

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
- Key Management Operations, page 6-5
- Accounting Log Information, page 6-40

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 When a cluster state is Archived (the key database has been archived) and you want to recover the keys, you will need the master key file or the smart cards.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 can not 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—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 data base 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
- Integrated access controls using AAA mechanisms



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.

| 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 the written to the smart card. To retrieve the master key, you need the smart card <i>a</i> the smart card pin. | | | | |
| Advanced | Advanced security requires 5 smart cards. When you create a cluster and select Advanced security mode, you designate the number of smart cards (2 or 3 of 5 smart cards or 2 of 3 smart cards) that are required to recover the master key when data needs to be retrieved. For example, if you specify 2 of 5 smart cards, then you will need 2 of the 5 smart cards to recover the master key. Each smart card is owned by a Cisco 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. | | | | |

Table 6-1 Master Key Security Levels

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.

| | Description | Considerations | | |
|--------------------------------|---|---|--|--|
| Shared | In shared key mode, only tape volume group keys are generated. All tape | Cisco KMC key database —Is smaller storing only the tape volume group keys. | | |
| | volumes that are part of a tape volume group share the same key. | 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 | | |
| Unique Key | In unique key mode, each individual tape has it's own unique key. | Cisco KMC key database —Is larger storing the tape volume group keys and | | |
| | The default value is enabled. | 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. | Cisco KMC key database — Increases scalability to support a large number of tape volumes by reducing the size of the | | |
| | You can select key-on-tape (when you select unique key mode) to configure the most secure and scalable key | Cisco KMC key database. Only the tape volume group keys are stored on the Cisco KMC. | | |
| | management system. | Security —High. A compromise to a tape | | |
| | The default value is disabled. | integrity of data on other tape volumes. | | |
| | Note When key-on-tape mode is enabled, the keys stored on the tape media are encrypted by the tape volume group wrap key. | Purging —Available at the volume group level. | | |

Table 6-2 Key Management Settings

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.

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

Key Management Operations

This section describes the following key management operations:

- Viewing Standard Security Mode Smart Cards, page 6-5
- Viewing Advanced Security Mode Smart Cards, page 6-6
- Viewing Keys, page 6-6
- Purging Volumes, page 6-7
- Purging Volume Groups, page 6-8
- Exporting Volume Groups, page 6-8
- Importing Volume Groups, page 6-10
- Rekeying Tape Volume Groups, page 6-12
- Basic Mode Master Key Download, page 6-13
- Replacing Smart Cards, page 6-16
- Exporting Volume Groups From Archived Clusters, page 6-29
- Accounting Log Information, page 6-40

Viewing Standard Security Mode Smart Cards

To view Standard security smart card information, follow these steps:

Step 1 Select Smartcards in the navigation pane to view the smart card information.

Figure 6-1 Viewing Standard Security Smart Card Information

| | | | | | Change Password I | Download Logout About Help |
|----------------------------|--|-------------------------|----------|---------------|-----------------------------------|----------------------------------|
| Fabric Manage | er | | | | | |
| CISCO | | | | | | |
| Health Performa | ince Inventory Cust | om SME Admin | | | | User ID: sm |
| SME + Key Manager Settings | | | | | | |
| 🗆 🎯 Clusters | SME: <u>Clusters</u> > <u>clusternar</u> | nel > Smartcards | | | | |
| 😑 🕸 clustername1 | | | | | | |
| | Recovery Shares | | _ | _ | | |
| Tape Groups | Smartcard Label | Smartcard Serial Number | Share ID | Share Version | Master Key GUID | Master Key Version |
| Smartcards | 🔘 card1 | 004000001426026B | 1 | 0 | 3dd7bedc8c67c2bd-ef2a71ee1adcdb4e | 0 |
| | Replace | | | | | |
| | | | | | | |

Viewing Advanced Security Mode Smart Cards

To view Advanced security smart card information, follow these steps:

Step 1 Select Smartcards in the navigation pane to view the smart card information.

Figure 6-2 Viewing Advanced Security Smart Card Information

| SME Key Manager Se | ttings 🔹 | | | | | | | |
|---|----------|----------------------------------|-------------------------|----------|---------------|-----------------------------------|--------------------|--|
| 🗏 🥥 Clusters | SME: | <u>Clusters</u> > <u>cluster</u> | name1 > Smartcards | | | | | |
| Gustemame1 Members | Rec | overy Shares | | | | | | |
| Smartcards | | Smartcard Label | Smartcard Serial Number | Share ID | Share Version | Master Key GUID | Master Key Version | |
| Sindi courda | 0 | admin1 | 0040000015D026B | 1 | 0 | 9a880acf91a0f424-0ef1da7ee6267684 | 0 | |
| | 0 | admin2 | 00800000C8D90269 | 2 | 0 | 9a880acf91a0f424-0ef1da7ee6267684 | 0 | |
| | 0 | SME3 | 004000001626026B | 3 | 0 | 9a880acf91a0f424-0ef1da7ee6267684 | 0 | |
| | 0 | SME4 | 0040000015E6026B | 4 | 0 | 9a880acf91a0f424-0ef1da7ee6267684 | 0 | |
| | 0 | CMEE | 004000001346026B | 5 | 0 | 9a880acf91a0f424-0ef1da7ee6267684 | 0 | |

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 archived. 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.

Figure

| 🔹 SME 🔹 Key Manager Setti | ngs 🔹 | | | | | | |
|---|----------------------------------|-----------------------------|--|----------|-----------|------------------------------|--------------|
| Clusters | SME: <u>Clusters</u> > <u>cl</u> | ustername1 > <u>Tape Gr</u> | oups > <u>TapeGroup1</u> > <u>Volume</u> | Groups : | > Default | : | |
| 🖻 🕸 clustername1 | Volume Group I | Details | | | | | |
| E P Tape Groups | Filter Method: | Regex (.*) | | | | | |
| Tape Devices | Volume Croup | / 0110 | | | | | |
| Image: Second | volume sroup | GUID | Туре | Status | Version | Creation Date | Archival Dat |
| - 🖏 Smartcards | 37a0be0e655dd5 | 546-ff36cf117fe796ac | TapeVolumeGroupWrapKey | Active | 0 | Thu Nov 01 00:49:55 PDT 2007 | |
| | Active Archived | | | | | | |
| | Volumes | | | | | | |
| | Barcode | | GUID | _ | | Creation Date | Versi |
| | 100000 | 5d2171c848f7ecbe | e-a41a1999618cb214 | | | Thu Nov 01 00:52:07 PDT 200 | 7 |
| | 100001 | f1ebf0c15018f862 | -9f994ec94c682833 | | | Thu Nov 01 00:52:15 PDT 200 | 7 |
| | 100002 | c9a20cb97f511285 | 5-812d215b1edd3353 | | | Thu Nov 01 00:52:29 PDT 200 | 7 |

