



CHAPTER 4

Configuring SME Cluster Management

DCNM-SAN provides a web browser interface that displays real-time views of your network fabrics and lets you configure the SME with easy-to-use wizards.

This chapter contains information about the SME initial configuration and the tasks that are used to manage SME clusters using DCNM-SAN.

This chapter includes the following topics:

- [Information About SME Cluster Management, page 4-1](#)
- [Configuring SME Cluster Management Using the CLI, page 4-5](#)
- [Configuring SME Cluster Management Using the GUI, page 4-10](#)
- [Verifying SME Cluster Management Configuration, page 4-18](#)
- [Monitoring SME Cluster Management, page 4-19](#)
- [Feature History for SME Cluster Management, page 4-24](#)

Information About SME Cluster Management

An SME cluster consists of a group of MDS switches running the SME application in a single fabric environment where each switch is a member or node. The cluster infrastructure enables the SME application to offer high availability and load balancing by providing the ability to communicate and coordinate with the other members to maintain a consistent and distributed view of the application's configuration and operational state.

The process of configuring SME on an MDS switch with an installed Cisco MSM-18/4 module, SSN-16 module, or on a Cisco MDS 9222i switch involves a number of configuration tasks that should be followed in chronological order. See the topics in the Before You Begin online help in DCNM-SAN Web Server. Configure SSH and refer to [Chapter 2, “Configuring SME”](#) and [Chapter 3, “Configuring SME Interfaces”](#) for information about the tasks must be completed before creating an SME cluster.

Cluster Quorum and Master Switch Election

This section describes the SME cluster quorum and the process for electing the master switch in a cluster.

- [Cluster Quorum, page 4-2](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- [Master Switch Election, page 4-2](#)

Node ID

Every switch in a cluster has a node ID. SME assigns a node ID to every new switch as it is added to the cluster. The switch where the cluster is created is assigned the node ID of 1. This is the master switch. When a new switch is added to the cluster, it is assigned the next available higher node ID. For example, when a second switch is added to the cluster it gets the node ID of 2 and the third switch gets the node ID of 3, and so on.

Cluster View

The cluster view is the set of switches that are part of the operational cluster.

Cluster Quorum

For a cluster to be operational, it must include more than half the number of configured switches in the cluster view. In an N-switch cluster, $N/2 + 1$ switches form a cluster quorum.

If N is even, the cluster quorum requires $N/2$ switches and also, the presence of the switch with the lowest node ID.

The quorum logic ensures that in the event of cluster partitions, at most one partition can be operational. All other switches are nonoperational. This guarantees the consistency of the cluster.

Master Switch Election

When a cluster is created, the switch on which the cluster is created becomes the cluster master switch. When the master switch fails or is rebooted, another switch takes over as the master switch. The master election logic uses the node ID and the latest cluster configuration to determine which switch in the cluster will become the master switch. The master election logic is describe as follows:

- If the master switch fails in an operational cluster, the switch with the next lowest node ID takes over as the master switch. Note that in an operational cluster, all the switches run the same cluster configuration.
 - When the previous master switch comes back online and joins the cluster, it does not immediately become the master.
- When all the switches of a cluster are coming up, the switch that has the latest cluster configuration becomes the master switch. If there are multiple switches with the same configuration, the switch with the lowest node ID is chosen to be the master switch.
 - Once a master switch is chosen and the cluster is operational (there is a quorum), even if a switch with a lower node ID joins the cluster at a later time, the master switch does not change.

For example, there are three switches S1, S2, and S3 with node IDs 1, 2, and 3, respectively. If switches S2 and S3 form a quorum then switch S2 becomes the master switch. Even if switch S1 with the node ID of 1 comes up and joins the cluster at a later time, switch S2 continues to be the master. However, if switch S2 goes down for any reason, switch S1 will become the master switch.



Note

Because there might be changes in the Master switch, all switches in the cluster need to be configured to handle SNMP configuration, SME roles, user credentials, and SSH. Switches in the cluster should directly communicate with KMC.

Send documentation comments to mdsfeedback-doc@cisco.com

Two-Switch Cluster Scenarios

According to the cluster quorum logic “[Cluster Quorum](#)” section on page 4-2, a cluster with two configured switches can be operational if both switches are operational or the switch with the lowest node ID is operational.

In the latter case, the switch with the lowest node ID is the master of the one-switch cluster. The other switch could have failed or simply lost connectivity to the operational switch. In either case, the switch with the higher node ID would become nonoperational. If the switch with the lower node ID failed, the other switch cannot form an operational cluster.

The examples that follow describe these scenarios. The first three examples consider single switch failures.

1. Assume that in a two-switch cluster with switches S1 (node ID 1) and S2 (node ID 2), S1 is the master (the master has the lower node ID).

When the switches lose connectivity between them, the master switch S1 continues to be operational since it has the lower node ID and can form an (N/2) switch cluster. Switch S2 becomes non-operational.

2. Assume that in a two-switch cluster with switches S1 (node ID 1) and S2 (node ID 2), S2 is the master (note that the master has the higher node ID because it has the latest configuration when both the switches came online).

