Configuring SME Key Management

This chapter contains information about SME comprehensive key management.

This chapter includes the following topics:

Information About SME Key Management

SME Key Management includes the following topics:

About Key Hierarchy

SME includes a comprehensive and secure system for protecting encrypted data using a hierarchy of security keys. The highest level key is the master key, which is generated when a cluster is created. Every cluster has a unique master key. In SME tape, the master key encrypts the tape volume group keys which in turn encrypts the tape volume keys using key wrapping. In SME disk, the master key encrypts the disk keys using key wrapping.

For recovery purposes, the master key can be stored in a password-protected file, or in one or more smart cards. When a cluster state is Archived (the key database has been archived) and you want to recover the keys, you will need the master key file or the smart cards. The master key cannot be improperly extracted by either tampering with the MSM-18/4 module or by tampering with a smart card.

Keys are essential to safeguarding your encrypted data and should not be compromised. Keys should be stored in the Cisco Key Management Center. In addition, unique tape keys can be stored directly on the tape cartridge. The keys are identified across the system by a globally unique identifier (GUID).

The SME key management system includes the following types of keys for SME tape:

- Master key
- Tape volume group keys

- Tape volume keys

Every backup tape has an associated tape volume key, tape volume group key, and a master key.

The SME key management system includes the following types of keys for SME disk:

- Master key
- Disk keys

Master Key

When a SME cluster is created, a security engine generates the master key. Considering that a single fabric can host more than one cluster, for example, to support the needs of multiple business groups within the same organization, there will be as many master keys as there are clusters. Each master key is unique and it is shared across all cluster members. The master key is used to wrap the tape volume group keys.

Tape Volume Group Key

The tape volume group key is used to encrypt and authenticate the tape volume keys, which are the keys that encrypt all tapes belonging to the same tape volume group. A tape volume group can be created on the basis of a bar code range for a set of backup tapes or it can be associated with a specific backup application. Tape volume group keys are occasionally rekeyed for increased security or when the security of the key has been compromised.

Tape Volume Key

The tape volume key is used to encrypt and authenticate the data on the tapes.

In unique key mode, the tape volume keys are unique for each physical tape and they can be stored in the Cisco KMC or stored on the tape. The Cisco KMC database does not need to store a tape volume key if the key is stored on the tape itself. The option to store the key on the tape may dramatically reduce the number of keys stored on the Cisco KMC.

In shared key mode, there is one tape volume key which is used to encrypt all volumes in a volume group.

Disk Key

The disk key is used to encrypt and decrypt the data on the disks.

About Cisco Key Management Center

The Cisco Key Management Center (Cisco KMC) is the centralized management system that stores the key database for active and archived keys. The keys stored in the Cisco KMC are not usable without the master key. To manage the potential increase in tape volume keys, SME provides the option to store the tape volume key on the tape itself. In this case, the Cisco KMC stores the tape volume group keys.

This option exponentially increases the number of managed tapes by reducing the number of keys stored on the Cisco KMC. However, this option also restricts the capability of purging keys at a later time.

The Cisco KMC provides the following advantages:

- Centralized key management to archive, purge, recover, and distribute tape keys.
- Integrated into DCNM-SAN Server depending on the deployment requirements.
- Integrated access controls using AAA mechanisms.

Note The Cisco KMC listens for key updates and retrieves requests from switches on a TCP port. The default port is 8800; however, the port number can be modified in the smeserver.properties file.

About Master Key Security Modes

To recover encrypted data-at-rest from a specific tape, you need access to the keys that are created for the specific tape cartridge. Because the master key is used to protect all other keys, SME provides three master key security modes to protect the master key: Basic, Standard, and Advanced. During cluster configuration, you designate the level of security for the master key. Basic security writes the encrypted master key to a disk. To unlock the master key, you need access to the file. The file is encrypted and requires a password to retrieve the master key. The Standard and Advanced security modes require the use of smart cards to access the master key. If you select Standard security, you will need one smart card to unlock the master key. If you select Advanced security during cluster configuration, you are prompted to set the minimum number of required smart cards that would unlock the master key.

The below table describes the master key security modes.