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

Figure 6-4 Viewing Archived Keys

| ululu Esbric Manag | or Woh Client | | | | | |
|--|---|----------------------------|-----------------|---------|------------------------------|---------------|
| cisco Fabric Manage Health Performance In | ventory Custom SME Admin | | | | | User ID: admi |
| 🔹 SME 🔹 Key Manager Settin | 38 🔹 | | | | | |
| 🗏 🎯 Clusters | SME: <u>Clusters</u> > <u>clustername1</u> > <u>Tape Gr</u> | oups > TapeGroup1 > Volume | <u>Groups</u> > | Default | | |
| - 4 clustername1 | Volume Group Details | | | | | _ |
| 🖻 🖤 Tape Groups 🖻 🔍 TapeGroup1 | Filter Method: Regex (.*) | | | | | |
| > Tape Devices =-> Volume Groups | Volume Group Keys | () | - | _ | | |
| Default | GUID | Туре | Status | Version | Creation Date . | Archival Date |
| Smartcards | 37a0be0e655dd546-ff36cf117fe796ac | TapeVolumeGroupWrapKey | Active | 0 | Thu Nov 01 00:49:55 PDT 2007 | |
| | Active Archived | | | | | |
| | Volumes | | | | | |
| | Barcode | GUID | | | Archive Date | Version |
| | 100003 9afe0ca9886b98ec | d-bb5c5efd2f5daeab | | | Thu Nov 01 15:56:22 PDT 200 | 7 0 |
| | 100004 621a5bb7b7538bc | 9-2c298d305c9ad06c | | | Thu Nov 01 15:56:22 PDT 200 | 7 0 |
| | Purge | | | | | |
| | | | | | | |
| | | | | | | |

Purging Volumes

Purging keys deletes archived or active keys from the Cisco KMC. You can delete the archived volume group which purges all keys. If you delete an active volume group, all the keys are archived.

Purging keys at the volume level in unique key mode allows you to purge specific volumes.



Purging keys from the Cisco KMC can not be undone.

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

- Step 1 Select a volume group and click Active or Archived to view the keys that are archived in the Cisco KMC.
- Step 2 Select the archived keys that you want to purge.
- Step 3 Click Remove.

Purging Volume Groups

To purge a volume group, delete an archived tape volume group:

| Step 1 | Select an archived volume group and click Remove. |
|--------|---|
| Step 2 | Click Confirm. |

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 6-29.

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.

Figure 6-5 Exporting a Volume Group



Step 4 Enter the volume group file password. Click **Next**.

| Figure 6-6 | Password Protect a Volume Group File |
|--------------------|---|
| 1 - Enter Password | Export Volume Group : Enter Password |
| 2 - Download File | Information for the volume group HR1 will be exported. Please provide and confirm the password you would like the file to be encrypted with. |
| | Password: |
| | Confirm Password: |
| | |
| | |
| | |
| | |
| | |
| | |
| | ω |
| | Back Next Cancel |

Step 5 Click **Download** to download the volume group file.

- Enter Password - Download File Your file is ready to be downloaded. Click "Download" to begin the download. When it is complete, you can click "Close" to close the wizard. Cluster: clustername1 Tape Group: TapeGroup1 Yolume Group: HR1 Back Download Cancel

Figure 6-7 Download the Volume Group File

Saving the Exported Volume Group File

Step 6 Save the .dat file.

Figure 6-8

<u>Note</u>

The exported volume group file can be used by the Offline Data Restore Tool (ODRT) software to convert the Cisco SME encrypted tape back to clear-text when the Cisco SME line card or the Cisco MDS switch is unavailable. For more information about Offline Data Restore Tool (ODRT), see Appendix B, "Offline Data Recovery in Cisco SME."

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**.



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.

Figure 6-9 Importing a Volume Group File



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.

| Choose file | | | | | ? 🗙 |
|------------------------|--------------------|--------------------|---|----------|------|
| Look <u>i</u> n: | 😂 export | | • | ← 🗈 📸 💷 | |
| 3 | ₿\$3_tg1_Default.c | dat | | | |
| My Recent Documents | | | | | |
| | | | | | |
| Desktop | | | | | |
| | | | | | |
| My Documents | | | | | |
| My Computer | | | | | |
| MAKDESHM-W | | | | | |
| Mv Network | | | | | |
| Places | | | | | |
| | File <u>n</u> ame: | s3_tg1_Detault.dat | | <u> </u> | Open |
| | Files of type: | All Files (".") | | • | |

Figure 6-11 Selecting a File to Import a Volume Group

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

| - Provide File | Import Volume Groups to TapeGroup1 in clustername1 : Confirmation | |
|-------------------|---|--------|
| - Confirmation | From Cluster: s3 | |
| | From Tape Backup Group: tg1 | |
| | From Volume Group: Default | |
| | # of Volume Group Wrap keys: 1 | |
| | # of Volumes Group Shared keys: 1 | |
| | Exported: Thu Oct 11 15:11:52 PDT 2007 | |
| | To Cluster: clustername1 | |
| | To Tape Backup Group: TapeGroup1 | |
| | To Volume Group: Default | ~ |
| | | |
| | | Concel |

Figure 6-12 Importing a Volume Group Confirmation

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.

Figure 6-13

Send documentation comments to mdsfeedback-doc@cisco.com

Selecting Volume Groups to Rekey

| Fabric Manager W | Change Pas eb Client | |
|--|--|----------------------------|
| Health Performance Inve | ntory Custom SME Admin | User ID: qa-admi |
| SME Key Manager Settings | Accounting Log 🔹 | |
| 🗉 🎲 Clusters (1) | SME: <u>Clusters</u> > <u>clustername1</u> > <u>Tape Groups</u> > <u>TapeGroup1</u> > Volume Groups | |
| 🗄 🕼 clustername1 | | |
| Members (1) | Volume Groups | |
| Hosts (1) | Volume Group Name 🔺 | Status |
| Tape Groups (1) | Default | Active |
| B → TapeGroup1 F → TapeGroup2 F → Tap | import Export Create Rekey Remove | |

Step 3 Click **Rekey**. A confirmation dialog box displays asking if the rekey operation is to be performed. Click **OK** to rekey the selected volume groups.



Figure 6-14 Rekeying Tape Volume Group

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.

