Cisco SME Key Management

This chapter contains information about Cisco Storage Media Encryption comprehensive key management. It includes the following topics:

- Key Hierarchy, page 6-1
- Cisco Key Management Center, page 6-2
- Master Key Security Modes, page 6-3
- Key Management Settings, page 6-4
- High Availability Key Management Center, page 6-5
- Key Management Operations, page 6-7
- Migrating a KMC Server, page 6-48

Key Hierarchy

Cisco 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. Using key wrapping, the master key encrypts the tape volume group keys, which in turn encrypts the tape volume keys.

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 When a cluster state is Archived (the key database has been archived) and you want to recover the keys, you will need the master key file or the smart cards.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. See the “Cisco Key Management Center” section on page 6-2 for information about 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 Cisco SME key management system includes the following types of keys:

- 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.
Master Key

When a Cisco 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.

Cisco Key Management Center

The 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, Cisco 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 Fabric Manager 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.
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, Cisco 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. Table 6-1 describes the three master key security modes.

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.

Table 6-1 describes the master key security modes.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>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.</td>
</tr>
<tr>
<td>Standard</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced</td>
<td>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 Cisco SME Recovery Officer.</td>
</tr>
</tbody>
</table>

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.
Key Management Settings

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

Table 6-2 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.

Table 6-2  Key Management Settings

<table>
<thead>
<tr>
<th>Key Management Settings</th>
<th>Description</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Unique Key</td>
<td>In unique key mode, each individual tape has its own unique key. The default value is enabled.</td>
<td>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.</td>
</tr>
<tr>
<td>Unique Key with Key-On-Tape</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Tape Recycling

If Tape Recycling is enabled, old keys for the tape volume are purged from Cisco KMC when the tape is relabeled and 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.
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 Cisco 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 fails over to the primary server once it is available.

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

Choosing High Availability Settings

To choose the primary or secondary server, follow these steps:

**Step 1**  
Go to the Fabric Manager Web Client and choose Key Manager Settings.

**Step 2**  
In the High Availability Settings area, click Edit HA Settings.

**Step 3**  
Choose the server to be the primary server and specify the IP address of the secondary server.  
Alternately, you can choose the server to be the secondary server and specify the IP address of the primary server.
Step 4  Click OK to save the settings to view the notification that the settings have been saved.
Chapter 6  Cisco SME Key Management

Key Management Operations

This section describes the following key management operations:

- Viewing Standard Security Mode Smart Cards, page 6-7
- Viewing Advanced Security Mode Smart Cards, page 6-8
- Viewing Keys, page 6-8
- Purging Volumes, page 6-9
- Purging Volume Groups, page 6-9
- Exporting Volume Groups, page 6-10
- Importing Volume Groups, page 6-12
- Rekeying Tape Volume Groups, page 6-14
- Auto Key Replication of Keys Across Data Centers, page 6-15
- Basic Mode Master Key Download, page 6-19
- Replacing Smart Cards, page 6-22
- Exporting Volume Groups From Archived Clusters, page 6-33
- Accounting Log Information, page 6-43

Viewing Standard Security Mode Smart Cards

To view Standard security smart card information, select Smartcards in the navigation pane to view the smart card information.
Viewing Advanced Security Mode Smart Cards

To view Advanced security smart card information, select **Smartcards** in the navigation pane to view the smart card information.

Viewing Keys

You can view information about unique tape volume keys, tape volume group keys, and shared tape volume group keys. Using Fabric Manager 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.

**Note**

To view keys using CLI, see Chapter 7, “Using the Command Line Interface to Configure SME.”

To view tape volume group keys, follow these steps:

**Step 1**

Click a volume group to display the volume group key information.

In the unique key mode, only the wrap key is showing. The wrap key is the tape volume group key that wraps volume keys. If shared mode is selected, the wrap key and a shared key are in view. The wrap key wraps the shared key. Keys are listed as **TapeVolumeGroupWrapKey** or the **TapeVolumeGroupSharedKey**.

There are no volume keys in shared key mode; you will see only the shared key.

**Step 2**

Click the **Active** tab to view all active keys.
Step 3  Click the **Deactivated** tab to view all keys that have been marked as deactivated and stored in the Cisco KMC. You can view the barcode, GUID (the unique key identifier generated by the switch), deactivated date, and version (the version of the tape key generated for the same barcode).

---

### Purging Volumes

Purging keys deletes deactivated or active keys from the Cisco KMC. You can delete the deactivated volume group, which purges all keys. If you delete an active volume group, all the keys are deactivated. Purging keys at the volume level in unique key mode allows you to purge specific volumes.