Table 1: Master Key Security Levels

Security Level	Definition
Basic	The master key is stored in a file and encrypted with a password. To retrieve the master key, you need access to the file and the password.
Standard	Standard security requires one smart card. When you create a cluster and the master key is generated, you are asked for the smart card. The master key is then written to the smart card. To retrieve the master key, you need the smart card and the smart card pin.

Security Level	Definition
Advanced	Advanced security requires five smart cards. When you create a cluster and select Advanced security mode, you designate the number of smart cards (two or three of five smart cards or two of three smart cards) that are required to recover the master key when data needs to be retrieved. For example, if you specify two of five smart cards, then you will need two of the five smart cards to recover the master key. Each smart card is owned by a SME Recovery Officer. **Note** The greater the number of required smart cards to recover the master key, the greater the security. However, if smart cards are lost or if they are damaged, this reduces the number of available smart cards that could be used to recover the master key.

About Key Management Settings

When creating a tape volume group, you need to determine whether to enable or disable the key management settings.

The below table provides a description of the key settings, considerations, and the type of keys that can be purged if a particular setting is chosen. All key settings are configured at the cluster level.

Note The Key Management Settings table shown below is applicable only for SME tapes.

Table 2: Key Management Settings

	Description	Considerations
Shared	In shared key mode, only tape volume group keys are generated. All tape volumes that are part of a tape volume group share the same key.	**Cisco KMC key database—**Is smaller storing only the tape volume group keys. **Security—**Medium. A compromise to one tape volume group key will compromise the data in all tapes that are part of that tape volume group. **Purging—**Available only at the volume group level.

	Description	Considerations
Unique Key	In unique key mode, each individual tape has it's own unique key. The default value is enabled.	**Cisco KMC key database—**Is larger storing the tape volume group keys and every unique tape volume key. **Security—**High. A compromise to a tape volume key will not compromise the integrity of data on other tape volumes. **Purging—**Available at the volume group and volume level.
Unique Key with Key-On-Tape	In the key-on-tape mode, each unique tape volume key is stored on the individual tape. You can select key-on-tape (when you select unique key mode) to configure the most secure and scalable key management system. The default value is disabled. **Note** When key-on-tape mode is enabled, the keys stored on the tape media are encrypted by the tape volume group wrap key.	**Cisco KMC key database—** Increases scalability to support a large number of tape volumes by reducing the size of the Cisco KMC key database. Only the tape volume group keys are stored on the Cisco KMC. **Security—**High. A compromise to a tape volume key will not compromise the integrity of data on other tape volumes. **Purging—**Available at the volume group level.

Tape Recycling

If Tape Recycling is enabled, old keys for the tape volume are purged from Cisco KMC when the tape is relabeled, and a new key is created and synchronized to the Cisco KMC. This setting should be selected when you do not need the old keys for previously backed-up data that will be rewritten.

The default setting is Yes. Setting this option to No is required only if tape cloning is done outside of the SME tape group.

About High Availability Key Management Center

The Cisco KMC server consists of a pair of KMC servers (KMS) that provides high availability and reliability. These high availability servers helps to avoid both downtime and loss of data through synchronization and redundancy. The KMS consists of a primary and a secondary KMC server which point to the same database.

Both the KMS should use the same Oracle 11g Enterprise installation to achieve high availability. The Oracle 11g Enterprise installation should be installed on the two servers and synchronized using Oracle Active Data guard.

Each SME cluster is configured with primary and secondary KMC servers. The primary server is preferred over the secondary server.

The cluster is connected to the primary server and, at any indication of failure, connects to the secondary server. The cluster periodically checks for the availability of the primary server and resumes connection to the primary server when it becomes available.

All the switches in a cluster use the same KMC server. When a switch connects to a secondary server, an automatic cluster-wide failover occurs to the secondary server. The switches in the cluster fail over to the primary server once it is available.

Note Configure the primary and secondary servers during the cluster creation or update the Key Manager Settings for a created cluster.

About Auto Key Replication of Keys Across Data Centers

Note Auto key replication of keys across data centers is applicable only for SME tape.

The auto replication of media keys enables the moving of tapes from one data center to another. The replication of keys allows the same tape media to be accessed by more than one SME cluster. In most cases, the SME clusters are located in different locations, such as a primary data center and a disaster recovery site. SME allows you to automatically replicate the media keys from one SME cluster to one or more clusters. The automated process of replicating keys eliminates the need for the manual key export and import procedures. The media key auto-replication is configured on per tape volume group basis.

