CHAPTER 9

Administering the DCNM Server

This chapter describes how to administer the DCNM server.

This chapter includes the following topics:

- Administering Device Discovery, page 9-1
- Administering Devices and Credentials, page 9-8
- Administering DCNM Licensed Devices, page 9-19
- Administering DCNM Server Users, page 9-24
- Administering Auto-Synchronization with Devices, page 9-31
- Administering Statistical Data Collection, page 9-37
- Administering DCNM Server Log Settings, page 9-43

Administering Device Discovery

This section includes the following topics:

- Information About Device Discovery, page 9-1
- Licensing Requirements for Device Discovery, page 9-3
- Prerequisites for Device Discovery, page 9-3
- Guidelines and Limitations for Device Discovery, page 9-3
- Performing Device Discovery, page 9-4
- Viewing the Status of Device Discovery Tasks, page 9-7
- Where to Go Next, page 9-7
- Field Descriptions for Device Discovery, page 9-7
- Additional References for Device Discovery, page 9-8

Information About Device Discovery

This section includes the following topics:

- Device Discovery, page 9-2
- Cisco Discovery Protocol, page 9-2

- Credentials and Discovery, page 9-2
- NX-OS Device Preparation, page 9-2
- Virtualization Support, page 9-3

Device Discovery

Device discovery feature creates devices in DCNM by connecting to an NX-OS device and retrieving the running configuration of each virtual device context (VDC) on the NX-OS device. DCNM displays each VDC as a device, including the default VDC. If the NX-OS device has only the default VDC, then device discovery creates only one device in DCNM.

When DCNM connects to a device to retrieve its configuration, it uses the XML management interface, which uses the XML-based Network Configuration Protocol (NETCONF) over secure shell (SSH). For more information, see the *Cisco NX-OS XML Management Interface User Guide*.

Cisco Discovery Protocol

Device discovery uses Cisco Discovery Protocol (CDP) to find devices that are connected to the initial device in the discovery process. CDP exchanges information between adjacent devices over the data link layer. The exchanged information is helpful in determining network topology and physical configuration outside of the logical or IP layer.

CDP allows DCNM to discover devices that are one or more hops beyond the first device (seed device) in the discovery process. When you start the discovery process using the Device Discovery feature, you can limit the number of hops that the discovery process can make.

After DCNM discovers an NX-OS device using CDP, it connects to the device and retrieves information, such as the running configuration of the device. The information collected allows DCNM to manage the device.

DCNM supports CDP hops on some Cisco switches that run Cisco IOS software. Although DCNM cannot manage these devices, the Topology feature shows them and the CDP links between them and other discovered devices.

Credentials and Discovery

Device discovery requires that you provide a username and password for a user account on the seed device. To successfully complete discovery of an NX-OS device, the user account that you specify must be assigned to either the network-admin or the vdc-admin role.

If you want to discover devices that are one or more hops from the seed device, all devices in the chain of hops must be configured with a user account of the same username and password. All NX-OS devices in the chain of hops must assign the user account to the network-admin or the vdc-admin role.

NX-OS Device Preparation

Before you perform device discovery, you should ensure that the NX-OS device configuration can support a successful discovery. For more information, see the “NX-OS Device Configuration Requirements” section on page 1-5.

Virtualization Support

When DCNM discovers an NX-OS device, it determines how many virtual device contexts (VDC) are on the NX-OS device. In DCNM, each VDC is treated as a separate device. The status of each VDC is tracked separately and you can configure each VDC independently of other VDCs on an NX-OS device.

Licensing Requirements for Device Discovery

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	Device discovery requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the *Cisco DCNM Licensing Guide*.

Prerequisites for Device Discovery

Prior to performing device discovery, you should be familiar with the following:

- VDCs
- CDP

Device discovery has the following prerequisites:

- The DCNM server must be able to connect to devices it discovers.
- NX-OS devices must be running a supported version of NX-OS.
- CDP must be enabled both globally and specifically on interfaces used for device discovery.
- The NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "NX-OS Device Preparation" section on page 9-2.

