a Cisco MDS 9000 family switch or director carrying at least one Cisco SME interface (Figure 1). One node can be equipped with one or more Cisco SME interfaces, but all cluster nodes share the same security context. Although a one-node cluster can provide all the Cisco SME functions, a cluster with at least two nodes helps ensure the high availability of the solution. A single cluster can be composed by up to four nodes.

Figure 1. Cisco SME Cluster



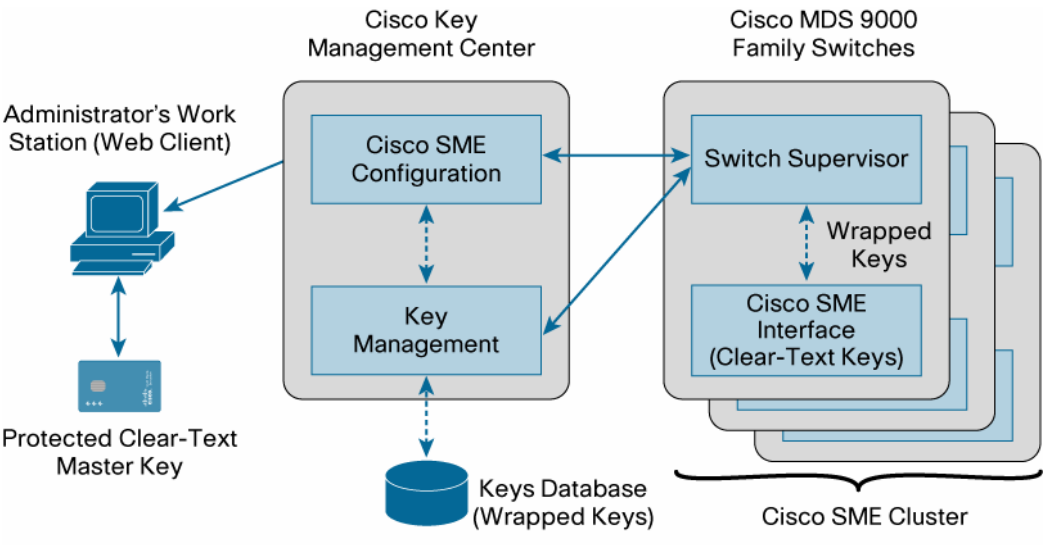
Cisco SME Configuration and Key Management

Configuration and management is performed using a simple web application integrated into the web client connected to the Cisco Fabric Manager Server (FMS). The web application allows the administrator to create and configure a Cisco SME cluster, create the encryption association between a given host and a given target, and group the physical tapes subject to different security policies.

The Cisco Key Management Center (KMC) is the centralized key management system that takes ownership of the lifecycle of keys used to encrypt and decrypt the data. Cisco KMS administration is performed through the same easy-to-use web application, embedded in the Cisco FMS web client, used to configure Cisco SME clustering and resources. Notice that the keys stored in the Cisco KMC are in encrypted form and cannot be used without access to the highest-level key-encryption key, the master key (Figure 2).

The Cisco FMS web client computer can provide the smart card driver to program the smart cards used for key recovery.

Figure 2. Cisco SME Configuration and Key Management



Cisco SME Media Format

The Cisco SME service uses an innovative (patent-pending) technology to store the information required to support encryption and media management.

When a backup application labels a tape, Cisco SME writes some control information, called the Cisco Tape Header, on the first block of the tape to be encrypted. The Cisco Tape Header stores per-tape global information such as the tape globally unique identifier (GUID). The original media header, generated by the backup application itself, is written on tape after the Cisco Tape Header; then the original data blocks follow.

The original data blocks, including the backup application header, are (optionally) compressed and then encrypted.

Key Management and Security Architecture

The keys are the most important and sensitive pieces of information in a cryptographic solution. For this reason, all the keys in the system are encrypted, or wrapped, using a higher-level key. The process of protecting a key by encrypting it with a higher-level key is called key wrapping, and the higher-level key is called the key-encrypting key (KEK). The keys are identified across the system by a GUID.

Tapes and Tape Groups

Large numbers of physical tapes, or tape volumes, are organized by the Cisco SME administrator into groups, and each group can be used for a different purpose. For example, a group can be dedicated to a specific user group, associated with a specific backup application, or used to provide data to a third party.

A tape volume group is a collection of tapes whose bar code matches a filtering criterion or the tapes that are accessed by a specific backup application. A tape can be manually assigned to a tape volume group using the bar code option, or it can be assigned automatically to the tape volume group associated with the specific backup application.

Key Hierarchy

The key at the highest level, which must ultimately be stored as clear text, is called the master key. Since the master key is in clear text, it is stored only in a highly secure location or, for recovery purposes, in a password-protected file or in one or more smart cards.

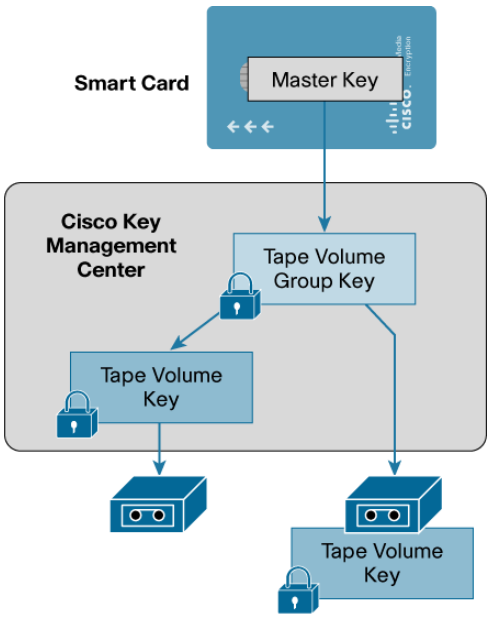
Since all the keys stored in the Cisco KMC are in wrapped format, if the contents of the Cisco KMC database are compromised, the keys are unusable and the data is safe. Notice that, as required by the FIPS 140-2 certification, any attempt to tamper with the crypto module or with a smart card results in the destruction of the resident keys, so the master key itself cannot be improperly extracted from these systems (Figure 3).