One KMC manages all the data centers and the replicated keys are stored on the KMC.

Translating Media Keys

Each cluster is associated with a translation context. The translation context contains the public key for the key pair generated by the crypto-module of one of the clusters.

A replication relationship is set between the volume groups in the different clusters and the replication context for the destination clusters need to be acquired. Once the relationship is set up between the clusters, whenever a key is generated in the source cluster, the key is automatically translated to the destination cluster.

The translation of the keys is a scheduled process and based on the preset frequency all the key pairs generated in that time period are translated to the destination cluster. Every key that is generated and scheduled for replication, since last job start time, are translated using the replication context, which is the public key of the destination cluster.

The key replication across data centers requires the translation of key hierarchy. The key from the source cluster is translated using the public key of the destination cluster and then sent to the destination cluster. In the destination cluster, the key is unwrapped with the private key of the destination cluster and then wrapped with the key hierarchy of the destination cluster.

About Accounting Log Information

This section describes the KMC accounting log messages.

The accounting.log file in the DCNM-SAN log directory displays the KMC accounting log messages. The accounting log records key-related operations, their resulting status, and any related information.

The log files are stored in a relational database and are searchable, archivable, and portable.

A log entry consists of the following information:

- hostname—The name of the host machine where the operation occurred.
- timestamp—The time at which an event was recorded to the accounting log system.
- username—The username associated with the operation.
- clusterName—The name of the cluster the operation was performed on.
- clusterId—The ID of the cluster the operation was performed on.
- operation—The type of operation.
- status—The status of the operation when the event was logged.
- details—Additional data, depending on the type of operation.

Configuring SME Key Management Using the CLI

This section describes configuring unique or shared key mode.

Configuring Unique or Shared Key Mode

Note Unique or shared key mode applies only to SME tapes.

Shared key mode is used to generate a single key that is used for a group of backup tapes.

Unique key mode is used to generate unique or specific keys for each tape cartridge.

Note Configure the Cisco KMC before configuring the key mode. See the About Cisco Key Management Center, on page 2.

To configure the shared key or unique key mode, follow these steps:

Step 1 switch# **configure terminal**
Enters configuration mode.

Step 2 switch(config)# **sme cluster clustername1**
switch(config-sme-cl)#

Specifies the cluster and enters SME cluster configuration submode.

Step 3 switch(config-sme-cl)# **shared-key mode**
switch(config-sme-cl)#

Specifies shared key mode.

Step 4 switch(config-sme-cl)# **no shared-key mode**
switch(config-sme-cl)#

Specifies shared unique key mode.