Figure 6-15

6-15 Downloading the Master Key (Basic Security Mode)

| ululu Eabric Manage | ar Moh Cliont | Change Password Download Logout About Help |
|---------------------------|-----------------------------------|--|
| cisco Fabric Manage | | Lieve TO Ladmin |
| SME ◆ Key Manager Setting | is • | User ID: admin |
| 🗏 🎯 Clusters | SME: <u>Clusters</u> > clusternam | el |
| Members | Cluster Details | |
| Tape Groups | Name: | dustername1 • Online |
| Sinar con us | Nodes: | 1 |
| | Interfaces: | 1 |
| | Fabrics: | Cisco_fabric1 |
| | Security Mode: | Basic Download Keyfle |
| | Master Key GUID: | c35c970d82699fdf-2e957598cbefddea |
| | Key Management Server: | 171.70.222.95 Modify |
| | Id: | 2bd40005300035e1 |
| | Key Settings | |
| | Unique Key Per Media: | res |
| | Tape Settings | |
| | Store Key On Tape: | No |
| | Auto Volume Grouping: | No |
| | Compression: | Yes |
| | Tape Recycle: | Yes |
| | | |

Step 3 Enter the password to protect the master key file. Click **Download** to begin downloading the encrypted file.

Figure 6-16 Enter the Password for the Master Key File

| 🙆 Download Keyfile | Microsoft Internet Explorer provided by Cisco S 🔳 🔲 🗙 | | | |
|--------------------|--|--|--|--|
| 1 - Download | Download Keyfile | | | |
| Keyfile | Provide the password to encrypt the master key file with. When you click "Download", your download of the encrypted file will begin. When you are finished downloading the file, you can click "Close" to close the wizard. File Password: Confirm Password: Back Download Cancel | | | |
| 🙆 Done | Sector Se | | | |

Step 4 Click Close to close the wizard.

| 1 - Download | Download Keyfile |
|--------------|--|
| Keyfile | Provide the password to encrypt the master key file with. When you click "Download", your download of the encrypted file will begin. When you are finished downloading the file, you can click "Close" to close the wizard. |
| | |

Figure 6-17 Confirming the Master Key File Download

Step 5 Click **Save** to save the downloaded master key file.

Figure 6-18 Saving the Download File (Basic Security)



Replacing Smart Cards

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

- Standard Mode, page 6-16
- Advanced Mode, page 6-18

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:

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

Figure 6-19 Display the Smart Card Details



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

Figure 6-20 Insert the New Smart Card

| 🙆 Replace Smartsard - M | icrosoft Internet Explorer provided by Cisco Systems, Inc. 📃 🔲 🔀 | | |
|-------------------------|--|--|--|
| 1 - Store Keyshare | Replace Smartcard : Store Keyshare | | |
| | Insert the smartcard you wish to store the replacement keyshare onto. Please insert a smartcard into the smartcard reader. Looking for smartcard | | |
| | | | |
| | Back Next Cancel | | |
| 🕘 Applet jsap inited | Second intranet | | |

Step 3 Insert the smart card and enter the password, PIN, and label for the smart card. Click Next.

Figure 6-21

Send documentation comments to mdsfeedback-doc@cisco.com

Inserting the Smart Card and Entering Credentials

| 1 - Store Keyshare | Replace Smartcard : Store Keyshare | |
|--------------------|--|--------|
| | Insert the smartcard you wish to store the replacement keyshare Enter your switch credentials and smartcard PIN, then dick next. Username: admin Password: •••••• PIN: •••• Label: SME3 | onto. |
| | | Concol |

Step 4 Click Finish to close the wizard.

Figure 6-22 Standard Security Smart Card Replacement Confirmation



Advanced Mode

In Advanced security mode, the master key is stored on 5 smart cards. Depending on the quorum required to recover the master key, 2 or 3 of the 5 smart cards or 2 of the 3 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.

| Fabric Manage Health Performance | r Web Invento ps • Ad | Client Custom SME A scounting Log + | dmin | | | User ID: qa-admin |
|-------------------------------------|-----------------------------|--|-------------------------|------------|-----------------------------------|--------------------|
| Clusters (1) | SME: | <u>Clusters</u> > <u>clusternam</u> e covery Shares | <u>el</u> > Smartcards | | | |
| Hosts (1) | | Smartcard Label | Smartcard Serial Number | Share ID 🔺 | Master Key GUID | Master Key Version |
| Smartcards | 0 | card1 | 004000018E6026B | 1 | a4a628e42bcb8f36-0b07714f2cd08474 | 0 |
| | ۲ | SME2 | 00400001866026B | 2 | a4a628e42bcb8f36-0b07714f2cd08474 | 0 |
| | 0 | SME3 | 004000001826026B | 3 | a4a628e42bcb8f36-0b07714f2cd08474 | 0 |
| | 0 | sc2-4 | 004000001C66026B | 4 | a4a628e42bcb8f36-0b07714f2cd08474 | 0 |
| | 0 | SME5 | 0040000018A6026B | 5 | a4a628e42bcb8f36-0b07714f2cd08474 | 0 |
| | C | Replace | | | | |

Figure 6-23 Display the Smart Card Details

Step 3 Insert the new smart card. Click **Next**.

Figure 6-24

Send documentation comments to mdsfeedback-doc@cisco.com

Insert the New Smart Card

| 1 - Provide Smartcard | Replace Smartcard : Provide Smartcard | |
|--|--|-----|
| 2 - Get Keyshares 3 - Store Keyshares | Insert the replacement smartcard you wish to store the new keyshare onto. Please insert a smartcard into the smartcard reader. Looking for smartcard | |
| | Back Next Can | cel |

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.

Figure 6-25 Enter the Switch Login and Smart Card Information

| 1 - Provide Smartcard | Replace Smartcard : Provide Smartcard |
|--|--|
| 2 - Get Keyshares 3 - Store Keyshares | Insert the replacement smartcard you wish to store the new keyshare onto. Enter your switch credentials and smartcard PIN, then click next. |
| | Username: ronew Password: ••••• PIN: •••• Label: scl-4 |
| | Back Next Cancel |

Each member of the Cisco Recovery Officer quorum is requested to log in and present their smart card to authorize and authenticate the operation.