When the switches lose connectivity between them, switch S2 becomes non-operational and S1 takes over as the master to form a 1-switch cluster. This is consistent with the quorum logic in a two-switch cluster (N/2 with lowest node ID).

3. Assume that in a two-switch cluster with switches S1 (node ID 1) and S2 (node ID 2). If S1 fails (regardless of which switch was the master), S2 will also become non-operational as long as S1 is down.

When S1 comes up, S1 and S2 will form a two-switch cluster.

The next set of examples describe reboots of both switches (S1 with node ID 1 and S2 with node ID 2).



Caution

If you perform any configuration change on a cluster, you must save the running configuration to the startup configuration by entering the **copy running-config startup-config** CLI command on all switches before rebooting them. Otherwise, the cluster may not form correctly after the reboot.

4. After a reboot, if both switches S1 and S2 come up about the same time, a two-switch cluster will be formed.
 - a. If the cluster configurations are the same, S1 (with the lower node ID) will become the master.
 - b. If the cluster configurations are different, the switch with the latest cluster configuration will become the master.
5. After a reboot, if switch S2 comes up first, it will not be able to form a cluster until S1 also comes up. After that, the algorithm explained in the previous case will be used.
6. After a reboot, if switch S1 comes up first, it will form a one-switch cluster (N/2 with lowest node ID). When S2 comes up, it will join the cluster to form a two-switch cluster.

When S2 comes up and if it happens to have the latest cluster configuration in the startup configuration (this can happen if you did not save the running configuration to the startup configuration on S1 but did so on S2), it will not be able to join the cluster formed by S1.

Send documentation comments to mdsfeedback-doc@cisco.com



Caution

It is critical that you save the running configuration on all switches before a reboot.

Three-Switch Cluster Scenarios

In a three-switch cluster, the quorum requires two switches to be in the cluster view ($N/2 + 1$). The examples below explain three scenarios in a three-switch cluster with switches S1 (node ID 1), S2 (node ID 2) and S3 (node ID 3). S1 is the master switch.

1. In a three-switch operational cluster, if switch S3 fails or loses connectivity with the other two switches, then S3 becomes nonoperational. Switches S1 and S2 will form an operational cluster. When S3 comes up again, it will rejoin the cluster.
2. In a three-switch operational cluster, if the master switch S1 fails or loses connectivity with the other two switches, then S1 becomes nonoperational. Switches S2 and S3 will form an operational cluster and S2 will be the master. When S1 comes up again, it will rejoin the cluster. Note that S2 will continue to be the master.
3. If two switches fail, the cluster will become nonoperational.

The examples below describe reboots on all switches in the cluster.



Caution

If you perform any configuration change on a cluster, you must save the running configuration to the startup configuration by entering the **copy running-config startup-config** command on all switches before rebooting them. Otherwise, the cluster may not form correctly after the reboot.

4. After a reboot, if all switches come up at about the same time, first a 2-switch cluster will be formed and later the third switch will be added.
 - a. If the cluster configurations are the same, S1 (with the lower node ID) will become the master switch and form the 2-switch cluster first; and then add the third switch.
 - b. If the cluster configurations are different, the switch that is running the latest configuration will become the master switch and then form a 2-switch cluster; and then add the third switch.
5. After a reboot, if the switches come up one at a time, a 2-switch cluster will be formed after the first two switches are up. Later, when the third switch comes online, it will join the cluster.

If the third switch happens to be running the latest cluster configuration in the startup configuration (this can happen if you save the running configuration only on this switch but not on the other two), the third switch will not be able to join the cluster.



Caution

It is critical that you save the running configuration on all switches before a reboot.

Four-Switch Cluster Scenarios

The four-switch cluster scenario is very similar to the examples above. The cluster will be operational if the cluster view has at least three switches ($N/2 + 1$), or if the cluster view has two switches including the switch with the lowest node ID ($N/2$ with lowest node ID).

Send documentation comments to mdsfeedback-doc@cisco.com

In-Service Software Upgrade in a Two-Node Cluster

In-Service Software Upgrade (ISSU) is a comprehensive, transparent software upgrade application that allows you to deploy bug fixes and add new features and services without any disruption to the traffic.

In a cluster consisting of the MDS 9222i switches as members, if the switches are not able to communicate, then the switch having the lowest node identifier (node ID) remains in the cluster while the other switch leaves the cluster. However, when an ISSU is performed on a switch having the lowest node identifier, a complete loss of the cluster results because both the switches leave the cluster.

This undesirable situation is addressed in a two-switch cluster as follows:

- The upgrading switch sends a message to the other switch of the intent to leave the cluster. The upgrading switch can either be a master switch or a slave switch.
- The remaining switch remains in the cluster and performs the role of the master switch if it was a slave switch. This switch continues to remain in the cluster with the quorum intact.
- After the ISSU is completed and the switches boot up, the upgraded switch rejoins the cluster as a slave switch.



Note

This feature is tied to the internals of ISSU logic and no additional commands need to be executed.

Server Clusters

A cluster is group of servers linked together to perform a common task.

Clusters provide the following features:

- High availability—If one server in the cluster goes down, the work assigned to that server is migrated to another server in the cluster.
- Load balancing—Clusters allow work to be distributed across different servers.

