Send documentation comments to mdsfeedback-doc@cisco.com

CHAPTER 2

Configuring SME

This chapter includes information about configuring SME, SME installation, and the preliminary tasks that you must complete before configuring SME.

This chapter includes the following topics:

Information About SME Configuration

You can use one of these two configuration management tools to configure SME:

- Cisco DCNM-SAN, page 2-1
- Command Line Interface, page 2-2

The Cisco DCNM-SAN Web Client can be used to configure and manage SME using a web browser.

Cisco DCNM-SAN

Cisco DCNM-SAN is a set of network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3). Cisco DCNM-SAN includes the following applications:

- DCNM-SAN Web Client—Provides a graphical user interface (GUI) that displays real-time views of your network fabric, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches.

Send documentation comments to mdsfeedback-doc@cisco.com

Note SME configuration is supported in DCNM-SAN Web Client only.

- DCNM-SAN —Installed on a server and must be started before running the DCNM-SAN client. It can be accessed by up to 16 DCNM-SAN Clients at a time.
- Device Manager—Provides two views of a switch.
  - Device View displays a continuously updated physical representation of the switch configuration, and provides access to statistics and configuration information for a single switch.
  - Summary View displays real-time performance statistics of all active interfaces and channels on the switch for Fibre Channel and IP connections.

Note During the DCNM-SAN installation, the use_ip flag in the smeserver.properties file is set to FALSE by default. If you choose to use IP addresses, the DNS server should not be configured on any switch in the fabric and the use_ip flag in the smeserver.properties file must be set to TRUE.

The smeserver.properties file is located at the following location: <fm install path>\dcm\fm\conf\

Once you make any modifications to the smeserver.properties file, you must restart DCNM-SAN.

The Cisco DCNM-SAN applications are an alternative to the CLI for most switch configuration commands.

For more information on configuring the Cisco MDS switch using DCNM-SAN, refer to the *Cisco DCNM Fundamentals Guide.*

Command Line Interface

With the CLI, you can type commands at the switch prompt, and the commands are executed when you press the **Enter** key. The CLI parser provides command help, command completion, and keyboard sequences that allow you to access previously executed commands from the buffer history.

Licensing Requirements for SME Configuration

To use the SME feature, you need the appropriate SME license. However, enabling SME without a license key starts a counter on the grace period. You then have 120 days to install the appropriate license keys or disable the use of SME. If at the end of the 120-day grace period the switch does not have a valid license key for SME, it will be automatically disabled.

Note Although you need to install DCNM-SAN, you do not need a DCNM-SAN license to use SME. Additional DCNM-SAN capabilities are not enabled by default with SME, so there is no free performance monitoring or other functionality.

To identify if the SME feature is active, use the **show license usage license-name** command.

Send documentation comments to mdsfeedback-doc@cisco.com

The Cisco MDS 9000 SME package is licensed on a per-encryption-engine basis. The total number of licenses needed for a SAN fabric is equal to the number of Cisco MDS 9000 18/4-Port Multiservice Modules plus the number of fixed slots on Cisco MDS 9222i switches used for SME plus the number of encryption engines on Cisco MDS 9000 16-Port Storage Services Nodes (SSN-16).

Each interface in the SSN-16 module is licensed and priced individually.

Table 2-1 lists the SME licenses that are available.

Table 2-1 SME Licenses

Part Number	Description	Applicable Product
M9500SME1MK9	SME package for MSM-18/4 module	MDS 9500 Series with MSM-18/4 module
M9200SME1MK9	SME package for MSM-18/4 module	MDS 9200 Series with MSM-18/4 module
M9200SME1FK9	SME package for fixed slot	MDS 9222i Switch only
M95SMESSNK9	SME package for one service engine on SSN-16 module, spare	MDS 9500 Series with SSN-16 module
M92SMESSNK9	SME package for one service engine on SSN-16 module, spare	MDS 9200 Series with SSN-16 module

The following table shows the licensing requirements for this feature:

License	License Description
SME_FOR_IPS_184_PKG	Activates SME for MSM-18/4 module.
SME_FOR_SSN16_PKG	Activates SME for a SSN-16 engine.
SME_FOR_9222i_PKG	Activates SME for the Cisco MDS 9222i Switch.

To obtain and install SME licenses, refer to the *Cisco MDS 9000 Family NX-OS Licensing Guide*.

Prerequisites for SME Configuration

This section includes the following topics:

- SME Installation Requirements, page 2-3
- FCIP Write Acceleration and Tape Acceleration Topology Requirements, page 2-4

SME Installation Requirements

SME configuration has the following installation requirements:

- Cisco MDS SAN-OS Release 3.2(2c) or later or Cisco NX-OS Release 4.x or later must be installed on the Cisco MDS 9222i switch or the Cisco MDS 9000 Family switch with an MSM-18/4 module for SME Tape.

Send documentation comments to mdsfeedback-doc@cisco.com

- Cisco NX-OS Release 5.2(1) must be installed on the Cisco MDS 9222i switch or the Cisco MDS 9000 Family switch with an MSM-18/4 module or SSN-16 module for SME Disk.
- Cisco DCNM-SAN must be installed on a server that you use to provide centralized MDS management services and performance monitoring. The Cisco Key Management Center (Cisco KMC) is on this server.
- DCNM-SAN Web Client can be used to configure and manage SME using a web browser.

For DCNM-SAN server installation that is specific to SME, see "Installing DCNM-SAN Server" section on page 2-6.

For more information about installing DCNM-SAN, see the *Cisco DCNM Installation and Licensing Guide*.

Caution If the Cisco Key Management Center (CKMC) is part of DCNM-SAN, then the switches and DCNM-SAN must not be upgraded at the same time.

FCIP Write Acceleration and Tape Acceleration Topology Requirements

SME Disk and SME Tape with FCIP write acceleration or tape acceleration topology has the following requirements:

- If an initiator is on a non-FC-Redirect-capable switch, SME switches should be on the target side of the FCIP tunnel.
- If an initiator is on an FC-Redirect-capable switch, SME switches should be on the host side of the FCIP tunnel.

Guidelines and Limitations

To design CFS regions for FC-Redirect, follow these guidelines:

- Ensure the CFS region configuration for FC-Redirect can be applied to all FC-Redirect-based applications. The applications include SME, Cisco DMM, and any future applications.
- Ensure that all FC-Redirect-capable switches that are connected to the hosts, targets, and the application switches (switches with MSM-18/4 modules in a cluster) are configured in the same region.
- If there are multiple SME clusters in a region, a target can be part of the SME configuration in only one cluster. To change the target to a different cluster, the configuration in the first cluster must be deleted before creating the configuration in the second cluster.
- All switches in the region must have a common VSAN.
- For existing SME installations, refer to "Configuring CFS Regions For FC-Redirect" section on page D-5 for steps on migrating to CFS regions.
- Remove all instances of the previous configurations when a switch is moved to a region or moved out of a region.

To configure a CFS region, refer to the "Configuring CFS Regions For FC-Redirect" section on page D-5.