)

Send documentation comments to mdsfeedback-doc@cisco.com

Step 5 Insert one of the smart cards that stores the master key. Click Next.

| 1 - Provide Smartcard | Replace Smartcard : Get Keyshares |
|-----------------------|---|
| 2 - Get Keyshares | |
| 3 - Store Keyshares | A quorum of recovery officers needs to present the smartcards to authorize this operation. |
| | 0 of 2 recovery officers have authorized this operation. |
| | Waiting for next smartcard |
| | |
| | |
| | Back Next Cancel |

Figure 6-26 Insert Existing Card (1)

- Step 6 Enter the switch login information and the smart card PIN and label. Click Next.
 - Figure 6-27 Entering Switch Login and Smart Card Credentials (1)

| 1 - Provide Smartcard | Replace Smartcard : Get Keyshares |
|--|---|
| 2 - Get Keyshares 3 - Store Keyshares | A quorum of recovery officers needs to present the smartcards to authorize this operation. Enter your smartcard PIN, then click next |
| | Visername: ro1 Password: ••••• |
| | Label: card1 |
| | Back Next Cancel |

Figure 6-28

Send documentation comments to mdsfeedback-doc@cisco.com

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

Insert an Existing Smart Card (2)



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

Figure 6-29 Entering the Switch Login and Smart Card Credentials (2)

| 2 - Get Keyshares A quorum of recovery officers needs to present the smartcards to authorize this operation. 3 - Store Keyshares Enter your smartcard PIN, then click next 1 of 2 recovery officers have authorized this operation. Username: ro2 Password: •••••• PIN: •••• Label: •••• |
|--|
| Laber. SMES |

Step 9 Insert the smart cards belonging to each recovery officer in any random order.

Figure (

| 6-30 | Inserting Smart Cards |
|------|-----------------------|
|------|-----------------------|

| 1 - Provide Smartcard | Replace Smartcard : Store Keysha | res |
|-----------------------|---------------------------------------|--|
| 2 - Get Keyshares | Now (in any order) insert the replace | ament smartcard, as well every smartcard |
| 3 - Store Keyshares | belonging to each recovery officer (n | ot including the replaced smartcard). |
| | | |
| | Waiting for next smartcard | Smartcards |
| | | 🛐 sc1-4 |
| | | 😰 card1 |
| | | SME3 |
| | | 🗊 sc2-4 |
| | | 🗊 SME5 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | Back Next Cancel |

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.

Entering Switch Credentials and PIN for the First Recovery Officer Figure 6-31

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | | | |
|-----------------------|--|--|--|--|
| 2 - Get Keyshares | New (in any order) incart the conference constant of well every exact and | | | |
| 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as well every smartcard belonging to each recovery officer (not including the replaced smartcard). Enter your smartcard PIN, then click next | | | |
| | Username: ro1 Smartcards Password: •••••• \$ sc1-4 PIN: •••• Label: card1 \$ SME3 \$ SME3 \$ SME5 | | | |
| | Back Next Cancel | | | |

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

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | |
|-----------------------|---|----------------------------------|
| 2 - Get Keyshares | New Concerned a Marco dalla concerned according to the | L |
| 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as well belonging to each recovery officer (not including the replaced | l every smartcard smartcard). |
| | Recovery share successfully stored. | |
| | Please remove your smartcard and insert the smartcard for | Smartcards |
| | the next recovery officer | 😰 sc1-4 |
| | | 🐻 card1 |
| | | 🗊 SME3 |
| | | 🗊 sc2-4 |
| | | 🗊 SME5 |
| | | |
| | | |
| | | |
| | | Back Next Cancel |

Figure 6-32 Storing Keyshare for First Recovery Officer

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

Figure 6-33 Entering Switch Credentials and PIN Information for Second Recovery Officer

| 1 - Provide Smartcard 2 - Get Keyshares | Replace Smartcard : Store Keyshares | |
|--|---|--|
| 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as belonging to each recovery officer (not including the repl Enter your switch credentials and smartcard PIN, then cli Username: ro2 Password: •••••• PIN: ••••• Label: SME3 | s well every smartcard aced smartcard). ck next. Smartcards sc1-4 card1 SME3 SME3 SME5 |
| | | Back Next Cancel |

r

Send documentation comments to mdsfeedback-doc@cisco.com

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

 1 - Provide Smartcard
 Replace Smartcard : Store Keyshares

 3 - Store Keyshares
 Now (in any order), insert the replacement smartcard, as well every smartcard belonging to each recovery officer (not including the replaced smartcard).

 Image: Comparison of the next recovery officer...
 Recovery share successfully stored.

 Please remove your smartcard and insert the smartcard for the next recovery officer...
 Smartcards

 Image: SME3
 Image: SME3

 Image: SME3
 Image: SME3

 Image: SME5
 Image: SME5

Figure 6-34 Storing Keyshare for the Second Recovery Office

c. Enter the switch credentials and PIN information for the third recovery officer. Click Next8

Figure 6-35 Entering Switch Credentials and PIN information for the Third Recovery Officer

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | |
|--|--|--|
| 2 - Get Keyshares 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, a belonging to each recovery officer (not including the rep Enter your switch credentials and smartcard PIN, then cl | s well every smartcard laced smartcard). ick next. |
| | Username: ro3 Password: •••••• PIN: •••• Label: sc1-4 | Smartcards sc1-4 card1 SME3 Sc2-4 SME5 |
| | | Back Next Cancel |

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

| Get Kevshares | | | | _ |
|---------------------|---|----------------|-----------|---|
| 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as well belonging to each recovery officer (not including the replaced | every smart | smartcard | |
| | Recovery share successfully stored. | | | |
| | Please remove your smartcard and insert the smartcard for | Smartcards | | |
| | the next recovery officer | 5 | sc1-4 | |
| | | 5 | card1 | |
| | | 5 | SME3 | |
| | | <u>5</u> | sc2-4 | |
| | | <u>5</u> | SME5 | |
| | | | | |
| | | | | |

Figure 6-36 Storing Keyshare for the Third Recovery Officer

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

Figure 6-37 Entering Switch Credentials and PIN information for the Fourth Recovery Office

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | |
|--|---|---|
| 2 - Get Keyshares 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as well belonging to each recovery officer (not including the replaced Enter your switch credentials and smartcard PIN, then click ne | every smartcard smartcard). xt. |
| | Username: ro4 Password: ••••• PIN: •••• Label: SME5 | Smartcards sc1-4 card1 SME3 sc2-4 SME5 |
| | | Back Next Cancel |

r

r

r

Send documentation comments to mdsfeedback-doc@cisco.com

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

Figure 6-38 Storing Keyshare for the Fourth Recovery Officer

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | | | |
|-----------------------|---|------------------|--|--|
| 2 - Get Keyshares | | | | |
| 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as well every smartcard belonging to each recovery officer (not including the replaced smartcard). | | | |
| | Recovery share successfully stored. | | | |
| | Please remove your smartcard and insert the smartcard for | Smartcards | | |
| | the next recovery officer | ₩ sc1-4 | | |
| | | 🐻 card1 | | |
| | | 🐻 SME3 | | |
| | | 😰 sc2-4 | | |
| | | NE5 SME5 | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | Back Next Cancel | | |

e. Enter the switch credentials and PIN information for the fifth recovery officer. Click Next.