Clusters can use the shared model or the nonshared model. The shared model requires distributed lock manager (DLM) to manage concurrent access to shared resources. The nonshared model does not require DLM and as a result, requires less overhead. For example, the MSCS (Microsoft clusters) use the nonshared model. This means that a node owns a resource and another node takes ownership of that resource when the owner node fails.

For more information on Cluster-Quorum, see the “[Cluster Quorum](#)” section on [page 4-2](#).

Configuring SME Cluster Management Using the CLI

You can configure SME Cluster Management using the CLI. This section includes the following topics:

- [Creating the SME Cluster, page 4-6](#)
- [Enabling and Disabling Clustering, page 4-8](#)
- [Enabling and Disabling SME Service, page 4-8](#)
- [Setting the SME Cluster Security Level, page 4-8](#)
- [Setting Up the SME Administrator and Recovery Office Roles, page 4-9](#)

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

SSH feature must be enabled in all the switches to be a part of a cluster.

Creating the SME Cluster

To create an SME tape cluster, identify the fabrics that you want to include in the cluster and configure the following:

- Automatic volume grouping
- Key Management Center (KMC)
- Target discovery
- Tape groups
- Key-on-tape mode
- Recovery
- Shared key mode
- Shutdown cluster for recovery
- Volume tape groups
- Tape compression

To create an SME disk cluster, identify the fabrics that you want to include in the cluster and you configure the following:

- CKMC
- Target discovery
- Disk groups
- Disk device
- Disk path
- Recovery
- Shutdown cluster for recovery

Detailed Steps

You can create an SME cluster for either a tape or a disk.

**Caution**

By default, the cluster is capable for SME tapes. However, when you enter the **cluster-capability disk** command, this cluster can be used only for the disk devices.

To create an SME cluster for tape, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.

Send documentation comments to mdsfeedback-doc@cisco.com

	Command	Purpose
Step 2	switch(config)# sme cluster <i>clustername1</i> switch(config-sme-cl)#	Specifies the cluster name and enters SME cluster configuration submode. A cluster name can include a maximum of 32 characters.
Step 3	switch(config-sme-cl)# fabric f1	Adds fabric f1 to the cluster.



Caution

You must enable the **cluster-capability disk** command before adding the first SME interface.

Prerequisites

Before creating disk clusters, ensure FC-Redirect version 2 is enabled on all switches that are part of the disk cluster. To verify the FC_Redirect version level, enter the following command. The expected output for configuration mode is Mode V2.

```
switch# show fc-redirect configs
Configuration Mode    = MODE_V2
```



Note

All switches in the fabric, where SME disk clusters are configured, cannot have FC-Redirect version1.

Detailed Steps

To create an SME cluster for disk, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# sme cluster <i>clustername1</i> switch(config-sme-cl)#	Specifies the cluster name and enters SME cluster configuration submode. A cluster name can include a maximum of 32 characters.
Step 3	switch(config-sme-cl)# cluster-capability disk	Defines the SME cluster capabilities for SME Disk.
Step 4	switch(config-sme-cl)# fabric f1	Adds fabric f1 to the cluster.
Step 5	switch(config-sme-cl)# fabric f2	Adds fabric f2 to the cluster.
	Note	For SME Disk, you can add up to two fabrics.



Caution

For the switches that are in the same fabric, the fabric membership configured in the CLI should be same.

Send documentation comments to mdsfeedback-doc@cisco.com

Enabling and Disabling Clustering

The first step in the process of configuring SME is to enable clustering.

Detailed Steps

To enable or disable the cluster, follow these steps:

	Command	Purpose
Step 1	switch# conf t switch(config)#	Enters configuration mode.
Step 2	switch(config)# feature cluster	Enables clustering.
Step 3	switch(config)# no feature cluster	Disables clustering.

Enabling and Disabling SME Service

SME services must be enabled to take advantage of the SME encryption and security features. After enabling the SME cluster, the second step in the process of configuring SME is to enable the SME service.

Detailed Steps

To enable the SME service, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# feature sme	Enables SME features.
Step 3	switch(config)# no feature sme	Disables SME features.

Setting the SME Cluster Security Level


There are three levels of security: Basic, Standard, and Advanced. Standard and Advanced security levels require smart cards.

Table 4-1 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.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 4-1 Master Key Security Levels (continued)

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

To set the SME cluster security level, follow these steps:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# sme cluster <i>clustername1</i> switch(config-sme-cl)#	Specifies the cluster and enters SME cluster configuration submode.
Step 3	switch(config-sme-cl)# security-mode basic	Sets the cluster security level to Basic.



Note

The CLI is not supported for enabling standard or advanced security mode. Basic mode is also supported through DCNM-SAN Web Client.

Setting Up the SME Administrator and Recovery Office Roles

To set up the SME Administrator, SME Storage Administrator, SME KMC Administrator, and SME Recovery Officer, follow this step:

Command	Purpose
switch# setup sme	Sets up the four security roles.

