



CHAPTER 6

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 When a cluster state is Archived (the key database has been archived) and you want to recover the keys, you will need the master key file or the smart cards.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.

Send documentation comments to mdsfeedback-doc@cisco.com

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 itself. 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



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.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)


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 6-1 Master Key Security Levels

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

Send documentation comments to mdsfeedback-doc@cisco.com

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

	Description	Considerations
Shared	In shared key mode, only tape volume group keys are generated. All tape volumes that are part of a tape volume group share the same key.	<p>Cisco KMC key database—Is smaller storing only the tape volume group keys.</p> <p>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.</p> <p>Purging—Available only at the volume group level</p>
Unique Key	In unique key mode, each individual tape has its own unique key. The default value is enabled.	<p>Cisco KMC key database—Is larger storing the tape volume group keys and every unique tape volume key.</p> <p>Security—High. A compromise to a tape volume key will not compromise the integrity of data on other tape volumes.</p> <p>Purging—Available at the volume group and volume level.</p>
Unique Key with Key-On-Tape	<p>In the key-on-tape mode, each unique tape volume key is stored on the individual tape.</p> <p>You can select key-on-tape (when you select unique key mode) to configure the most secure and scalable key management system.</p> <p>The default value is disabled.</p> <p>Note When key-on-tape mode is enabled, the keys stored on the tape media are encrypted by the tape volume group wrap key.</p>	<p>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.</p> <p>Security—High. A compromise to a tape volume key will not compromise the integrity of data on other tape volumes.</p> <p>Purging—Available at the volume group level.</p>

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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:

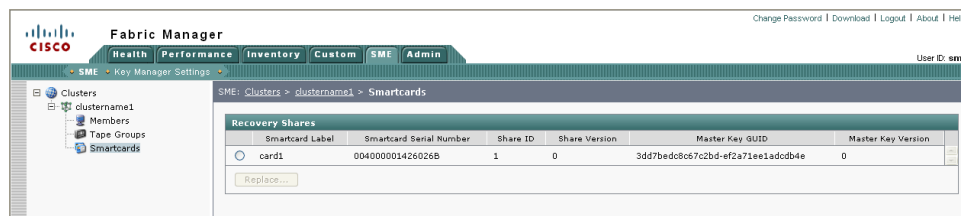
- [Viewing Standard Security Mode Smart Cards, page 6-5](#)
- [Viewing Advanced Security Mode Smart Cards, page 6-6](#)
- [Viewing Keys, page 6-6](#)
- [Purging Volumes, page 6-7](#)
- [Purging Volume Groups, page 6-8](#)
- [Exporting Volume Groups, page 6-8](#)
- [Importing Volume Groups, page 6-10](#)
- [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



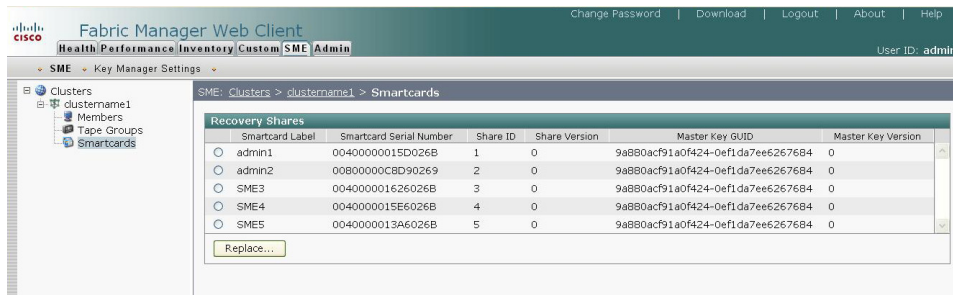
Send documentation comments to mdsfeedback-doc@cisco.com

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



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.

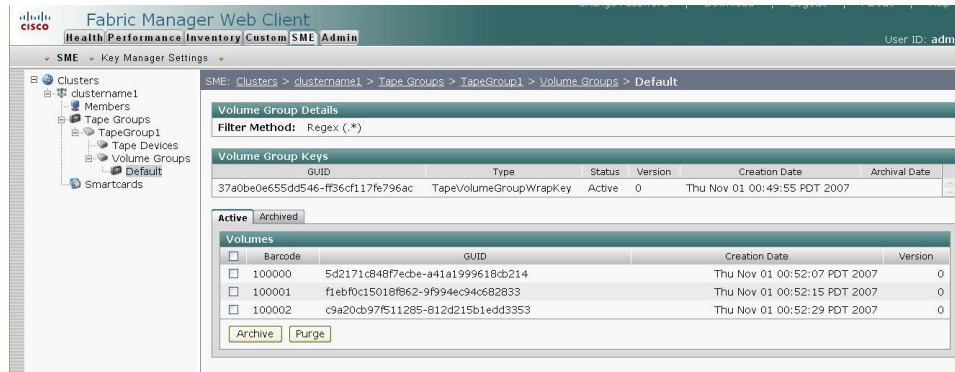
In the unique key mode, only the wrap key is showing. The wrap key is the tape volume group key that wraps volume keys. If shared mode is selected, the wrap key and a shared key are in view. The wrap key wraps the shared key. Keys are listed as TapeVolumeGroupWrapKey or the TapeVolumeGroupSharedKey.

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.

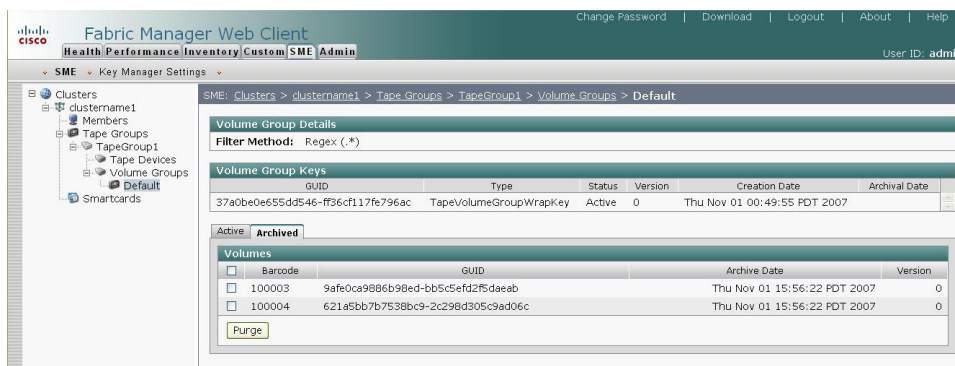
Send documentation comments to mdsfeedback-doc@cisco.com

Figure 6-3 Viewing Active Keys



- 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



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.



Caution

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**.

Send documentation comments to mdsfeedback-doc@cisco.com

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**.

Send documentation comments to mdsfeedback-doc@cisco.com

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:

185618

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

Figure 6-7 Download the Volume Group File

- Enter Password **Export Volume Group : Download File**

- 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.

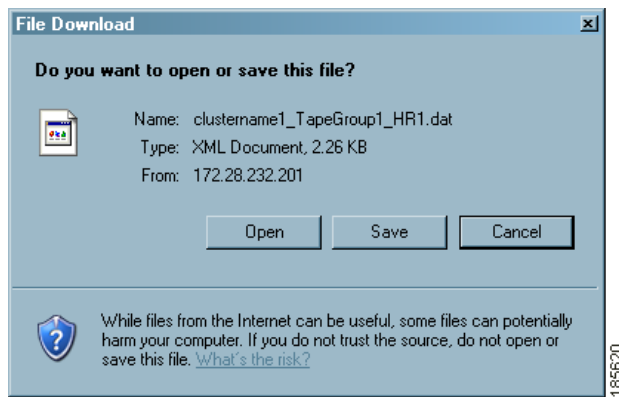
Cluster: clustername1
Tape Group: TapeGroup1
Volume Group: HR1

185619

Send documentation comments to mdsfeedback-doc@cisco.com

Step 6 Save the .dat file.

Figure 6-8 Saving the Exported Volume Group File



Note

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.

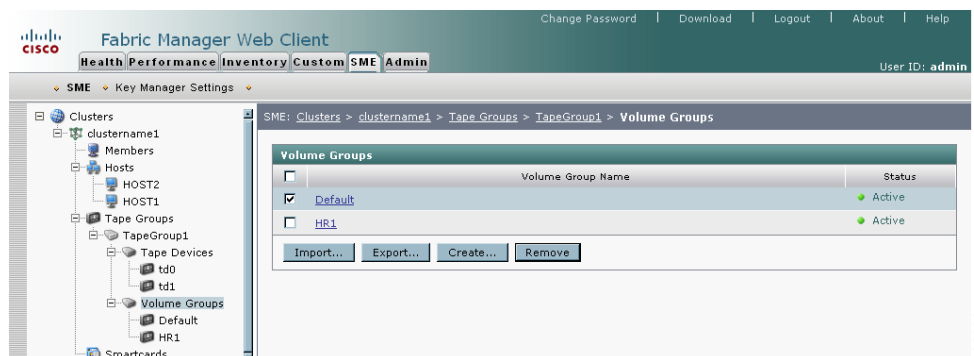
Step 2 Select a volume group and click **Import**.



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.

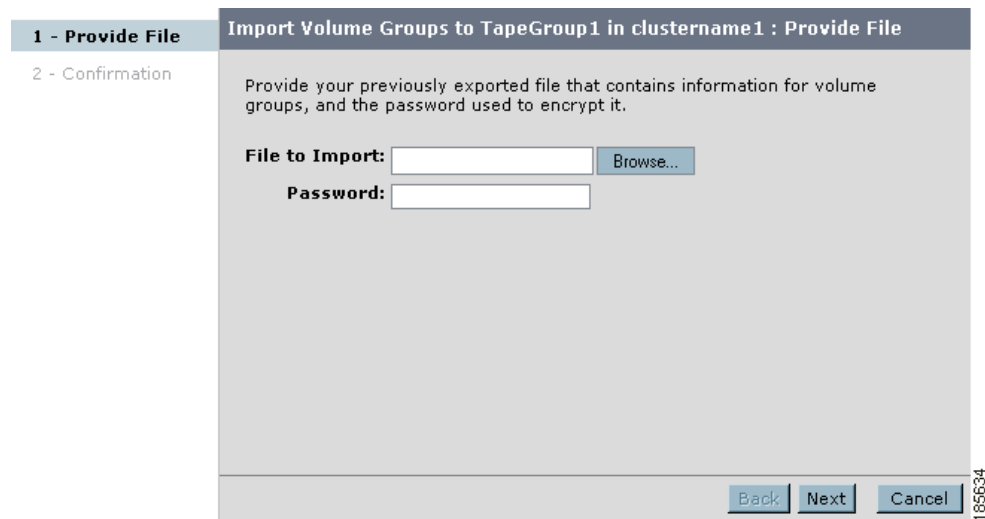
Figure 6-9 Importing a Volume Group File