Figure 6-39 Entering Switch Credentials and PIN information for the Fifth Recovery Officer

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | |
|--|--|---|
| 2 - Get Keyshares 3 - Store Keyshares | Now (in any order), insert the replacement smartcard, as well eve belonging to each recovery officer (not including the replaced sma Enter your switch credentials and smartcard PIN, then click next. | ery smartcard artcard). |
| | Username: ro5 Sn Password: ••••• PIN: •••• Label: sc2-4 | sc1-4 card1 SME3 sc2-4 SME5 |
| | В | ack Next Cancel |

A notification is shown that the fifth keyshare is successfully stored. Click **Next** to begin the automatic synchronization of volume groups.

| 1 - Provide Smartcard | Replace Smartcard : Store Keyshares | |
|-----------------------|--|--|
| 2 - Get Keyshares | | |
| 3 - Store Keyshares | Recovery share(s) successfully stored. | |
| | Please click Next to begin automatic synchronization of volume groups. | Smartcards Sc1-4 Card1 SME3 SME5 SME5 |
| | | Back Next |

Figure 6-40 Storing Keyshare for the Fifth Recovery Officer

You will see an indication that the operation is in progress until the synchronization of volume groups is completed.

Figure 6-41 Synchronizing Volume Groups



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.

| 1 - Provide Smartcard | Replace Smartcard : Finish |
|-----------------------|----------------------------|
| 2 - Get Keyshares | |
| 3 - Store Keyshares | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | Rade Class |

Figure 6-42 Completing Smart Card Replacement

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.

Figure 6-43 Viewing the New Smart Card Information

| Fabric Manager | Web Clie | ent | | | Change Password Dow | nload Logout About | l Help |
|--|------------------------------|---|-----------------------------------|------------|-----------------------------------|------------------------|--------|
| Health Performance In | ventory Cu | ustom SME Adm | in | | | User ID: qa- | -adm |
| SME + Key Manager Settings | Accounti | ing Log 🔹 | | | | | |
| E 🌍 Clusters (1) | SME: C | lusters > <u>clusternan</u> | nel > Smartcards | | | | |
| tustername1 Members (1) | | | | | | | |
| Hosts (1) | M N | laster key success olume groups reke | fully rekeyed. v successfully. | | | | |
| E D Tape Groups (1) | V | olume groups syne | chronized successfully. | | | | |
| Smartcards | Poc | avon Sharos | | | | | |
| | Kecc | Smartcard Label | Smartcard Serial Number | Share ID 🔺 | Master Key GUID | Master Key Version | |
| | 0 | card1 | 0040000018E6026B | 1 | 6530c892e2588c3c-a2703831fc63fc14 | 1 | ~ |
| | 0 | SME3 | 00400001826026B | 2 | 6530c892e2588c3c-a2703831fc63fc14 | 1 | |
| | 0 | sc1-4 | 004000061DB026A | 3 | 6530c892e2588c3c-a2703831fc63fc14 | 1 | |
| | 0 | SME5 | 004000018A6026B | 4 | 6530c892e2588c3c-a2703831fc63fc14 | 1 | |
| | 0 | sc2-4 | 00400001C66026B | 5 | 6530c892e2588c3c-a2703831fc63fc14 | 1 | |
| | | | | | | | V |
| | Re | eplace | | | | | |
| | | | | | | | |
| | Old I | Recovery Shares | | | | | |
| | Sm | nartcard Label | Smartcard Serial Number | Share ID A | Master Key GUID | Master Key Version | - |
| | Carda | | 040000018660268 | - | a4a528642bcb6136-0507714f2cd08474 | 0 | |
| | CMES | | 040000018060268 | 2 | a4a6286428C66136-080771412C606474 | 0 | |
| | SPIE 2 | | 04000001020020B | 4 | a4a628e42bcb8f35-0b07714f2cd08474 | 0 | |
| | SC2-4 | | 04000001000268 | | a4a528a42bcb6136-0507/14120008474 | 0 | |
| | SMES | 5 U | 04000010400268 | 5 | a4a6206420c06f36-000//14f2cd084/4 | U | |

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 6-29
- Standard Mode, page 6-32
- Advanced Mode, page 6-35

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**.

Figure 6-44 Select the Volume Group to Export

| Fabric Manage Health Performance In | er Web Client rentory Custom SME Admin | Change Password | Download | Logout | About Help User ID: admin |
|--|--|-----------------|----------|--------|--------------------------------|
| E 🥹 Clusters E-IP dustername1 | SME: <u>Clusters</u> > <u>clustername1</u> > <u>Tape Groups</u> > <u>tapegroup1</u> > <u>Volume Groups</u> | | | | _ |
| Tape Groups Tape Groups Tape Devices Solution Tape Devices Solution Default Smartcards | Volume Group Name Ocfault Import Create Remove | | | | Status Archived |
| | | | | | |

Step 2 Click **Browse** to locate the volume group master key file.

| 🙆 Export Volume G | roup - Microsoft Internet Explorer provided by Cisc 🔳 🔲 🔀 |
|--|---|
| 1 - Upload File | Export Volume Group : Upload File & Enter Password |
| 2 - Provide Password 3 - Download File | Information for the archived volume group Default will be exported. Please provide the master key file, and the password used to encrypt the master key. Master Key File: Browse |
| | |
| | Back Next Cancel |
| 🙆 Done | Second Intranet |

Figure 6-45 Export Volume Group Wizard

Step 3 Select the master key file. Click **Open**.

| Choose file | | | | | ? 🗙 |
|---|--|---|------------------|---|------------------------|
| Look <u>i</u> n: | 🔁 basic | | • E | ≠ | |
| My Recent Documents Desktop | dustername1_c | 35c970d82699fdf-2e957598cbe | fddea_mk.dat | | |
| My Documents My Computer MAKDESHM-W My Network Places | | | | | |
| | File <u>n</u> ame: Files of <u>t</u> ype: | clustername1_c35c970d82699fi All Files (*.*) | 1f-2e957598cbefi | | <u>O</u> pen Cancel |

Figure 6-46 Select the Master Key File

Step 4 Enter the password that protects the master key for the archived volume group. Click Next.

Figure 6-47 Enter the Master Key File Name and Password

| 🙆 Export Volume G | roup - Microsoft Internet Explorer provided by Cisc 📃 🔲 🔀 |
|--|---|
| 1 - Upload File | Export Volume Group : Upload File & Enter Password |
| 2 – Provide Password 3 – Download File | Information for the archived volume group Default will be exported. Please provide the master key file, and the password used to encrypt the master key. |
| | Master Key File: C:\Documents and Se Browse Master Key File Password: |
| 🙆 Done | Succal intranet |

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.