For more information, see the [Appendix 2, “Creating and Assigning SME Roles Using the CLI”](#)

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

Configuring SME Cluster Management Using the GUI

You can configure the SME Cluster Management using the GUI. This section includes the following topics:

- [Creating a SME Cluster Using the SME Wizard, page 4-10](#)
- [Deactivating and Purging an SME Cluster, page 4-17](#)

Creating a SME Cluster Using the SME Wizard

The SME Wizard is an easy-to-use interface that guides you through the process of creating a SME cluster.

The following sections describe the steps in this process:

- [Launching SME Wizard, page 4-10](#)
- [Choosing a Cluster Name, page 4-11](#)
- [Selecting Fabrics, page 4-11](#)
- [Selecting Interfaces, page 4-11](#)
- [Selecting Master Key Security Levels, page 4-11](#)
- [Selecting Media Key Settings, page 4-13](#)
- [Specifying the Key Management Center Server, page 4-14](#)
- [Selecting Transport Settings, page 4-14](#)
- [Confirming the Cluster Creation, page 4-15](#)
- [Downloading Key File and Storing Keyshares, page 4-15](#)

Launching SME Wizard



Note

The Node option is available only from Release 4.2(1).

Detailed Steps

To launch the SME wizard, follow these steps:

- Step 1** Open the web browser to DCNM-SAN Web Client. Log in with the user name and password.
For login information, refer to the *Cisco DCNM-SAN Fundamentals Guide*.
- Step 2** In the DCNM-SAN Web Client, click the **SME** tab.



Note

When you are accessing SME from Cisco DCNM for the first time, you will be asked to choose the Key Management role for the given DCNM. See the [“Configuring Key Management Operations” section on page 6-54](#) section for more information.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 3 Select **Clusters** in the navigation pane.

Step 4 Click **Create** in the information pane.

The SME wizard launches to guide you through the easy configuration process.

Choosing a Cluster Name



Note

Cluster names must not contain spaces or special characters.

To choose a cluster name, in the Choose Name screen, enter a cluster name. Click **Next**.



Note

You can create an SME cluster for either a tape or a disk. However, when you provide the cluster name and select the **Include Disk Support** check box, it specifies that the cluster can be used only for disk devices. Unselecting this check box specifies that the cluster can be used only for tape devices.

Select the **Disk Signature Mode** check box to create signature mode clusters.

Selecting Fabrics

To select a fabric, highlight the fabric that you want to include in the cluster. Click **Next**.

Selecting Interfaces



Note

Cisco MDS SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later supports one cluster per switch.

To select interfaces, in the Select Interfaces screen, highlight the SME interfaces that you want to include in your cluster. Click **Next**.

For information about adding interfaces, see [Chapter 3, “Configuring SME Interfaces.”](#)

Selecting Master Key Security Levels

There are three master key security levels: Basic, Standard, and Advanced. Standard and Advanced security levels require smart cards. [Table 4-2](#) describes the master key security levels.



Caution

You cannot modify the cluster security level after a cluster is created. Before confirming the cluster creation, you are prompted to review the cluster details. At that time, you can return to modify the security level.




Note

For information on cluster security, see the “[SME Security Overview](#)” section on page 1-14 and the “[About Master Key Security Modes](#)” section on page 7-3.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 4-2 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 prompted to insert the smart card into the smart card reader. 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	Advanced security requires five smart cards. When you create a cluster and select Advanced security mode, you designate the number of smart cards (two, three or five smart cards or two of three smart cards) that are required to recover the master key when data needs to be retrieved. For example, if you specify two of five smart cards, then you will need two of the five smart cards to recover the master key. Each smart card is owned by a SME Recovery Officer.
	 Note The greater the number of required smart cards to recover the master key, the greater the security. However, if smart cards are lost or if they are damaged, this reduces the number of available smart cards that could be used to recover the master key.

In the Master Key Security screen, select the cluster security type that you want to use. You can choose any of the following security levels:

- [Selecting Basic Security, page 4-12](#)
- [Selecting Standard Security, page 4-12](#)
- [Selecting Advanced Security, page 4-13](#)

Selecting Basic Security

To select basic security, in the Master Key Security screen, select **Basic**. Click **Next**.

For the Basic security level, after the cluster is created, the switch generates the master key file and you are prompted for a password to protect the file.



Note

You must download the Master Key file to activate the cluster. If you close the window before downloading the file, navigate to the cluster details page to download the Master Key file and finish the cluster setup.

Selecting Standard Security

To select standard security, in the Master Key Security screen, select **Standard**. Click **Next**.



Note

For Standard security, one SME Recovery Officer must be present to log in and enter the smart card PIN.

Send documentation comments to mdsfeedback-doc@cisco.com

Selecting Advanced Security

When Advanced security is selected, you need to designate the number of cards that are required to recover the master key. This can be two, three, or five smart cards or two of three smart cards. You need to configure all five smart cards during the cluster creations process; however, you only need the quorum number (that you designated in this step) to recover the master key.

To select Advanced Security, in the Master Key Security screen, select **Advanced**. Enter the number of required smart cards for the quorum (two of three or two of five or three of five). Click **Next**.