Table 2-2 lists the SME configurations and the corresponding limits.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2-2 SME Tape Configuration Limits

Configuration	Limit
Number of clusters per switch	1
Switches in a cluster	4
Number of fc-redirect capable switches in a fabric	10
Fabrics in a cluster	2
Modules in a switch	11
Cisco MSM-18/4 modules in a cluster	32
Initiator-Target-LUNs (ITLs)	1024
LUNs behind a target	32
Host and target ports in a cluster	128
Number of hosts per target	128
Tape backup groups per cluster	4
Volume groups in a tape backup group	32
Keys in a Tape volume group	8000
Number of disk groups	128
Number of SME disks (LUNs)	2000
Cisco Key Management Center (number of keys)	32,000
Targets per switch that can be FC-redirected	32
IT connections per SME interface (soft limit)	256 **Note** Beyond this limit, a syslog message will be displayed. It is recommended that you provision more SME interfaces in the cluster.[1]
IT connections per SME interface (hard limit)	512 **Note** Beyond this limit, new IT connections will not be assigned to that particular SME interface and a critical syslog will be displayed.[2]

[1] Applicable from NX-OS Release 4.2(1) and later

[2] Applicable from NX-OS Release 4.2(1) and later

Table 2-3 SME Disk Configuration Limits

Configuration	Per Cluster	Per Switch	Per Crypto Node
Number of clusters	NA	2	1
Number of physical fabrics	2	NA	NA

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2-3 SME Disk Configuration Limits (continued)

Configuration	Per Cluster	Per Switch	Per Crypto Node
Number of switches	8	NA	NA
Number of modules (line cards—SSN 16 or MSM-18/4 modules)	NA	11	NA
Cisco SME interfaces (crypto nodes used for encryption)	32	32	NA
Initiator-Target-LUNs (ITLs)	2048	2048	512
LUNs behind a target	512	512	512
Number of initiator ports	128	NA	NA
Number of target ports	128	NA	NA
Maximum number of IT nexus	128	NA	NA
Number of paths per LUN (physical paths per SME disk)	8	8	8
Number of disk groups	128	128	128
Number of SME disks (LUNs)	2048	2048	512
Cisco Key Management Center (KMC) number of keys	32,000	32,000	32,000
Maximum number of concurrent data preparations (offline data preparations)	NA	NA	64
Total number of Disk key replication relationships	2048		

NA—Not applicable

Installing DCNM-SAN Server

This section describes how to install Cisco DCNM-SAN for SME. The installation steps explained here are for Windows. The installation procedure is similar for all of the supported platforms.

Note Ensure you follow the Cisco DCNM upgrade procedure and the upgrade path if you have an existing Cisco DCNM or Fabric Manager installation. For more information on Cisco DCNM upgrade, see the *Cisco DCNM Installation and Licensing Guide*, Release 6.x.

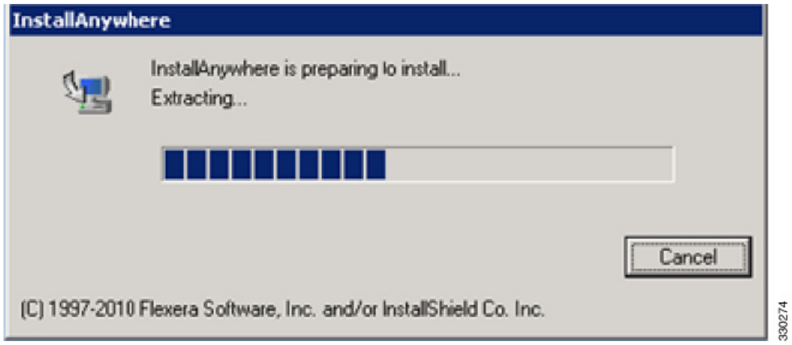
If you have an existing DCNM/FM installation for SME, you should follow the DCNM Upgrade guide, and follow the documented DCNM upgrade path. See the DCNM installation / configuration guide for more information.

To install DCNM-SAN server, follow these steps:

Step 1 Copy the appropriate installer for the appropriate supported platform.

Step 2 Double-click the installer. The Installer Anywhere screen is displayed.

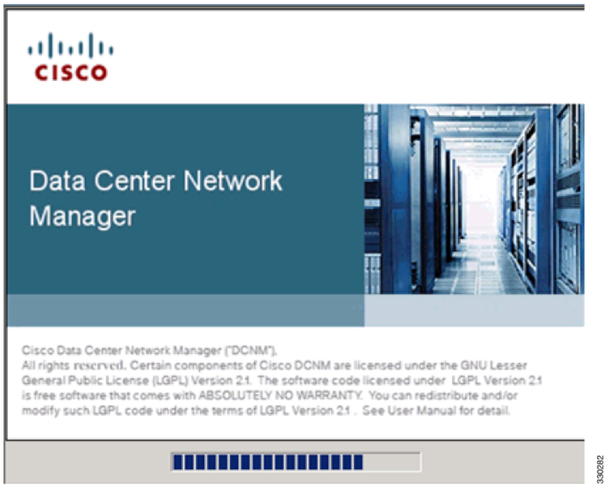
Send documentation comments to mdsfeedback-doc@cisco.com


InstallAnywhere

InstallAnywhere is preparing to install...
Extracting...

(C) 1997-2010 Flexera Software, Inc. and/or InstallShield Co. Inc.

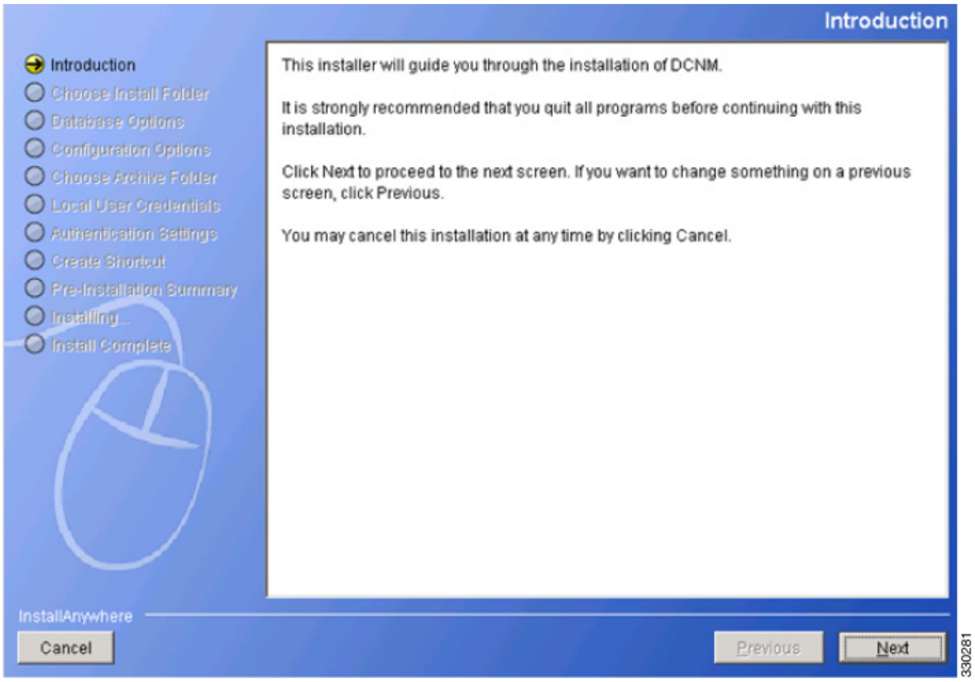
The installer begins extracting the files. Once it is completed, the Data Center Network Manager screen is displayed showing the progress of the setup.


Data Center Network Manager

Cisco Data Center Network Manager ("DCNM").
All rights reserved. Certain components of Cisco DCNM are licensed under the GNU Lesser General Public License (LGPL) Version 2.1. The software code licensed under LGPL Version 2.1 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such LGPL code under the terms of LGPL Version 2.1 . See User Manual for detail.

Once the DCNM setup process is completed, the DCNM installation wizard Introduction screen is displayed.

Send documentation comments to mdsfeedback-doc@cisco.com



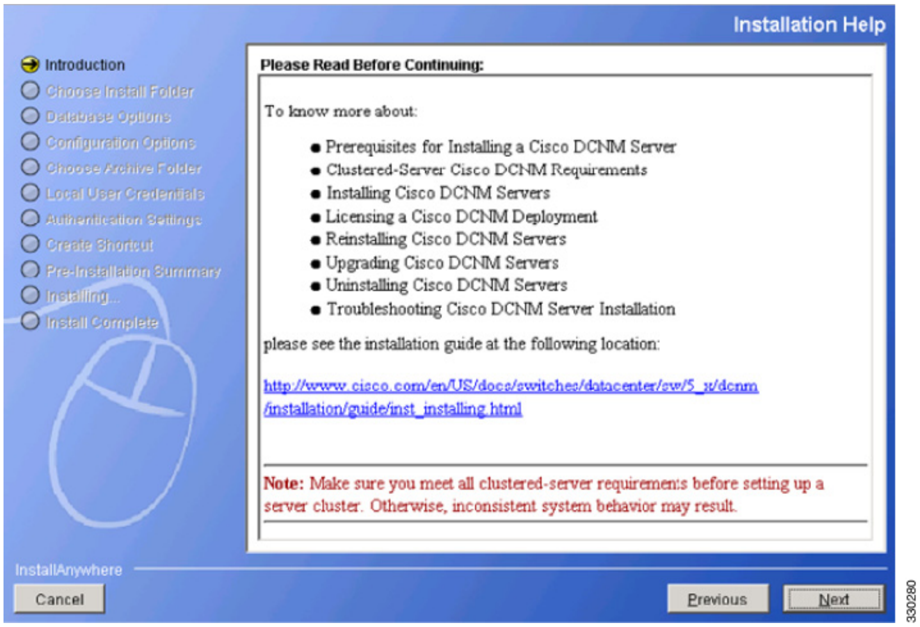
This installer will guide you through the installation of DCNM.