**Caution**  Purging keys from the Cisco KMC cannot be undone.

To purge keys that are currently active or deactivated, follow these steps:

**Step 1**  Select a volume group and click **Active** or **Deactivated** to view the keys that are deactivated in the Cisco KMC.

**Step 2**  Select the deactivated keys that you want to purge.

**Step 3**  Click **Remove**.

---

### Purging Volume Groups

To purge a volume group, follow these steps:

**Step 1**  Select a deactivated volume group and click **Remove**.
Exporting Volume Groups

Exporting tape volume groups can be advantageous when tapes are moved to a different cluster. In that scenario, you will need the keys if you have to restore those tapes. If the source cluster is online, follow the steps in this section. If the source cluster is archived, follow the steps in the “Exporting Volume Groups From Archived Clusters” section on page 6-33.

To export volume groups from an online cluster, follow these steps:

Step 1  Select a volume group to display the volume groups in the cluster.
Step 2  Select a volume group.
Step 3  Click Export.
Step 4  Enter the volume group file password. Click Next.
Step 5  Click **Download** to download the volume group file.

Step 6  Save the .dat file.
**Importing Volume Groups**

You can import a previously exported volume group file into a selected volume group.

To import a volume group file, follow these steps:

**Step 1** Select Volume Groups in the navigation pane to display the volume groups in the cluster.

**Step 2** Select a volume group and click Import.

**Note** You must select an existing volume group. To import into a new volume group, create the volume group first, and then import a volume group.
Step 3  Locate the file to import. Enter the password that was assigned to encrypt the file. Click Next.

Step 4  Select the volume group .dat file. Click Open.
Key Management Operations

Send documentation comments to mdsfeedback-doc@cisco.com

Step 5  Click Confirm to begin the import process or click Back to choose another volume group file.

Note  The imported keys in tape volume groups are read-only by default. However, if the entry “sme.retain.imported.key.state=true” is set in the conf/smeserver.properties file and the FM server is restarted, the state of the imported keys are retained and both read and write operations can be performed.

Rekeying Tape Volume Groups

Tape volume groups can be rekeyed periodically to ensure better security and also when the key security has been compromised.

In the unique key mode, the rekey operation generates a new tape volume group wrap key. The current tape volume group wrap key is archived. The current media keys remain unchanged, and the new media keys are wrapped with the new tape volume group wrap key.

In the shared key mode, the rekey operation generates a new tape volume group wrap key and a new tape volume group shared key. The current tape volume group wrap key is archived while the current tape volume group shared key remain unchanged (in active state).

The volume groups can be rekeyed monthly even if you do not use the unique key mode.

To rekey tape volume groups, follow these steps:

Step 1  In the Fabric Manager Web Client navigation pane, select Volume Groups to display the volume groups in the cluster.

Step 2  Select one or more volume groups.
**Step 3**  Click **Rekey**. A confirmation dialog box is displayed asking if the rekey operation is to be performed. Click **OK** to rekey the selected volume groups.

---

**Auto Key Replication of Keys Across Data Centers**

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 Cisco SME cluster. In most cases, the SME clusters are located in different locations, such as a primary data center and a disaster recovery site. Cisco SME allows you to automatically replicate the media keys from one Cisco 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.

This section describes the following topics:

- Translating Media Keys, page 6-15
- Auto Replicating Keys in Fabric Manager Web Client, page 6-16

**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.
Key Management Operations

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.

Auto Replicating Keys in Fabric Manager Web Client

This section describes how to auto replicate the media keys in the Fabric Manager Web Client. The following topics are covered:

- Creating Remote Replication Relationships, page 6-16
- Removing Remote Replication Relationships, page 6-18

Creating Remote Replication Relationships

To auto replicate the media keys, follow these steps:

**Step 1** In the Fabric Manager Web Client, click the SME tab.

**Step 2** Select Clusters in the navigation pane to display the clusters.

**Step 3** Select a cluster and select Remote Replication. The Remote Replication Relationships pane appears.
Step 4  Click Create to create a remote replication relationship. A Create Replication Relationship area appears where the source cluster and the destination clusters are displayed.

Step 5  Select the clusters to expand or collapse the list of the Source Volume Group and the Destination Volume Group. Choose tape groups from the Source Volume Group and the Destination Volume Group to create a remote replication relationship context.

Step 6  Click Submit to save the settings. A notification window appears to indicate the creation of the remote replication relationship and the replication status shows as Created.
Removing Remote Replication Relationships

To remove a remote replication relationship, follow these steps:

**Step 1**  Click Clusters in the navigation pane to display the clusters and select Remote Replication. The Remote Replication Relationships area appears on the right-hand pane.