The keys are encrypted according to the following hierarchy:

- Master key: This key is generated in the crypto module at the time of Cisco SME cluster creation. It is the most critical piece of information in the security context of any given cluster, and it is unique and shared across all the cluster members. The master key is used to wrap the tape volume group keys when exporting them outside the crypto boundary: for instance, to be stored on the Cisco KMC.

- Tape volume group key: This key is used to encrypt and authenticate the tape volume key of all the tapes belonging to the same tape group. A tape group can be selected on the basis of the bar code of the tapes or can be associated with a specific backup application.
- Tape volume key: This key is used to encrypt and authenticate the user's data in the tapes. The tape volume key is unique on a per–physical tape basis and can be stored in the Cisco KMC or on the physical tape itself. The Cisco KMC database does not need to store the tape volume keys if the key is on the tape, dramatically reducing the number of keys to be stored in the Cisco KMC. If the user knows the tape volume group key and if the tape volume key is on the tape, the tape can be decrypted; as a consequence, this option poses some limits to virtual shredding of an individual tape.

Figure 3. Key Hierarchy



Key Storage Locations

Figure 4 summarizes the locations where keys can be stored. Note that keys are always encrypted or password protected unless they are resident on secure hardware or in a password-protected file.

Figure 4. Key Storage Locations

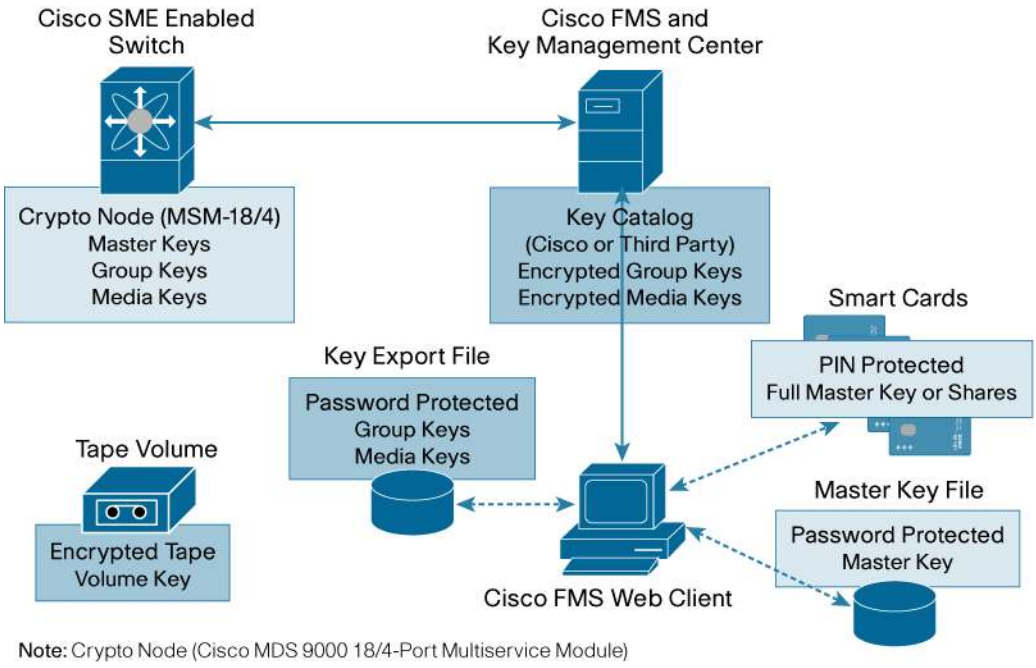


Table 1 describes the location, format, and rationale for the format in which the keys are stored.

Table 1. Key Locations and Formats

Location	Keys	Format	Reason
Crypto Node	Permanent storage: • Master key Stored only when in use: • Tape group key • Tape volume keys	Clear text	• Master key: Used to encrypt and decrypt the other keys • Tape volume key: Used to encrypt and decrypt the tape volume key • Tape volume keys: Used to access data
Cisco KMC Key Catalog	• Tape group key • Tape volume keys	Encrypted (use master key)	Long-term repository
Key Export File	• Tape group key • Tape volume keys	Encrypted (use password)	Backup and distribution
Tape Volume	Tape volume key	Encrypted (use tape group key)	Long-term repository; simplification of key management operations
Master Key File	Master key	Encrypted (use password)	Cluster recovery (basic security level)
Smart Cards	Master key	Encrypted	Cluster recovery (standard and advanced security levels)

The following sections describe the functions associated with the key storage locations and the associated procedures and options.

Master Key Security Levels

A Cisco SME cluster has a master key context, which is created when the first interface is added successfully to the cluster. When new interfaces are added to the cluster, the master key context is synchronized from an existing interface. Thus, if the last interface is removed from the cluster, the master key context will be permanently lost from the Cisco SME cluster.

The master key is the single piece of information that can enable the ultimate recovery of the key database, and consequently of the data, if the Cisco SME cluster totally fails. Cisco SME provides

recovery shares of the master key stored in the external smart cards (or password-protected files) for failed-cluster recovery operations.

During cluster creation, the administrator can choose among three master key security levels: basic, standard, and advanced.

Basic Security Level

With the basic security level, the master key is stored in a password-protected file. By providing the file and the password, the Cisco SME recovery officer can recover the master key and unlock the key database. The key file must be stored in a secure location, possibly in multiple copies.