It is strongly recommended that you quit all programs before continuing with this installation.

Click Next to proceed to the next screen. If you want to change something on a previous screen, click Previous.

You may cancel this installation at any time by clicking Cancel.

Step 3 Click **Next**. The Installation Help screen is displayed.



Please Read Before Continuing:

To know more about:

- Prerequisites for Installing a Cisco DCNM Server
- Clustered-Server Cisco DCNM Requirements
- Installing Cisco DCNM Servers
- Licensing a Cisco DCNM Deployment
- Reinstalling Cisco DCNM Servers
- Upgrading Cisco DCNM Servers
- Uninstalling Cisco DCNM Servers
- Troubleshooting Cisco DCNM Server Installation

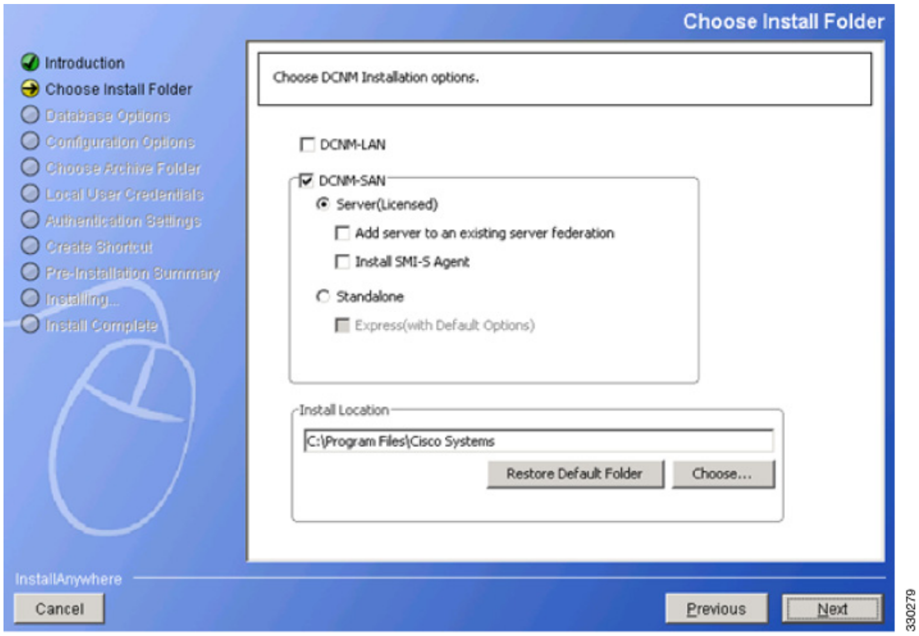
please see the installation guide at the following location:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/dcnm/installation/guide/inst_installing.html

Note: Make sure you meet all clustered-server requirements before setting up a server cluster. Otherwise, inconsistent system behavior may result.

Step 4 Click **Next**. The Choose Install Folder screen is displayed.

Send documentation comments to mdsfeedback-doc@cisco.com



Choose Install Folder

- Introduction
- Choose Install Folder
- Database Options
- Configuration Options
- Choose Archive Folder
- Local User Credentials
- Authentication Settings
- Create Shortcut
- Pre-Installation Summary
- Installing...
- Install Complete

Choose DCNM Installation options.

□ DCNM-LAN

☑ DCNM-SAN

● Server(Licensed)

□ Add server to an existing server federation

□ Install SMI-S Agent

○ Standalone

□ Express(with Default Options)

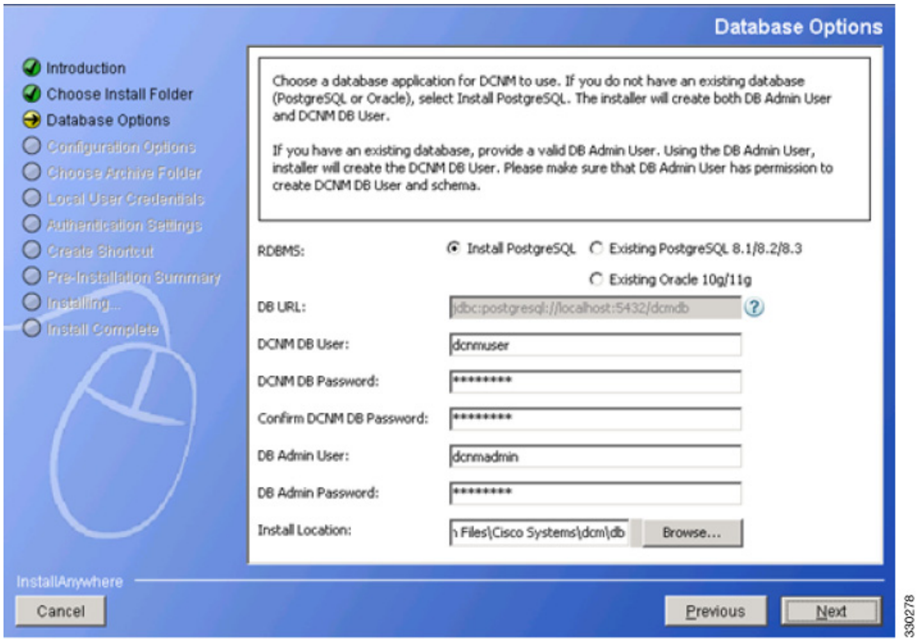
Install Location

C:\Program Files\Cisco Systems

Select DCNM-SAN and select Server (Licensed). You must select these specifically for SME.

Note You must select Add server to an existing server federation option if you are looking for high availability with respect to KMC. If you need to link two servers that act as primary and secondary, you must install DCNM on the first server without selecting this option. However, while installing on the secondary server, you must select the Add server to an existing server federation option to link to the primary server.

Step 5 Click **Next**. The Database Options screen is displayed.



Choose a database application for DCNM to use. If you do not have an existing database (PostgreSQL or Oracle), select Install PostgreSQL. The installer will create both DB Admin User and DCNM DB User.

If you have an existing database, provide a valid DB Admin User. Using the DB Admin User, installer will create the DCNM DB User. Please make sure that DB Admin User has permission to create DCNM DB User and schema.

RDBMS: ● Install PostgreSQL ○ Existing PostgreSQL 8.1/8.2/8.3 ○ Existing Oracle 10g/11g

DB URL: jdbc:postgresql://localhost:5432/dcmdb

DCNM DB User: dcnmuser

DCNM DB Password: *********

Confirm DCNM DB Password: *********

DB Admin User: dcnmadmin

DB Admin Password: *********

Install Location: n Files\Cisco Systems\dcm\db Browse...

You can choose the PostgreSQL database that comes up with DCNM package by choosing the Install PostgreSQL option. You can also choose an existing or installed database by choosing either the Existing PostgreSQL 8.1/8.2/8.3 or the Existing Oracle 10g/11g option.

Note The DCNM package installation does not provide the Oracle database.