Send documentation comments to mdsfeedback-doc@cisco.com

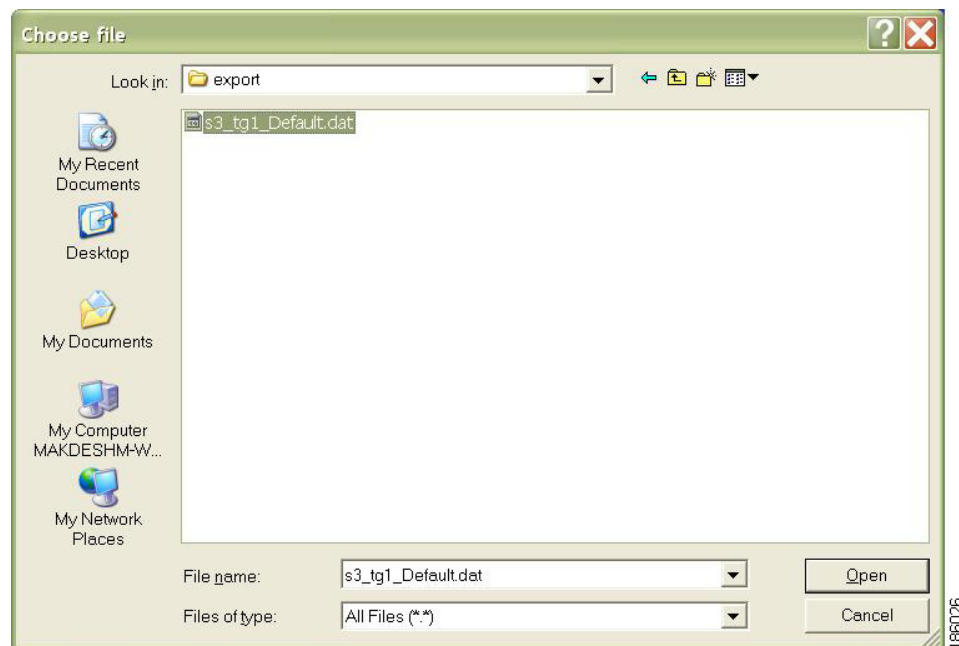
Step 3 Locate the file to import. Enter the password that was assigned to encrypt the file. Click **Next**.

Figure 6-10 Importing a Volume Group to an Existing Tape Group



Step 4 Select the volume group **.dat** file. Click **Open**.

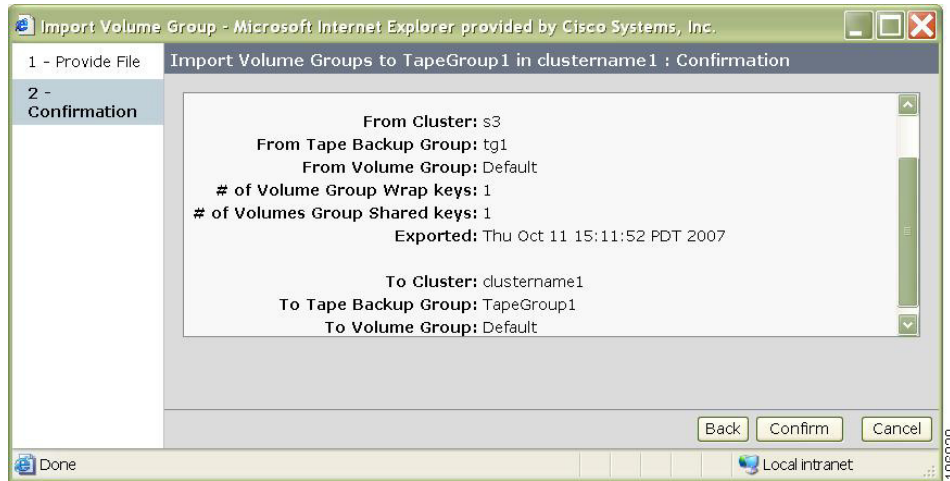
Figure 6-11 Selecting a File to Import a Volume Group



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

Send documentation comments to mdsfeedback-doc@cisco.com

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).

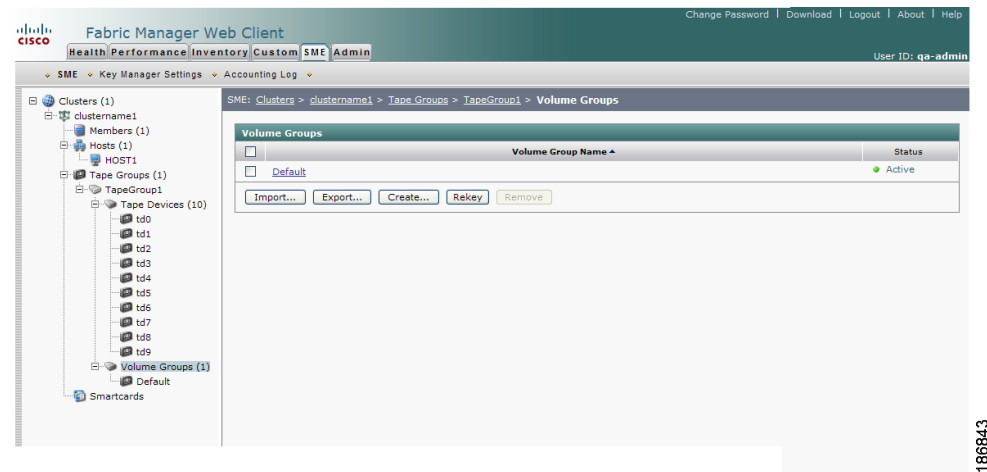
The volume groups can be rekeyed monthly even if you do not use the unique key mode.

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.

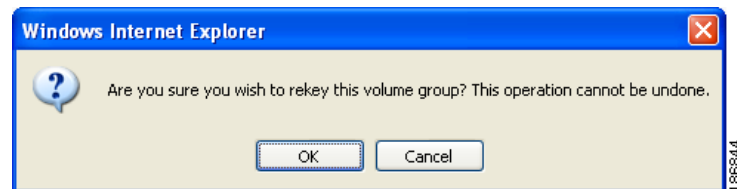
Send documentation comments to mdsfeedback-doc@cisco.com

Figure 6-13 **Selecting Volume Groups to Rekey**



- 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

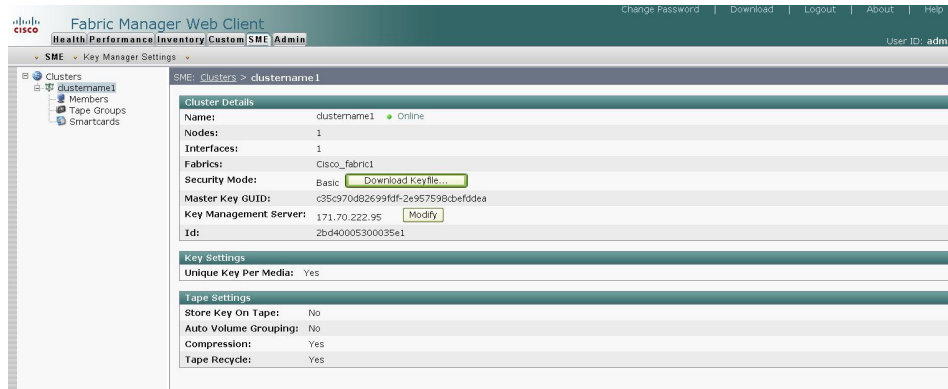
In Basic security mode, the master key file can be downloaded multiple times from the Fabric Manager Web Client. The cluster detail view includes a button to download the master key file.

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.

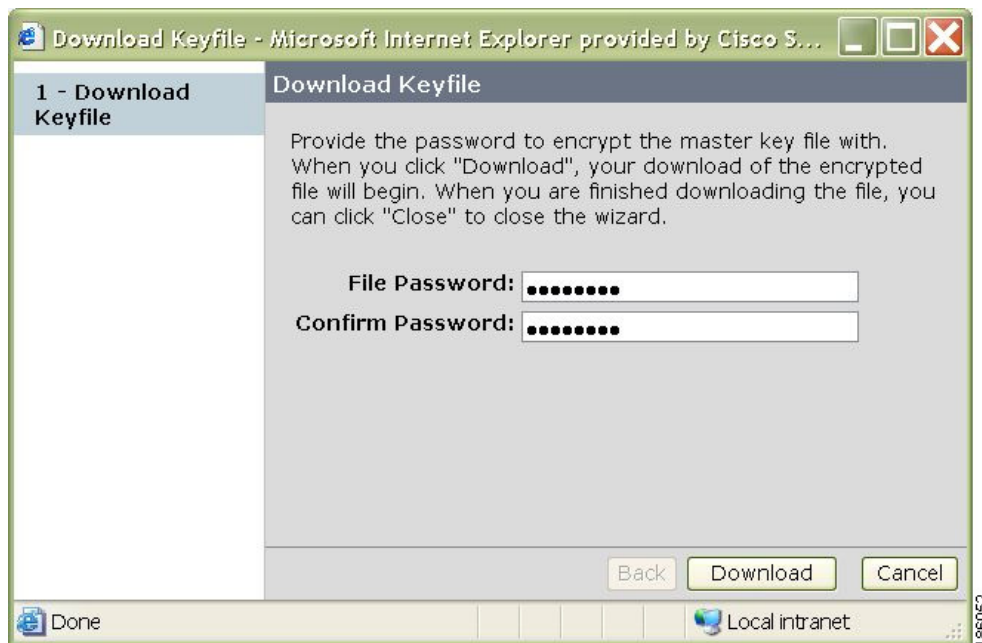
Send documentation comments to mdsfeedback-doc@cisco.com

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



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

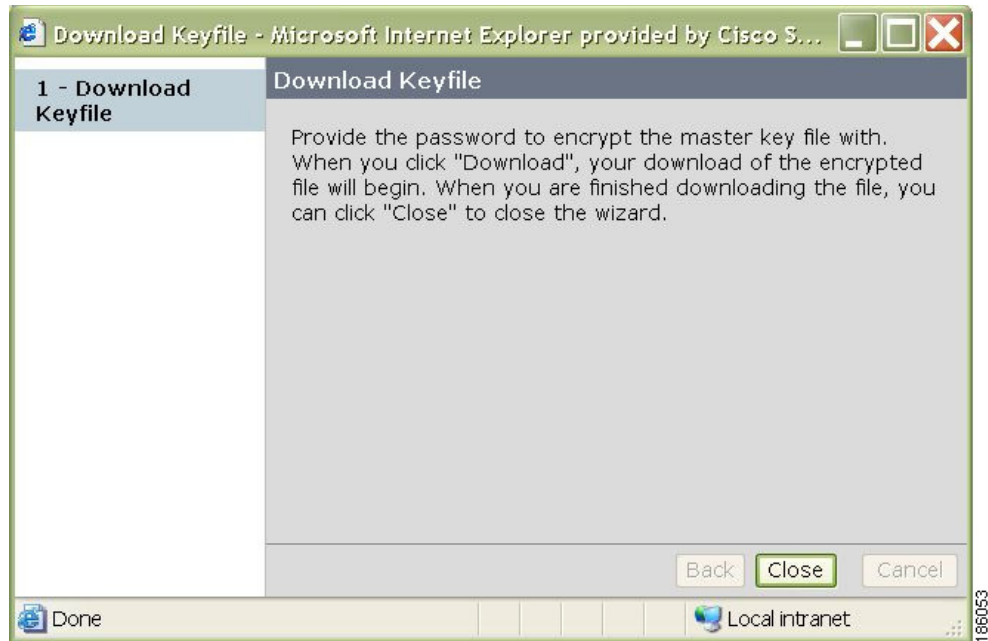
Figure 6-16 Enter the Password for the Master Key File



- Step 4** Click **Close** to close the wizard.

