



CHAPTER 2

Prerequisites

This chapter details the general prerequisites for installing the Cisco DCNM.

- [Prerequisites for Programmable Fabric Installation, page 2-1](#)
- [Prerequisites for non-Programmable Fabric Installation, page 2-3](#)
- [Supported Software, page 2-18](#)
- [Oracle Database for DCNM Servers, page 2-19](#)
- [Configuring Certificates for Cisco DCNM, page 2-25](#)
- [Configuring Secure Client Communications for Cisco DCNM Servers, page 2-28](#)
- [Server Ports, page 2-30](#)

Prerequisites for Programmable Fabric Installation

This sections details the various prerequisites, hardware and software requirements that you must equip with, before installing Programmable Fabric DCNM. This section contains prerequisites for the following:

- [Prerequisites for DCNM Open Virtual Appliance, page 2-1](#)
- [Prerequisites for DCNM ISO Virtual Appliance, page 2-2](#)

Prerequisites for DCNM Open Virtual Appliance

Before you install the Cisco DCNM Open Virtual Appliance, you will need to meet following software and database requirements:

- Cisco DCNM Release 10.4(1) supports the running of the Cisco DCNM server on the following hypervisors:
 - VMware ESXi 6.0
 - VMware ESXi 6.5
 - VMware ESXi 6.7
 - VMware ESXi 6.7 U1
 - VMware vCenter 6.0
 - VMware vCenter 6.5

- VMware vCenter 6.7
- VMware vCenter 6.7 U1
- Two port groups on the ESXi host:
 - DCNM Management Network
 - Enhanced Fabric Management Network



Note The DCNM Open Virtual Appliance cannot be deployed by connecting the vSphere client directly to the ESXi server.

- Determine the number of switches in your Cisco Programmable Fabric that will be managed by the Cisco DCNM Open Virtual Appliance.
- Ensure that no anti-virus software (such as McAfee) is running on the host where the VMware vCenter web client is launched for the DCNM OVA installation. If the anti-virus software is running, the DCNM installation might fail.



Note Once you start using the PostgreSQL database that is built in to the Cisco DCNM Open Virtual Appliance, you cannot migrate the data to an Oracle database.



Note On vCenter Server 6.5 web client, when an OVA VM is deployed, enable the administrator role and privileges before clicking the Power-On button.



Note To accommodate for HA application functions, additional prerequisites are required.



Note The DCNM Open Virtual Appliance is compatible to be deployed in ESXi 5.5 host as well. For deploying in the ESXi 5.5 host, VMware vSphere Client application is mandatory.

Prerequisites for DCNM ISO Virtual Appliance

You have to setup the host or the hypervisor before you install the Cisco DCNM ISO Virtual Appliance. Based on the requirement, setup the host.

You can setup one of the following hosts to install the DCNM ISO Virtual Appliance.

- [VMware ESXi, page 2-2](#)
- [Kernel-based Virtual Machine \(KVM\), page 2-3](#)
- Cisco UCS C-Series bare metal host

VMware ESXi

The host machine is installed with ESXi and two port groups are created—one for EFM network and the other for DCNM Management network.

Kernel-based Virtual Machine (KVM)

The host machine is installed with Red Hat Enterprise Linux 6.x with KVM libraries and Graphical User Interface (GUI) access. The GUI allows to access the Virtual Machine Manager, to deploy and manage the Cisco DCNM Virtual Appliances. Two networks are created—EFM network and DCNM Management network. Typically, the DCNM management network is bridged to gain access from other subnets. Refer the KVM documentation on how to create different types of networks.

**Note**

KVM on other platforms like CentOS/Ubuntu will not be supported as it increases the compatibility matrix.

Prerequisites for non-Programmable Fabric Installation

This sections details the various prerequisites, hardware and software requirements that you must equip with, before installing Cisco non-Programmable Fabric DCNM. This section contains prerequisites for the following:

- [General Prerequisites for Installing the Cisco DCNM on Windows and Linux, page 2-3](#)
- [Prerequisites for Windows Installer, page 2-16](#)
- [Prerequisites for Linux RHEL Server, page 2-17](#)
- [Prerequisites for non-Programmable Fabric Open Virtual Appliance, page 2-17](#)
- [Prerequisites for non-Programmable Fabric ISO Virtual Appliance, page 2-17](#)

General Prerequisites for Installing the Cisco DCNM on Windows and Linux

This section includes the following topics:

- [Before you begin, page 2-3](#)
- [Initial Setup Routine, page 2-5](#)
- [Preparing to Configure the Switch, page 2-5](#)
- [Default Login, page 2-6](#)
- [Setup Options, page 2-6](#)
- [Assigning Setup Information, page 2-7](#)
- [Configuring Out-of-Band Management, page 2-7](#)
- [Configuring In-Band Management, page 2-11](#)
- [Using the setup Command, page 2-14](#)
- [Starting a Switch in the Cisco MDS 9000 Family, page 2-15](#)
- [Accessing the Switch, page 2-15](#)

Before you begin

Before you can install Cisco DCNM, ensure that the Cisco DCNM system meets the following prerequisites:

- Before installing Cisco DCNM, ensure that the host name is mapped with the IP address in the hosts file under the following location:
 - Microsoft Windows–C:\WINDOWS\system32\drivers\etc\hosts
 - Linux–/etc/hosts



Note If Oracle RAC is chosen as the database for Cisco DCNM, ensure that the database host IP addresses and virtual IP addresses are added to the hosts file with their host-names.

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command:

sysctl -w kernel.shmmax=268435456

This setting, kernel.shmmax=268435456, should be saved in the /etc/sysctl.conf file. If this setting is not present or if it is less than 268435456, the Cisco DCNM server will fail after the server system is rebooted. For more information, visit the following URL:

<http://www.postgresql.org/docs/8.3/interactive/kernel-resources.html>

The server system must be registered with the DNS servers. The server hosting DCNM application must be dedicated to run DCNM alone and must not be shared with any other applications which utilizes memory and system resources.

- While using Remote PostgreSQL Database server, ensure that the Cisco DCNM Host IP addresses are added to the pg_hba.conf file present in the PostgreSQL installation directory. After the entries are added, restart the DB.
- Users installing Cisco DCNM must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. These ports are used by Cisco DCNM Server and the PostgreSQL database: 1098, 1099, 4444, 4445, 8009, 8083, 8090, 8092, 8093, 514, 5432.
- When you connect to the server for the first time, Cisco DCNM checks to see if you have the correct Sun Java Virtual Machine version installed on your local workstation. Cisco DCNM desktop clients look for version 1.7(x) during installation. If required, install the Sun Java Virtual Machine software.