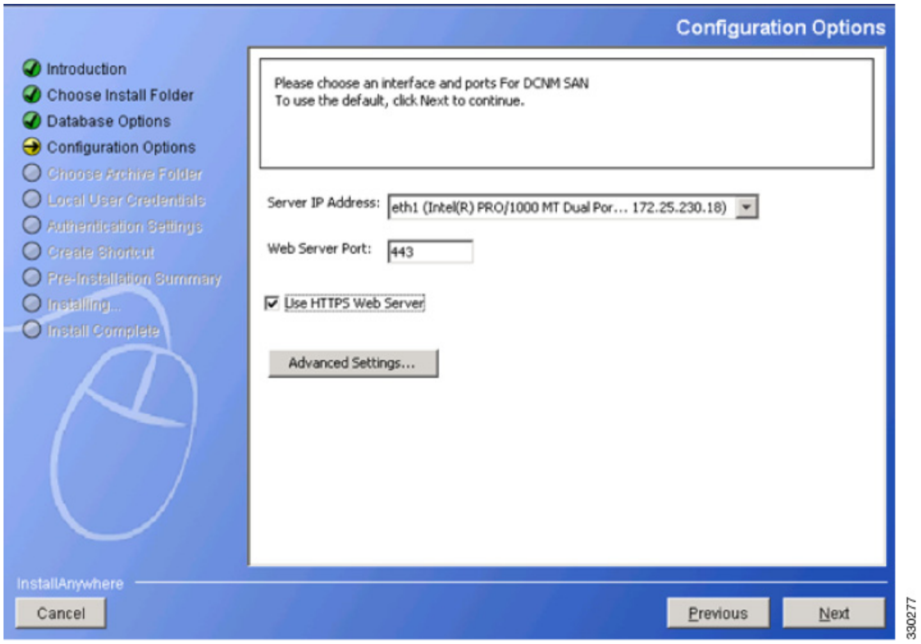
If you prefer to select the Add server to an existing server federation option on a secondary server, you must select the existing database option and point towards the primary server database through which the link is established. A configuration using Postgres provides KMC high availability and does not provide database high availability. Only the Cisco DCNM installation using the Oracle database with the dataguard option provides high availability,

You must provide the DCNM DB User and DB Admin user credentials with which the respective user can access the database. You also can browse the location where this installation can will reside.

Note The DCNM Database and the DCNM Admin user names must be different.

Step 6 Click **Next**. The Configuration Options screen is displayed.

Send documentation comments to mdsfeedback-doc@cisco.com



Please choose an interface and ports For DCNM SAN
To use the default, click Next to continue.

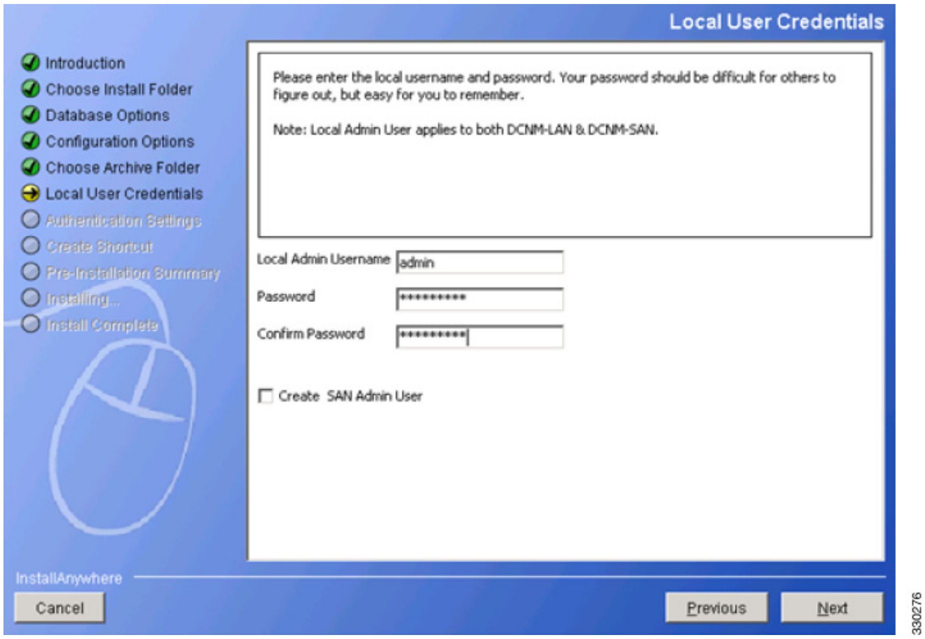
Server IP Address: eth1 (Intel(R) PRO/1000 MT Dual Por... 172.25.230.18)

Web Server Port: 443

☑ Use HTTPS Web Server

Select the Use HTTPS Web Server option which is SME specific.

Step 7 Click **Next**. The Local User Credentials screen is displayed.



Please enter the local username and password. Your password should be difficult for others to figure out, but easy for you to remember.

Note: Local Admin User applies to both DCNM-LAN & DCNM-SAN.

Local Admin Username admin

Password **********

Confirm Password **********

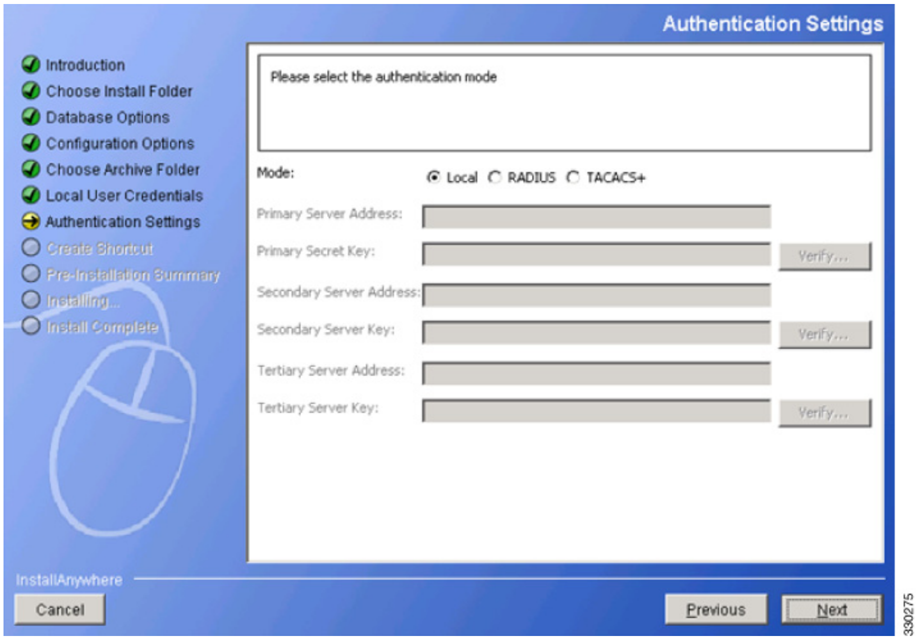
☐ Create SAN Admin User

Provide the Local Admin Username and password details that are required to log in to DCNM server.

Send documentation comments to mdsfeedback-doc@cisco.com

Note You must ensure that the Local Admin Username and Password values are the same as the switch username and password that are a part of a cluster. If not, the cluster creation fails.

Step 8 Click **Next**. The Authentication Settings screen is displayed.