Guidelines and Limitations for Device Discovery

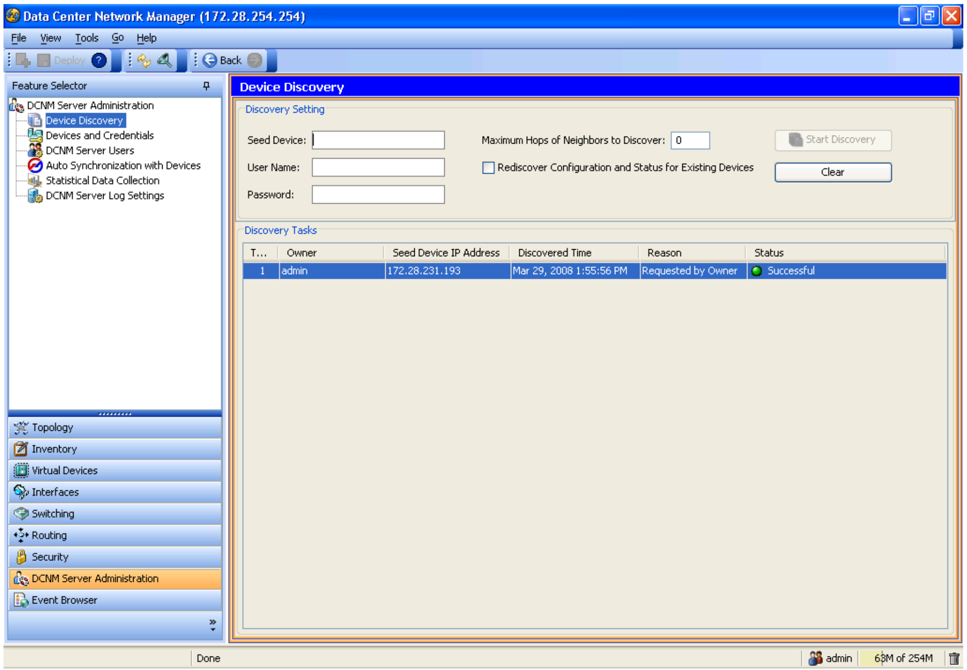
Device discovery has the following configuration guidelines and limitations:

- Ensure that NX-OS devices that you want to discover have been prepared for discovery. For more information, see the "NX-OS Device Configuration Requirements" section on page 1-5.
- DCNM can manage only devices that run NX-OS 4.0.
- CDP-based discovery of devices requires that all devices in the chain of CDP hops use the same username and password specified for the seed device. If your security practices do not allow the same username and password to be used on each device, you can perform device discovery for each device individually.
- Devices that are CDP hops but which are not running Cisco IOS software appear in the Topology feature but cannot be managed by DCNM.

Performing Device Discovery

Figure 9-1 shows the Device Discovery content pane.

Figure 9-1 Device Discovery Content Pane



Seed Device:

User Name:

Password:

Maximum Hops of Neighbors to Discover: 0

☐ Rediscover Configuration and Status for Existing Devices

T...	Owner	Seed Device IP Address	Discovered Time	Reason	Status
1	admin	172.28.231.193	Mar 29, 2008 1:55:56 PM	Requested by Owner	● Successful

This section includes the following topics:

- Discovering Devices, page 9-4
- Rediscovering Devices, page 9-6

Discovering Devices

You can discover one or more devices. When a discovery task succeeds, DCNM retrieves the running configuration and status information of discovered NX-OS devices.

Use this procedure for the following purposes:

- To discover devices that are not currently managed by DCNM. For example, you should use this procedure when DCNM has not yet discovered any devices, such as after a new installation.
- To discover devices that you have added to your network without rediscovering devices that DCNM already has discovered.
- To rediscover the topology when CDP links have changed, without rediscovering devices that DCNM has already discovered.

Note You must successfully discover an NX-OS device before you can use DCNM to configure the device.

BEFORE YOU BEGIN

Ensure that you have configured the NX-OS device so that the DCNM server can connect to it. For more information, see the "NX-OS Device Configuration Requirements" section on page 1-5.

Determine the IPv4 address of the device that you want DCNM to connect to when it starts the discovery task. This is the seed device for the discovery.

Determine whether you want to discover devices that are CDP neighbors of the seed device. If so, determine the maximum number of hops from the seed device that the discovery process can make.

Note The discovery process can perform complete discovery of neighbors only if the neighboring devices are configured with the same credentials as the seed device.

DETAILED STEPS

To discover one or more NX-OS devices, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The discovery tasks appear in the Discovery Tasks area of the Contents pane.

Step 2 In the Seed Device field, enter the IPv4 address of the device that you want DCNM to connect to when it starts the discovery task. Valid entries are in dotted decimal format.

Step 3 In the User Name field, enter the username of a user account on the device. The user account must have a network-admin or vdc-admin role.

Step 4 In the Password field, enter the password for the user account that you entered in the User Name field.

Step 5 (Optional) If you want DCNM to discover devices that are CDP neighbors of the seed device, in the Maximum Hops of Neighbors to Discover field, enter the desired maximum number of hops. By default, the maximum hops is 0 (zero).