- For Advanced security, five SME Recovery Officers must be present to log in and enter the smart card PIN for each of the 5 smart cards.
- Be sure that the smart card reader is connected using the USB port (see “[Installing Smart Card Drivers](#)” section on page 2-25 in [Chapter 2, “Configuring SME”](#)).
- When you insert a smart card into the reader, the card is verified. You are prompted to initialize the card if the card has not been previously initialized.



Note

For Basic and Standard security modes, one user should hold the SME Administrator and the SME Recovery Officer roles.

Selecting Media Key Settings



Note

You cannot modify the media key settings after a cluster is created.

To select media key settings, in the Media Key Settings screen, select the required media key settings. Click **Next**.

[Table 4-3](#) lists the media key settings and definitions.



Note

The media key settings are applicable only for SME Tape and not for SME disk.

For additional information on media key settings, see [Chapter 7, “Configuring SME Key Management.”](#)

Table 4-3 Media Key Settings

Media Key Setting	Definition
Use unique key per media	In unique key mode, a unique key is issued for each tape volume. The default is unique key mode.
Store key on tape	<p>If you choose unique key mode (see above), this mode allows you to store the encrypted media key on the tape volume not in the Cisco Key Management Center (KMC). This provides better scaling when your backup environment includes a large number of tapes.</p> <p>This is recommended for managing a large number of tape volume keys.</p> <p>Key-on-tape mode is disabled by default.</p>

Send documentation comments to mdsfeedback-doc@cisco.com

Table 4-3 Media Key Settings (continued)

Media Key Setting	Definition
Auto-volume grouping	SME automatically creates a volume group and categorizes the appropriate tape volumes encrypted under this group based on the backup application's volume pool configuration. Auto-volume grouping is disabled by default.
Compression	SME can perform compression followed by encryption if this option is selected. Compression is enabled by default. Note Compression will be enabled for a tape drive in one of two ways: (a) configuration or (b) if the compression is not enabled through configuration and the tape drive is enabled for compression, compression is implicitly enabled for this tape drive. For case (b), a syslog is generated to indicate that the compression is enabled for this tape drive.
Recycle Tapes	Select this option to enable purging of the keys upon tape recycling. When a tape is recycled or relabeled, a new key is generated and used for encryption. Enabling this option purges the key that was used to encrypt data before the tape was recycled. Note This option must be disabled if the tapes are cloned offline without the involvement of the backup application itself. Tape recycling is enabled by default.

Specifying the Key Management Center Server

To specify the Key Management Center server, in the Key Management Server screen, you can choose the primary and the secondary Key Management Center servers from the drop-down menu. You can specify an IP address or a host name for the servers. Click **Next**.

The dual server settings is available after you configure the high availability settings in the Key Manager Settings screen.

Selecting Transport Settings

To enable transport settings in the Transport Settings screen, click **On**. If Transport Settings is enabled, specify the Trust Point from the drop-down menu.

For more information about trust points, see the *IP Services Configuration Guide, Cisco DCNM for SAN* and the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*.

If On is selected in the Transport Settings list, SSL is enabled on KMC with the following results:

- New clusters are created. If Off is selected, cluster creation fails.
- Previously created clusters are updated by enabling SSL with trustpoint on the switches. KMC server connection state remains as none until the cluster is updated.

To disable transport settings, click **Off**.

Send documentation comments to mdsfeedback-doc@cisco.com

Confirming the Cluster Creation

To confirm the cluster creation, in the Confirmation screen, review the cluster configuration information. Click **Back** to change any settings. Click **Confirm** to create the cluster.

You will see an indication that the operation is in progress and to wait until the entire configuration is applied.

Downloading Key File and Storing Keyshares

This section describes how to download the key file for basic security level and store keyshares for the standard and advanced security level.

- [Downloading the Key File for Basic Security, page 4-15](#)
- [Configuring Standard Security Level, page 4-15](#)
- [Configuring Advanced Security Level, page 4-16](#)

Downloading the Key File for Basic Security

Detailed Steps

To download the key file basic security level, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Enter the password to encrypt the master key file. Retype the password to confirm it. Click Download . |
| Step 2 | A File Download screen prompts you to open or save the encrypted file. |
-

Configuring Standard Security Level

Detailed Steps

To configure the standard security level, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | In the Confirmation screen, click Confirm to create the cluster. A Store Keyshares screen appears. |
| Step 2 | After the smart card applet finishes loading, click Next .

When entering smart card information, note the following: <ul style="list-style-type: none">• Be sure that the smart card reader is connected using the USB port (see the “Installing Smart Card Drivers” section on page 2-25 in Chapter 2, “Configuring SME”).• When you insert a smart card into the reader, the card will be verified. You will be prompted to initialize the card if the card has not been previously initialized.• Make sure that you have the appropriate smart card drivers installed before proceeding. |
| Step 3 | Enter the switch login information (username and password used to log in to DCNM-SAN), the PIN number for the smart card, and a label that identifies the smart card. The PIN number and label were defined during the smart card initialization. Click Next . |
| Step 4 | Click Finish to create a cluster. |

Send documentation comments to mdsfeedback-doc@cisco.com

Step 5 Click **Close** to return to the DCNM-SAN Web Client and to view the smart card information after the cluster creation is completed.

Step 6 View the smart card information.