Figure 6-49 Download the Volume Group File



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

Figure 6-50

File Download Do you want to open or save this file? Image: clustername1_tapegroup1_Default.dat Type: XML Document From: localhost Image: Open Save Cancel Image: While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file.

Save the Exported Volume Group File

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**.

Figure 6-51 Viewing Volume Groups

| Fabric Manage Health Performance In SME + Key Manager Setting | er Web Client ventory Custom SME Admin | | User ID: admi |
|---|---|---|---------------|
| Clusters Clustername1 Small Ammbers Small Ammbe | SME: <u>Clusters</u> > <u>dustername1</u> > <u>Tap</u> Volume Groups | <u>e Groups > tapegroupi</u> > Volume Groups | |
| Tape Groups Tape Devices Volume Groups Volume Groups Smartcards | Default Import Export Creation | Volume Group Name | Status |

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.

Figure 6-53 Enter the Smart Card PIN and Label

| 1 - Get Recovery | Export Volume Group : Get Recovery Shares |
|---|---|
| Shares 2 - Provide Password 3 - Download File | Information for the archived volume group Default will be exported. Enter your smartcard PIN, then dick next 0 of 1 keyshares retrieved. Label: SME3 PIN: •••• |
| | Back Next Cance |
| Applet isap started | Second intranet |

Step 4 Enter the password to encrypt the volume group file. Click Next.

Figure 6-54 Enter the Password to Encrypt the Volume Group File

| 1 - Get Recovery Shares | Export Volume Group : Provide Password |
|----------------------------|--|
| 2 - Provide Password | Provide the password that will be used to encrypt the exported file. |
| 3 - Download File | Password: ••••••• |
| | Back Next Cancel |

Step 5 Click **Download** to begin downloading the file.

Figure 6-55 Download the Volume Group File

| 🛎 Export Volume Grou | ıp - Microsoft Internet Explorer provided by Cisc 📃 🔲 🔀 |
|----------------------------|--|
| 1 - Get Recovery Shares | Export Volume Group : Download File |
| 2 - Provide Password | Your file is ready to be downloaded. Click "Download" to |
| 3 - Download File | "Close" to close the wizard. |
| | Cluster: dustername1 Tape Group: tapegroup1 |
| | Volume Group: Default |
| | |
| | |
| | |
| | Back Download Cancel |
| 🕘 Applet jsap started | Second Se |

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**.

Figure 6-57 Viewing Volume Groups



Figure 6-58

Send documentation comments to mdsfeedback-doc@cisco.com

Step 2 Insert one of the five smart cards into the smart card reader. Click Next.

Insert a Smart Card

| Charac | |
|---|--|
| 2 - Provide Password 3 - Download File | Information for the archived volume group Default will be exported. Please insert a smartcard into the smartcard reader. 0 of 2 keyshares retrieved. Looking for smartcard |
| | Back Next Cance |

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

rt Card Pin and Labol . . ~

| Figure 6-59 | Enter the Smart Card Pin and Label | |
|-------------|------------------------------------|--|
| J | | |

| 🖲 Export Volume Grou | p - Microsoft Internet Explorer provided by Cisc 📃 🔲 🔀 |
|---|--|
| 1 - Get Recovery | Export Volume Group : Get Recovery Shares |
| Shares 2 - Provide Password 3 - Download File | Information for the archived volume group Default will be exported. Enter your smartcard PIN, then dick next 0 of 2 keyshares retrieved. Label: <u>SME5</u> PIN: •••• |
| | Back Next Cancel |
| 🕘 Applet jsap started | 🚽 🔤 Local intranet |

The keyshare is retrieved.

Send documentation comments to mdsfeedback-doc@cisco.com

```
Step 4 Insert the next smart card into the smart card reader. Click Next.
```



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, 2 of 5 smart cards.

Figure 6-60 Insert the Second Smart Card

| L - Get Recovery | Export Volume Group : Get Recovery Shares |
|---|---|
| 2 - Provide Password 3 - Download File | Information for the archived volume group Default will be exported. Keyshare successfully retrieved. Please insert the next smartcard 1 of 2 keyshares retrieved. Waiting for next smartcard |
| | Back Next Cancel |

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

Figure 6-61 Enter the Smart Card PIN and Label for the Second Smart Card

| Charee | Export Volume Group : Get Recovery Shares | | | | | | | |
|---|--|--|--|--|--|--|--|--|
| 2 - Provide Password 3 - Download File | Information for the archived volume group Default will be exported. Enter your smartcard PIN, then dick next 1 of 2 keyshares retrieved. Label: SME PIN: ••••• | | | | | | | |
| | Back Next Cance | | | | | | | |

Step 6 Enter the volume group file password. Click **Next**.



Figure 6-62 Enter the Volume Group File Password

Step 7 Click **Download** to begin downloading the volume group.

| 1 - Get Recovery Shares | Export Volume Group : Download File | | | | | | | | |
|----------------------------|---|--|--|--|--|--|--|--|--|
| 2 - Provide Password | Your file is ready to be downloaded. Click "Download" to | | | | | | | | |
| 3 - Download File | begin the download. When it is complete, you can dick "Close" to close the wizard. | | | | | | | | |
| | Cluster: dustername1 | | | | | | | | |
| | Tape Group: tapegroup1 Volume Group: Default | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | Back Download Cancel | | | | | | | | |
| Applet isap started | 🔍 Local intranet | | | | | | | | |

Figure 6-63 Download the Volume Group

Step 8 Click **Save** to save the **.dat** file.

Figure 6-64 Save the Volume Group File

| Do you v | vant to open or save this file? |
|----------|---|
| | Name: clustername1_tapegroup1_Default.dat |
| | Type: XML Document |
| | From: localhost |
| | Open Save Cancel |
| | While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. |

I

Accounting Log Information

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

- Viewing Accounting Log Information, page 6-40
- KMC Accounting Log Messages, page 6-41

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.