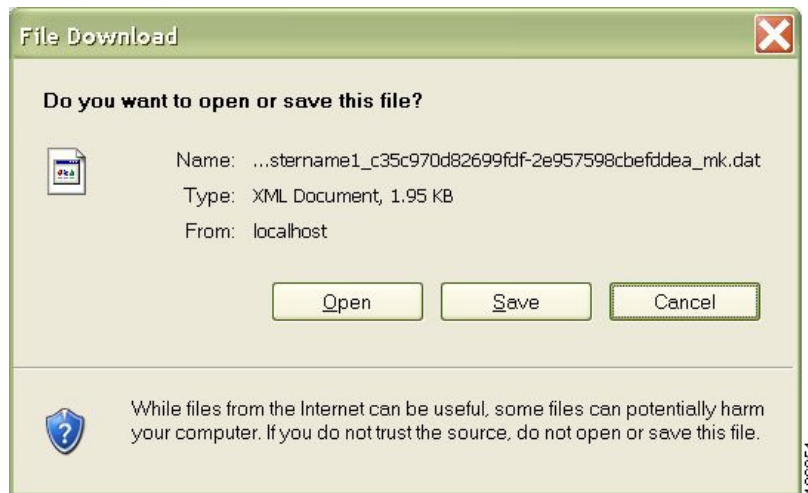
Send documentation comments to mdsfeedback-doc@cisco.com

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)**



Send documentation comments to mdsfeedback-doc@cisco.com

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](#)

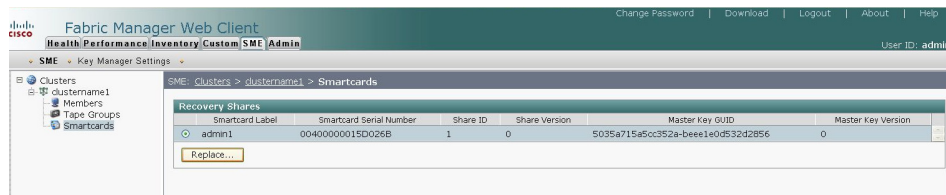
Standard Mode

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:

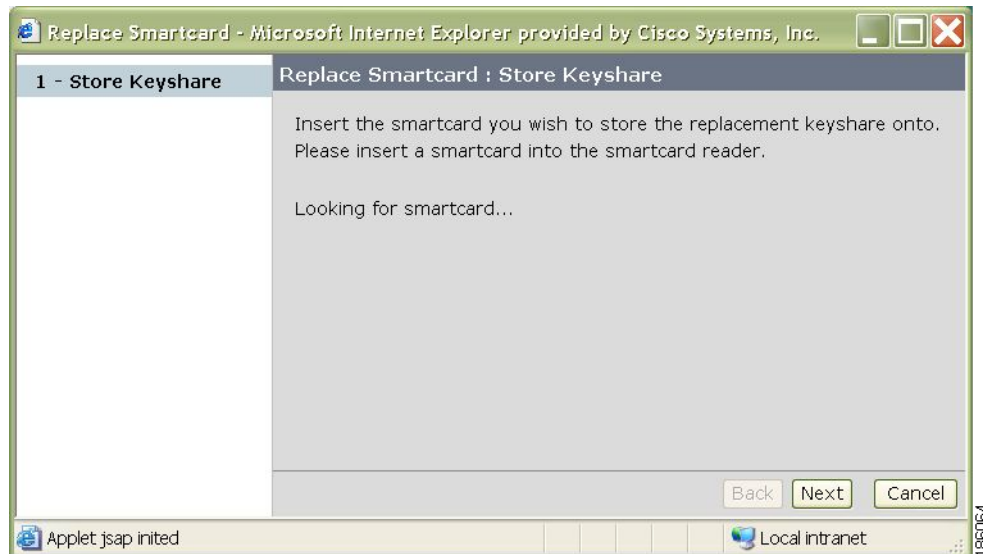
- Step 1** Select **Smartcards** to display the smart card information for the cluster.

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*



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

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 6-21 Inserting the Smart Card and Entering Credentials

Replace Smartcard - Microsoft 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. Enter your switch credentials and smartcard PIN, then click next.

Username: admin

Password:

PIN:

Label: SME3

Back Next Cancel

Applet jsap started Local intranet

Step 4 Click **Finish** to close the wizard.

Figure 6-22 Standard Security Smart Card Replacement Confirmation

Replace Smartcard - Microsoft Internet Explorer provided by Cisco Systems, Inc.

1 - Store Keyshare

Replace Smartcard : Store Keyshare

Recovery share(s) successfully stored.

Please click Finish to close the wizard.

Back Finish

Applet jsap started Local intranet

Send documentation comments to mdsfeedback-doc@cisco.com

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.

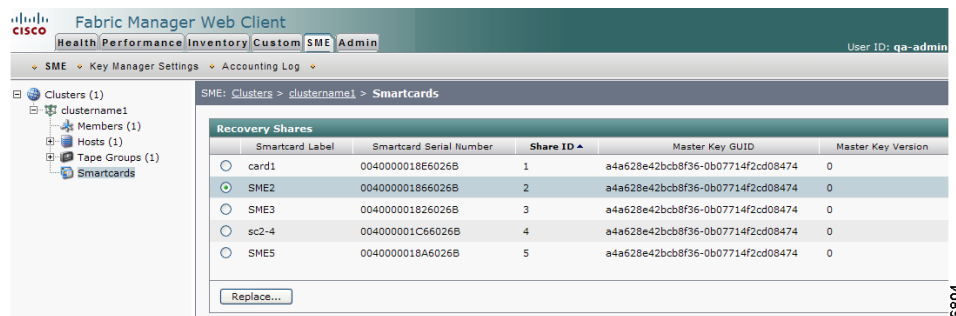
In the unique key mode, a new tape volume group wrap key is generated for each volume group. The existing tape volume group wrap key is duplicated with the new master key and put in the archived state.

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.

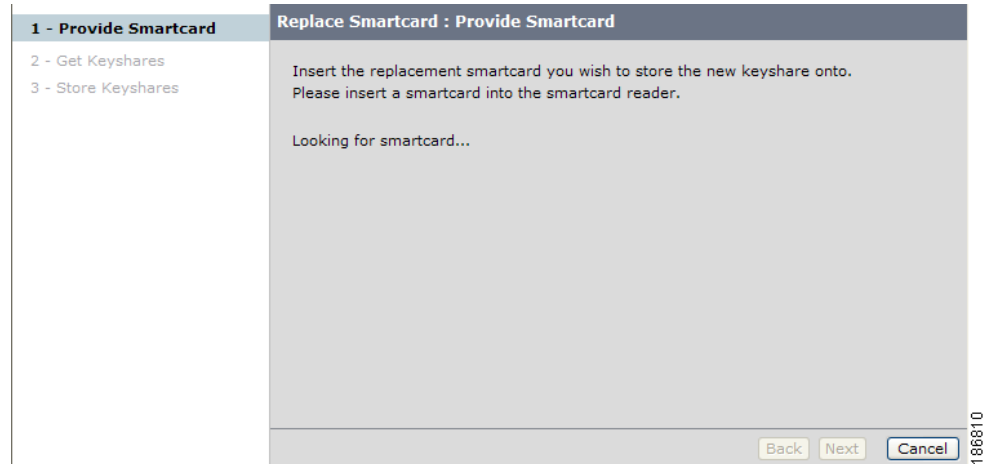
Figure 6-23 Display the Smart Card Details



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

Send documentation comments to mdsfeedback-doc@cisco.com

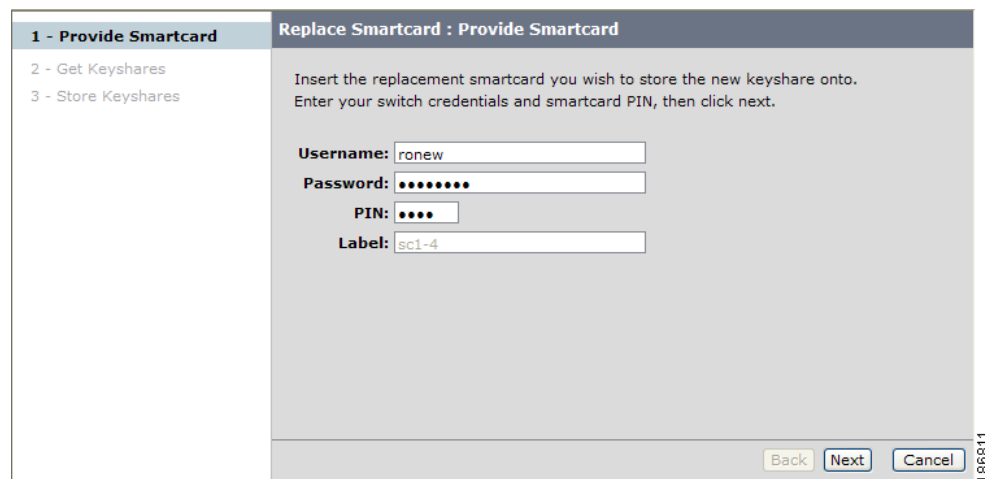
Figure 6-24 **Insert the New Smart Card**



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**



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**.

Figure 6-26 Insert Existing Card (1)

1 - Provide Smartcard

2 - Get Keyshares

3 - Store Keyshares

Replace Smartcard : Get 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

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

2 - Get Keyshares

3 - Store Keyshares

Replace Smartcard : Get Keyshares

A quorum of recovery officers needs to present the smartcards to authorize this operation.

Enter your smartcard PIN, then click next

0 of 2 recovery officers have authorized this operation.

Username: ro1

Password:

PIN:

Label: card1

Back Next Cancel

Send documentation comments to mdsfeedback-doc@cisco.com

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

Figure 6-28 Insert an Existing Smart Card (2)

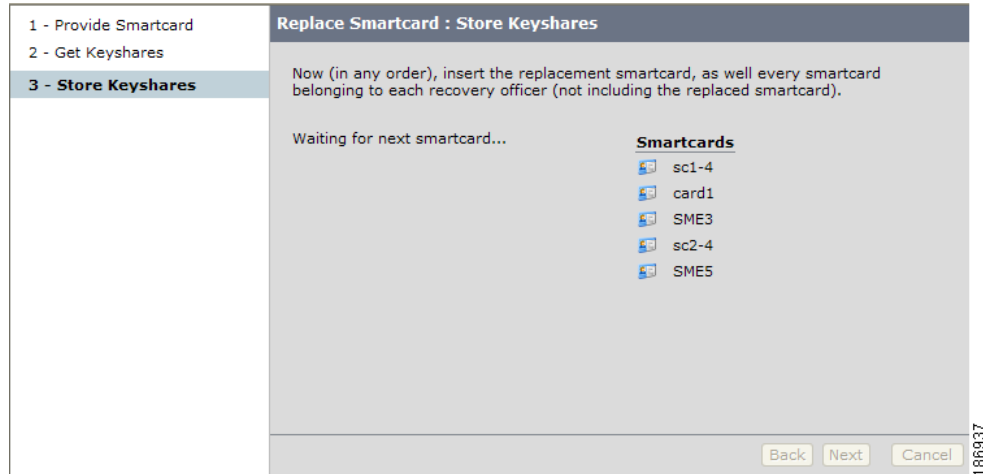
Step 8 Enter the switch login information and the smart card PIN and label. Click **Next**.