Note

When an error occurs while storing shares on the cards, the cluster should be deleted and recreated.



Note

The smart card reader is only supported on Windows platforms. This includes only the Windows XP 32 bit and Windows server 2003 32 bit platforms

Configuring Advanced Security Level



Note

When an error occurs while storing shares on the cards, the cluster should be deleted and recreated.

Detailed Steps

To configure the advanced security level, follow these steps:

-
- Step 1** In the Create Cluster: Confirmation screen, click **Confirm** to create the cluster. The Create Cluster: A Store Keyshares screen appears.
- Step 2** After the smart card applet finishes loading, click **Next**.
- When entering smart card information, note the following:
- Be sure that the smart card reader is connected using the USB port (see the [“Installing Smart Card Drivers”](#) section on page 2-25 in Chapter 2, “Configuring SME”).
 - When you insert a smart card into the reader, the card will be verified. You will be prompted to initialize the card if the card has not been previously initialized.
 - For each smart card, each SME Recovery Officer must log in and enter the smart card PIN.
 - Make sure that you have the correct smart card drivers installed before proceeding.
- Step 3** Enter the switch login information (username and password used to log in to DCNM-SAN), the PIN number for the smart card, and a label that identifies the smart card. The PIN number and label were defined during the smart card initialization.
- Step 4** Click **Next**.
- You will see a notification that the keyshare is being stored. This notification is shown after each keyshare is stored.
- Step 5** Click **Next**.
- Step 6** Enter the switch credentials and PIN information for the second recovery officer. Click **Next**.
- Step 7** Enter the switch credentials and PIN information for the third recovery officer. Click **Next**.
- Step 8** Enter the switch credentials and PIN information for the fourth recovery officer. Click **Next**.
- Step 9** Enter the switch credentials and PIN information for the fifth recovery officer. Click **Next**.
- Step 10** Click **Finish** to return to the DCNM-SAN Web Client to view the smart card information.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 11 View the smart card information by selecting **Smartcards**.

Deactivating and Purging an SME Cluster

You can archive clusters that are Online, Pending, or Deprecated. For information on cluster states, see the [“Viewing Cluster States”](#) section on page 4-22.

Archiving and then purging a SME tape cluster involves the following steps:

- Delete all tape groups, tape devices, and tape volume groups. (See [Chapter 5, “Configuring SME Tapes.”](#))
- Delete all switches and SME interfaces from the cluster. (See [Chapter 3, “Configuring SME Interfaces.”](#))
- Change the cluster state to deactivated. (See [“Deactivating an SME Cluster”](#) section on page 4-17.)
- Purge (permanently delete) a SME cluster. (See [“Purging an SME Cluster”](#) section on page 4-18.)

Archiving and then purging a SME disk cluster involves the following steps:

- Delete all disk groups and disk devices. (See [Chapter 6, “Configuring SME Disks.”](#))
- Delete all switches and SME interfaces from the cluster. (See [Chapter 3, “Configuring SME Interfaces.”](#))
- Change the cluster state to deactivated. (See [“Deactivating an SME Cluster”](#) section on page 4-17.)
- Purge (permanently delete) a SME cluster. (See [“Purging an SME Cluster”](#) section on page 4-18.)

This section covers the following topics:

- [Deactivating an SME Cluster, page 4-17](#)
- [Purging an SME Cluster, page 4-18](#)

Deactivating an SME Cluster

Deactivating deletes the cluster from the switch and retains the keys in the Cisco KMC.

Detailed Steps

To change the cluster state to Deactivated, follow these steps:

Step 1 Click **Clusters** in the navigation pane to display the clusters.

Step 2 Select a cluster in the information pane and click **Remove**.



Note

Changes the cluster state to deactivated and retains the keys in the Cisco KMC.



Caution

Do not click Remove again unless you want to permanently delete the cluster configuration information and the master key information from the Cisco KMC.

Send documentation comments to mdsfeedback-doc@cisco.com

- Step 3** Click **OK**.
- Step 4** Refresh DCNM-SAN Web Client to view the notification that the cluster has been deactivated.

Purging an SME Cluster

Purging an SME cluster includes the following steps:

- Delete all cluster elements (tape paths, tape devices, volume groups, tape groups, and switches).
- Delete (unbind) any SME interfaces that are configured in the cluster.
- Change the cluster state to deactivated.
- Purge the cluster to remove the cluster and the master keys from the Cisco KMC.

Restrictions

- You can only purge a cluster that is in the deactivated state.

Detailed Steps

To purge an SME cluster, follow these steps:

- Step 1** Click **Clusters** in the navigation pane to display the SME clusters.
- Step 2** Select an deactivated cluster in the information pane and click **Remove**.
- Step 3** Click **OK** to delete the cluster.



Caution

Do not click **OK** unless you want to permanently delete the cluster configuration information and the master key from the Cisco KMC.

- Step 4** Refresh the DCNM-SAN Web Client to view the notification that the cluster has been purged.