Authentication Settings

Please select the authentication mode

Mode: ● Local ○ RADIUS ○ TACACS+

Primary Server Address:

Primary Secret Key:

Secondary Server Address:

Secondary Server Key:

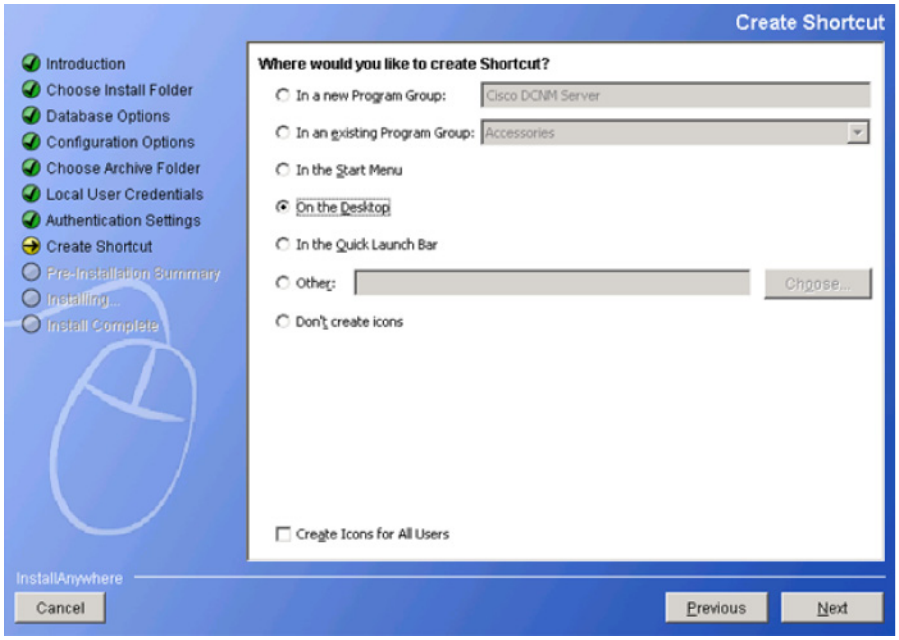
Tertiary Server Address:

Tertiary Server Key:

Select one of the modes from the Local, RADIUS, or TACACS+ options. If you select either the RADIUS or the TACACS+ option, you must provide the server address and secret key (remote authentication).

Step 9 Click **Next**. The Create Shortcut screen is displayed.

Send documentation comments to mdsfeedback-doc@cisco.com



Where would you like to create Shortcut?

○ In a new Program Group: Cisco DCNM Server

○ In an existing Program Group: Accessories

○ In the Start Menu

● On the Desktop

○ In the Quick Launch Bar

○ Other: Choose...

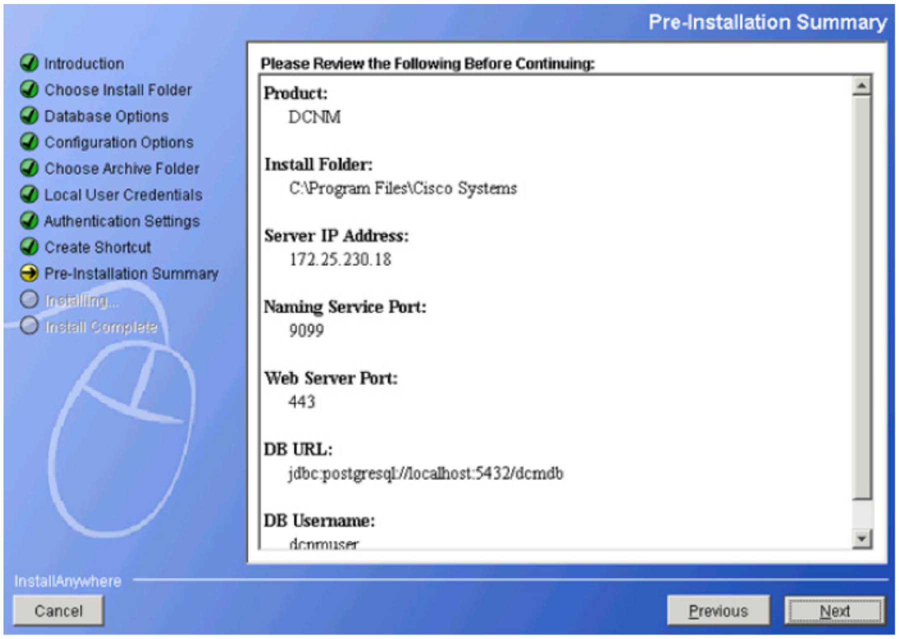
○ Don't create icons

□ Create Icons for All Users

330287

You must select one of the options where you want the shortcut to be created.

Step 10 Click **Next**. The Pre-Installation Summary screen is displayed.



Please Review the Following Before Continuing:

Product:
DCNM

Install Folder:
C:\Program Files\Cisco Systems

Server IP Address:
172.25.230.18

Naming Service Port:
9099

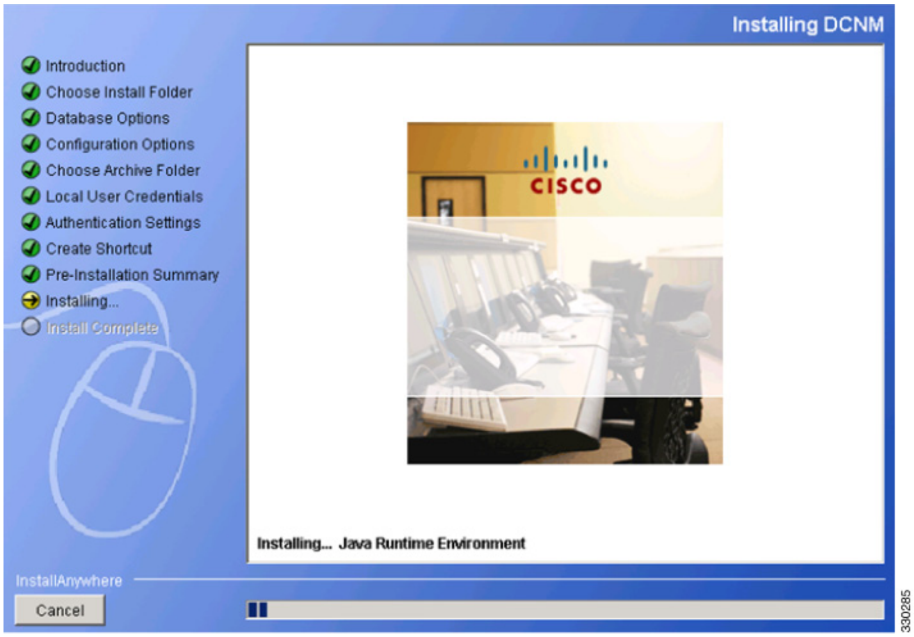
Web Server Port:
443

DB URL:
jdbc:postgresql://localhost:5432/dcmdb

DB Username:
dcnmuser

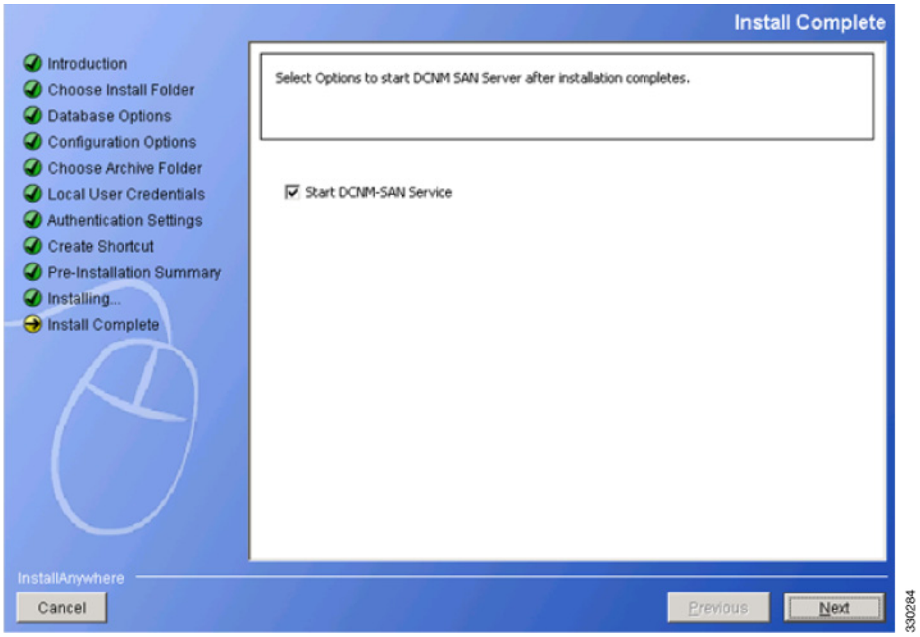
330286

Step 11 Review this information and click **Next**. The Installing DCNM screen is displayed that shows the progress of installation.