- Advantages and limitations: Basic level provides a simple way to store the master key, but preventing a malicious user from getting a copy of the key file may be difficult. After gaining possession of a copy of the key file, the malicious user can try to learn the password to open the file and unlock the key database.
- Recovery procedure: The recovery procedure is performed on the Cisco FMS web client by a single recovery officer by submitting the password-protected file and entering the password.

Standard Security Level

With the standard security level, the master key is stored in a PIN-protected smart card. By providing the smart card and the PIN, the Cisco SME recovery officer can recover the master key and unlock the key database. The smart card must be stored in a secure location; it is advisable to generate more than one smart card for redundancy.

- Advantages and limitations: Standard level provides a simple way to store the master key, since a single recovery officer can perform the recovery operation. However, a malicious user needs just a single smart card and the PIN to be able to unlock the key database.
- Recovery procedure: The recovery procedure is performed by a single recovery officer on the Cisco FMS web client, by submitting the smart card and entering the PIN.

Advanced Security Level

With the advanced security level, the information needed to generate the master key is stored in multiple PIN-protected smart cards. At cluster creation, recovery officers must each provide a smart card and select a PIN. Two or three smart cards are needed to provide enough information to recover the master key. By providing the required number of smart cards and associated PINs, a quorum of two or three Cisco SME recovery officers can recover the master key and unlock the key database. The smart cards must be stored in a secure location. In a five-card set, if two smart cards are required, three are for redundancy; if three are required, two are for redundancy.

- Advantages and limitations: Advanced level is complex, since it requires the involvement of five recovery officers at cluster creation time and of the specified number of recovery officers to recover the master key, but it provides a high level of security. The specified quorum of recovery officers must approve and contribute to the recovery operation; as a consequence, a malicious user would need to obtain multiple smart cards and PINs.
- Recovery procedure: The recovery procedure is performed by the specified quorum of recovery officers on the Cisco FMS web client; each officer is prompted in sequence to submit his or her smart card and to enter the associated PIN.

Smart Card Management

With the standard and advanced security levels, the information needed to recover the master key is stored on one or more PIN-protected smart cards. Thus, the cards must be stored in a safe but easily accessible place, and the PINs must be recorded in a different location.

- Single smart card: In standard mode, a single smart card is enough to recover the master key. It is advisable to initialize at least three smart cards in case one or two get lost or damaged.
- Multiple smart cards: In advanced mode, two or three smart cards out of five are required. Two or three spare cards should be available in case some get lost or damaged.

Note that the same smart card can be used for up to eight different clusters, so the same person can be the recovery officer in different locations using the same smart card.

Best practices require that smart cards be stored in a safe place, such as a bank safety deposit box, or that they be given to a third-party authority that can act like an escrow account to protect the data and police access.

Table 2 describes the best approach for long-term master key management and storage.

Table 2. Master Key Management and Storage Options

Master Key Security Level	Redundancy	In Escrow	In Use
Basic	Create multiple copies of the master key file (password protected)	One or more copies	One or more copies
Standard	Create multiple copies of the recovery smart card (PIN protected)	One or more smart cards	At least one smart card
Advanced	Create three or five smart cards (PIN protected)	All remaining smart cards (for example, two)	The specified number of smart cards (for example, three)

Cisco Key Manager Center

The Cisco KMC is responsible for archiving the cryptographic keys generated and used by the crypto modules. Such cryptographic keys may be cipher keys or key wrapping keys.

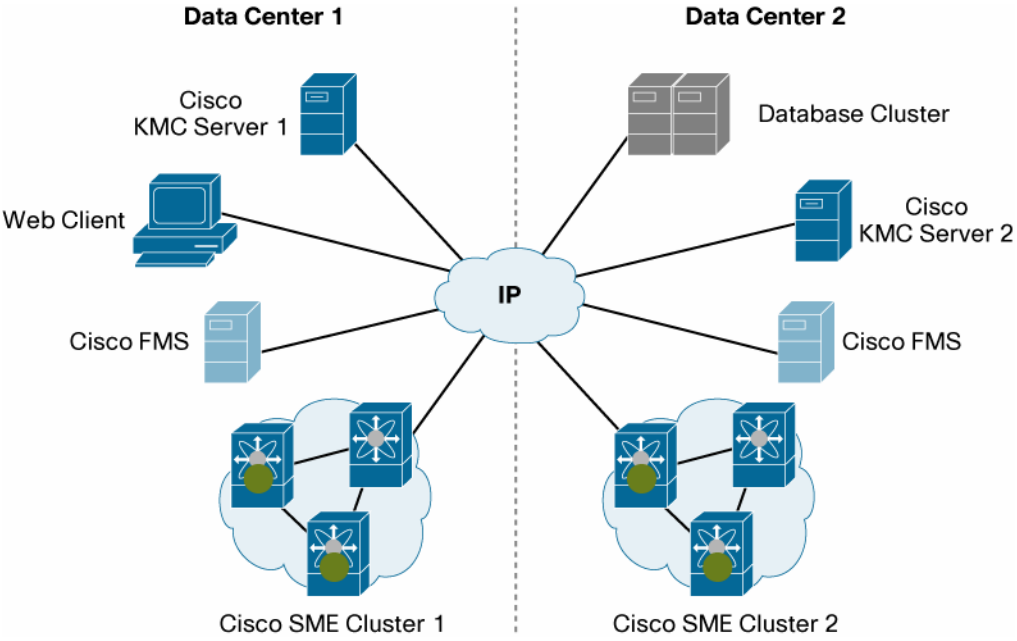
High Availability

Cisco KMC provides a high-availability solution for key management. Clusters can be configured with both primary and secondary Cisco KMC servers along with a high-availability database. High availability for Cisco KMC is achieved using primary and secondary Cisco KMC servers. Each Cisco SME cluster can be configured with primary and secondary Cisco KMC servers. The KMC servers can be located in different data centers to reduce the risk of loss of any one data center.