Verifying SME Cluster Management Configuration

To display SME Cluster Management configuration information, perform one of the following tasks:

Command	Purpose
show sme	Displays a specific cluster configuration, internal information, and transport information.
show sme cluster	Displays additional cluster information.
show sme cluster key	Displays information about the cluster key database.
show sme cluster node	Displays information about a local or remote switch.
show sme cluster recovery officer	Displays information about a specific Recovery Officer or for all the Recovery Officers for a specific cluster.

Send documentation comments to mdsfeedback-doc@cisco.com

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family NX-OS Command Reference*.

Monitoring SME Cluster Management

This section covers the following topics:

- [Viewing SME Cluster Details Using the CLI, page 4-19](#)
- [Viewing SME Cluster Details Using the GUI, page 4-22](#)
- [Viewing Cluster Information Using DCNM-SAN Client, page 4-23](#)
- [Viewing Cluster Information Using Device Manager, page 4-23](#)

Viewing SME Cluster Details Using the CLI

This section covers the following topics:

- [Viewing SME Cluster, Internal, and Transport Information, page 4-19](#)
- [Viewing SME Cluster Details, page 4-19](#)
- [Viewing Cluster Key Information, page 4-20](#)
- [Viewing Cluster Node Information, page 4-21](#)
- [Viewing Recovery Officer Information, page 4-21](#)

Viewing SME Cluster, Internal, and Transport Information

To verify SME cluster configurations, you can use the **show sme** command to view a specific cluster configuration, internal information, and transport information.

A sample output of the **show sme cluster** command follows:

```
switch# show sme cluster clustername1
SME Cluster is clustername1
  Cluster ID is 2e:00:00:05:30:01:ad:f4
  Cluster is Operational
  Cluster is Not Shutdown
  Cluster config version is 27
  Security mode is basic
  Cluster status is online
  Total Nodes are 1
  Recovery Scheme is 1 out of 1
  Fabric[0] is f1
  CKMC server has not been provisioned
  Master Key GUID is 8c57a8d82d2098ee-3b27-6c2b116a950e, Version: 0
  Shared Key Mode is Enabled
  Auto Vol Group is Not Enabled
```

Viewing SME Cluster Details

Additional cluster information can be displayed with the **show sme cluster** command. Use this command to show the following:

- SME cluster details

Send documentation comments to mdsfeedback-doc@cisco.com

- SME cluster interface information
- Hosts and targets in the cluster
- SME cluster key database
- Cluster node
- SME cluster Recovery Officer information
- Summary of the SME cluster information
- Tapes in a cluster
- Tape volume group information
- Disk group in a cluster
- Disks in a cluster
- SME role configuration

Sample outputs of the **show sme cluster** command follow:

```
switch# show sme cluster clusternam1 ?
  detail      Show sme cluster detail
  interface   Show sme cluster interface
  it-nexus    Show it-nexuses in the cluster
  key         Show sme cluster key database
  node        Show sme cluster node
  recovery    Show sme cluster recovery officer information
  summary     Show sme cluster summary
  tape        Show tapes in the cluster
  tape-bkgrp  Show crypto tape backup group information
  |           Output modifiers.
  >           Output Redirection.
  <cr>        Carriage return.
```

```
switch# show sme cluster clusternam1 interface
Interface sme4/1 belongs to local switch
Status is up
```

```
switch# show sme cluster clusternam1 interface it-nexus
```

Host WWN	VSAN	Status	Switch	Interface
10:00:00:00:c9:4e:19:ed,				
2f:ff:00:06:2b:10:c2:e2	4093	online	switch	sme4/1

Viewing Cluster Key Information

Use the **show sme cluster key** command to view information about the cluster key database.

A sample output of the **show sme cluster key** command for SME tape is as follows:

```
switch# show sme cluster clusternam1 key database
Key Type is tape volumegroup shared key
  GUID is 3b6295e111de8a93-e3f9-e4ae372b1626
  Cluster is clusternam1, Tape backup group is HR1
  Tape volumegroup is Default

Key Type is tape volumegroup wrap key
  GUID is 3e9ef70e0185bb3c-ad12-c4e489069634
  Cluster is clusternam1, Tape backup group is HR1
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
Tape volumegroup is Default
```

```
Key Type is master key
GUID is 8c57a8d82d2098ee-3b27-6c2b116a950e
Cluster is clusternam1, Master Key Version is 0
```

A sample output of the **show sme cluster key** command for SME disk is as follows:

```
switch# show sme cluster clusternam1 key database
Key Type is disk key
GUID is aa8c86a783c8a0d9-34ba9cf3af0a17af
Cluster is C_SSL, Crypto disk group is DG
Crypto disk is Disk0

Key Type is master key
GUID is fc66b503982e816d-a68eba9850f29450
Cluster is C_SSL, Master Key Version is 0
```

Viewing Cluster Node Information

Use the **show sme cluster node** command to view information about a local or remote switch.