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

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

Send documentation comments to mdsfeedback-doc@cisco.com

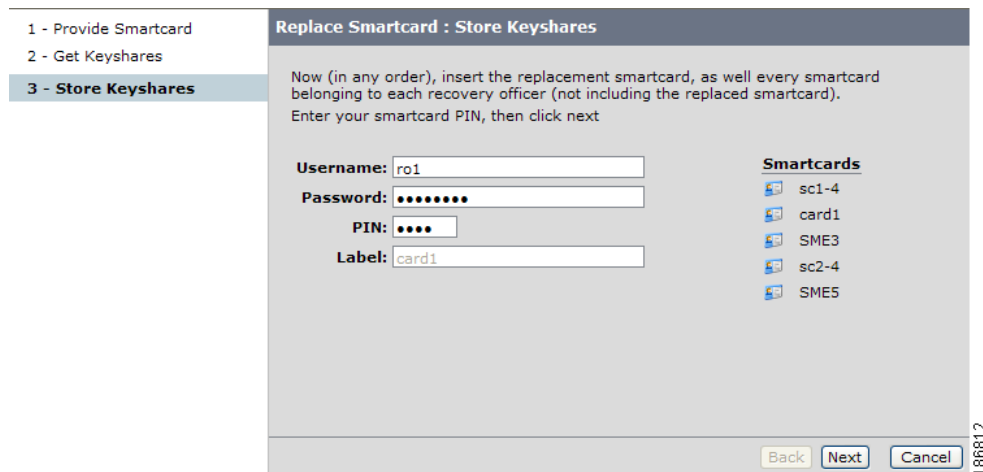
Figure 6-30 Inserting Smart Cards



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**.

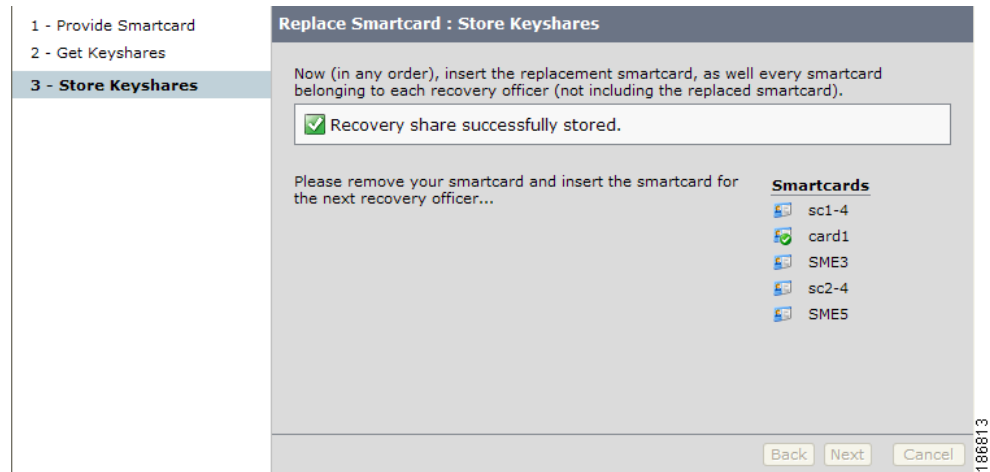
Figure 6-31 Entering Switch Credentials and PIN for the First Recovery Officer



Send documentation comments to mdsfeedback-doc@cisco.com

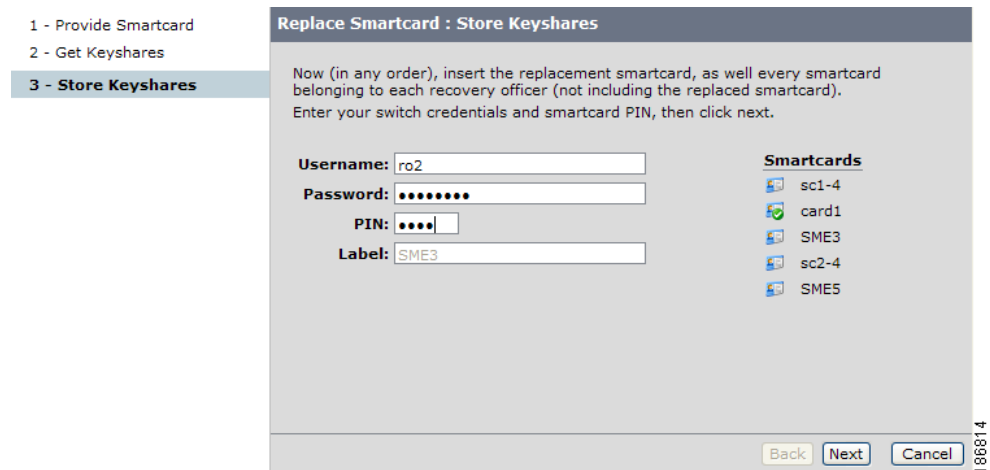
A notification is shown that the first keyshare is successfully stored.

Figure 6-32 Storing Keyshare for First Recovery Officer



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

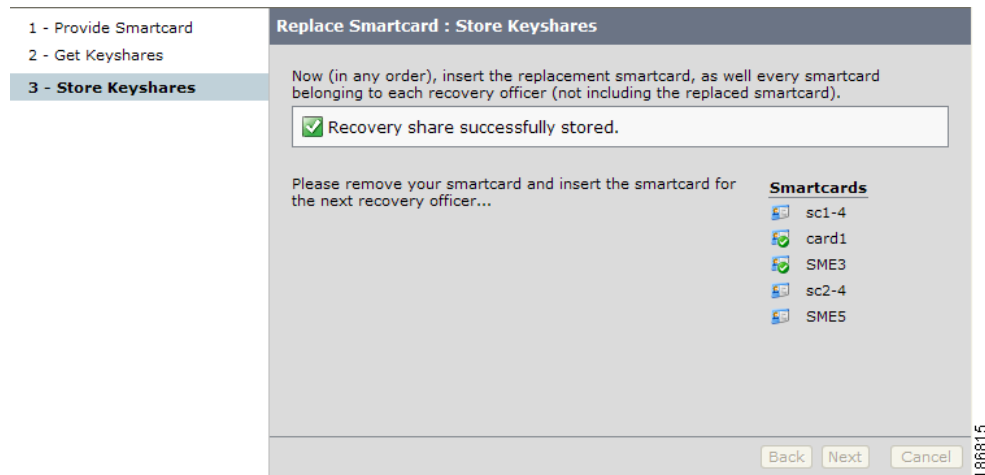
Figure 6-33 Entering Switch Credentials and PIN Information for Second Recovery Officer



Send documentation comments to mdsfeedback-doc@cisco.com

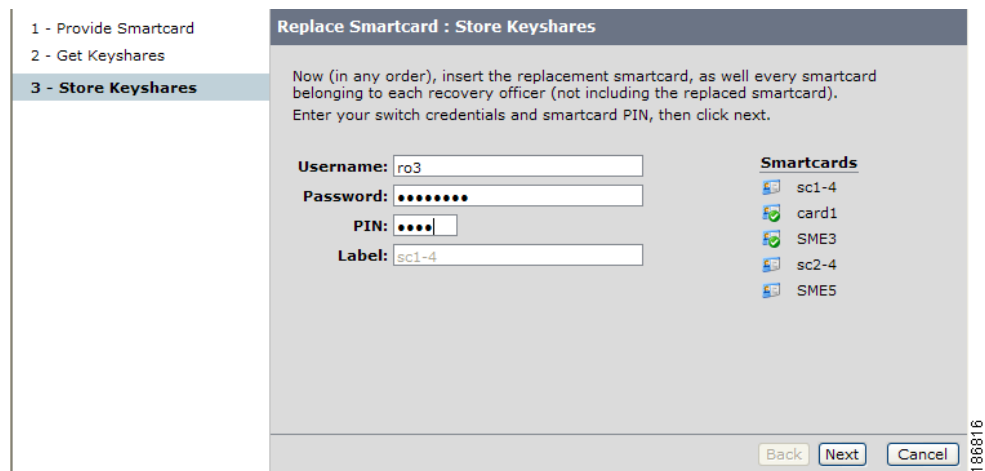
A notification is shown that the second keyshare is successfully stored.

Figure 6-34 Storing Keyshare for the Second Recovery Office



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

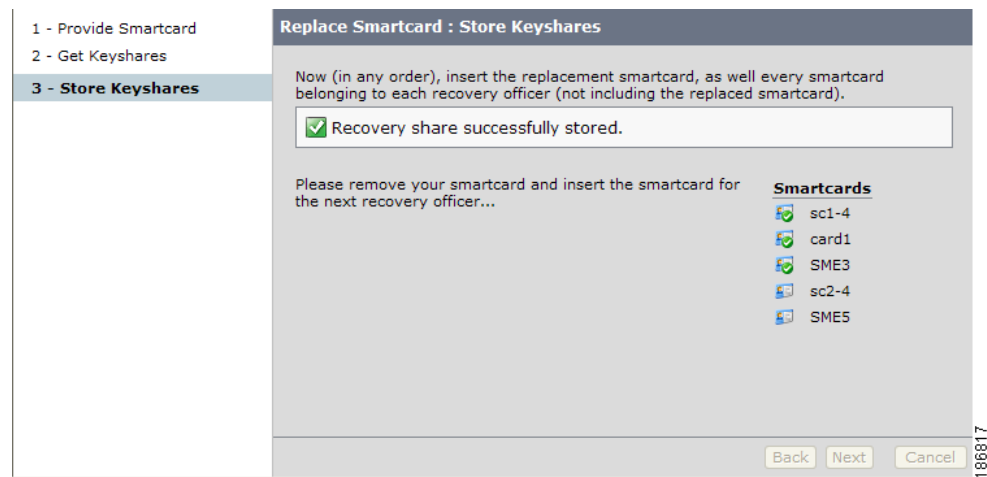
Figure 6-35 Entering Switch Credentials and PIN information for the Third Recovery Officer



Send documentation comments to mdsfeedback-doc@cisco.com

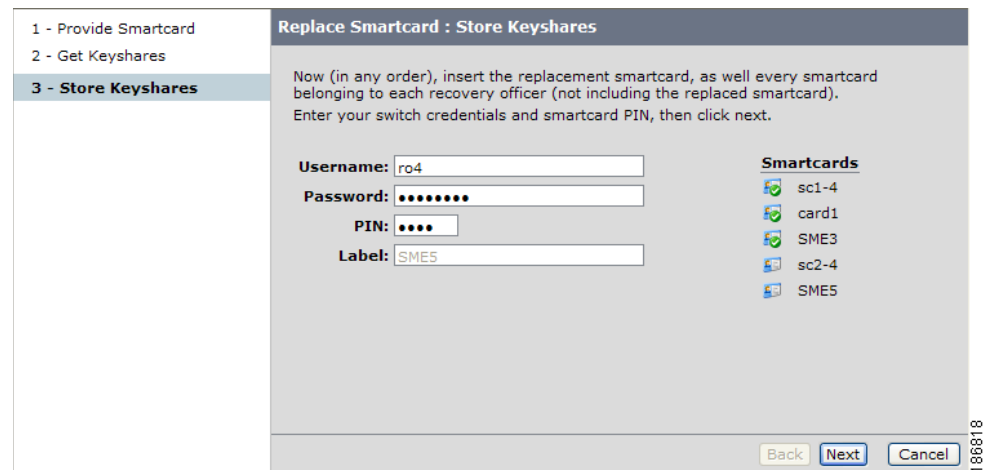
A notification is shown that the third keyshare is successfully stored.