The solution uses a high-availability key database that is shared by the primary and secondary Cisco KMC servers. The primary KMC server is preferred for all key transactions. If the primary server fails, Cisco SME triggers automatic clusterwide failover to the secondary server until the primary Cisco KMC server recovers. Figure 5 shows a Cisco KMC high-availability topology spanning two data centers.

This feature also facilitates transparent scheduling of maintenance operations on the Cisco KMC servers, without interruption of key and tape media access.

Figure 5. High-Availablity Cisco KMC Configuration



Key Catalog Dimensions for Shared-Key Mode, Individual-Key Mode, or Keys on Tape

If the tape volume key is individual per tape, the tape volume key is not stored on tape and the tape groups are large, the maxiumum number of keys qualified for the Cisco KMC becomes the limiting factor for the number of tapes that can be managed. The actual Cisco KMC key catalog limits are listed in the Cisco MDS 9000 Family Storage Media Encryption Configuration Guide.

To increase the number of managed tapes, Cisco SME provides the option of storing the tape volume key on the tape itself. In this case, the tape volume keys for individual tapes are not stored in the Cisco KMC, but the Cisco KMC stores the tape group key only, leading to an essentially unlimited number of managed tapes. Shared-key mode also greatly reduces the number of tape volume keys, providing benefits similar to those of keys stored on tape. These options impose some restrictions on the capability to virtually shred an individual tape.

Deployment of Third-Party Key Managers

An organization may be willing to consolidate the keys used throughout different systems and applications, as well as those used by different storage media encryption technologies, in a single repository. Using a single repository can simplify administrative procedures such as access control and regular backup.

Cisco SME supports third-party key managers, providing a mechanism for storing Cisco SME preexisting keys as well as new keys. The generation of keys is still performed by the highly secure crypto module, and all the keys leaving the crypto module are in wrapped format.

The wrapped key data loaded into third-party key managers is treated as opaque data, since there is no need to know the attributes associated with a key such as the generation algorithm or the key size.

The lifecycle of the key is still administered by the Cisco SME KMC, using an API. The keys used by Cisco SME are uniquely identified in the third-party key manager using the key GUID.

Backup of Key Database

Keys are critical for restoring data from encrypted tapes, so special care must be devoted to backing up all key information. Backup can be performed using the procedures described here.

Backup of Key Database

The key database used by the Cisco KMC to store the keys is subjected to regular backup, like any other database in the enterprise.

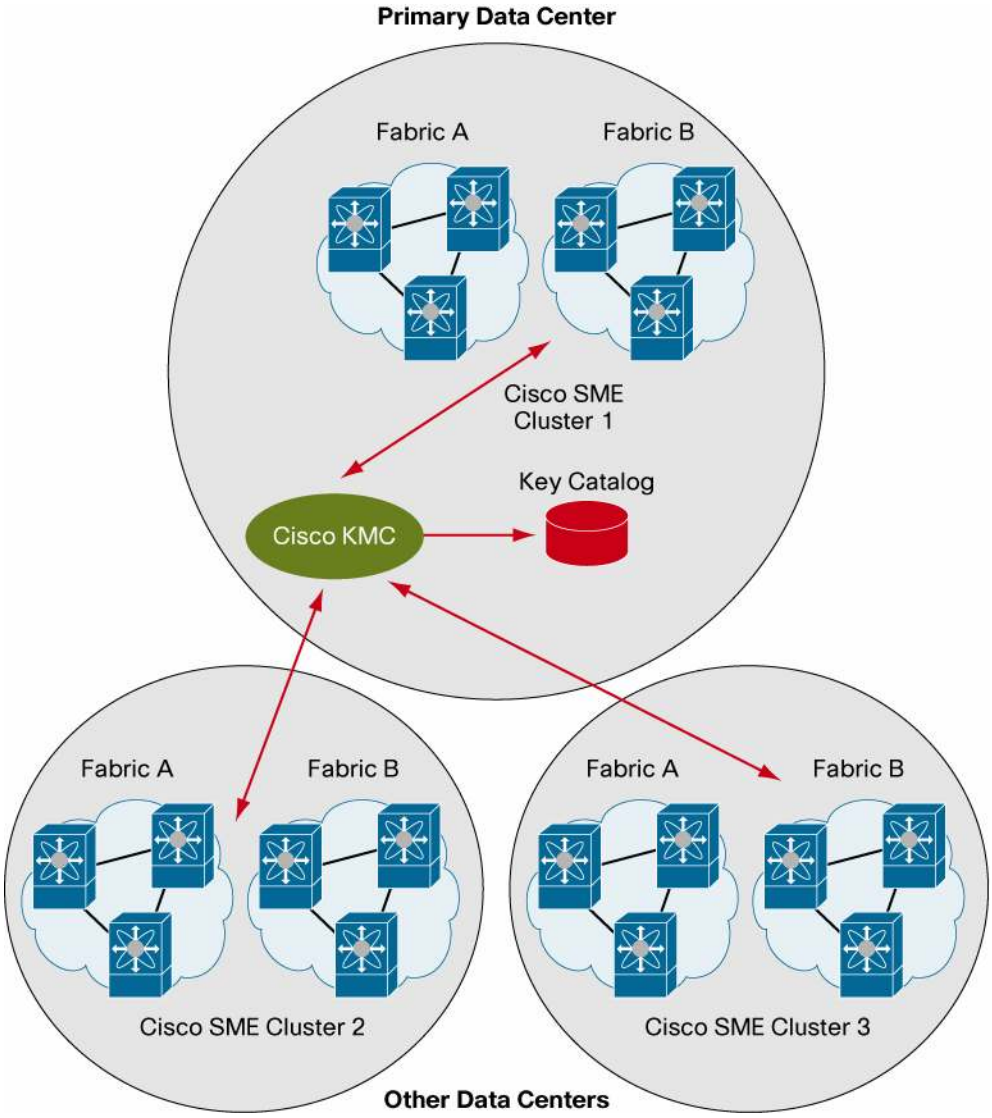
- Advantages: The key data is treated homogenously like any other critical data in the organization and can be subjected to the appropriate policy.
- Limitations: Unless the Cisco SME administrators have direct control over when the backup is performed, care must be taken to avoid missing important new keys in the backup operation. Also, this method still requires the security officers to perform an export to the password-protected key catalog file if the Cisco SME cluster is lost (see “Cluster Failure Recovery” later in this document). This method also is not suitable for transferring data to a third party.