Note When launching the Cisco DCNM installer, the *console* command option is not supported.



Note Using the Cisco DCNM installer in GUI mode requires that you must log in to the remote server using VNC or XWindows. Using Telnet or SSH to install Cisco DCNM in GUI mode is not possible.

Before you can use Cisco DCNM to manage network switches, you must complete the following tasks:

- Install a supervisor module on each switch that you want to manage.
- Configure the supervisor module with the following values using the setup routine or the CLI:
 - IP address assigned to the mgmt0 interface
 - SNMP credentials (v3 user name and password or v1/v2 communities), maintaining the same user name and password for all the switches in the fabric.

Initial Setup Routine

The first time that you access a Cisco NXOS-based switch for MDS or Nexus, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch. All Cisco Nexus or Cisco MDS switches have the network administrator as a default user (Admin). You cannot change the default user at any time. You must explicitly configure a strong password for any switch in the Cisco Nexus or Cisco MDS. The setup scenario differs based on the subnet to which you are adding the new switch:

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port.
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS).

**Note**

IP address for a Cisco Nexus switch or a Cisco MDS switch can be set via CLI or USB key or POAP

Preparing to Configure the Switch

Before you configure a switch in the Cisco Nexus or Cisco MDS 9000 Family for the first time, you need the following information:

- Administrator password, including:
 - Creating a password for the administrator (required).
 - Creating an additional login account and password (optional).
- IP address for the switch management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface (recommended).
- Subnet mask for the switch's management interface (optional).
- IP addresses, including:
 - Destination prefix, destination prefix subnet mask, and next-hop IP address if you want to enable IP routing. Also, provide the IP address of the default network (optional).
 - Otherwise, provide an IP address of the default gateway (optional).
- SSH service on the switch—To enable this optional service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- DNS IP address (optional).
- Default domain name (optional).
- NTP server IP address (optional).
- SNMP community string (optional).
- Switch name—This is your switch prompt (optional).

**Note**

Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

**Note**

You should verify that the Cisco DCNM-SAN Server host name entry exists on the DNS server, unless the Cisco DCNM-SAN Server is configured to bind to a specific interface during installation.

Default Login

All Cisco Nexus and Cisco MDS 9000 Family switches have the network administrator as a default user (Admin). You cannot change the default user at any time (see the *Security Configuration Guide, Cisco DCNM for SAN*).

You have an option to enforce a secure password for any switch in the Cisco MDS 9000 Family. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a secure password (see the *Security Configuration Guide, Cisco DCNM for SAN*). If you configure and subsequently forget this new password, you have the option to recover this password (see the *Security Configuration Guide, Cisco DCNM for SAN*).

**Note**

The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (_), and hyphen (-).

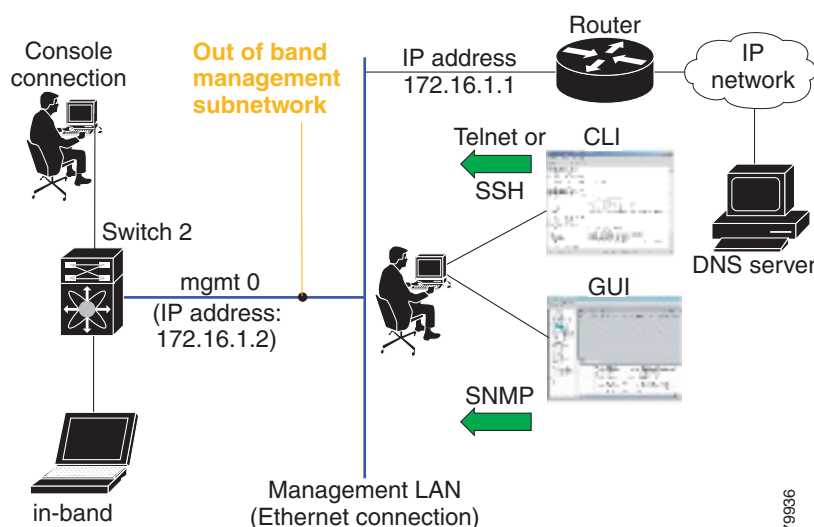
Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a Cisco MDS 9000 Family switch or a Cisco Nexus switch with an IP address to enable management connections from outside of the switch (see [Figure 2-1](#)).

**Note**

Some concepts such as out-of-band management and in-band management are briefly explained here. These concepts are explained in more detail in subsequent chapters.

Figure 2-1 Management Access to Switches



Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.



Note

Press **Ctrl + C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point. Entering a new password for the administrator is a requirement and cannot be skipped.



Tip

If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

Configuring Out-of-Band Management

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 11c](#) and [Step 11d](#) in the following procedure.

DETAILED STEPS

Step 1 Power on the switch. Switches in the Cisco Nexus and Cisco MDS 9000 Family boot automatically.

Do you want to enforce secure password standard (Yes/No)?

Step 2 Enter **Yes** to enforce a secure password.

a. Enter the administrator password.

Enter the password for admin: **2008asdf*1kjh17**



Note

The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (_), and hyphen (-).

b. Confirm the administrator password.

Confirm the password for admin: **2008asdf*1kjh17**



Tip

If a password is trivial (short, easy to decipher), your password configuration is rejected. Be sure to configure a secure password as shown in the sample configuration. Passwords are case sensitive.

Step 3 Enter **yes** to enter the setup mode.



Note

This setup utility guides you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services.

Press Enter anytime you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl + C** at any prompt to end the configuration process.

Step 4 Enter the new password for the administrator (Admin is the default).

Enter the password for admin: **admin**

Step 5 Enter **yes** (no is the default) to create additional accounts.

Create another login account (yes/no) [n]: **yes**

While configuring your initial setup, you can create an additional user account (in the network administrator role) in addition to the administrator's account. See the *Security Configuration Guide, Cisco DCNM for SAN* for information on default roles and permissions.



Note User login IDs must contain non-numeric characters.

a. Enter the user login ID [administrator].

Enter the user login ID: *user_name*

The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (_), and hyphen (-).

b. Enter the user password.

Enter the password for user_name: *user-password*

c. Confirm the user password.

Confirm the password for user_name: *user-password*

Step 6 Enter **yes** (no is the default) to create an SNMPv3 account.