Figure 6-65 Accounting Log

| | | | | | | | | | | | | Change Passw | ord | Download | Logout | About | l Hel | р |
|------|-------------------------|--|---------------|------------------------------|------------------------------------|----------------------------|-----------------------------|--------------------------|-------------------------------|-------------------------|------------|------------------------|------------|---------------|-------------|----------|-------|----|
| aha | 10 | Fabric Man | ager W | eb Client | | | | | | | | | | | | | | |
| ciso | H | ealth Performa | nce Inve | ntory Custo | m SME Adr | min | | | | | | | | | | | | |
| | | | | | | _ | _ | _ | | | | | | | | USER ID: | aum | |
| | SME | Key Manager | Settings 🔹 | Accounting | Log 🔹 | | | | | | | | | | | | | |
| Ac | countir | ng Log | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | _ | _ |
| I r | () vw | CLealestion / | uar/local/ala | | //ogo/como.Acco | ounting lo | ~ | | | | | | | | | | | 1 |
| | W KIN | c Log Location. /c | isi/iucai/cis | co_mas9000, | /logs/silleAcco | Junting.10 | y | | | | | | | | | | _ | |
| | | | | | | | | | | | | | | | | | | |
| | Accou | nting Log | | | | | | | | | | | | | | | | 1 |
| | Filter: | | Go | Clear Filter | | | | | | | | | | | | | | |
| | 2008.0 | 2 12 11-31-48 INFC | ISME ACC | 1 Stored tane | volume key fo | r cluster: / | -1 id- 24540 | 10053001a3 | 2c5 tane grou | in: t tane volu | ime aroun | Default barcode | e Unk | nown GUID: | 547a2077 | 91acbd91 | | |
| | 563038 | de5c59a251 | |) Detrived lape | for for all the | | | 14-225-2 | 1-61-7246-00 | 1-04 | anie group | | | | 54762577 | | | |
| | 2008.0 | 2.12 11:31:48 INFC | SME.ACC | Archived key | for for cluster | r: c1 GUID | : 0c6d6215 | 1de325e2- | dafde734fc06 | 51e24 | | | | | | | | |
| | 2008.0 25c7ad | 2.12 11:31:48 INFC 0ce85e99fc | SME.ACC | Stored tape | volume key to | r cluster: (| c1 id: 24540 | 00053001a2 | 2c5 tape grou | ip: t tape volu | ime group | Default barcode | s: Unk | nown GUID: | 20ec7c644 | t7a6dle | | |
| | 2008.0 | 2.12 11:31:48 INFC | SME.ACC | Retrived key | for for cluster | C c1 GUID | e98676b1 | 6556b519- | c5b717db9da | 0049c | | | | | | | | |
| | 2008.0 | 2.12 11:31:48 INFO | SME.ACC | Stored tape | volume key fo | r cluster: o | c1 id: 24540 | 00053001a2 | 2c5 tape grou | ip: t tape volu | ime group | Default barcode | s: Unk | nown GUID: | 0a39fed9b | f899832- | | |
| | 2008.0 | 2.12 11:31:48 INFC | SME.ACC | Retrived key | for for cluster | c1 GUID | : 547a2077 | 91acbd91-9 | 5b3038de5c59 | 9a251 | | | | | | | | |
| | 2008.0 | 2.12 11:31:48 INFC 2.12 11:31:49 INFC | SME.ACC | Archived key Stored tape | / for for cluster volume kev fo | r: c1 GUIE r cluster: (|): 547a2077 c1 id: 24540 | 791acbd91- 00053001a2 | 5b3038de5c5 2c5 tape grou | 9a251 ip:ttape.volu | ume aroup | Default barcode | : Unk | nown GUID: | 256081a6 | e5f0826b | | |
| | c4db23 | b1cf31f071 2 12 11:31:49 INFC | ISME ACC | I Retrived key | for for cluster | | 20ec7c644 | 4f7a6d1e=2 | 5c7ad0ce85e | aafe | | | | | | | | |
| | 2008.0 | 2.12 11:31:49 INFC | SME.ACC | Archived key | for for cluster | r: c1 GUID | : 20ec7c64 | 4f7a6d1e-2 | 25c7ad0ce85e | a99fc | | | | | | | | |
| | 2008.0. 5d4264 | 2.12 11:31:49 INFC 0f6e8edf7f | ISME.ACC | j Stored tape | volume key to | r cluster: (| ci id: 24540 | JUU53UU1a2 | 2c5 tape grou | ip: t tape volu | ime group | Default barcode | s: Unk | nown GUID: | TatdU946D | 80225CD- | | |
| | 2008.0 | 2.12 11:31:49 INFC 2.12 11:31:49 INFC | SME.ACC | Retrived key Archived key | for for cluster for for cluster | r: c1 GUID r: c1 GUID | : 0a39fed9b): 0a39fed9b | bf899832-1 bf899832-1 | 6d419793bdb 6d419793bdb | off2a bff2a | | | | | | | | |
| | 2008.0 | 2.12 11:31:49 INFC | SME.ACC | Stored tape | volume key fo | r cluster: (| c1 id: 24540 | 00053001a2 | 2c5 tape grou | ip: t tape volu | ime group | Default barcode | e: Unk | nown GUID: | 1763d41fe | c9c1713 | • | |
| | 2008.0 | 2.12 11:31:49 INFC | SME.ACC | Retrived key | for for cluster | : c1 GUID | : 256081a6 | e5f0826b-c | 4db23b1cf31 | f071 | | | | | | | | |
| | 2008.0 | 2.12 11:31:49 INFC | SME.ACC | Stored tape | volume key fo | r cluster: o | c1 id: 24540 | 00053001a2 | 2c5 tape grou | ip: t tape volu | ume group | Default barcode | : Unk | nown GUID: | dbd8e9b1 | 3c34c4ae | - | |
| | aa1597 2008.0 | '2ad6bec3f4 2.12 11:31:49 INFC | SME.ACC | Retrived key | for for cluster | c1 GUID | : fafd0946b | 80225cb-5 | d42640f6e8ec | df7f | | | | | | | | |
| | 2008.0 | 2.12 11:31:49 INFC | SME.ACC | Archived key | / for for cluster | r: c1 GUID |): fafd0946b | 080225cb-5 | id42640f6e8e | df7f in: t tane volu | ime aroun | Default barcode | e Unk | nown GUID: | 6c6e89b1 | 72aa81c5 | | |
| | 2e82f6 | 76504b4bbc | | Journal aper | volume key to | r cluster. t | | 0.4740.5 | co cape grou | ip. c tape voio | ine group | . Derault barcoue | 5. Olik | nown Gorb. | 00060301 | 2000100 | | |
| | 2008.0 | 2.12 11:31:50 INFC | SME.ACC | Archived key | for for cluster | r: c1 GUID |): 1763d41fe | ec9c1/13-5 ec9c1713-5 | 9c52/ar46c50 59c527af46c5 | b131 | | | | | | | | |
| | 2008.0 773adc | 2.12 11:31:50 INFC 2699195ba4 | SME.ACC |] Stored tape | volume key fo | r cluster: (| c1 id: 24540 | 00053001a2 | 2c5 tape grou | ip: t tape volu | ime group | Default barcode | a: Unk | nown GUID: | 2f5438e70 | be166c3 | - | |
| | 2008.0 | 2.12 11:31:50 INFC | SME.ACC | Retrived key | for for cluster | : c1 GUID | : dbd8e9b1 | 3c34c4ae-a | aa15972ad6b | ec3f4 | | | | | | | | |
| | 2008.0 | 2.12 11:31:50 INFC | SME.ACC | Stored tape | volume key fo | r cluster: o | c1 id: 24540 | 00053001a2 | 2c5 tape grou | ip: t tape volu | ume group | Default barcode | e: Unk | nown GUID: | 2549191b | 4daa06c9 | I- | |
| | 2008.0 | 2.12 11:31:50 INFC | SME.ACC | Retrived key | for for cluster | c1 GUID | : 6c6e89b13 | 72aa81c5-2 | 2e82f676504b | o4bbc | | | | | | | | |
| | 2008.0 | 2.12 11:31:50 INFC 2.12 11:31:50 INFC | SME.ACC | Archived key Stored tape | / for for cluster volume key fo | r: c1 GUIE r cluster: (|): 6c6e89b1 c1 id: 24540 | 72aa81c5- | 2e82f676504b 2c5 tape grou | b4bbc ip:ttape.volu | ume aroup | Default barcode | a: Unk | nown GUID: | 104a71e1 | Da3e5a9d | - | ÷ |
| | 57cbe1 | 29f4f352ce | ISME ACC | Petrived key | for for cluster | et GUTD | 2f5438e70 | 0be166c2-7 | 73adc269010 | asha4 | 5 | | | | | | | 0 |
| | 2008.0 | 2.12 11:31:50 INFC | SME.ACC | Archived key | for for cluster | r: c1 GUID | : 2f5438e70 | Obe166c3-7 | 773adc269919 | 95ba4 | | | | | | | ~ | 5 |
| | < | The second second second | the me aren | is found tone . | united from to | e constant i | an ian fiasan | and shows. | | and there well | | i i internite harroade | the letter | Come Chilling | S CORDECTAL | | > | 12 |