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**.

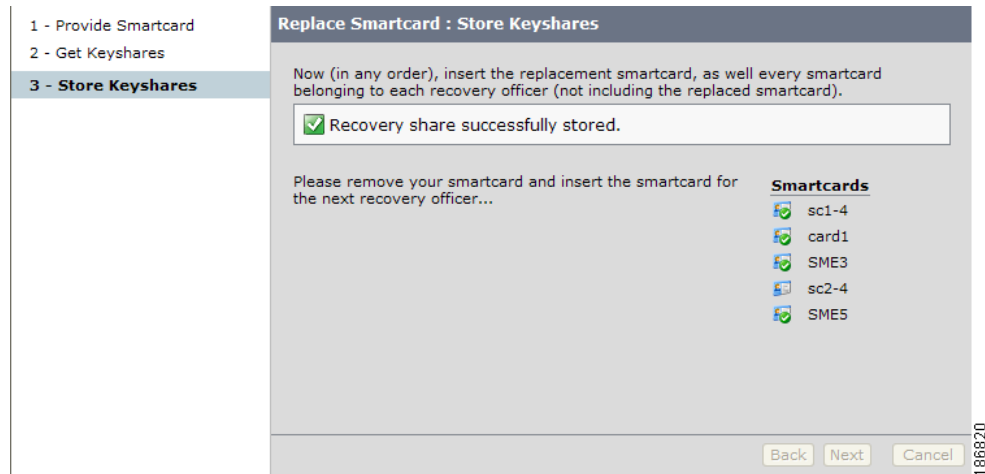
Figure 6-37 Entering Switch Credentials and PIN information for the Fourth Recovery Office



Send documentation comments to mdsfeedback-doc@cisco.com

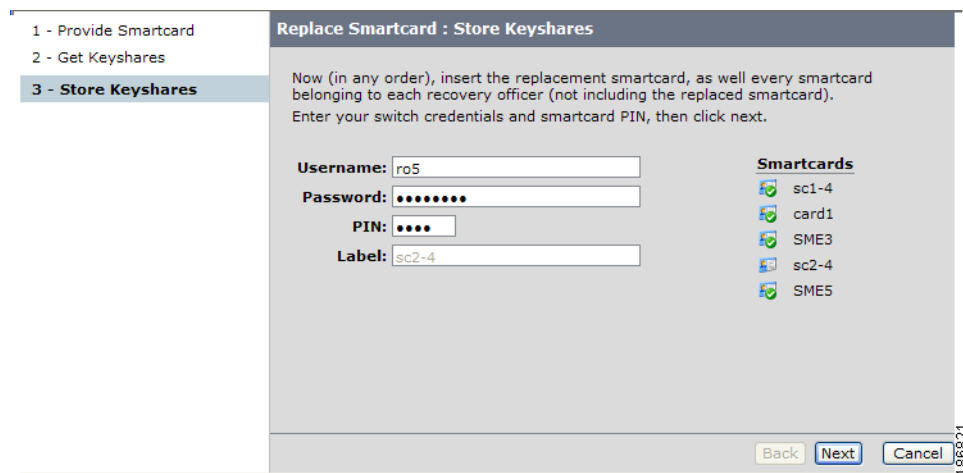
A notification is shown that the fourth keyshare is successfully stored.

Figure 6-38 Storing Keyshare for the Fourth Recovery Officer



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

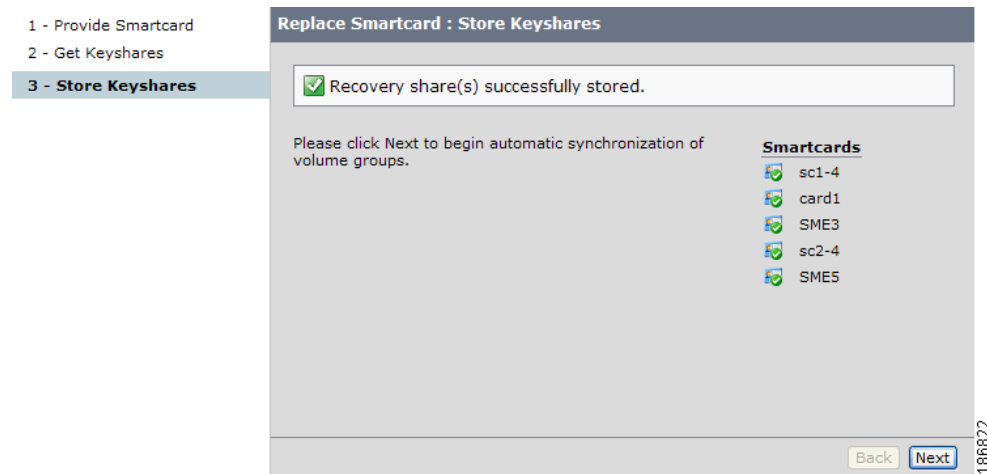
Figure 6-39 Entering Switch Credentials and PIN information for the Fifth Recovery Officer



Send documentation comments to mdsfeedback-doc@cisco.com

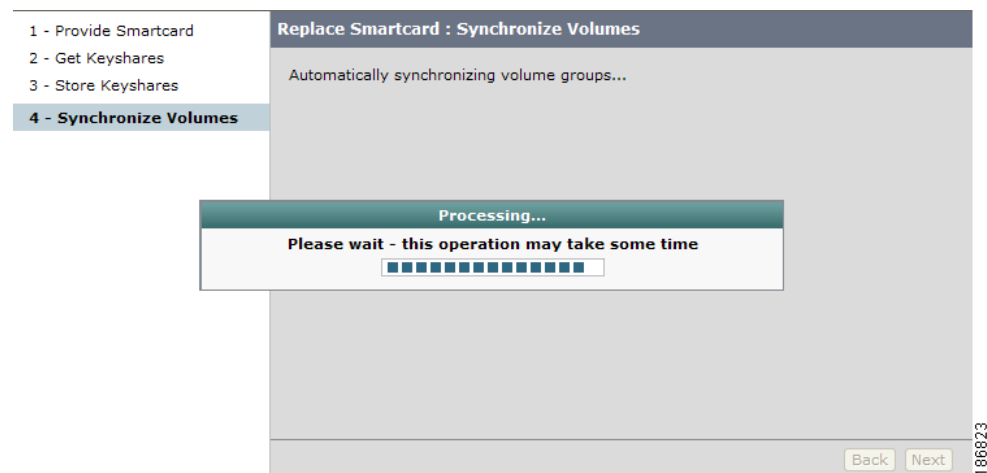
A notification is shown that the fifth keyshare is successfully stored. Click **Next** to begin the automatic synchronization of volume groups.

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.

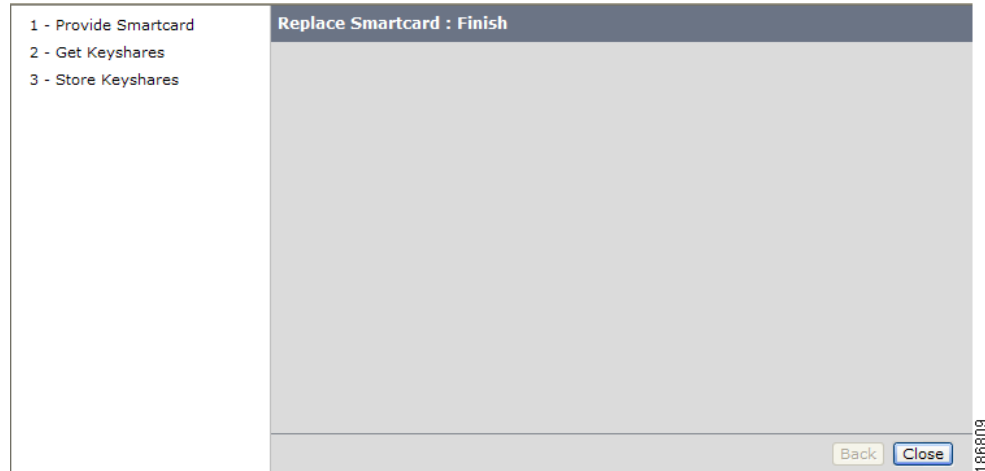
Figure 6-41 Synchronizing Volume Groups



Send documentation comments to mdsfeedback-doc@cisco.com

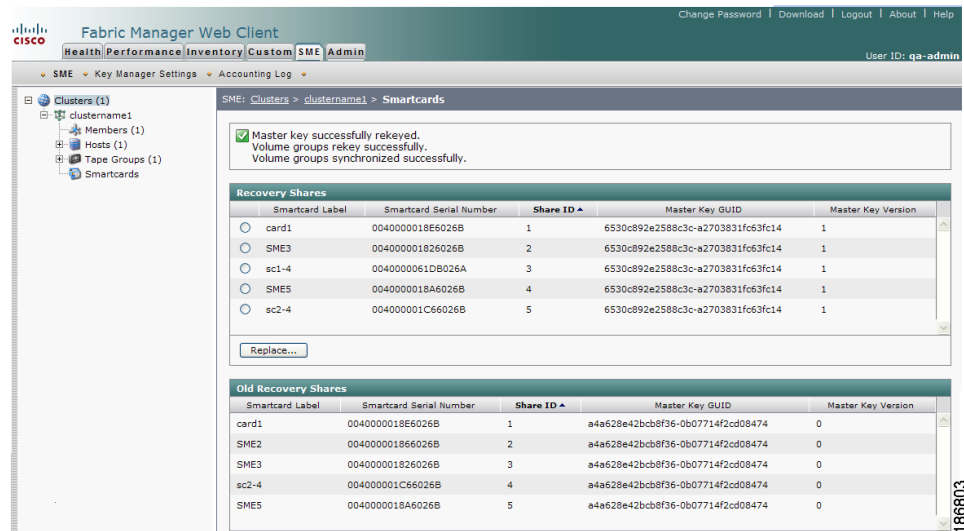
- Step 10** The smart card replacement is completed. Click **Close** to return to the Fabric Manager Web Client and to view the smart card information.