Remote replication

Keys are replicated across clusters in different data centers or across data centers and disaster recovery sites using remote-replication rules (Figure 6). Replication automates the translation of the key hierarchy from one cluster to another, thus eliminating manual key export and import operations. Remote-replication rules can be created for each volume group between one Cisco SME cluster and another Cisco SME cluster, which may be located in a remote data center.

- Advantages: Keys are automatically copied at the scheduled interval across data centers and disaster recovery sites. Configuration is simple and performed once for each volume group. Keys in each volume group can be replicated to multiple clusters. In addition, replication does not require the direct involvement of the security officers and use of smart cards.
- Limitations: Replication is performed on online clusters only, because the operation is performed on the switches. Also, both the source and target clusters must be maintained by the same Cisco KMC.

Figure 6. Remote Replication



Export to a Password-Protected Key Catalog File

Keys can be exported to a password-protected file that can be imported later to populate the Cisco KMC database.

- Advantages: The procedure is simple: the file can be easily copied, stored, and shared with a third party. In addition, restoration does not require the direct involvement of the security officers and the use of smart card. Further, the export can be for a specific tape volume group only, to share a specific volume group with a third party.
- Limitations: An export operation must be performed every time a new key is generated, a process most convenient when using the same key across a group of tapes (shared key mode). In addition, care must be taken when using the Auto Volume Group option, since the creation of a new tape group can be automatic.

Auditing Log

All procedures related to key management, such as the export of the key data to a file, are logged for auditing purposes.

User Roles

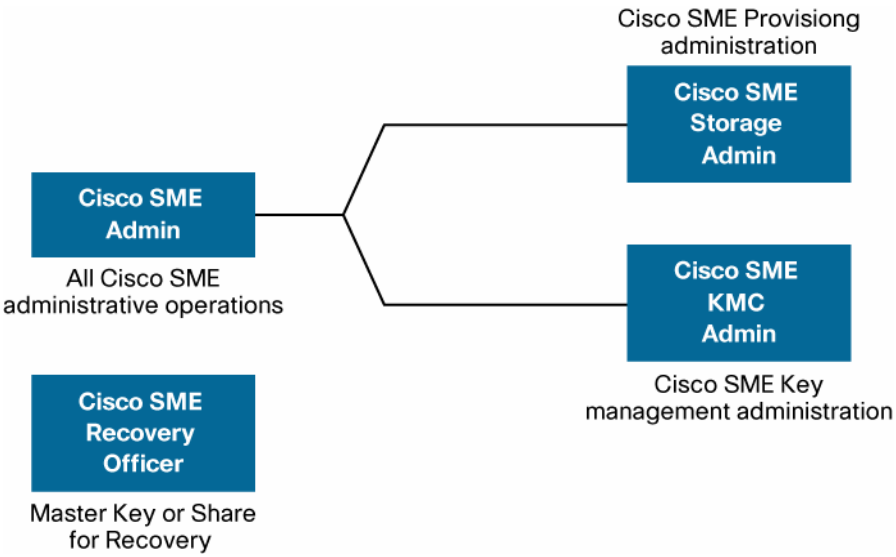
Data management and protection requires user roles that map to the different responsibilities and daily activities of the people in charge of administering the security of data at rest (Table 3).

The Cisco SME recovery officers are a group of trusted individuals charged with recovery of critical key data. Smart cards are provided only to the recovery officers, one each, who are likely senior managers in the organization and not involved in the day-to-day administration of the system. The specified quorum of recovery officers is required for any recovery operation. The default is two out of five, to help ensure that no single person can threaten the security of the data. According to this model, the Cisco SME recovery officer role is limited to master key recovery.

The operations related to the configuration of the SME service are executed by Cisco SME storage administrator. All operations related to key management are executed by the Cisco SME KMC administrator. Actions by all users can be audited using authentication, authorization, and accounting (AAA) log procedures and system logging.

The Cisco SME administrator role has the authority to execute operations related to both Cisco SME storage administration and key management administration (Figure 7). Note the potential threat that an administrator may compromise the security of the data at rest, even though actions are audited, but a security administrator is expected to be a highly reliable member of the organization.

Figure 7. SME Management Roles



All other day-to-day operations not specific to Cisco SME but involving storage and SAN management are performed by the SAN administrators, as defined for the underlying Cisco MDS 9000 family fabric.