Configure read-only SNMP community string (yes/no) [n]: **yes**

a. Enter the username (Admin is the default).

SNMPv3 user name [admin]: **admin**

b. Enter the SNMPv3 password (minimum of eight characters). The default is **admin123**.

SNMPv3 user authentication password: *admin_pass*

Step 7 Enter **yes** (no is the default) to configure the read-only or read-write SNMP community string.

Configure read-write SNMP community string (yes/no) [n]: **yes**

a. Enter the SNMP community string.

SNMP community string: *snmp_community*

Step 8 Enter a name for the switch.

Enter the switch name: *switch_name*

Step 9 Enter **yes** (yes is the default) to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **yes**

a. Enter the mgmt0 IP address.

Mgmt0 IPv4 address: *ip_address*

b. Enter the mgmt0 subnet mask.

Mgmt0 IPv4 netmask: *subnet_mask*

Step 10 Enter **yes** (yes is the default) to configure the default gateway (recommended).

Configure the default-gateway: (yes/no) [y]: **yes**

a. Enter the default gateway IP address.

IPv4 address of the default gateway: *default_gateway*

Step 11 Enter **yes** (**no** is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

Configure Advanced IP options (yes/no)? [n]: **yes**

a. Enter **no** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **no**

b. Enter **yes** (no is the default) to enable IP routing capabilities.

Enable the ip routing? (yes/no) [n]: **yes**

c. Enter **yes** (no is the default) to configure a static route (recommended).

Configure static route: (yes/no) [n]: **yes**

Enter the destination prefix.

Destination prefix: *dest_prefix*

Enter the destination prefix mask.

Destination prefix mask: *dest_mask*

Enter the next-hop IP address.

Next hop ip address: *next_hop_address*



Note

Be sure to configure the IP route, the default network IP address, and the default gateway IP address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

d. Enter **yes** (no is the default) to configure the default network (recommended).

Configure the default network: (yes/no) [n]: **yes**

Enter the default network IP address.



Note

The default network IP address is the destination prefix provided in [Step 11c](#).

Default network IP address [dest_prefix]: *dest_prefix*

- e. Enter **yes** (no is the default) to configure the DNS IP address.

Configure the DNS IPv4 address? (yes/no) [n]: **yes**

Enter the DNS IP address.

DNS IPv4 address: *name_server*

- f. Enter **yes** (default is no) to configure the default domain name.

Configure the default domain name? (yes/no) [n]: **yes**

Enter the default domain name.

Default domain name: *domain_name*

- Step 12** Enter **yes** (no is the default) to enable Telnet service.

Enable the telnet server? (yes/no) [n]: **yes**

- Step 13** Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH server? (yes/no) [n]: **yes**

- Step 14** Enter the SSH key type.

Type the SSH key you would like to generate (dsa/rsa)? **dsa**

- Step 15** Enter the number of key bits within the specified range.

Enter the number of key bits? (768 to 2048): **768**

- Step 16** Enter **yes** (no is the default) to configure the NTP server.

Configure NTP server? (yes/no) [n]: **yes**

Configure clock? (yes/no) [n] :**yes**

Configure clock? (yes/no) [n] :**yes**

Configure timezone? (yes/no) [n] :**yes**

Configure summertime? (yes/no) [n] :**yes**

Configure the ntp server? (yes/no) [n] : **yes**

- a. Enter the NTP server IP address.

NTP server IP address: *ntp_server_IP_address*

- Step 17** Enter **noshut** (shut is the default) to configure the default switch port interface to the shut state.

Configure default switchport interface state (shut/noshut) [shut]: **noshut**

- Step 18** Enter **on** (on is the default) to configure the switch port trunk mode.

Configure default switchport trunk mode (on/off/auto) [on]: **on**

- Step 19** Enter **no** (no is the default) to configure switchport port mode F.

Configure default switchport port mode F (yes/no) [n] : **no**

- Step 20** Enter **permit** (deny is the default) to deny a default zone policy configuration.

Configure default zone policy (permit/deny) [deny]: **permit**

This step permits traffic flow to all members of the default zone.

- Step 21** Enter **yes** (no is the default) to disable a full zone set distribution (see the *Fabric Configuration Guide, Cisco DCNM for SAN*). Disables the switch-wide default for the full zone set distribution feature.

Enable full zoneset distribution (yes/no) [n]: **yes**

You see the new configuration. Review and edit the configuration that you have just entered.

Step 22 Enter **no** (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
username user_name password user_pass role network-admin
snmp-server community snmp_community ro
switchname switch
interface mgmt0
  ip address ip_address subnet_mask
  no shutdown
ip routing
ip route dest_prefix dest_mask dest_address
ip default-network dest_prefix
ip default-gateway default_gateway
ip name-server name_server
ip domain-name domain_name
telnet server enable
ssh key dsa 768 force
ssh server enable
ntp server ipaddr ntp_server
system default switchport shutdown
system default switchport trunk mode on
system default port-channel auto-create
zone default-zone permit vsan 1-4093
zoneset distribute full vsan 1-4093
```

Would you like to edit the configuration? (yes/no) [n]: **no**

Step 23 Enter **yes** (yes is default) to use and save this configuration:

Use this configuration and save it? (yes/no) [y]: **yes**



Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Enter **yes** to save the new configuration to ensure that the kickstart and system images are also automatically configured.

Configuring In-Band Management

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each switch should have its VSAN 1 interface configured with an IP address in the same subnetwork. A default route that points to the switch that provides access to the IP network should be configured on every switch in the Fibre Channel fabric (see *Fabric Configuration Guide, Cisco DCNM for SAN*).



Note

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 9c](#) and [Step 9d](#) in the following procedure.

DETAILED STEPS

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

Enter the password for admin: **2004asdf*1kjh18**

**Tip**

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case sensitive. The password can contain a combination of alphabets, numeric, and special characters. The supportive special characters are dot (.), plus (+), underscore (_), and hyphen (-).

Step 3 Enter **yes** to enter the setup mode.

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter **no** (no is the default) if you do not wish to create additional accounts.

Create another login account (yes/no) [no]: **no**

Step 5 Configure the read-only or read-write SNMP community string.

a. Enter **no** (no is the default) to avoid configuring the read-only SNMP community string.

Configure read-only SNMP community string (yes/no) [n]: **no**

Step 6 Enter a name for the switch.

**Note**

The switch name is limited to 32 alphanumeric characters. The default is **switch**.

Enter the switch name: *switch_name*

Step 7 Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **no**

Step 8 Enter **yes** (yes is the default) to configure the default gateway.

Configure the default-gateway: (yes/no) [y]: **yes**

a. Enter the default gateway IP address.

IP address of the default gateway: *default_gateway*

Step 9 Enter **yes** (**no** is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

Configure Advanced IP options (yes/no)? [n]: **yes**

- a. Enter **yes** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **yes**

Enter the VSAN 1 IP address.

VSAN1 IP address: *ip_address*

Enter the subnet mask.

VSAN1 IP net mask: *subnet_mask*

- b. Enter **no** (yes is the default) to enable IP routing capabilities.

Enable ip routing capabilities? (yes/no) [y]: **no**

- c. Enter **no** (yes is the default) to configure a static route.

Configure static route: (yes/no) [y]: **no**

- d. Enter **no** (yes is the default) to configure the default network.

Configure the default-network: (yes/no) [y]: **no**

- e. Enter **no** (yes is the default) to configure the DNS IP address.

Configure the DNS IP address? (yes/no) [y]: **no**

- f. Enter **no** (no is the default) to skip the default domain name configuration.

Configure the default domain name? (yes/no) [n]: **no**

- Step 10** Enter **no** (yes is the default) to disable Telnet service.

Enable the telnet service? (yes/no) [y]: **no**

- Step 11** Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH service? (yes/no) [n]: **yes**

- Step 12** Enter the SSH key type (see the *Security Configuration Guide, Cisco DCNM for SAN*) that you would like to generate.

Type the SSH key you would like to generate (dsa/rsa/rsal)? **rsa**

- Step 13** Enter the number of key bits within the specified range.

Enter the number of key bits? (768 to 1024): **1024**

- Step 14** Enter **no** (no is the default) to configure the NTP server.

Configure NTP server? (yes/no) [n]: **no**

- Step 15** Enter **shut** (shut is the default) to configure the default switch port interface to the shut state.

Configure default switchport interface state (shut/noshut) [shut]: **shut**



Note The management Ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

- Step 16** Enter **auto** (off is the default) to configure the switch port trunk mode.

Configure default switchport trunk mode (on/off/auto) [off]: **auto**

Step 17 Enter **deny** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: deny
```