- **Step 3** Enter a pattern in the Filter and click **Go**. The accounting pattern is displayed based on the selected pattern.
- **Step 4** Click **Clear Filter** to display the complete accounting log information.

KMC Accounting Log Messages

The accounting.log file in the FM log directory displays the KMC accounting log messages. These messages appear as follows:

Stored master key for cluster: <cluster name> id: <cluster Id> GUID: <guid>

Failed to store master key for cluster: <cluster name> id: <cluster Id> GUID: <guid> Error: <description>

Stored tape volume group shared key for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> GUID: <guid>

Failed to store tape volume group shared key for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> GUID: <guid> Error: <description>

Stored tape volume group wrap key for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> GUID: <guid>

Failed to store tape volume group wrap key for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> GUID: <guid> Error: <description>

Stored tape volume key for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> GUID: <guid> barcode <barcode>

Failed to store tape volume key for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> GUID: <guid> barcode <barcode> Error: <description>

Archived key for for cluster: <clusterName> GUID: <guid>

Failed to archive key for cluster: <clusterName> GUID: <guid> Error: <description>

Archived all keys for for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name>

Failed to archive keys for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> Error: <description>

Archived all keys for for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> barcode <barcode>

Failed to archive keys for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name> barcode <barcode> Error: <description>

Purged key for for cluster: <cluster name> GUID: <guid>

Failed to purge key for cluster: <cluster name> GUID: <guid> Error: <description>

Retrieved key for for cluster: <cluster name> GUID: <guid>

Failed to retrieve key for cluster: <cluster name> GUID: <guid>

Retrieved key for for cluster: <cluster name> Cloned from GUID: <guid>

Failed to retrieve key for cluster: <cluster name> Cloned from GUID: <guid>

Delete Tape Volume Keys for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>

Delete Tape Volume Keys for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>

Delete Tape Volume Group Wrap Keys for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>

Export initiated for archived cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name>

Export failed for archived cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Error: masterKey was null

Export failed for archived cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Error: failed to unwrap wrapKey

Export failed for archived cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Error: failed to rewrap wrap key w/ password

Export completed for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name>. Exported <count> keys.

Failed to start master key rekey transaction for cluster <cluster name>. Failed to send message to switch. Error: <description>

Master key rekey started for cluster <cluster name>

Failed to start master key rekey for cluster <cluster name>. Error: <description>

Failed to start master key rekey for cluster <cluster name>. Failed to parse message from switch. Error: <description>

Failed to commit master key rekey transaction for cluster <cluster name>. Failed to send message to switch. Error: <description>

Master Key rekey transaction successful for cluster <cluster name>

Failed to commit master key rekey transaction for cluster <cluster name>. Error: <description>

Failed to commit master key rekey transaction for cluster <cluster name>. Failed to parse message from switch. Error: <description>

Aborted old pending Master Key rekey transaction for cluster <cluster name>

Failed to abort old Master Key re-key transaction for cluster <cluster name>. Error: <description>

Failed to abort old Master Key re-key transaction for cluster <cluster name>. Failed to parse message from switch. Error: <description>

Master key share retrieved for share index <index> for guid <guid> for cluster <cluster name> smartcard label: <label> smartcard serial number: <serial number>

Failed to retrieve master key share for index <index> for guid <guid> for cluster <cluster name> smartcard label: <label> smartcard serial number: <serial number>. Error: <description>

Cloning Volume group keys failed after master key rekey for cluster: <cluster name>. <count> keys of <total count> cloned

Cloned tape volumegroup wrap keys because of master key rekey for cluster: <cluster name>

Successfully cloned <count> of <total count> Tape Volume Group wrap keys

Export initiated for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name>

Export completed for cluster: <cluster name> id: <cluster Id> tape group: <tape group name> tape volume group: <tape volume group name>. Exported <count> keys.

Import initiated for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>.

Import failed for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Error: <description>

Import completed for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>.

Import failed for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Failed to Import keys. Imported <count> of <total count> Tape Volume Group wrap keys. Skipped: <skipped count>. Error: <description>

Import failed for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Invalid response received from switch. Imported <count> of <total count> Tape Volume Group wrap keys. Skipped: <skipped count>

Import failed for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Failed to Import keys. Imported <count> of <total count> Tape Volume media keys. Skipped: <skipped count>. Error: <description>

Import failed for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Invalid response received from switch. Imported <count> of <total count> Tape Volume media keys. Skipped: <skipped count>

Import for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Successfully imported <count> of <total count> Tape Volume Group wrap keys. Skipped: <skipped count>

Import for cluster: <cluster name> tape group: <tape group name> tape volume group: <tape volume group name>. Successfully imported <count> of <total count> Tape Volume media keys. Skipped: <skipped count>