Table 3. Cisco SME User Roles

Role	Responsibilities
Cisco SME Administrator	• Cluster configuration, including addition and removal of switches and nodes • Cisco KMC configuration and operation • VSAN-based restriction may be enforced in this role if required • Cisco SME storage administrator and Cisco SME KMC administrator roles are subset of Cisco SME administrator role

Role	Responsibilities	
	Cisco SME storage administrator	• Cisco SME provisioning, but not key management operations • Includes cluster creation and deletion and addition and removal of nodes, Cisco SME interfaces, tape groups, tape devices, volume groups, etc.
	Cisco SME KMC administrator	• Key management operations, but not Cisco SME provisioning • Includes addition, removal, export,, import, and rekeying of volume groups; archival and purging of keys; rekeying and replacement of smart cards; etc.
Cisco SME Recovery Officer	• In basic and standard modes, possesses the master key, either in a file or on a smart card • In advanced mode, possesses one recovery share of the master key on a smart card; quorum is required for any operation involving master-key recovery	

Media Key

The tape volume key, or media key, is the actual key used to encrypt user data. Cisco SME supports some options for the generation and archival of the tape volume key. The following sections describe the available options and their practical implications.

Cisco SME Cluster Options

Several clusterwide parameters need to be set before creating a tape backup group:

- Key mode: To achieve a high level of security, each individual tape is assigned its own unique key, working in individual-key mode. To simplify key management procedures and reduce the size of the key database, the cluster can optionally use the same key for all tape volumes belonging to the same group, working in shared-key mode. If the common key, called the tape volume group shared key, is compromised, all the tapes are compromised.
- Key on tape: This option allows storage of the media keys on the tape itself. The tape volume keys are wrapped with the tape volume group key for protection. In this mode, these keys are not stored in the Cisco KMC, increasing scalability to support a large number of tape volumes. This option simplifies export of tapes to a remote site, since there is no need to export the media keys routinely; the wrapping tape volume group key can be exported just once. Note that if the key is on the tape and the tape volume group key is compromised, all the tapes are compromised.
- Volume group mode: A group of physical tapes, also known as volumes, can be manually identified on the basis of the cartridge bar code or can be assigned automatically to a group by the backup application.
- Tape compression: Tape compression must be performed before encryption, since the compression ratio for encrypted data is usually very low. This option enables data compression to be performed by the crypto module. Note that Cisco SME does not prevent the backup application from configuring the tape driver in the compression mode, but if compression is enabled in the cluster, you are advised to disable compression in any other element of the backup system.
- Tape recycle: This option controls the way that the media key used for a tape cartridge is managed when the specific tape is labeled again by the backup application. Note that one or more copies (clones) of the original tape may have been generated outside the Cisco SME environment, with the goal of having redundant physical copies of the data located, for instance, in different geographical locations. If a tape is recycled, when labeling occurs a new media key is generated and the previous media key is purged from the Cisco KMC database. All copies of the original tape are virtually shredded. If a tape is not recycled, a new media key is generated and will be used for the given tape, but the old media key will

be left in the Cisco KMC database. As a consequence, any copy of the original tape will still be readable.

Key Management

Key management is the set of operations related to the creation, archival, retrieval, purging, and delivery of keys. All these operations can be performed through the web-based Cisco FMS client interface.

Key Export for Archival

Keys can be exported from the Cisco KMC database as a password-protected file, which can be safely stored. The file can contain a copy of the entire database, to perform a full backup, for instance; or it can be limited to a specific tape volume group, to transfer a group of tapes to a partner, for instance.

Key Shredding

Because an encrypted tape is practically unreadable unless the associated keys are known, encrypted tapes can be virtually shredded just by purging the encryption key. This option is very convenient since it does not require physical destruction of expensive media or use a time-consuming zeroing procedure.

The same tape volume group key wraps the tape volume key for all the tapes within the group; as a consequence, all the tapes belonging to the same volume group can be virtually shredded by deleting the tape volume group key. It is a good practice to create tape groups small enough to allow virtual shredding of the entire group. A group too large will likely include tapes that cannot be shredded, preventing the administrator from taking advantage of the virtual shredding option.

If an individual tape must be shredded, the process is different depending on whether the tape volume key has been stored on tape. If the tape volume key is not on tape but is archived in the Cisco KMC only, deleting this key from the Cisco KMC is sufficient to virtually shred the tape.

If the tape volume key has been stored on the tape itself, the tape volume group key must be deleted. If the tape group does not include any tape that must be preserved, the tape volume group key can be deleted, virtually shredding all the tapes in the group, including the specific tape that was to be shredded. If one or more tapes in the group must be preserved, the only option is to physically shred the individual tape.

Note that virtual shredding is a very practical option when the key are secure and the objective is to purge obsolete data, but physical shredding is still needed when a key has been compromised.

Delivery of Tapes and Keys to a Partner or Third Party

Tapes in a tape volume group can be given to any third party for auditing or for any other legitimate purpose. The Cisco SME administrator can export all the keys associated with a given tape volume group to a password-protected file. The third party can import the keys from the password-protected file to easily retrieve the data from the tape devices.

The file contains:

- Tape volume group key used for wrapping the tape volume keys for the tapes in the group
- Tape volume group shared key if in shared-key mode
- Tape volume keys if the tape volume key is not on tape

The file does not contain the cluster master key, since each key is unwrapped and then rewrapped in the file using the password provided by the user. This procedure is performed in the secure crypto module, but the master key does not leave the crypto boundaries, and it is never shared with the third party.

The password-protected file is imported by the third party into its own Cisco SME installation, in an existing cluster. The keys, contained in the password-protected file, are first unwrapped and then rewrapped in the security context and within the crypto boundaries of the new Cisco SME cluster. The third party needs only the export file and the password to perform the import operation.

Key Management Using Media Key Options

Table 4 describes how the media key options, selected at cluster creation time, affect the media and key management operations.