This step denies traffic flow to all members of the default zone.

Step 18 Enter **no** (no is the default) to disable a full zone set distribution.

```
Enable full zoneset distribution (yes/no) [n]: no
```

This step disables the switch-wide default for the full zone set distribution feature.

You see the new configuration. Review and edit the configuration that you have just entered.

Step 19 Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
username admin password admin_pass role network-admin
snmp-server community snmp_community rw
switchname switch
interface vsan1
    ip address ip_address subnet_mask
    no shutdown
ip default-gateway default_gateway
no telnet server enable
ssh key rsa 1024 force
ssh server enable
no system default switchport shutdown
system default switchport trunk mode auto
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
```

```
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 20 Enter **yes** (yes is default) to use and save this configuration.

```
Use this configuration and save it? (yes/no) [y]: yes
```



Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Enter **yes** to save the new configuration. To ensure that the kickstart and system images are also automatically configured.

Using the setup Command

To make changes to the initial configuration at a later time, you can enter the **setup** command in EXEC mode.

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
```

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process.


Starting a Switch in the Cisco MDS 9000 Family

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.

**Note**

You must use the CLI for initial switch start up.

DETAILED STEPS

-
- Step 1** Verify the following physical connections for the new Cisco MDS 9000 Family switch:
- The console port is physically connected to a computer terminal (or terminal server).
 - The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.
- See the *Cisco MDS 9000 Family Hardware Installation Guide* (for the required product) for more information.
-  **Tip** Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.
-
- Step 2** Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:
- 9600 baud
 - 8 data bits
 - 1 stop bit
 - No parity
- Step 3** Power on the switch. The switch boots automatically and the switch# prompt appears in your terminal window.
-

Accessing the Switch

After initial configuration, you can access the switch in one of the three ways:

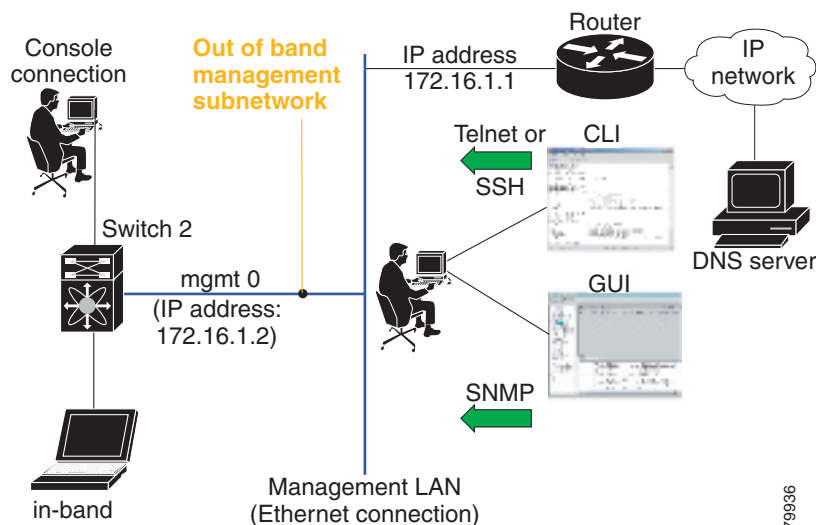
- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.

After initial configuration, you can access the switch in one of three ways (see [Figure 2-2](#)):

- Serial console access—You can use a serial port connection to access the CLI.

- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco DCNM-SAN to access the switch.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco DCNM-SAN to access the switch.

Figure 2-2 **Switch Access Options**



Prerequisites for Windows Installer

- During the initial installation, disable all security and anti virus tools that are running on your Windows server.
- Do not run any other management applications on the Cisco DCNM server or the Cisco DCNM database server.
- Before installing Cisco DCNM, ensure that the host name is mapped with the IP address in the hosts file under the location C:\WINDOWS\system32\drivers\etc\hosts.
- On Windows, remote Cisco DCNM installations or upgrades should be done through the console using VNC or through the Remote Desktop Client (RDC) in console mode (ensuring RDC is used with the /Console option). This process is very important if the default PostgreSQL database is used with Cisco DCNM, because this database requires the local console for all installations and upgrades.
- Before installing Cisco DCNM on a Windows Vista or Windows 2008 server system, turn the User Account Control (UAC) off. To turn off UAC, choose **Start > Control Panel > User Accounts > Turn User Account Control on or off**, clear the **Use User Account Control (UAC)** to help protect your computer check box, and then click OK. Click **Restart Now** to apply the change.
- Telnet Client application is not installed by default on Microsoft Windows Vista. To install Telnet Client, choose **Start > Programs > Control Panel > Click Turn Windows features on or off** (if you have UAC turned on, you need to give it the permission to continue). Check the **Telnet Client** check box and then click **OK**.

- You can run CiscoWorks on the same PC as Cisco DCNM even though the Java requirements are different. When installing the later Java version for Cisco DCNM, make sure that it does not overwrite the earlier Java version required for CiscoWorks. Both versions of Java can coexist on your PC.

Prerequisites for Linux RHEL Server

For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command:

```
sysctl -w kernel.shmmax=268435456
```

This setting, `kernel.shmmax=268435456`, should be saved in the `/etc/sysctl.conf` file. If this setting is not present or if it is less than 268435456, the Cisco DCNM server will fail after the server system is rebooted. For more information, visit the following URL:

<http://www.postgresql.org/docs/8.4/interactive/kernel-resources.html>

The server system must be registered with the DNS servers. No other programs are running on the server. Ensure that you select English as the preferred language during RHEL installation.

Antivirus exclusion

Scanning the Cisco DCNM includes the scanning of the database files. This process will hamper the performance on the DCNM while operation. While scanning the Cisco DCNM on Linux RHEL server, exclude the directory `/usr/local/cisco/dcm/db` and `/var/lib/dcnm`.

For more information, refer to

https://wiki.postgresql.org/wiki/Running_%26_Installing_PostgreSQL_On_Native_Windows#Antivirus_software.



Note

We recommend you to stop Anti-Virus scanning while installing DCNM because the port being used or blocked might cause failures. After the installation, you can enable or install Anti-Virus application with specific guidelines to avoid DCNM directories as part of the scan.

This recommendation is also applicable to DCNM installations in an ISO/OVA format.

Prerequisites for non-Programmable Fabric Open Virtual Appliance

For information on prerequisites to install DCNM Open Virtual Appliance, refer to [Prerequisites for DCNM Open Virtual Appliance, page 2-1](#).

Prerequisites for non-Programmable Fabric ISO Virtual Appliance

For information on prerequisites to install ISO Virtual Appliance, refer to [Prerequisites for DCNM ISO Virtual Appliance, page 2-2](#).

Supported Software

**Note**

For the latest information on supported software, see the *Cisco DCNM Release Notes, Release 10.4(2)*.

The following are the supported software for Cisco DCNM 10.4(2):

Supported Software for DCNM Windows/Linux Installers

- Java Requirements
 - Cisco DCNM Server is distributed with Java JRE 1.8.0_101. The DCNM installer installs JRE 1.8.0_101 to the following directory: **DCNM_root_directory/java/jre1.8**
 - Cisco DCNM Client has been validated with Java versions JRE 1.8.0_101.
- Operating System
 - Microsoft Windows 2008 R2 SP2 (64-bit only)
 - Microsoft Windows 2012 R2
 - Red Hat Enterprise Linux Release 6.6 and 7.0
 - Red Hat Enterprise Linux Release 7 (64-bit)

Supported Software for DCNM Virtual Appliances (OVA/ISO)

- Databases:
 - Oracle 11g Express (XE), Standard, and Enterprise Editions, and Oracle 11g Real Application Clusters (RAC)
 - PostgreSQL 9.4.5
 - Oracle 12c Enterprise Edition (Conventional)–Non-pluggable Installation

**Note**

Cisco DCNM Release 10.4(2) does not support Oracle 12c pluggable database version installation.

- Oracle 12c RAC–Non-pluggable installation

**Note**

The Cisco DCNM database size is not limited, and increases according to the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. If you choose Oracle database, we recommend that you use Oracle SE or Enterprise edition, instead of Oracle XE due to table space limitations.

**Note**

Customers are responsible for all support associated with Oracle database, including maintenance, troubleshooting, and recovery. Cisco recommends that customers perform regular database backups, either daily or weekly, to ensure that all data is preserved.

Supported Security for all DCNM Virtual Appliances (Windows/Linux/OVA/ISO)

- Security
 - Cisco ACS 3.1 and 4.0
 - PIX Firewall
 - IP Tables
 - SSH v2
 - Global Enforce SNMP Privacy Encryption
 - HTTPS

Oracle Database for DCNM Servers

This section details about the database required for the installation of DCNM server.

**Note**

This section is not applicable for Cisco DCNM Native HA installation.

Cisco DCNM supports the following databases:

- Oracle Database 11g
- Oracle Database 12c
- Oracle RAC 11g, and 12c

You can change from the local database to an external Oracle database, if required. For instructions, see [Change from Local Database to an External Database, page 6-11](#).

**Note**

Cisco DCNM is configured with AL32UTF8 character set.

This section contains the following:

- [Oracle SQL*Plus Command-Line Tool, page 2-20](#)
- [init.ora File, page 2-20](#)
- [Backing up the Oracle Database, page 2-20](#)
- [Preparing the Oracle Database, page 2-21](#)
- [Database for HA environment, page 2-24](#)
- [Database for Federation Setup, page 2-25](#)
- [Antivirus exclusion, page 2-25](#)

**Note**

The Cisco DCNM Database size is not limited and increases based on the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. Cisco recommends that you use Oracle SE or Enterprise edition, instead of Oracle XE, due to table space limitations.

Oracle SQL*Plus Command-Line Tool

The Oracle database procedures in this section require the use of the SQL*Plus command-line tool. The SQL*Plus executable is typically installed in the bin directory under the Oracle home directory.

Linux Environment Variables

If you are using Linux, before you use the SQL*Plus command-line tool, ensure that the ORACLE_HOME and ORACLE_SID environment variables are set to correct values. For example, if you are using Oracle 11g on Linux, the following commands set the environment variables to the default Oracle home directory and SID if you are using a bash shell:

```
export ORACLE_HOME=<usr_home_directory>/app/oracle/product/11.2.0/
(or identify the Oracle home on the Oracle installed server)
export ORACLE_SID=XE
```

init.ora File

The init.ora file specifies startup parameters. The default name and location of the file is platform specific, as shown in [Table 2-1](#).

Table 2-1 Name and Default Location of init.ora File

Oracle Version	Operating System	Content of init.ora File
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dfs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dfs/initORCL.ora

The init.ora file should contain only one line, which is the full path of the server parameter file, as shown in [Table 2-2](#).

Table 2-2 Content of init.ora File

Oracle Version	Operating System	Content of init.ora File
11g	Microsoft Windows	SPFILE='C:\oracle\app\oracle\product\11.1.0\server\dfs\spfileXE.ora
	Linux	SPFILE='/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dfs/spfileXE.ora

Backing up the Oracle Database

Copy the oracle backup/restore script from the Cisco DCNM server directory `DCNM_SERVER_Install/dcm/dcnm/bin`.

For Linux, the script name is `backup-remote-oracledb.sh/restore-remote-oracledb.sh` and edit the `DB_HOME` variable to point to the Oracle installation.

For Windows, the script name is backup-remote-oracledb.bat/restore-remote-oracledb.bat and edit *DB_HOME* variable to point to the Oracle installation.

Use the following path for Oracle DBHOME:

- On Linux— /usr/lib/oracle/xe/app/oracle/product/10.2.0/server



Note Replace /usr/lib/oracle with the Oracle installation path.

- On windows—C:\oraclexe\app\oracle\product\10.2.0\server



Note Replace C:\oraclexe with the Oracle installation path.

Preparing the Oracle Database

You can prepare an Oracle database.

DETAILED STEPS

-
- | | |
|---------------|--|
| Step 1 | Increase the number of sessions and processes to 150 each. For more information, see the “Increasing the Number of Sessions and Processes to 150 Each” section on page 2-22. |
| Step 2 | Increase the number of open cursors to 1000. For more information, see the “Increasing the Number of Open Cursors to 1000” section on page 2-23. |
-

This section includes the following:

- [Logging Into Oracle, page 2-21](#)
- [Increasing the SYSTEM Tablespace, page 2-22](#)
- [Increasing the Number of Sessions and Processes to 150 Each, page 2-22](#)
- [Increasing the Number of Open Cursors to 1000, page 2-23](#)
- [Creating an Oracle DB User using the Command Prompt, page 2-24](#)
- [Connecting to an Oracle RAC with SCAN Feature Type DB, page 2-24](#)
- [Adding a CA signed SSL Certificate in Cisco DCNM, page 2-29](#)

Logging Into Oracle

You can log into the Oracle database by using the SQL*Plus command-line tool.

BEFORE YOU BEGIN

Ensure that you know the database administrator username and password.

DETAILED STEPS

-
- | | |
|---------------|------------------------------|
| Step 1 | Run the SQL*Plus executable. |
|---------------|------------------------------|

A command prompt appears.

Step 2 Enter the **connect** command.

The Username prompt appears.

Step 3 Enter the database administrator username.

The Password prompt appears.

Step 4 Enter the password for the username that you specified.

For example, if the Oracle administrator username is system and the password is oracle, you would log in as follows:

```
Username: sys as sysdba
Password: oracle
```

For more information about using SQL*Plus, see the documentation for the Oracle database version that you are using.

Increasing the SYSTEM Tablespace

You can increase the SYSTEM tablespace.

DETAILED STEPS

Step 1 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the [“Oracle SQL*Plus Command-Line Tool” section on page 2-20](#).

Step 2 Enter the following command:

```
select file_name, bytes, autoextensible, maxbytes
from dba_data_files
where tablespace_name='SYSTEM';
```

Step 3 Enter the following command:

```
alter database datafile 'filename' autoextend on next 100m maxsize 2000m;
```

where *file_name* is the filename from the output of the **select** command in [Step 2](#).

The SYSTEM tablespace is increased.

Step 4 Enter the **exit** command.

Increasing the Number of Sessions and Processes to 150 Each

For each DCNM instance configured in the same Oracle database, the number of cursors and processes must be increased to more than the 150 and 1000.

For example, if two DCNM standalone (non HA) instances are configured to use the same Oracle database, the cursors and process must be increased to 300 and 2000 approximately, depending on any performance degradation or SQL Exception errors occurred during normal operations of either of the DCNM instances.

DETAILED STEPS

-
- Step 1** Ensure that the `init.ora` file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines, remove them.
- For more information, see the [“init.ora File” section on page 2-20](#).
- Step 2** Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the [“Oracle SQL*Plus Command-Line Tool” section on page 2-20](#).
- Step 3** Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.
- Step 4** Enter the following command:
- ```
startup pfile='init_file_name';
```
- where `init_file_name` is the `init.ora` filename for your Oracle database installation. For more information, see the [“init.ora File” section on page 2-20](#).
- Step 5** Set the number of sessions to 150 by entering the following command:
- ```
alter system set sessions = 150 scope=spfile;
```
- Step 6** Set the number of processes to 150 by entering the following command:
- ```
alter system set processes = 150 scope=spfile;
```
- Step 7** Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.
- Step 8** Start up the system by entering the **startup** command.
- Step 9** Verify that the number of sessions and processes is changed to 150 by entering the following command:
- ```
show parameter sessions
```
- Step 10** Exit by entering the **exit** command.
-

Increasing the Number of Open Cursors to 1000

You can increase the number of open cursors to 1000.

DETAILED STEPS

-
- Step 1** Ensure that the `init.ora` file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines in the file, remove them.
- For more information, see the [“init.ora File” section on page 2-20](#).
- Step 2** Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the [“Oracle SQL*Plus Command-Line Tool” section on page 2-20](#).
- Step 3** Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.
- Step 4** Enter the following command:
- ```
startup pfile='init_file_name';
```

where *init\_file\_name* is the init.ora filename for your Oracle database installation. For more information, see the [“init.ora File” section on page 2-20](#).

**Step 5** Set the number of open cursors to 1000 by entering the following command:

```
alter system set open_cursors = 1000 scope=spfile;
```

**Step 6** Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

**Step 7** Start up the system by entering the **startup** command.

**Step 8** Verify that the number of open cursors is changed to 1000 by entering the following command:

```
show parameter open_cursors
```

**Step 9** Exit by entering the **exit** command.

---

## Creating an Oracle DB User using the Command Prompt

To create an Oracle DB user using the command prompt, follow these steps:

```
export ORACLE_SID=XE
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
cd $ORACLE_HOME/bin
sqlplus
sys as sysdba
create user dcnmdbusername identified by dcnmdbuserpassword default tablespace users
temporary tablespace temp;
grant connect, resource to dcnmdbusername;
grant create session to dcnmdbusername;
grant dba to dcnmdbusername;
```

**Note**

Ensure you set the Oracle\_SID and Oracle\_Home and enter the values for the DB Username and password fields.

---

**Note**

When a DBA account cannot be created, an account with DML/DDl/schema privilege is sufficient.

---

## Connecting to an Oracle RAC with SCAN Feature Type DB

To connect to an Oracle RAC with SCAN Feature type DB, enter the following command:

```
appmgr update -u jdbc:oracle:thin:@//[ip_addr]:1521/[service name] -n [username] -p [password]
```

## Database for HA environment

If you need High Availability (HA) for DCNM database, utilize the Oracle HA solutions.

**Note**

Ensure that the NTP server is synchronized between the DCNM active and standby peers. This is essential for the functioning of DCNM applications in HA environment.

---



## Database for Federation Setup

Cisco DCNM can be deployed as Cisco DCNM-SAN federation. For Cisco DCNM-SAN federation, the database URL (properties) must remain the same for all Cisco DCNM-SAN nodes in the federation.



### Note

Ensure that you do not provide multicast addresses to form the federation.

## Antivirus exclusion

Scanning the Cisco DCNM includes the scanning of the database files. This process will hamper the performance on the DCNM while operation. While scanning the Cisco DCNM on Oracle database, exclude the directory that you have selected during Oracle installation.

## Configuring Certificates for Cisco DCNM

This section describes three ways on how to configure the certificates in Cisco DCNM.

This section contains the following topics:



- [Using a self signed SSL Certificate, page 2-25](#)
- [Using a SSL Certificate when certificate request is generated using OpenSSL, page 2-26](#)
- [Using a SSL Certificate when certificate request is generated using Keytool, page 2-27](#)

## Using a self signed SSL Certificate

- 
- |               |                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | From command prompt, navigate to <b>&lt;DCNM install root&gt;/dcm/java/jre1.8/bin/</b> .                                                                                                                                                                                                                     |
| <b>Step 2</b> | Rename the keystore located at<br><b>&lt;DCNM_install_root&gt;\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks</b><br>to<br><b>&lt;DCNM_install_root&gt;\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old</b>                                                               |
| <b>Step 3</b> | Generate a self signed certificate using following command<br><pre>keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore &lt;DCNM_install_root&gt;\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048</pre> |
| <b>Step 4</b> | Stop the DCNM services, or DCNM application by using the <b>appmgr stop dcnm</b> command.                                                                                                                                                                                                                    |
| <b>Step 5</b> | Start the DCNM services, or the DCNM applications in the server by using the <b>appmgr start dcnm</b> command.                                                                                                                                                                                               |
-

## Using a SSL Certificate when certificate request is generated using OpenSSL

To configure SSL certificates in Cisco DCNM, using certificate request generated using open SSL, perform the following steps.

- 
- Step 1** From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.8/bin/**.
- Step 2** Rename the keystore located at:  
**<DCNM\_install\_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks**  
 to  
**<DCNM\_install\_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks.old**
- Step 3** Generate the RSA private key using OpenSSL.  
**openssl genrsa -out dcnm.key 2048**
- Step 4** Generate a certificate-signing request (CSR) by using following command:  
**openssl req -new -key dcnm.key -sha256 -out dcnm.csr**
- Step 5** Submit the CSR to Certificate signing authority, and download the signed certificate chain in Base-64 format which creates the **.p7b** file.  
 CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provides the PKCS 7 format, go to [Step 6](#) to convert it to PEM format. If CA provides the PEM format, go to [Step 7](#).
- Step 6** Convert the PKCS 7 certificate chain to X509 certificate chain.  
**openssl pkcs7 -print\_certs -in cert-chain.p7b -out cert-chain.pem**
- Step 7** Convert the X509 certificate chain and private key to PKCS 12 format  
**openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password fmserver\_1\_2\_3 -name sme**
- 
-  **Note** Ensure that the user provides either absolute path or relative path to the correct location of **dcnm.key** & **dcnm.p12** files in the above command.
- 
- Step 8** Import the intermediate certificate, the root certificate, and the signed certificate in the same order.  
**./keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore <DCNM\_install\_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks -deststoretype JKS -name sme**
- 
-  **Note** Ensure that the user provides either absolute path or relative path to the correct location of **cert-chain.pem**, **dcnm.key**, and **dcnm.p12** files in the above command.
- 
- Step 9** Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.
- Step 10** Start the DCNM services, or the DCNM applications in the server by using the **appmgr start dcnm** command.
-

## Using a SSL Certificate when certificate request is generated using Keytool

- Step 1** From command prompt, navigate to the appropriate folder:
- For Linux/CentOS DCNM installation, use the following path:  
`<DCNM install root>/dcm/java/jre1.8/bin/`
  - For Windows DCNM sever installation, use the following path:  
`<DCNM install root>\dcm\java\jre1.8\bin\`
- Step 2** Rename the keystore.
- For Linux/CentOS DCNM installation, rename the keystore located at:  
`<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks`  
to  
`<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks.old`
  - For Windows DCNM sever installation, rename the keystore located at:  
`<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks`  
to  
`<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old`
- Step 3** Generate the public-private key pair in DCNM keystore by using the following command:
- For Linux/Centos environment use the following command:  
`./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore  
<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks  
-storepass fmserver_1_2_3 -validity 360 -keysize 2048`
  - For Windows DCNM sever installation, use the following command:  
`keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore  
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks  
-storepass fmserver_1_2_3 -validity 360 -keysize 2048`
- Step 4** Generate the certificate-signing request (CSR) from the public key generated in [Step 6](#).
- For Linux/Centos environment use the following command:  
`./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install  
root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks" -storepass  
fmserver_1_2_3`
  - For Windows DCNM sever installation, use the following command:  
`keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install  
root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass  
fmserver_1_2_3`



**Note** The dcnm.csr file is created in the keytool directory, located at  
`/usr/local/cisco/dcm/java/jre1.8/bin`

- Step 5** Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the .p7b file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to [Step 6](#) to convert it to PEM format. If CA provided PEM format, then go to [Step 7](#).

**Step 6** Convert the PKCS 7 certificate chain to X509 certificate chain using openssl.

```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```



**Note** Ensure that the user provides either absolute or relative path to the correct location of cert-chain.p7b file in the above command.