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



Send documentation comments to mdsfeedback-doc@cisco.com

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:

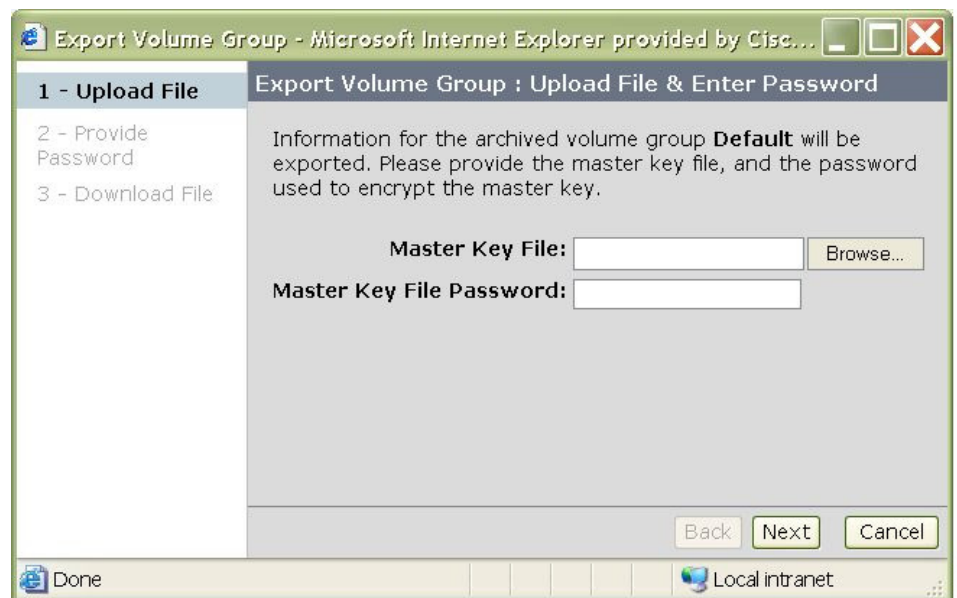
- Step 1** Select a volume group to display the volume groups in the cluster. Click **Export**.

Figure 6-44 *Select the Volume Group to Export*



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

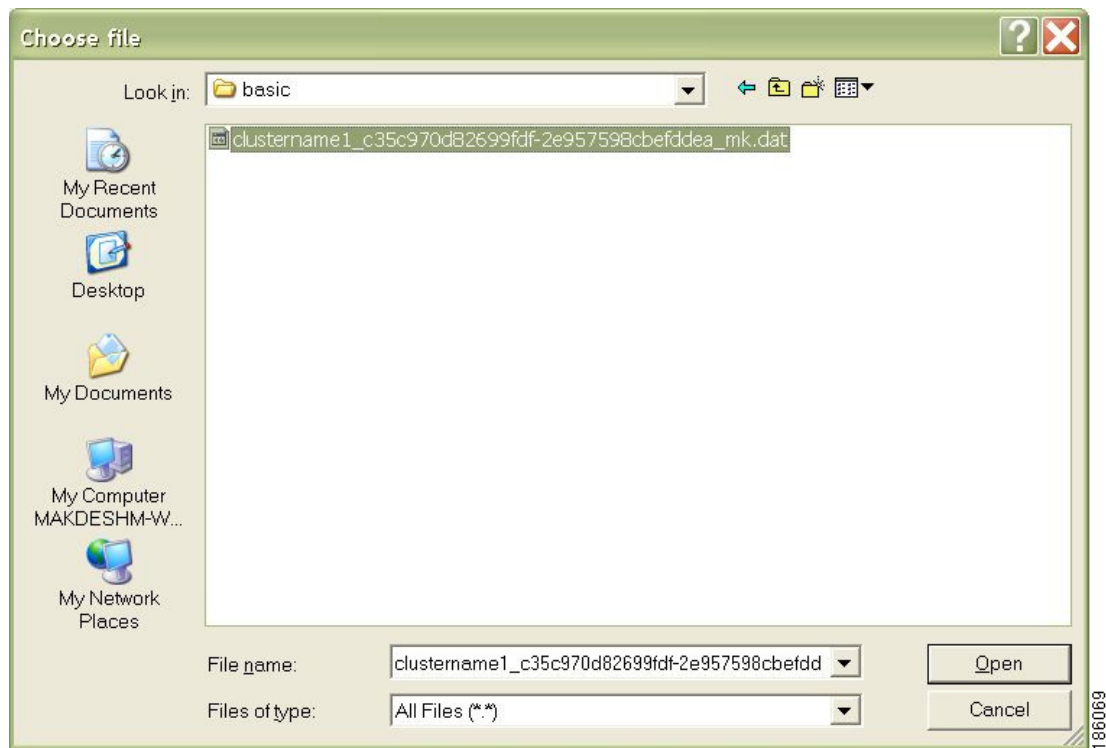
Figure 6-45 *Export Volume Group Wizard*



Send documentation comments to mdsfeedback-doc@cisco.com

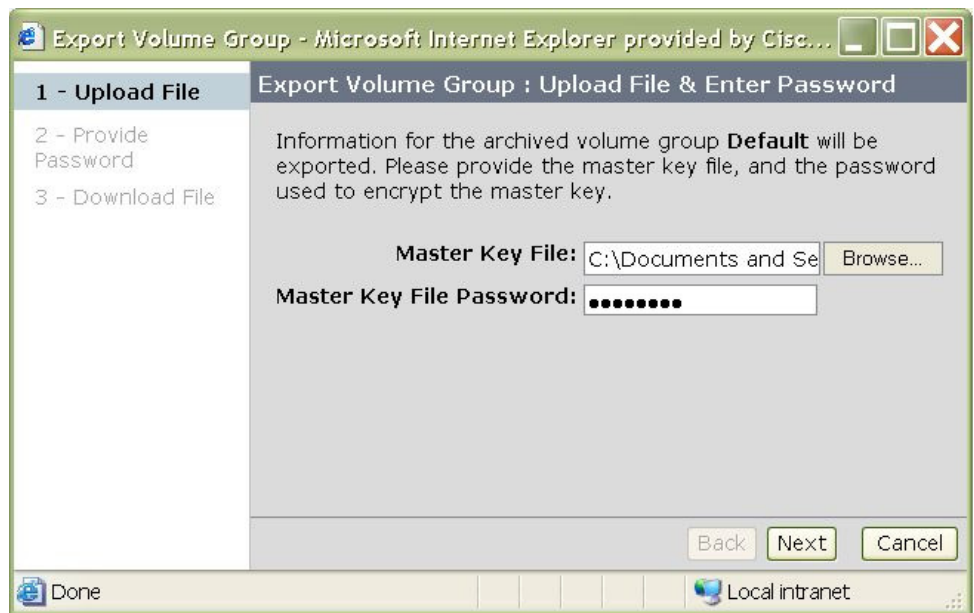
Step 3 Select the master key file. Click **Open**.

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



Send documentation comments to mdsfeedback-doc@cisco.com

Step 5 Enter the password that will be used to encrypt the exported file. Click **Next**.

Figure 6-48 Enter the Password for the Encrypted Exported File

The screenshot shows a web browser window titled "Export Volume Group - Microsoft Internet Explorer provided by Cisc...". The main content area is titled "Export Volume Group : Provide Password". It contains the instruction "Provide the password that will be used to encrypt the exported file." followed by two input fields: "Password:" and "Confirm Password:", both masked with dots. At the bottom right are "Back", "Next", and "Cancel" buttons. A left sidebar shows a progress list: "1 - Upload File", "2 - Provide Password" (highlighted), and "3 - Download File". The status bar at the bottom shows "Done" and "Local intranet".

Step 6 Click **Download** to begin downloading the volume group file.

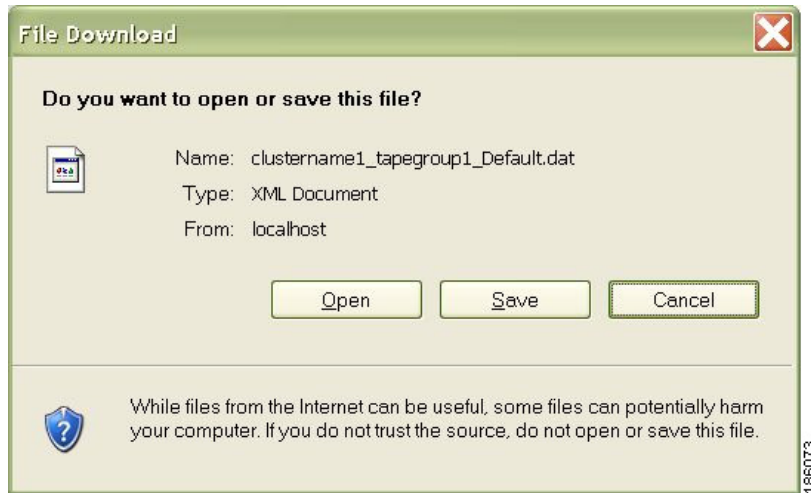
Figure 6-49 Download the Volume Group File

The screenshot shows the same web browser window, now titled "Export Volume Group : Download File". The main content area contains the instruction "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." Below this, it lists the export details: "Cluster: clustername1", "Tape Group: tapegroup1", and "Volume Group: Default". At the bottom right are "Back", "Download", and "Cancel" buttons. The left sidebar shows the progress list: "1 - Upload File", "2 - Provide Password", and "3 - Download File" (highlighted). The status bar at the bottom shows "Done" and "Local intranet".

Send documentation comments to mdsfeedback-doc@cisco.com

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

Figure 6-50 Save the Exported Volume Group File

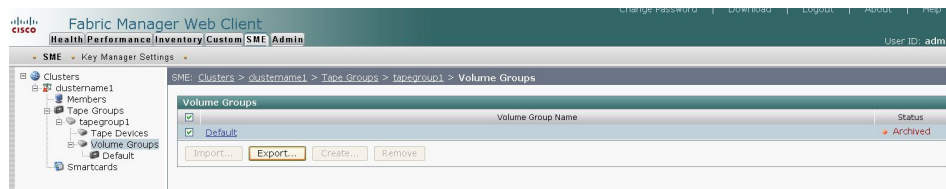


Standard Mode

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**.