Installing... Java Runtime Environment

Step 12 After the installation process is completed, the Install Complete screen is displayed.



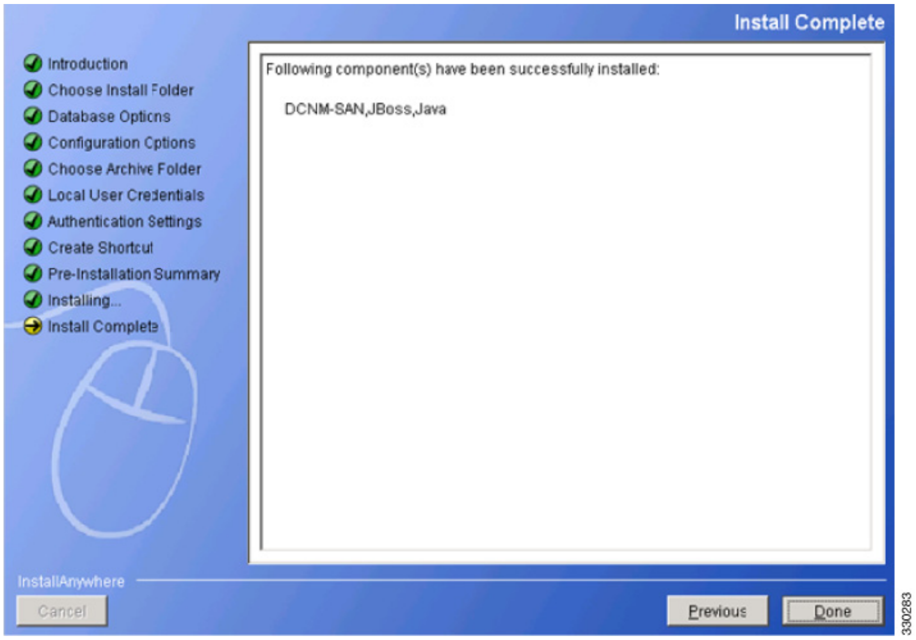
Select Options to start DCNM SAN Server after installation completes.

☑ Start DCNM-SAN Service

Send documentation comments to mdsfeedback-doc@cisco.com

Select Start DCNM-SAN Service.

Step 13 Click **Next**. The Install Complete screen is displayed.



Install Complete

Following component(s) have been successfully installed:

DCNM-SAN,JBoss,Java

Step 14 Click **Done** to complete the installation. The DCNM installation includes JBOSS and JAVA.

Note After the installation process is complete, you must update the JCE policy files under the JAVA directory created by the DCNM package installation.

Configuring SME Tasks

The process of configuring SME on an MDS-18/4 module or Cisco MDS 9222i switch involves a number of configuration tasks that should be followed in chronological order.

This process includes the following configuration tasks:

1. Enable clustering on the Cisco MDS-18/4 module, Cisco MDS SSN-16 module, or through the CLI.
2. Enable SME on the Cisco MDS-18/4 module, Cisco MDS SSN-16 module, or through the CLI.
3. Add the SME interface to the Cisco MDS-18/4 module or Cisco MDS SSN-16 module.
4. Add a fabric that includes the Cisco MDS-18/4 module or Cisco MDS SSN-16 module with the SME interface.
5. Create a cluster.

Send documentation comments to mdsfeedback-doc@cisco.com

Note The cluster can either be defined for SME Disk or SME Tape. By default, the cluster is tape capable. However, the **cluster-capability disk** command under the cluster defines the cluster as disk capable. For more information, see the "Creating the SME Cluster" section on page 4-6.

a. Name the cluster.

b. Select the fabrics that you want to create a cluster from.

c. Select the SME interfaces from the fabrics that you are including in the cluster.

d. Select the master key security level (Basic, Standard, or Advanced).

e. Select the security key (shared or unique) and tape preferences (store the key on tape, automatic volume grouping, and compression).

f. Specify the Key Management Center server and key certificate file.

g. Specify the password to encrypt the master key and download the key file.

Required Preconfiguration Tasks

This section describes the required tasks that must be completed before you configure SME.

This section includes the following topics:

- Enabling Clustering, page 2-16
- Enabling SME, page 2-18
- Enabling DNS, page 2-18
- IP Access Lists for the Management Interface, page 2-19
- Creating and Assigning SME Roles and SME Users, page 2-19
- Installing DCNM-SAN and DCNM-SAN Client, page 2-23
- Adding a Fabric and Changing the Fabric Name, page 2-23
- Choosing a Key Manager, page 2-24
- Using FC-Redirect with CFS Regions, page 2-25
- Installing Smart Card Drivers, page 2-25
- SME Configuration Process, page 2-25
- SME Configuration Restrictions, page 2-26

Before configuring SME, you must explicitly enable clustering, SME, SSH, and DNS on the MDS switch with an installed MSM-18/4 module or on the MDS 9222i switch. By default, these are disabled. The configuration and verification operations for SME are only available when these are enabled on a switch.

Enabling Clustering

You can enable clustering on the Cisco MDS 9000 switch with an installed MSM-18/4 module using DCNM-SAN and Device Manager 3.2(2c) or later, or Cisco NX-OS 4.x or later.

Send documentation comments to mdsfeedback-doc@cisco.com

Note Be sure to enable clustering first, and then enable SME.

This section includes the following topics:

- Enabling Clustering Using DCNM-SAN, page 2-17
- Enabling Clustering Using Device Manager, page 2-17

Enabling Clustering Using DCNM-SAN

Note All the MDS switches with SME interfaces in the cluster should match the authentication credentials used by DCNM-SAN.

Detailed Steps

To enable clustering using DCNM-SAN, follow these steps:

Step 1 In the Physical Attributes pane, select **Intelligent Features > SME > Clusters**.

Step 2 From the Control tab in the information pane, locate the switch.

Step 3 From the drop-down menu in the Command column, select **enable**. The default is noSelection.

Note You can select **enable** on multiple switches, and then click **Apply**.

Step 4 Click **Apply**.

Enabling Clustering Using Device Manager

Detailed Steps

To enable clustering using Device Manager, follow these steps for a specific switch:

Step 1 From the Admin menu in the device screen, select **Feature Control.**

Step 2 Select **cluster**.

Step 3 From the Action column drop-down menu, select **enable**.

Step 4 Click **Apply**.

Send documentation comments to mdsfeedback-doc@cisco.com

Enabling SME

You can enable SME using DCNM-SAN or Device Manager.

Note Be sure to enable clustering first, and then enable SME.

This section includes the following topics:

- Enabling SME Using DCNM-SAN, page 2-18
- Enabling SME Using Device Manager, page 2-18

Enabling SME Using DCNM-SAN

Detailed Steps

To enable SME using DCNM-SAN, follow these steps:

Step 1 In the Physical Attributes pane, select **Intelligent Features > SME > Clusters**.

Step 2 From the Control tab in the information pane, locate the switch.

Step 3 From the drop-down menu in the Command column, select **enable**. The default is noSelection.

Note You can select **enable** on multiple switches, and then click **Apply**.

Step 4 Click **Apply**.

Enabling SME Using Device Manager

Detailed Steps

To enable SME using Device Manager, do the following for a specific device:

Step 1 From the Admin menu in the device screen, select **Feature Control.**

Step 2 Select **sme**.

Step 3 From the Action column drop-down menu, select **enable**.

Step 4 Click **Apply**.

Enabling DNS

DNS offers services to map a host name to an IP address in the network through a DNS server. When you configure DNS on the switch, you can substitute the host name for the IP address with all IP commands, such as **ping**, **telnet**, **upload**, and **download**.

If you use DNS, the following requirements apply:

- All switches should be configured using DNS.
- The domain name (or the domain list), and the IP name server must be configured to reach remote switches.
- The DNS server should be configured on the same server where DCNM-SAN is installed.

If you use IP addresses, the DNS should not be configured on any switch in the fabric and the use_ip flag in the smeserver.properties must be set to TRUE.