A sample output of the **show sme cluster node** command follows:

```
switch# show sme cluster clusternam1 node
Node switch is local switch
Node ID is 1
Status is online
Node is the master switch
Fabric is f1
```

Viewing Recovery Officer Information

You can view information about a specific Recover Officer or for all Recovery Officers for a specific cluster.

```
switch# show sme cluster clusternam1 recovery officer
Recovery Officer 1 is set
Master Key Version is 0
Recovery Share Version is 0
Recovery Share Index is 1
Recovery Scheme is 1 out of 1
Recovery Officer Label is
Recovery share protected by a password

Key Type is master key share
Cluster is clusternam1, Master Key Version is 0
Recovery Share Version is 0, Share Index is 1
```

```
switch# show sme cluster clusternam1 summary
```

Cluster	ID	Security Mode	Status
clusternam1	2e:00:00:05:30:01:ad:f4	basic	online

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

Viewing SME Cluster Details Using the GUI

To view cluster details, click the cluster name and the cluster detail page is displayed.

**Note**

You can use the links across the top of the information pane to navigate within the cluster.

This section covers the following topics:

- [Viewing Cluster States, page 4-22](#)
- [Viewing Members in a Cluster, page 4-22](#)
- [Viewing and Modifying Transport Settings in Cluster Detail Page, page 4-22](#)
- [Viewing and Modifying Key Management Servers Settings, page 4-23](#)

Viewing Cluster States

SME clusters can be in one of the following cluster states:

- **Online**—The SME cluster is available on the switches and is reachable from the DCNM-SAN Server.
- **Deactivated**—The SME cluster has been removed from the switches; however, the keys belonging to the cluster are deactivated in the Cisco KMC.
- **Pending**—The first SME interface has not been added to a cluster and it is not yet online.
- **Offline**—The switches of the cluster are not reachable from DCNM-SAN.
- **Deprecated**—The SME cluster with all SME interfaces removed; the cluster is unusable.

Detailed Steps

To view the cluster status, follow these steps:

-
- Step 1** Click **Clusters** in the navigation pane to view a list of all SME clusters and their status.
- Step 2** Alternately, click **Clusters** in the navigation pane, and then click a cluster name to view the status of a specific cluster.
-

Viewing Members in a Cluster

When you view members of a cluster, you see the switches and the interfaces that have been added to a cluster.

To view the SME interfaces and switches in a cluster, click **Members** in the navigation pane.

Viewing and Modifying Transport Settings in Cluster Detail Page

Detailed Steps

To view and modify the transport settings, follow these steps:

Send documentation comments to mdsfeedback-doc@cisco.com

-
- Step 1** Select the newly created cluster in the navigation pane to display the cluster detail page.
The transport settings details are displayed when SSL is selected.
The transport settings details are displayed when SSL is Off.
You can also modify the transport settings in the cluster detail page by clicking **Modify**.
- Step 2** Select **SSL** and choose a Trust Point from the drop-down menu. Click **Apply** to save the settings.
-

Viewing and Modifying Key Management Servers Settings

Detailed Steps

To view and modify the primary and secondary key management servers settings, follow these steps:

-
- Step 1** Select the cluster in the navigation pane to display the cluster detail page. Scroll to the Key Management Settings section and click **Modify** to edit the server settings.
- Step 2** Enter the IP addresses for the primary and/or the secondary servers. Click **Apply** to save the changes. Click **Cancel** to revert back to previous settings.



Note KMC server can also be modified through the cluster list view.

- Step 3** Refresh the DCNM-SAN Web Client to view the notification that the cluster has been modified.
-

Viewing Cluster Information Using DCNM-SAN Client

Detailed Steps

To view SME cluster information using DCNM-SAN Client, follow these steps:

-
- Step 1** In the Physical Attributes pane, select **Intelligent Features > SME > Clusters**.
- Step 2** Click the **Members** tab to view members in a cluster.
- Step 3** Click the **Interfaces** tab to view information about SME interfaces.
-

Viewing Cluster Information Using Device Manager

Detailed Steps

To view SME cluster information using Device Manager, follow these steps:

Send documentation comments to mdsfeedback-doc@cisco.com

-
- Step 1** In the Interface menu, select **SME Clusters**.
- Step 2** Click the **Clusters** tab to view the cluster name, state, and Master IP address.
- Step 3** Click the **Members** tab to view the cluster name, switch, fabric name, and whether or not the cluster or fabric is local.
- Step 4** Select **Interfaces** to view cluster interface information.
- Step 5** Select **Hosts** to view the information about the hosts in the cluster.
-

Feature History for SME Cluster Management

Table 4-4 lists the release history for this feature.

Table 4-4 Feature History for SME Cluster Management

Feature Name	Releases	Feature Information
Software change	5.2(1)	In Release 5.2(1), Fabric Manager is changed to DCNM for SAN (DCNM-SAN).
	4.1(1c)	In Release 4.1(1b) and later, the MDS SAN-OS software is changed to MDS NX-OS software. The earlier releases are unchanged and all references are retained.
High availability KMC server	4.1(3)	High availability KMC can be configured by using a primary and secondary servers. In 4.1(3), HA settings are available on the Key Manager Settings page. The primary and secondary servers can be chosen during cluster creation. The primary and secondary server settings can be modified in the Cluster detail page.
Host names are accepted as server addresses	4.1(3)	You can enter IP addresses or host names for the servers.
Target-based load balancing	3.3(1c)	Clustering offers target-based load balancing of SME services.
Transport settings	3.3(1c)	Allows users to enable or disable transport settings for SME.