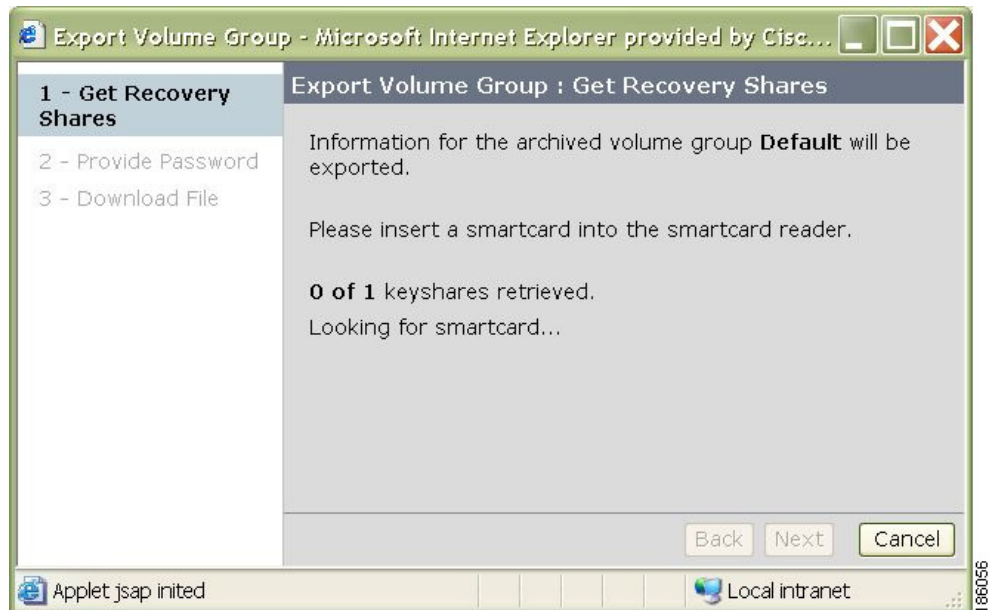
Figure 6-51 Viewing Volume Groups



Send documentation comments to mdsfeedback-doc@cisco.com

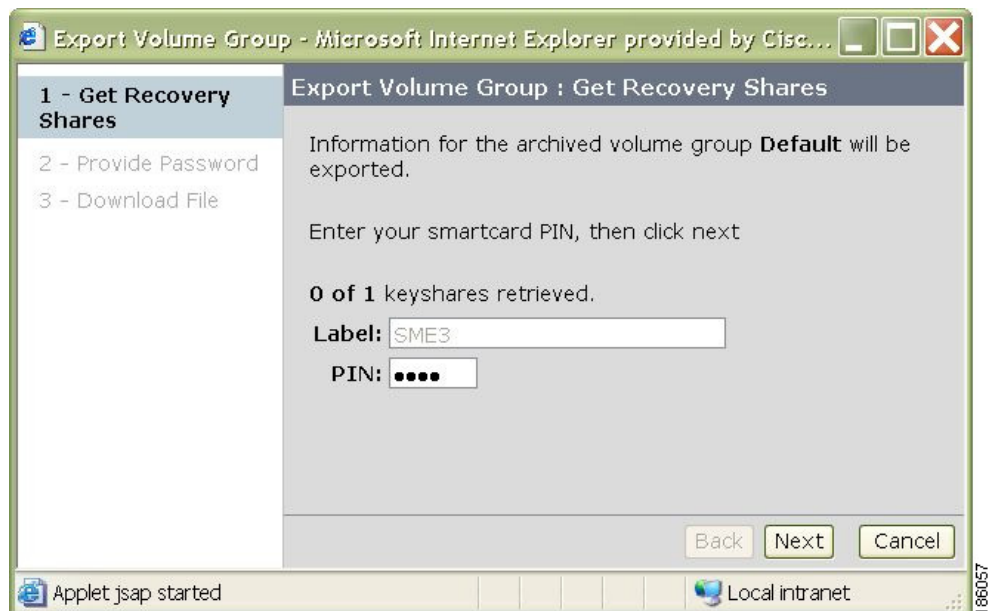
Step 2 Insert one of the five smart cards into the smart card reader. Click Next.

Figure 6-52 *Insert a Smart Card*



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

Figure 6-53 *Enter the Smart Card PIN and Label*



Send documentation comments to mdsfeedback-doc@cisco.com

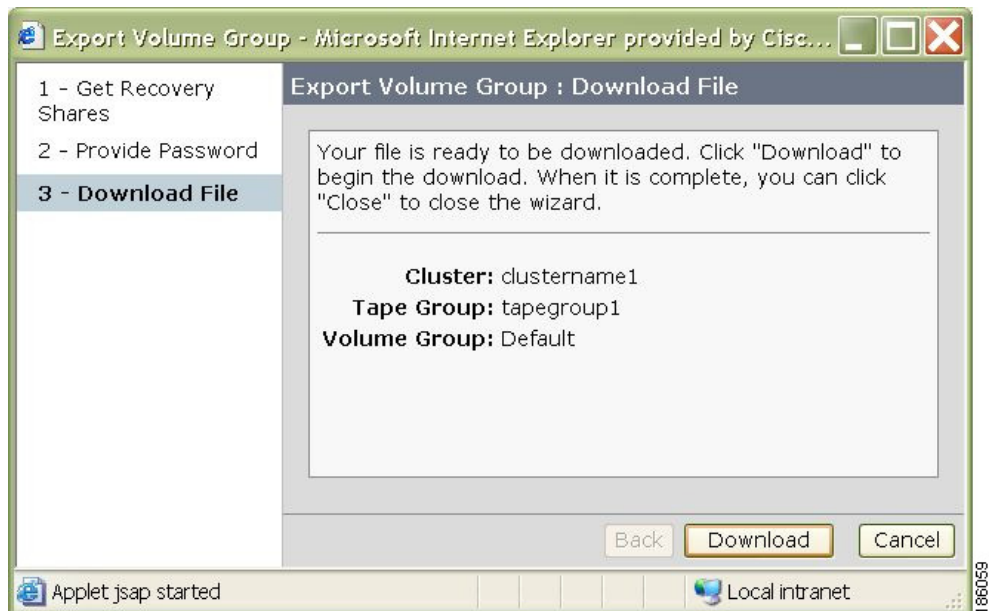
Step 4 Enter the password to encrypt the volume group file. Click **Next**.

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



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

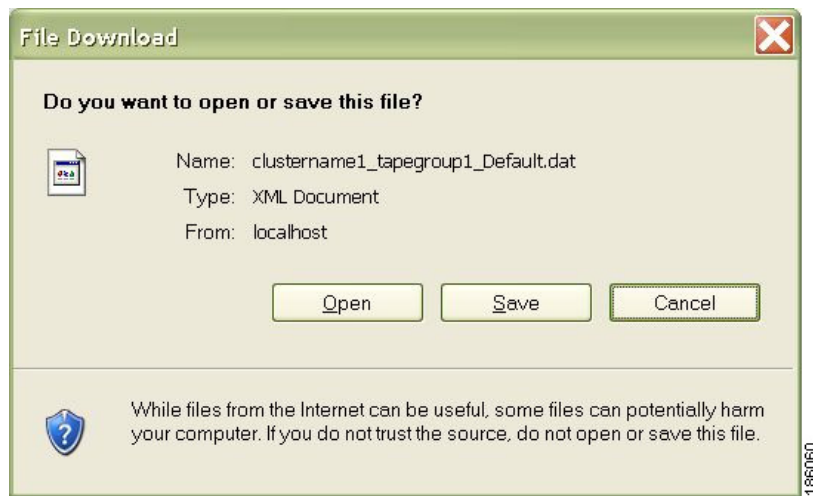
Figure 6-55 Download the Volume Group File



Send documentation comments to mdsfeedback-doc@cisco.com

Step 6 Save the .dat file. Click Next.

Figure 6-56 Save the Volume Group File

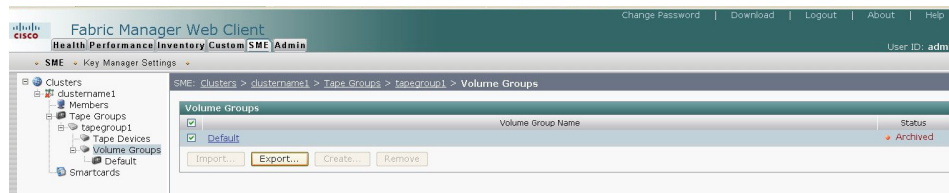


Advanced Mode

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**.

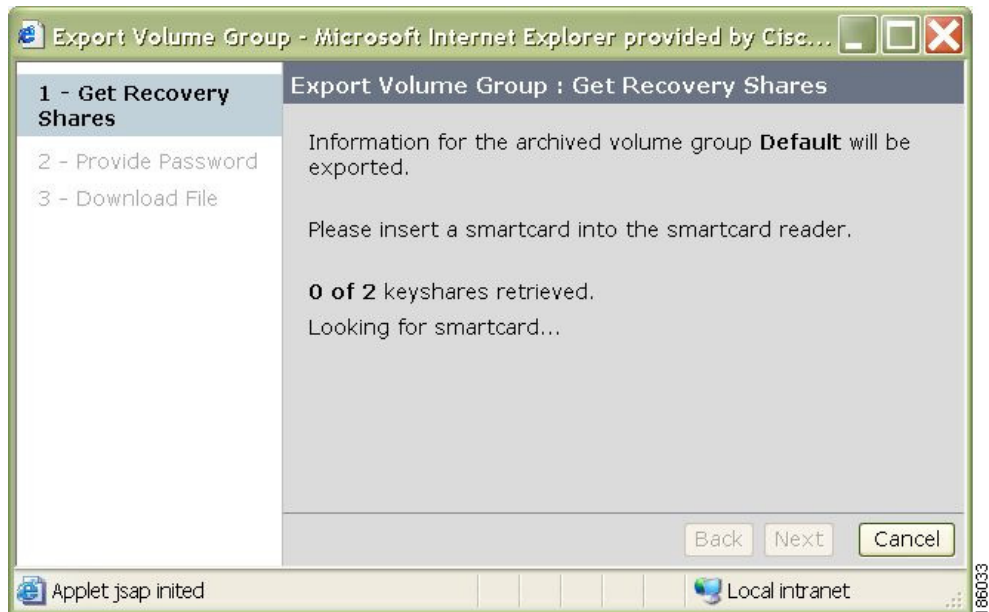
Figure 6-57 Viewing Volume Groups



Send documentation comments to mdsfeedback-doc@cisco.com

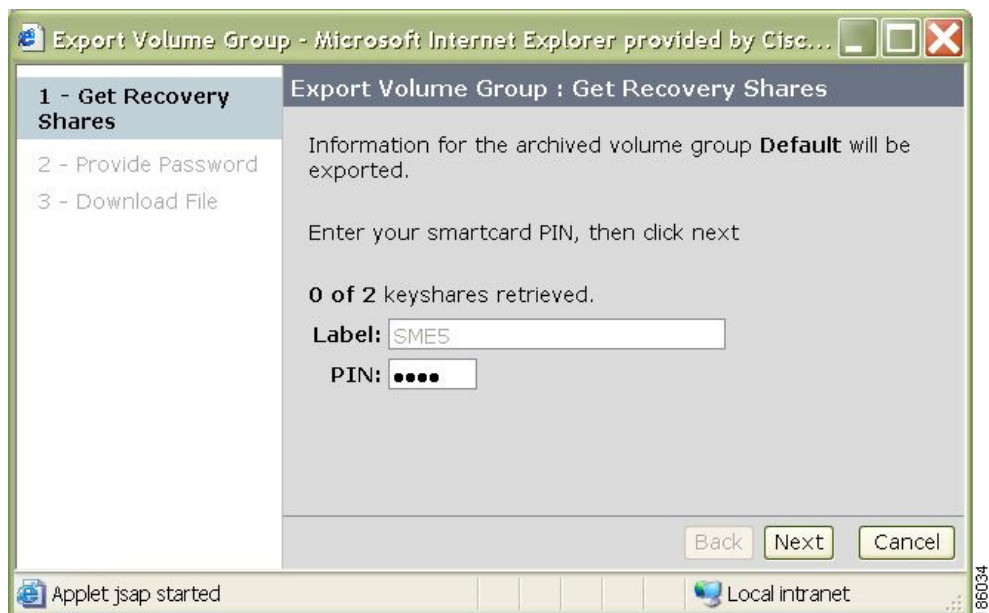
Step 2 Insert one of the five smart cards into the smart card reader. Click **Next**.