For information on configuring DNS, refer to the *IP Services Configuration Guide, Cisco DCNM for SAN* and the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide.*

sme.useIP for IP Address or Name Selection

If you do not have DNS configured on all switches in the cluster, you can use sme.useIP. The smeserver.properties file is located in the following location: <fm install path>\dcm\fm\conf\.

During the DCNM-SAN installation, the use_ip flag in the smeserver.properties file is set to FALSE by default. If you choose to use IP addresses, the DNS server should not be configured on any switch in the fabric and the use_ip flag in the smeserver.properties file must be set to TRUE. Once you make any modifications to the smeserver.properties file, you must restart DCNM-SAN.

Ensure you enable clustering first, and then enable SME.

You must decide to use DNS completely or to use IP addresses fully in your fabric. A combination of these will not work with the SME feature.

To verify that DNS is enabled everywhere in the cluster, ping between the DCNM-SAN server and the MDS switches and also between the MDS switches with DNS names.

IP Access Lists for the Management Interface

Cluster communication requires the use of the management interface. IP ACL configurations must allow UDP and TCP traffic on ports 9333, 9334, 9335, and 9336.

Creating and Assigning SME Roles and SME Users

The SME feature provides two primary roles: SME Administrator and the SME Recovery Officer. The SME Administrator role also includes the SME Storage Administrator and SME KMC Administrator roles. By default, SME assigns both the SME Administrator and the SME Recovery Officer to the same user. This assignment works well for small scale deployments of SME.

Note The DCNM-SAN user credentials must be the same as the switch user.

Table 2-4 shows a description of the SME roles and the number of users that should be considered for each role.

Send documentation comments to mdsfeedback-doc@cisco.com

Note SME is configured from the DCNM-SAN Web Client. Internally, the actual switch operations are executed on behalf of the user that is logged into the Web Client and not the user monitoring the fabrics. Therefore, in a multifabric configuration the SME administrators must have the same username and password across all the fabrics to perform the SME operations.

Table 2-4 SME Roles and Responsibilities

SME Role	Master Key Security Mode	Required # of Users for This Role	What Operations is This Role Responsible For?
SME Administrator	Basic mode Standard mode	One user should hold the SME Administrator and the SME Recovery officer roles. One per VSAN is the minimum for day to day operations; must have access to all VSANs (if there are many VSANs and multiple VSAN administrators are assigned, then SME administrators, then there may be one SME Administrator per VSAN for key recovery operations.	• SME management • Tape management • Disk management • Export/import tape volume groups • Export/import disk keys
SME KMC Administrator	Basic mode Standard mode	The number of users is the same as for the SME Administrator role.	• Key Management operations • Archive/purge volumes • Add/remove volume groups • Add/remove disk groups and disk devices • Import/export volume groups • Import/export disk keys • Rekey/replace smart cards

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2-4 SME Roles and Responsibilities (continued)

SME Role	Master Key Security Mode	Required # of Users for This Role	What Operations is This Role Responsible For?
Cisco Storage Administrator	Basic mode Standard mode	The number of users is the same as for the SME Administrator role.	- SME provisioning operations - Create/update/delete cluster - Create/update/delete tape backup groups - Create/update/delete disk groups - Add/remove tape devices - Add/remove disk devices - Create volume groups - View smart cards
SME Recovery Officer	Advanced mode	Five users (one for each smart card). Each smart card holder must be present during the cluster creation to provide the user login and password information and smart card pin.	- Master key recovery - Replace smart card

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

Configuring the AAA Roles

For information on configuring the AAA roles for the SME Administrator and the SME Recovery Officer, refer to the *Cisco MDS 9000 Family NX-OS Security Configuration Guide* and the *Security Configuration Guide, Cisco DCNM for SAN*.

Creating and Assigning SME Roles Using DCNM-SAN

For detailed information on creating and assigning roles, refer to the *Security Configuration Guide, Cisco DCNM for SAN* and the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.

Note SME role names must begin with “sme.” For example, valid role names could be sme-admin, sme-recovery, or sme-admin-vsan1.

You need to create a SME role and then assign users to the SME role.

To create a SME role, follow these steps:

Step 1 Click the **Admin** tab. Select **Management Users** and select **Local**.

The Add Local User dialog box is displayed.

Step 2 Type the username.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 3 From the role drop-down menu, select one of the options: **network-admin, server-admin, sme-admin, sme-recovery**, or **sme-stg-admin**.

Step 4 Type the password and confirm the password.

Step 5 Click **Add**.

Creating and Assigning SME Roles Using the CLI

For detailed information on creating and assigning roles, refer to the *Security Configuration Guide, Cisco DCNM for SAN* and the *Cisco MDS 9000 Family NX-OS Security Configuration Guide*.

Prerequisites

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

Restrictions

- Only users belonging to the network-admin role can create roles.
- The four security roles required by SME can be implicitly created by using the **setup sme** command. For VSAN-based access control, you must create the custom roles.

Detailed Steps

To create a SME role or to modify the profile for an existing SME role, follow these steps:

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

Step 2	`switch(config)# role name sme-admin`
	`switch(config-role)#`
		Places you in the mode for the specified role (sme-admin).
		Note: The role submode prompt indicates that you are now in the role submode. This submode is now specific to SME.

Step 3	`switch(config)# no role name sme-admin`	Deletes the role called sme-admin.
Step 4	`switch(config-role)# rule 1 permit read-write feature sme-stg-admin`	Allows you to add SME configuration commands.
Step 5	`switch(config-role)# rule 2 permit read feature sme-stg-admin`	Allows you to add SME show commands.
Step 6	`switch(config-role)# rule 3 permit debug feature sme`	Allows you to add SME debug commands to the sme-admin role.
Step 7	`switch(config-role)# description SME Admins`	Assigns a description to the new role. The description is limited to one line and can contain spaces.
Step 8	`switch(config)# username usam role sme-admin`	Adds the specified user (usam) to the sme-admin role.

Send documentation comments to mdsfeedback-doc@cisco.com

Installing DCNM-SAN and DCNM-SAN Client

To be able to manage SME, you need to install DCNM-SAN Enterprise edition as a server. For information on installing Cisco DCNM-SAN, refer to the *Cisco DCNM Installation and Licensing Guide*.

Caution If the Cisco KMC is part of DCNM-SAN, then the switches and DCNM-SAN must not be upgraded at the same time.

Note To configure SME, the DCNM-SAN user credentials must be the same as the switch user.

To configure SME in a dual-fabric environment, all the switches in the cluster should have the same credentials for SME user.

Adding a Fabric and Changing the Fabric Name

You need to add the fabric that includes the Cisco MDS switch with the Cisco MSM-18/4 module installed. You also can add a fabric that includes an Cisco MDS 9222i switch.

Restrictions

- Cisco MDS SAN-OS Release 3.2(2c) or later or Cisco Release NX-OS 4.x supports one cluster per switch. Consider this support during your planning.

Detailed Steps

To add a fabric using DCNM-SAN Web Server, follow these steps:

Step 1 Log in to DCNM-SAN Web Client.

Step 2 Click the **Admin** tab.

Step 3 Click **General** and select **Data Sources**.

The Add Fabric screen displays fields to log in to the fabric seed switch.

Step 4 Enter the Fabric Seed Switch name or IP address, user name and password, and select the Auth-Privacy from the drop-down list. Check the **Use SNMPv3** check box.

Step 5 Click **Add**.

Note It takes a few minutes after you click **Add** to connect to the seed switch.

A notification window indicates that monitoring has started and that the fabric will be available after discover is complete.

Step 6 Click **OK** to return to the main screen.

Send documentation comments to mdsfeedback-doc@cisco.com

Note The fabric name is identified as **Fabric_** and the switch name. If you reopen the fabric with a different seed switch, you need to manually change the fabric name to what it was called before so that the fabric name remains the same. If you reopen the fabric with a different seed switch and do not manually change the fabric name, the fabric might be renamed to show the new switch name. This will conflict with the configured SME fabric name in the MDS switches. Choose a unique name that is easily identifiable.

Step 7 Select the fabric and click **Edit**.

Step 8 Enter a unique fabric name, user name, and password.