**Step 7** Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

- For Linux/Centos environment use the following command:

```
./keytool -importcert -trustcacerts -file cert-chain.pem -keystore
<DCNM_install_root>/dcm/jboss-as-7.2.0.Final/standalone/configuration/fmserver.jks
-storepass fmserver_1_2_3 -alias sme
```

- For Windows DCNM sever installation, use the following command:

```
keytool -importcert -trustcacerts -file cert-chain.pem -keystore
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks
-storepass fmserver_1_2_3 -alias sme
```



**Note** Ensure that the user provides either the absolute path or relative path to the correct location of the cert-chain.pem file in the above command.

**Step 8** Stop the DCNM application by using the **appmgr stop dcnm** command.

**Step 9** Start the applications in the server by using the **appmgr start dcnm** command.

## Configuring Secure Client Communications for Cisco DCNM Servers

This section describes how to configure HTTPS on Cisco Data Center Network Manager Servers.



**Note** You must enable SSL/HTTPS on the Cisco DCNM before you add a CA signed SSL certificate. Therefore, perform the procedure in the below mentioned order.

This section includes the following topics:

- [Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance, page 2-29](#)
- [Enabling SSL/HTTPS on Cisco DCNM in HA Environment on RHEL or Windows, page 2-29](#)
- [Adding a CA signed SSL Certificate in Cisco DCNM, page 2-29](#)

## Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance

To enable SSL/HTTPS on a Virtual Appliance for Cisco DCNM in HA mode, perform the following:

**Step 1** Configure the primary server with a self signed SSL certificate.



**Note** In a CA signed certificate, each server has their own certificate generated by using the procedure [Configuring Certificates for Cisco DCNM, page 2-25](#). Ensure that the certificate is signed by the signing certificate chain which is common for both the servers.

**Step 2** On the secondary server, locate the keystore.

**Step 3** Rename the keystore located at

```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration
\fmserver.jks
```

to

```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration
\fmserver.jks.old
```

**Step 4** Copy the file “fmserver.jks” generated in primary server to secondary server into folders

```
<dcnm-home> /dcm/jboss-as-7.2.0.Final/standalone/configuration/
<dcnm-home>/dcm/fm/conf/cert/
```

## Enabling SSL/HTTPS on Cisco DCNM in HA Environment on RHEL or Windows

To enable SSL/HTTPS on RHEL or Windows for Cisco DCNM in HA mode, perform the following:

**Step 1** Configure the primary server with a self signed SSL certificate.



**Note** In a CA signed certificate, each server has their own certificate generated by using the procedure [Configuring Certificates for Cisco DCNM, page 2-25](#). Ensure that the certificate is signed by the signing certificate chain which is common for both the servers.

**Step 2** On the secondary server, perform one of the following:

- While executing the installer, choose HTTPS upfront and select to run in the HTTPs mode.
- While silent installation, choose HTTPs while you execute the installer.

## Adding a CA signed SSL Certificate in Cisco DCNM



**Note** This section applies to both all the Cisco DCNM installers.

To add CA signed SSL certificate for DCNM Windows or RHEL Setup, perform the following:

- 
- Step 1** From command prompt, navigate to **<DCNM install root>/dcm/java/jre1.8/bin/**.
- Step 2** Rename the keystore located at
- ```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks
```
- to
- ```
<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks.old
```
- Step 3** Generate the certificate-signing request (CSR) from the public key generated in [Step 2](#).
- ```
keytool -certreq -alias sme -file dcm.csr -keystore "<DCNM install root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3
```
- Step 4** Submit the CSR to certificate signing authority to digitally sign it.
- CA provides the certificate and signing certificate in as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file.
- If CA provided PKCS 7 format go to [Step 5](#) to convert it to PEM format. If CA provided PEM format then go to [Step 6](#).
- Step 5** Convert the PKCS 7 certificate chain to X509 certificate chain using openssl
- ```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```
- Step 6** Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:
- ```
keytool -importcert -trustcacerts -file cert-chain.pem -keystore <DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -alias sme
```
- Step 7** Stop the DCNM application by using the **appmgr stop dcnm** command.
- Step 8** Start the applications in the server by using the **appmgr start dcnm** command.



Note

You must configure the Cisco DCNM Web Port again, after adding a ca signed SSL certificate. For more information, see [Reconfigure DCNM to use an external Oracle database, page 6-11](#).

Server Ports

Cisco DCNM is installed with default port set. If you need to change the default port values due to security considerations, update the port details in **installer.properties** file and install DCNM in the silent installation mode. Ensure that you set the **RESOLVE_PORT_CONFLICTS** to **FALSE**. This ensures that the DCNM installer does not auto-resolve ports when the specified ports are unavailable.

For Windows PCs running Cisco DCNM-SAN, Device Manager, behind a firewall, certain ports need to be available. For more information, see [Running Cisco DCNM Behind a Firewall, page 3-35](#).

**Note**

This is of significance to the users deploying DCNM on a Windows or Linux system, and not applicable to the Open Virtual Appliance. This is not applicable to the Open Virtual Appliance (OVA), as the operating system controls the ports set.

Table 2-3 lists the default ports that services on a Cisco DCNM-SAN server listen to for client communications. One port is not configurable. You can configure the other ports. The server installer can resolve port conflicts automatically.

Table 2-3 **Default TCP Ports for Client Communications**

Service Name	Default Port for SAN	Configurable?
RMI	1198	During installation
Naming Service	9099	During installation
SSL	3943	During installation
EJB	3973	During installation
Server Bind 1	5644	During installation
Server Bind 2	5446	During installation
JMS	5457	During installation
Syslog (system message) Receiver	5545	During installation
AJP Connector	9009	During installation
Web Server	80	During installation
Web Services	9093	During installation
RMI Object	244444	During installation
UIL2	—	During installation

Table 2-4 displays the default server ports with DCNM installed in HTTPS mode.

Table 2-4 **Default Server Ports**

Service Name	Default Port
SAN Server Bind	5644
Web Services Port	8083
SAN invoker bind port	5446
DCNM Server	1099
EJB SSL	3843
SAN Management Native	9999
SAN JMS	5457
RMI Object	14444

Table 2-4 **Default Server Ports (continued)**

Service Name	Default Port
EJB	3873
DCNM Server Bind	4445
DCNM Web Port	8443
Invoker Bind	4446
SAN Management HTTP Port	9990
SAN AJP Connector	9009
RMI	1098
SAN Syslog	5545
AJP Connector	8009
SAN Management HTTP Port	9443
SAN Server	4447
SAN Web Services	9093
SAN RMI Object	24444
SAN EJB	3973
SAN Web	443
JMS Port	4457
SAN RMI	1198
SAN EJB SSL	3943
Syslog	5445
External Oracle Database	1521