Figure 6-58 Insert a Smart Card



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

Figure 6-59 Enter the Smart Card Pin and Label



The keyshare is retrieved.

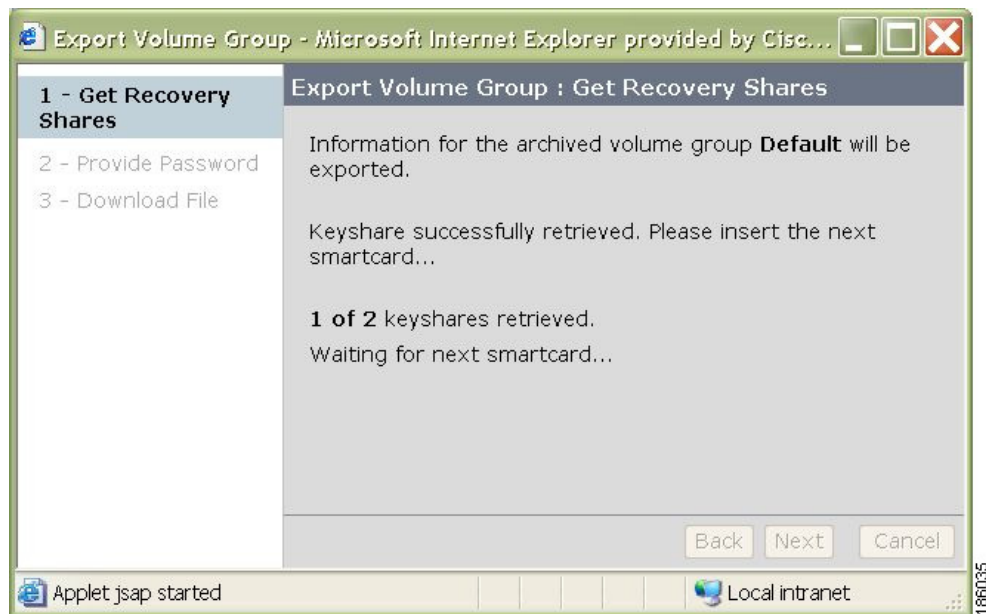
Send documentation comments to mdsfeedback-doc@cisco.com

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



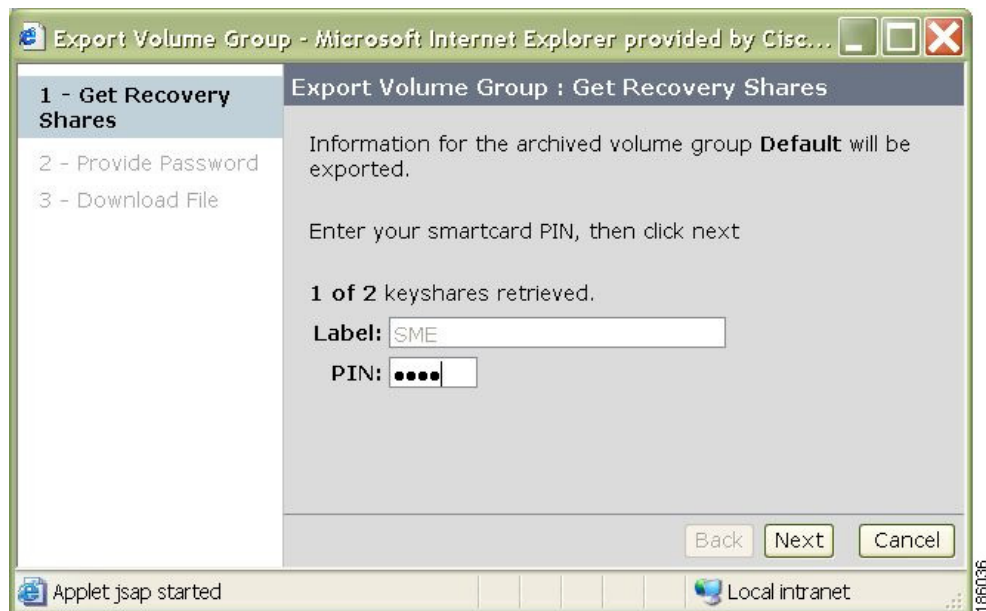
Note Repeat this step for each smart card that is required to unlock the master key. The number of required smart cards depends on the quorum number selected during the cluster creation, for example, 2 of 5 smart cards.

Figure 6-60 *Insert the Second Smart Card*



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*



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

Send documentation comments to mdsfeedback-doc@cisco.com

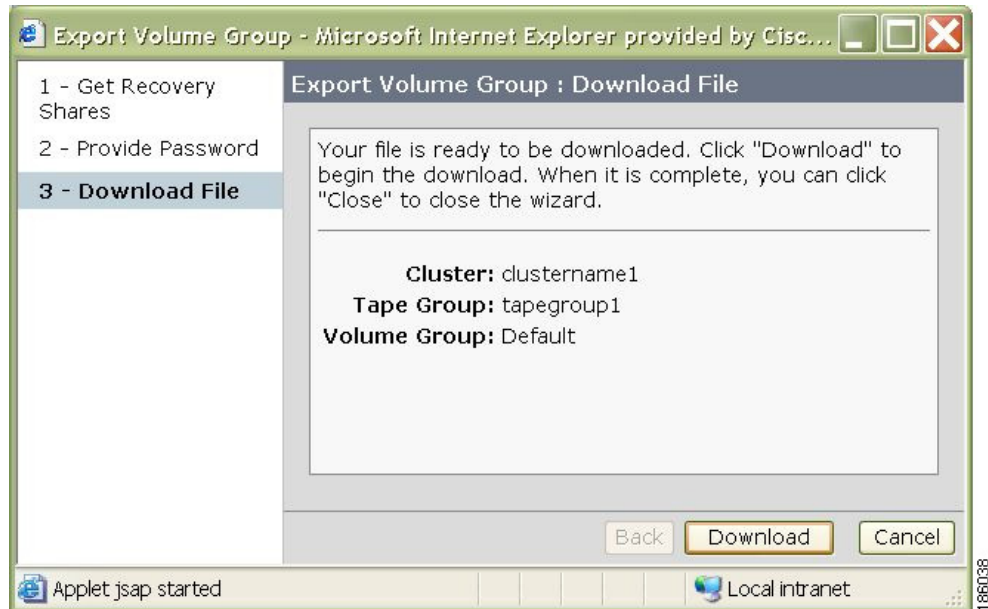
Figure 6-62 Enter the Volume Group File Password



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

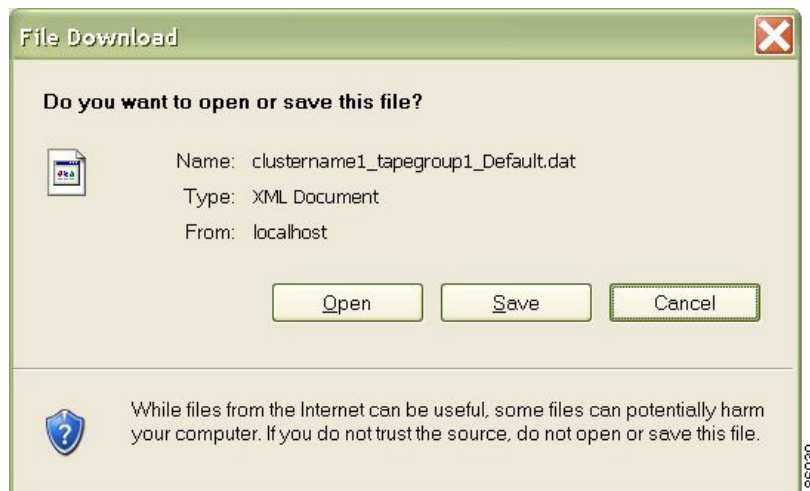
Send documentation comments to mdsfeedback-doc@cisco.com

Figure 6-63 Download the Volume Group



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

Figure 6-64 Save the Volume Group File



Send documentation comments to mdsfeedback-doc@cisco.com

Accounting Log Information

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

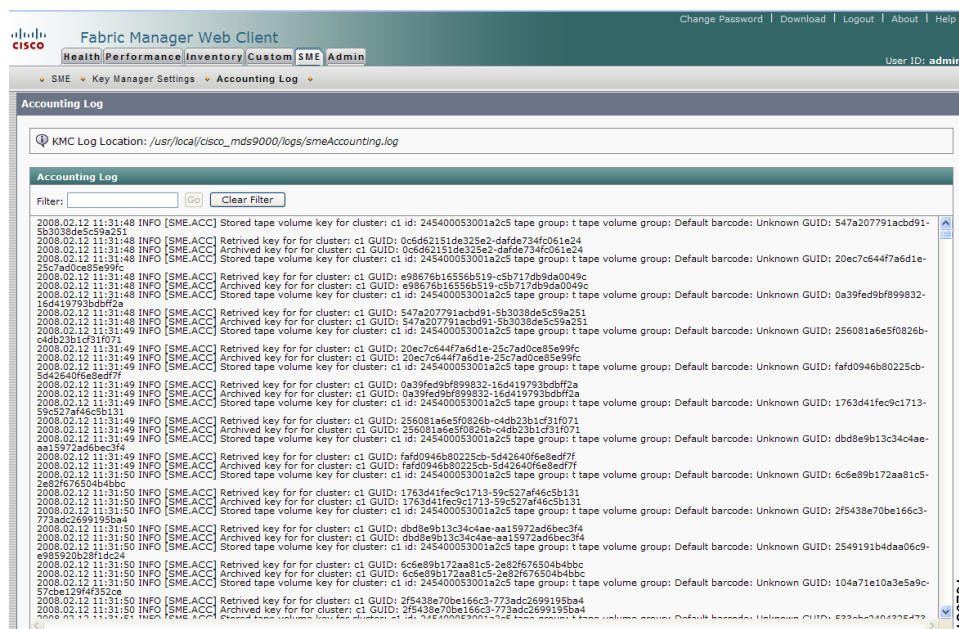
- [Viewing Accounting Log Information, page 6-40](#)
- [KMC Accounting Log Messages, page 6-41](#)

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



- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

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>

Send documentation comments to mdsfeedback-doc@cisco.com

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.

Send documentation comments to mdsfeedback-doc@cisco.com

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

Send documentation comments to mdsfeedback-doc@cisco.com

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>