**Step 2**  Select the tape group whose replication relationship needs to be removed. Click Remove.

**Step 3**  A confirmation dialog box is displayed asking if the relationship needs to be removed. Click OK to remove the replication relationship of the selected volume groups.
Step 4 A notification window appears that indicates the removal of the remote replication relationship.

**Basic Mode Master Key Download**

In Basic security mode, the master key file can be downloaded multiple times from the Fabric Manager Web Client. The cluster detail view includes a button to download the master key file.

To download the master key file (Basic security mode), follow these steps:

**Step 1** Select a cluster name in the navigation pane to view the cluster details.

**Step 2** Click the **Download Master Key** button to download the master key file.
Step 3  Enter the password to protect the master key file. Click Download to begin downloading the encrypted file.
Step 4  Click Close to close the wizard.

Step 5  Click Save to save the downloaded master key file.
Replacing Smart Cards

This section describes how to replace smart cards for clusters in the following modes.

- **Standard Mode**, page 6-22
- **Advanced Mode**, page 6-24

### Standard Mode

In Standard security mode, the master key can be downloaded to a replacement smart card from the Fabric Manager Web Client.

To replace a smart card (Standard security mode), follow these steps:

1. **Step 1** Select **Smartcards** to display the smart card information for the cluster.

2. **Step 2** Click **Replace** to launch the smart card replacement wizard. Click **Next**.

3. **Step 3** Insert the smart card and enter the password, PIN, and label for the smart card. Click **Next**.
Step 4  Click **Finish** to close the wizard.
Advanced Mode

In Advanced security mode, the master key is stored on five smart cards. Depending on the quorum required to recover the master key, two or three of the five smart cards or two of the three smart cards will be required to unlock the master key. The master key is stored securely on a PIN-protected smart card.

To replace a lost or damaged smart card, the quorum of Cisco SME Recovery Officers must be present with their smart cards to authorize the master key recovery. This ensures that the split-knowledge security policy of the master key is maintained throughout the lifetime of the Cisco SME cluster. This method guarantees that following the creation of the Cisco SME cluster in Advanced security mode, the master key can only be retrieved by the quorum of Cisco Recover Officers and both the replacement operation as well as the new smart card are authorized and authenticated by the quorum.

The smart card replacement triggers a master key recreation (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.

In the unique key mode, a new tape volume group wrap key is generated for each volume group. The existing tape volume group wrap key is duplicated with the new master key and put in the archived state.

In the shared key mode, a new tape volume group wrap key and tape volume group shared key are generated. The existing tape volume group wrap key is duplicated with the new master key and put in the archived state. The existing tape volume group shared key remains as it were.

To replace a smart card (Advanced security mode), follow these steps:

Step 1  Select Smartcards to display the smart card information for the cluster.

Step 2  Select the smart card that you want to replace. Click Replace to launch the smart card replacement wizard.

Step 3  Insert the new smart card. Click Next.
The Cisco SME Recovery Officer who owns the replacement smart card is prompted to log in and to insert the smart card to download the master key.

**Step 4** Enter the switch login information and the smart card PIN and label. Click **Next**.

Each member of the Cisco Recovery Officer quorum is requested to log in and present their smart card to authorize and authenticate the operation.
Step 5  Insert one of the smart cards that stores the master key. Click Next.

Step 6  Enter the switch login information and the smart card PIN and label. Click Next.
**Step 7**  Enter the switch login information and the smart card PIN and label. Click **Next**.

**Step 8**  Enter the switch login information and the smart card PIN and label. Click **Next**.

**Step 9**  Insert the smart cards belonging to each recovery officer in any random order.
To store the new master keyshares, follow these steps:

a. Enter the switch login information, the PIN number for the smart card, and a label that will identify the smart card. Click Next.

A notification is shown that the first keyshare is successfully stored.
Chapter 6   Cisco SME Key Management

Key Management Operations

Send documentation comments to mdsfeedback-doc@cisco.com

b. Enter the switch credentials and PIN information for the second recovery officer. Click Next.

A notification is shown that the second keyshare is successfully stored.

c. Enter the switch credentials and PIN information for the third recovery officer. Click Next.
A notification is shown that the third keyshare is successfully stored.

d. Enter the switch credentials and PIN information for the fourth recovery officer. Click Next.

A notification is shown that the fourth keyshare is successfully stored.
e. Enter the switch credentials and PIN information for the fifth recovery officer. Click Next.

A notification is shown that the fifth keyshare is successfully stored. Click Next to begin the automatic synchronization of volume groups.
You will see an indication that the operation is in progress until the synchronization of volume groups is completed.