Step 9 Select **Managed Continuously** and click **Modify**.

Note SME requires that you select **Manage Continuously** to receive continuous updates from the switches.

Step 10 Click **Close** to return to the main screen and view the modified fabric name.

Choosing a Key Manager

Prerequisites

- Before configuring SME, you need to choose a key manager.
- To use an installation as a key manager, you should configure the settings for the key manager.

Restrictions

- After you choose a key manager, the key manager cannot be changed. You should be logged into the appropriate role to select or edit any key manager settings.

Detailed Steps

To choose a key manager using DCNM-SAN, follow these steps:

Step 1 Log in to DCNM-SAN Web Client.

Step 2 Click the **SME** tab and select Key Manager Settings. The Key Manager Settings window is displayed.

Note If you try to select SME before choosing a key manager, DCNM-SAN redirects you to the Key Manager Settings screen so that a key manager can be selected.

RSA key manager is not supported for SME disk.

Step 3 Choose any of the available three options.

a. Select **None** if you do not want to use this installation as a key manager.

b. Select **Cisco** if you want to use the installation as a Cisco key manager.

c. Select **RSA** if you want to choose the RSA key manager.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 4 Click **Submit Settings** to save changes.

Using FC-Redirect with CFS Regions

The Fibre Channel redirect (FC-Redirect) feature uses Cisco Fabric Services (CFS) regions to distribute the FC-Redirect configuration.

By default, the configuration is propagated to all FC-Redirect-capable switches in the fabric. CFS regions can be used to restrict the distribution of the FC-Redirect configuration.

Note Using FC-Redirect with CFS regions is an optional procedure.

To learn more about CFS regions, refer to *System Management Configuration Guide, Cisco DCNM for SAN* and the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*.

Installing Smart Card Drivers

The smart card reader must be connected to a management workstation that is used to configure SME. The smart card driver and the smart card drivers library file must be installed in the workstation.

You can download the latest drivers from the **Config > Install Smartcard Driver** link on the DCNM-SAN Web Client.

Restrictions

The smart card reader is only supported on Windows platforms. This includes only the Windows XP 32 bit, Windows server 2003 32 bit and Windows 7 64-bit platforms.

Note For Windows 7 64-bit smart card system, you must contact Gemalto for access to their Classic Client 6.1 for 64-bit systems. Smart cards are only tested on 6.10.020.001. Any other version of Classic Client for Windows 7 64-bit is at best effort only, and is not Cisco supported. Windows 7 32-bit is not supported.

Troubleshooting Tips

When connecting a new smart card reader after the installation of smart card drivers, you may be required to restart the computer. If the card reader is not recognized on your workstation, you may need to install the latest smart card drivers.

SME Configuration Process

Before configuring SME on your switch, it is important to become familiar with the SME configuration process. This section provides an overview of the SME configuration process.

Send documentation comments to mdsfeedback-doc@cisco.com

- Initial SME Configuration, page 2-26
- Saving SME Cluster Configurations, page 2-26

Initial SME Configuration

Note For information about what you need to do *before* you initially configure SME, see the "Required Preconfiguration Tasks" section on page 2-16.

Complete the SME configuration tasks on the switch with an installed Cisco MSM-18/4 module or on a Cisco MDS 9222i switch.

These basic configuration tasks provide an overview of the basic SME configuration process:

- Create the SME interface (Chapter 3, "Configuring SME Interfaces")
- Create a cluster for SME (Chapter 4, "Configuring SME Cluster Management")
- Add the interfaces to the cluster (Chapter 4, "Configuring SME Cluster Management")
- Create a tape group (including selecting the backup server and discovering backup libraries) (Chapter 5, "Configuring SME Tapes")

Saving SME Cluster Configurations

Note Configuration changes must be saved on all switches in the cluster for correct cluster operation. This must be done after the initial cluster creation and after all subsequent changes are made to the cluster configuration.

You must save configuration changes whenever switches or interfaces are added or deleted from a cluster.

SME Configuration Restrictions

This section includes information on SME configuration restrictions and includes the following topics:

- FICON Restriction, page 2-26
- iSCSI Restriction, page 2-26

FICON Restriction

SME is not supported on FICON devices and SME cluster devices cannot be part of a FICON VSAN.

iSCSI Restriction

You cannot configure SME and iSCSI on the same Cisco MDS MSM-18/4 module because SME uses the iSCSI port indices.

Send documentation comments to mdsfeedback-doc@cisco.com

Field Descriptions for SME Configuration

This section describes the following fields that are used in the SME configuration:

- Members, page 2-27
- SME Interfaces, page 2-27
- Hosts, page 2-28

Members

Field	Description
Cluster	SME cluster name.
State	The operational state of the SME cluster.
Master	Identifies the SME cluster master's IP address.
Members	Identifies the IP address of the switch that is a member of the SME cluster.
IsLocal?	Identifies if the switch is a local or remote member of this cluster.

SME Interfaces

Field	Description
Cluster	Identifies the cluster to which this SME interface belongs.
Switch	Name of the switch.
Interface	Identifies the SME interface.
State	Operational state of this SME interface.
Cluster State	The operational state of the cluster.
Cluster Name	Name of the cluster.
Description	Description of the switch.
Speed Admin	Configured port speed.
Speed Oper	Operational speed.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
StatusFailureCause	The reason for the current operational state of the port.
StatusLastChange	The value of sysUpTime when the interface entered its current operational state. If the current state was prior to the last reinitialization of the local network management subsystem, then this object will have a zero value.

Related Topics

Send documentation comments to mdsfeedback-doc@cisco.com

Configuring SME Interfaces.

Hosts

Field	Description
Host	Fibre Channel port name (P_WWN) of the host Nx_Port.
Cluster	Identifies the cluster to which this host port belongs.

Feature History for SME Configuration

Table 2-5 lists the release history for this feature.

Table 2-5 Feature History for SME Configuration

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.
Enabling Clustering Using Fabric Manager	3.3(1c)	The enable feature allows the user to enable clustering using the Fabric Manager. In 3.3(1c), the command menu of the Control tab was changed to enable clustering using the Fabric Manager. The following commands are introduced or modified: **enable** command.
Enabling SME Using Fabric Manager	3.3(1c)	The SME enable feature allows the user to enable the SME using the Fabric Manager. In 3.3(1c), the command menu of the Control tab was changed to enable the SME using the Fabric Manager. The following commands are introduced or modified: **enable** command.
Enabling SSH Using Fabric Manager	3.3(1c)	An error message dialog box displays if the Fabric Manager GUI is used to enable SSH before using the Device Manager or the CLI to generate the SSH keys. In 3.3(1c), the Error dialog box in Fabric Manager was changed to display an error message dialog box.
Enabling SSH Using Device Manager	3.3(1c)	In 3.3(1c), the SSH Telnet windows were modified to support this feature. The users should first create and then enable SSH using the Device Manager.

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2-5 Feature History for SME Configuration (continued)

Feature Name	Releases	Feature Information
SME Roles	4.1(1c)	The SME feature provides two primary roles: SME Administrator and the SME Recovery Officer. The SME Administrator role also includes the SME Storage Administrator and SME KMC Administrator roles. In 4.1(1c), the Cisco Storage Administrator and Cisco SME KMC Administrator roles were added.
Key Management	4.1(1c)	In 4.1(1c), the Cisco KMC can be separated from Fabric Manager for multisite deployments.
Key Manager Settings	4.1(1c)	A key manager needs to be selected before configuring Cisco SME. There are three options for key manager available now. In 4.1(1c), a new option 'None' is added to the Key Manager Settings page in the DCNM-SAN web client.
FC-Redirect and CFS Regions	4.1(1c)	In 4.1(1c), the support for CFS Regions and SME are available.
16 port Storage Service Node (SSN-16) module	4.2(1)	The Cisco MDS 9000 Family 16-Port Storage Services Node is new hardware that provides a high-performance, unified platform for deploying enterprise-class disaster recovery and business continuance solutions with future support for intelligent fabric applications.
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.

Send documentation comments to mdsfeedback-doc@cisco.com