Table 4. Key Management Operations Using Media Key Options

	Shared Key Across a Group of Tapes: Media Key Stored in Catalog	Unique Key per Tape	
		Media Key Stored in Catalog	Media Key Stored on Tape
Advantages	• The catalog size is reduced. • A single key allows decoding of all tapes in the group, which is very practical when a single backup spans multiple tapes or when a group of tapes is shared with a third party. • If a tape volume group key is compromised, the hacker still needs to access the catalog to access the data.	• This approach is more secure. • Each tape can be managed or transferred to a third party independently. • If a tape volume key is compromised, only the given tape can be accessed. • If a tape volume group key is compromised, the hacker still need to access the catalog to access the data	• The catalog size is reduced. • A single key allows decoding of all tapes in the group, which is very practical when a single backup spans multiple more tapes or when a group of tapes is shared with a third party. • The tapes in a group use different media keys, making the solution cryptographically more secure than when the same key is used for many tapes.
Limitations	• This approach is less secure. • If the single common tape volume key is compromised, all the tapes in the group can be accessed.	• The catalog contains an entry for each tape, so the catalog may be very large.	• If a tape volume group key is compromised, a hacker can decrypt the tape volume key and the data of all tapes in the group.
Recovery Procedure	• Key export is required only when a new tape volume group is created, either manually or by automatic grouping.	• Key export is required every time a tape volume is labeled.	• Key export is required only when a new tape volume group is created, either manually or by automatic grouping.
Shredding Implications	• Only a tape group can be shredded.	• Shredding can be performed at the individual tape level.	• Only a tape group can be shredded.
Tape Recycling	• The key catalog size remains constant.	• The key catalog adds a new entry every time a tape is relabeled, unless the recycle option is selected.	• The key catalog size remains constant.

Recommendations for Key Settings

- Small to medium-sized SAN environments: Unique-key mode provides a high level of security.
- Large SAN environments with stringent security policies: Unique-key mode with key on tape provides scalability along with a high level of security.
- Large SAN environments with less stringent security policies: Shared-key mode provides a scalable data encryption solution.
- SAN environments requiring offsite tape duplication: Tape recycle mode should be disabled

Cluster Failure Recovery

Any recovery procedure requires the availability of the key catalog contents and of the master key to enable the group and media keys stored in the catalog to be unwrapped.

To prevent any data loss from failures, the Cisco SME administrator should employ the following practices:

- Configure high availability for the Cisco KMC server.
- Configure high availability for the key database.
- Schedule regular backups for the key database.
- Configure a remote cluster with remote key replication.

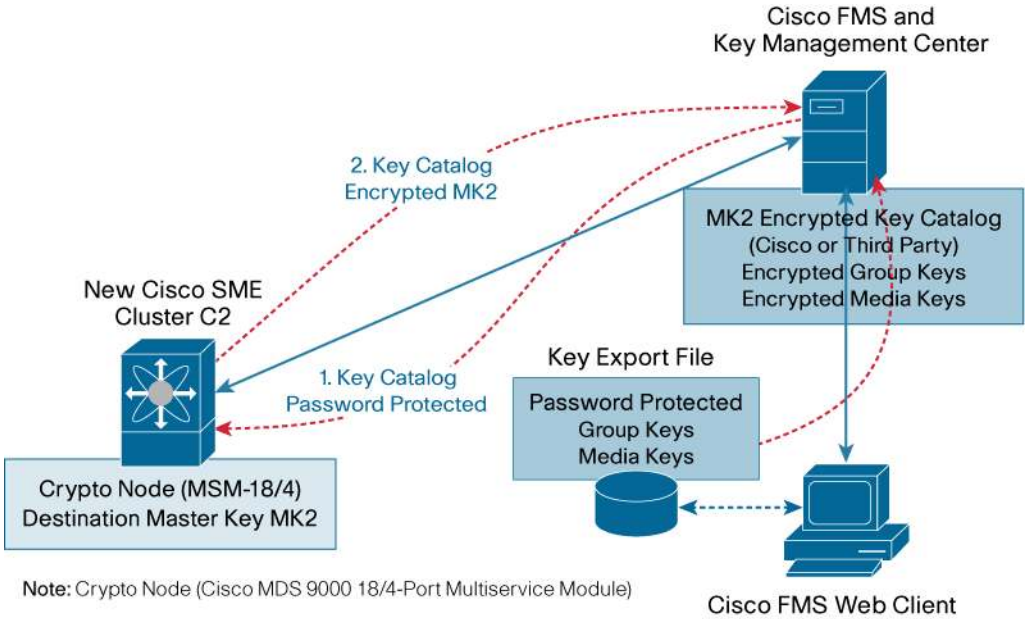
Failures in Cisco KMC servers or the key database without the loss of the Cisco SME cluster can be recovered by rebuilding or reinstalling the Cisco FMS and restoring the key database.

Data recovery in the case of an offline or decommissioned cluster or loss of the data center requires generation of a new key catalog password-protected file using an export operation followed by an import operation in the new cluster. The generation of a new key catalog password-protected file is logged for auditing purposes. This key catalog password-protected file should be stored with care. When unlocked with the password, it includes all the information needed to access the data from the original cluster.

Data Recovery Example Using the Key Catalog Password-Protected File

The file containing the keys of the original cluster C1 can be imported on an existing secondary cluster C2 to insert the saved keys in an existing key catalog; this step requires knowledge of the file password. After this procedure, the keys in the catalog are encrypted using the master key of the secondary cluster (MK2), and the tapes are accessible. Figure 8 shows the process.

Figure 8. Key Import from Password-Protected File



If for any reason the key catalog password-protected file is obsolete or not available, but the Cisco KMC and the key catalog are still available, the data can be recovered using the archived cluster recovery procedure.