**Step 10** The smart card replacement is completed. Click **Close** to return to the Fabric Manager Web Client and to view the smart card information.
Step 11 To view the new smart card information, select Smartcards. The smart card details displays the old recovery shares and the new recovery shares.

Exporting Volume Groups From Archived Clusters

When a Cisco SME cluster is archived, all key management operations such as exporting volume groups, are performed at the Cisco KMC. Exporting volume keys is a critical operation and must be authorized by Cisco SME Recovery Officers.

The following sections describes the exporting of volume groups in the three modes:

- Basic Mode, page 6-33
- Standard Mode, page 6-36
- Advanced Mode, page 6-39

Basic Mode

To export a volume group from an archived cluster (Basic security mode), follow these steps:

Step 1 Select a volume group to display the volume groups in the cluster. Click Export.
Step 2  Click **Browse** to locate the volume group master key file.

Step 3  Select the master key file. Click **Open**.
Step 4 Enter the password that protects the master key for the archived volume group. Click Next.

Step 5 Enter the password that will be used to encrypt the exported file. Click Next.
Step 6  Click **Download** to begin downloading the volume group file.

Step 7  To save the exported volume group, click **Save**.

**Standard Mode**

To export a volume group from an archived cluster (Standard security mode), follow these steps:

Step 1  Select **Volume Groups** (in an archived cluster) to display the volume groups in the cluster. Select a volume group and click **Export**.
Step 2  Insert one of the five smart cards into the smart card reader. Click Next.

Step 3  Enter the smart card PIN and label. Click Next.
Step 4 Enter the password to encrypt the volume group file. Click Next.

Step 5 Click Download to begin downloading the file.
Step 6  
Save the .dat file. Click Next.

Advanced Mode

To export a volume group from an archived cluster (Advanced security mode), follow these steps:

Step 1  
Select Volume Groups (in an archived cluster) to display the volume groups in the cluster. Select a volume group and click Export.
Step 2  Insert one of the five smart cards into the smart card reader. Click Next.

Step 3  Enter the smart card PIN and label. Click Next.

The keyshare is retrieved.
Step 4  Insert the next smart card into the smart card reader. Click Next.

**Note**  Repeat this step for each smart card that is required to unlock the master key. The number of required smart cards depends on the quorum number selected during the cluster creation, for example, two of five smart cards.

Step 5  Enter the smart card PIN and label. Click Next.

Step 6  Enter the volume group file password. Click Next.
Step 7 Click Download to begin downloading the volume group.
Chapter 6  Cisco SME Key Management

Accounting Log Information

Send documentation comments to mdsfeedback-doc@cisco.com

Step 8  Click Save to save the .dat file.

Accounting Log Information

This section describes how to view the accounting information and how the accounting log messages display.

- Viewing Accounting Log Information, page 6-43
- KMC Accounting Log Messages, page 6-44

Viewing Accounting Log Information

To view the rekey operations and their status, follow these steps:

Step 1  Click the SME tab in the Fabric Manager Web Client.

Step 2  Click the Accounting Log in the SME tab to display the log information. The location of the accounting log in the Cisco KMC database is displayed in the KMC Log Location.

Step 3  Enter a pattern in the Filter and click Go. The accounting pattern is displayed based on the selected pattern.
Accounting Log Information

KMC Accounting Log Messages

The accounting.log file in the FM 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.

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.

---

KMC Accounting Log Messages

The accounting.log file in the FM 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.

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.
Accounting Log Information

---

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>"

---
Accounting Log Information

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"

---

**Migrating a KMC Server**

To migrate a KMC server, follow these steps:

**Step 1** Migrate all keys to the new KMC server. Refer to the backup and restore procedures outlined in Appendix E, “Database Backup and Restore.”

**Step 2** After restoring the database, install Fabric Manager in the new KMC server and point the Fabric Manager to the database. This ensures that all the keys are maintained across the KMC migration.
Step 3  Update the cluster with the new KMC server details when the new KMC server is active.

a. Go to the Fabric Manager Web Client and click the SME tab.

b. Select the cluster. The cluster details page displays.

c. Click Modify and choose the new KMC server.

If the KMC server is integrated with RSA Key Manager, modify the settings and select the RKM server.

Step 4  Uninstall the Fabric Manager server instance of the previous KMC server. This removes the previous KMC server.

Note  If the KMC server is integrated with RSA Key Manager, both the KMC and RSA Key Manager must be synchronized. If a KMC server is removed to purge all the keys, follow the required procedures to purge all the keys first before you uninstall the KMC server. This ensures that the keys in the RSA Key Manager are also purged.
Migrating a KMC Server

Send documentation comments to mdsfeedback-doc@cisco.com