Monitoring SME Key Management

Viewing KMC Accounting Log Messages Output

The output of the log entry is displayed in the following format:

```
"<timestamp> User: <username> Host: <host> Cluster: <cluster name> Id:
<cluster id> Operation: <operation> Status: <status> Details: <details>"
The following is a complete listing of logged SME operations and
expected status values. The logged details for an operation depends
upon the resulting status of the operation and/or other criteria
documented below.
-------------------------------------
Operation: STORE_KEY         Logged as: "Store key"
Description: A new key is being written to the keystore. The details
for the accounting log of a STORE_KEY operation depends upon the
KEY_TYPE and the STATUS for the operation.
Details:
KEY_TYPE: MasterKey
SUCCESS:  "key type: <key type> GUID: <guid>"
FAILURE:  "key type: <key type> GUID: <guid> error: <description>"
KEY_TYPE: TapeVolumeGroupSharedKey
SUCCESS:  "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name>"
FAILURE:  "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> error: <description>"
KEY_TYPE: TapeVolumeGroupWrapKey
SUCCESS:  "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name>"
FAILURE:  "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> error: <description>"
KEY_TYPE: TapeVolumeKey
SUCCESS:  "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> barcode: <barcode>"
FAILURE:  "key type: <key type> GUID: <guid> tape group: <tape group
name> tape volume group: <tape volume group name> barcode: <barcode>
error: <description>"
-------------------------------------
Operation: GET_KEY         Logged as: "Retrieve key"
Description: A key is being requested from keystore. The details for
the accounting log of a GET_KEY operation depend upon the query
parameter and STATUS for the operation.
Details:
QUERY PARAMETER: Guid
SUCCESS:  "GUID: <guid>"
FAILURE:  "GUID: <guid>"
QUERY PARAMETER: Cloned from Guid
SUCCESS:  "Cloned from GUID: <guid>"
FAILURE:  "Cloned from GUID: <guid>"
-------------------------------------
Operation: ARCHIVE_KEY         Logged as: "Archive key"
Description: A key is removed from "active" state and moved to
"archived" state.
Details:
SUCCESS:  "GUID: <guid>"
FAILURE:  "GUID: <guid> error: <description>"
-------------------------------------
Operation: ARCHIVE_ALL_KEYS         Logged as: "Archive all keys"
Description:  All keys are archived for an instance of a KEY_TYPE.
The details for the accounting log of a ARCHIVE_ALL_KEYS operation
depends upon the KEY_TYPE and the STATUS for the operation.
```

```
Details:
KEY_TYPE: TapeVolumeGroupSharedKey
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name>"
FAILURE:  "tape group: <tape group name> tape volume group: <tape
volume group name> error: <description>"
KEY_TYPE: TapeVolumeGroupWrapKey
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name>"
FAILURE:  "tape group: <tape group name> tape volume group: <tape
volume group name> error: <description>"
KEY_TYPE: TapeVolumeKey
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name> barcode: <barcode>"
FAILURE:  "tape group: <tape group name> tape volume group: <tape
volume group name> barcode: <barcode> error: <description>"
-------------------------------------
Operation: PURGE_KEY         Logged as: "Purge key"
Description: A key and references to it are removed from the keystore.
Details:
SUCCESS:  "GUID: <guid>"
FAILURE:  "GUID: <guid> error: <description>"
-------------------------------------
Operation: DELETE_ALL_TAPE_VOLUME_KEYS         Logged as: "Delete Tape
Volume Keys"
Description: All tape volume keys for the given tape volume are
removed from the keystore.
Details:
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name>"
-------------------------------------
Operation: DELETE_ALL_TAPE_VOLUME_SHARED_KEYS         Logged as:
"Delete Tape Volume Group Shared Keys for cluster"
Description: All shared keys for the given tape volume are removed
from the keystore.
Details:
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name>"
-------------------------------------
Operation: DELETE_ALL_TAPE_VOLUME_WRAP_KEYS         Logged as: "Delete
Tape Volume Group Wrap Keys for cluster"
Description: All wrap keys for the given tape volume are removed from
the keystore.
Details:
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name>"
-------------------------------------
Operation: EXPORT_ARCHIVED         Logged as: "Export archived cluster"
Description: An archived cluster is being exported. The operation is
being logged per tape volume group exported for the requested cluster.
Details:
INITIATED:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: null"
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: <count>"
FAILURE:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: <count> error: <description>"
-------------------------------------
Operation: EXPORT         Logged as: "Export cluster"
Description: A cluster is being exported. The operation is being
logged per tape volume group exported from the requested cluster.
Details:
INITIATED:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: null"
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: <count>"
FAILURE:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys exported: <count> error: <description>"
-------------------------------------
Operation: IMPORT         Logged as: "Import keys"
Description: Keys are imported into a cluster. The operation is being
logged per tape volume group.
Details:
```

```
INITIATED:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys imported: null"
SUCCESS:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys imported: <count>"
FAILURE:  "tape group: <tape group name> tape volume group: <tape
volume group name> keys imported: <count> of <total count> total.
Skipped : <count> error: <description>"
-------------------------------------
Operation: REKEY_MASTER_KEY         Logged as: "Master key rekey"
Description: A master key is being "re-keyed" or replaced with a new
master key. All keys wrapped w/ the old master key are unwrapped and
re-wrapped with the new master key.
Details:
INITIATED:  ""
SUCCESS:  ""
FAILURE:  "error: <description>"
-------------------------------------
Operation: ABORT_REKEY_MASTER_KEY         Logged as: "Abort master key
rekey"
Description: A re-key operation has been aborted. If the operation
cannot be aborted, the failure is logged.
Details:
SUCCESS:  ""
FAILURE:  "error: <description>"
-------------------------------------
Operation: GET_MASTER_KEY_SHARE         Logged as: "Master key share
retrieved"
Description: When storing master key shares on smartcards, the share
is verified as being written correctly by reading the share and
comparing. This logs the result of that GET operation.
Details:
SUCCESS:  "share index: <share index> smartcard label: <smartcard
label> smartcard serial number: <serial number> GUID: <guid>"
FAILURE:  "share index: <share index> smartcard label: <smartcard
label> smartcard serial number: <serial number> GUID: <guid> error:
<description>"
-------------------------------------
Operation: REKEY_CLONE_WRAP_KEYS         Logged as: "Clone tape volume-
group wrap keys"
Description: Part of Master Key re-key involves cloning wrap keys and
re-wrapping them with the new master key. This logs the result of
that cloning and re-wrap operation.
Details:
SUCCESS:  "<count> keys of <total count> cloned successfully"
FAILURE:  "<count> keys of <total count> cloned successfully"
```