Note that the hardware failure of the last Cisco SME interface in a cluster causes definitive loss of the cluster and of the associated security context because the only clear-text copy of the master key is no longer available in the fabric to unwrap the key catalog information.

In case of definitive loss of the cluster, assuming that the master key file and the associated password are available or that a quorum of the recovery officers' smart cards is present, the master key can still be used to decrypt the key catalog by following the archived cluster recovery procedure.

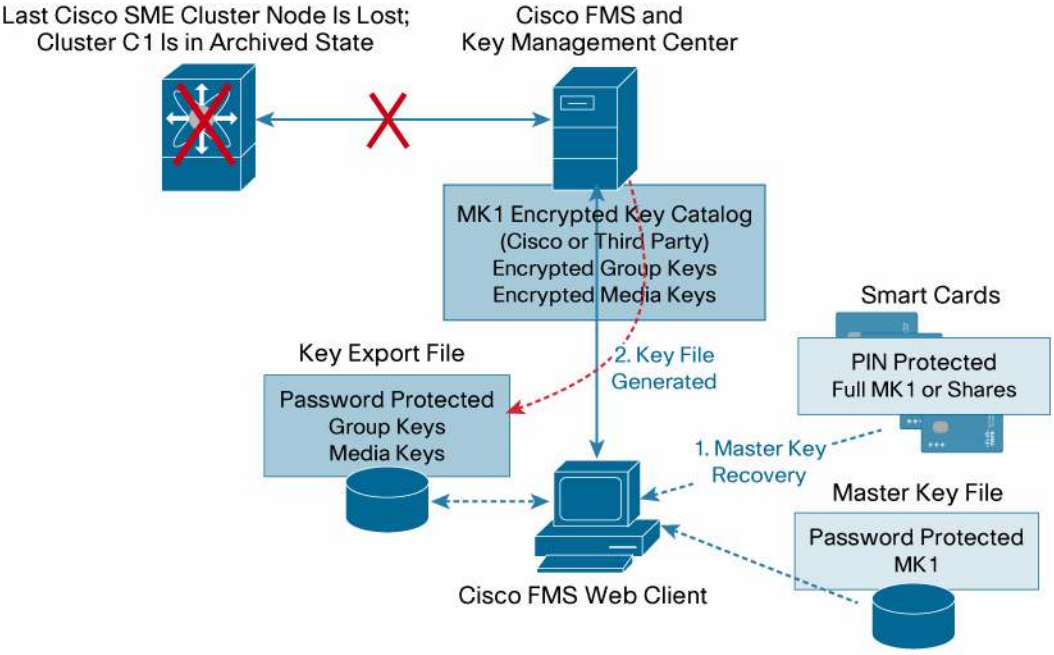
Data Recovery Example Using the Archived Cluster Recovery Procedure

The archived cluster recovery procedure, performed at the Cisco KMC, decrypts the surviving key catalog database using the original master key MK1.

The whole process is performed at the Cisco KMC and requires loading of the master key MK1 from the master key file or from the smart cards. After the master key is available, the keys stored in encrypted format in the key catalog database can be translated and exported to a key catalog password-protected file. This file is ready to be imported into any secondary cluster C2 and to be wrapped using the secondary cluster master key MK2. Figure 9 shows this process.

Notice that the last part of the archived cluster recovery process is exactly the same as the process when an updated key catalog password-protected file is available from the start.

Figure 9. Archived Cluster Key Export



Total Loss of Data Center: Both Cisco SME Cluster and Key Catalog Database Are Lost

In a total-loss scenario, the entire primary data center has experienced a local disaster, so both the cluster hardware and the local key catalog are unavailable. The disaster recovery procedure requires restarting of the Cisco SME service in the secondary data center. This procedure involves the recovery of an archived Cisco SME cluster in a different geographic location.

As a normal backup procedure, the original encrypted tape media, or their clones, must be shipped from the primary location to the secondary site. The key catalog database must be restored from its latest backup. Install a new Cisco KMC server with the database pointing to the restore key catalog database. The Cisco KMC server will retrieve the original cluster from the primary database in archived status. From this point, the key catalog password-protected file can be generated using an export operation as detailed in the section “Data Recovery Example Using the Key Catalog Password-Protected File” earlier in this document.

In the secondary data center, the keys can be imported from the key catalog password-protected file for use in an existing Cisco SME cluster in the secondary data center.

The simple operation of importing the password-protected file does not require the recovery officers.

To import the key catalog from the password-protected file, the administrator of the secondary Cisco SME cluster needs to know the file password. Since the Cisco SME cluster hardware is different, the master key is different, and during the import operation the key catalog will be encoded with the master key of the secondary cluster.

Conclusion

The Cisco SME solution integrated into the Cisco MDS 9000 family of Fibre Channel fabric switches and directors is a fabric-based distributed solution capable of protecting data being written to tape.

The actual cryptographic processing is performed in a distributed fashion on high-speed secure processors, and the key management and administration is centralized for operational efficiency.

This document introduced the principles of the Cisco SME key management strategy, including the system architectures and the configuration options. This document also discussed how the Cisco SME key management technology supports the sharing of encryption keys and tapes among business partners and presented the approach to disaster recovery, which requires that encrypted data be decrypted in a secondary site after a disaster.

The Cisco SME solution is completed with a data recovering application, creating a solution designed for long-term storage of encrypted data.

For More Information

Please refer to the following documents for specific technical details:

- For a detailed description of configuration procedures and scalability information, see the Cisco MDS 9000 Family Storage Media Encryption Configuration Guide.
- For information about supported interoperability configurations, see the Cisco MDS 9000 Family Interoperability Support Matrix: Fabric Services Interoperability Matrix.

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 C11-462423-02 02/09