The SME accounting log is configurable as of 4.2.x. Accounting entries are made in the database, and then flushed to a file on a defined schedule. By default, this happens weekly. The logs are written to a uniquely named file for example: **sme_accounting_log.2011-01-30-12-00-01.log**. This file is available in the host where the DCNM application is running, for example in the **<Install Path>/dcm/fm/logs** directory.

Step 1 Edit the **<Install Path>/dcm/fm/conf/smeserver.properties** file.

Step 2 Add **sme.kmc.archive.accounting.log.frequency=**
The valid values are:

- hourly
- daily
- weekly
- monthly
- test (if you want to validate, which does it every 5 minutes). This should NOT be left enabled. It will flood your machine with files.

Note Due to the nature of the files, SME will not delete or overwrite these files. Test or even hourly settings will generate a significant number of files over time. The accounting log entries not yet flushed from the database are visible in the Accounting Log Tab.

Viewing Keys for SME Tape

You can view information about unique tape volume keys, tape volume group keys, and shared tape volume group keys. Using DCNM-SAN Web Client, you can view keys that are stored in the Cisco KMC. When keys are generated, they are marked as active; keys that are imported are marked as deactivated. The keys are never displayed in clear text.

Viewing Keys for SME Disk

You can view information about disk keys. Using DCNM-SAN Web Client, you can view keys that are stored in the Cisco KMC. When keys are generated, they are marked as active; keys that are imported are marked as deactivated. The keys are never displayed in clear text.

Feature History for SME Key Management

The below table lists the release history for this feature.

Table 3: Feature History for SME Key Management

Feature Name	Releases	Feature Information
Software change	5.2(1)	In Release 5.2(1), Fabric Manager is changed to DCNM for SAN (DCNM-SAN).
	4.1(1c)	In Release 4.1(1b) and later, the MDS SAN-OS software is changed to MDS NX-OS software. The earlier releases are unchanged and all references are retained.
Migrating KMC server	4.1(1c)	In 4.1(1c), the KMC server can be migrated.
Accounting log	4.1(1c)	In 4.1(1c) and later, users can view the rekey operations and their status in the SME tab of the Fabric Manager Web Client.

Feature Name	Releases	Feature Information
High availability KMC server	4.1(3)	High availability KMC can be configured by using a primary and secondary servers. In 4.1(3), HA settings are available on the Key Manager Settings page. The primary and secondary servers can be chosen during cluster creation. The primary and secondary server settings can be modified in the Cluster detail page.
Auto replication of media keys	4.1(3)	In 4.1(3) Tape Key replication was known as Remote Replication. A remote replication relationship can be set between volume groups. SME allows you to automatically replicate the media keys from one SME cluster to one or more clusters. In 4.1(3), remote replication relationship settings are available.
Host names are accepted as server addresses	4.1(3)	You can enter IP addresses or host names for the servers.
Volume key rekey	3.3(1c)	Volume keys are rekeyed to ensure better security or when key security is compromised.
Master key rekey	3.3(1c)	In the advanced mode, the smart card replacement triggers a master key rekey and a new version of the master key is generated for the cluster. The new set of master keyshares are stored in the smart cards. All the volume group keys are also synchronized with the new master key.