Step 6 Ensure that **Rediscover Configuration and Status for Existing Devices** is unchecked. By default, this check box is unchecked.

By leaving this check box unchecked, you enable DCNM to use previously discovered devices as CDP hops without retrieving their running configuration and status information.

Step 7 Click **Start Discovery**.

After a short delay, the discovery task appears at the bottom of the list of tasks in the Discovery Tasks area. DCNM updates the task status periodically.

Step 8 Wait until the status for the task is Successful. This step may take several minutes.

After the status is Successful, you can use DCNM to configure and monitor the discovered devices.

You do not need to save your changes.

Rediscovering Devices

You can rediscover one or more devices.

Note Rediscovery replaces any configuration data that DCNM has for an NX-OS device with the configuration data retrieved during the rediscovery. If you need to discover one or more devices without retrieving configuration and status information for already discovered devices, see the "Discovering Devices" section on page 9-4.

You must successfully discover an NX-OS device before you can use DCNM to configure the device.

BEFORE YOU BEGIN

Ensure that you have configured the NX-OS device so that the DCNM server can connect to it. For more information, see the "NX-OS Device Preparation" section on page 9-2.

DETAILED STEPS

To rediscover one or more NX-OS devices, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The discovery tasks and their status appear in the Discovery Tasks area of the Contents pane.

Step 2 In the Seed Device field, enter the IPv4 address of the device that you want DCNM to connect to when it starts the discovery task. Valid entries are in dotted decimal format.

Step 3 In the User Name field, enter the username of a user account on the device. The user account must have a network-admin or vdc-admin role.

Step 4 In the Password field, enter the password for the user account that you entered in the User Name field.

Step 5 (Optional) If you want DCNM to rediscover devices that are CDP neighbors of the seed device, in the Maximum Hops of Neighbors to Discover field, enter the desired maximum number of hops. By default, the maximum hops is 0 (zero).

Step 6 Check **Rediscover Configuration and Status for Existing Devices**. By default, this check box is unchecked.

By checking this check box, you enable DCNM to replace any configuration and status information that it has about a previously discovered device with the running configuration and status information retrieved from the device.

Step 7 Click **Start Discovery**.

After a short delay, the discovery task appears at the bottom of the list of tasks in the Discovery Tasks area. DCNM updates the task status periodically.

Step 8 Wait until the status for the task is Successful. This step may take several minutes.

After the status is Successful, you can use DCNM to configure and monitor the discovered devices.

You do not need to save your changes.

Viewing the Status of Device Discovery Tasks

To view the status of device discovery tasks, from the Feature Selector pane, choose **DCNM Server Administration > Device Discovery**.

The device discovery tasks, including the task status, appear in the Discovery Tasks area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Device Discovery" section on page 9-7.

Where to Go Next

View the discovered devices and configure unique device credentials, as needed. For more information, see the "Administering Devices and Credentials" section on page 9-8.

Field Descriptions for Device Discovery

This section includes the following field descriptions for device discovery:

- Device Discovery Content Pane, page 9-7
- Related Fields, page 9-8

Device Discovery Content Pane

Table 9-1 Device Discovery Content Pane

Field	Description
Discovery Setting	
Seed Device	IPv4 address of the first device that you want to discover. Valid entries are in dotted decimal format. By default, this field is blank.
User Name	Name of the device user account that the DCNM server uses to access the device. The user account must have network-admin or vdc-admin privileges on the device. By default, this field is blank.
Password	Password for the device user account specified in the User Name field. By default, this field is blank.
Maximum Hops of Neighbors to Discover	Largest permissible number of CDP hops between the DCNM server and the device. If the server connects to the device but exceeds this number of hops, the discovery fails. The default setting is 0 (zero), which disables the discovery of neighboring devices.
Rediscover Configuration and Status for Existing Devices	Whether the discovery task you are configuring is to replace an existing device discovery that has already completed. By default, this check box is unchecked.
Discovery Tasks	
Task ID	*Display only.* Number assigned to the discovery task. The task ID indicates the order in which discovery tasks occurred.

Table 9-1 Device Discovery Content Pane (continued)

Field	Description
Owner	*Display only.* The DCNM server user account used to start the discovery task.
Seed Device IP Address	*Display only.* The IPv4 address of the seed device.
Discovered Time	*Display only.* The date and time of the most recent update to the Status field.
Status	*Display only.* The state of the discovery task. Valid values are as follows: • In progress—The discovery tasks is ongoing. • Successful—The discovery task completed without errors. • Failed—The discovery task completed with errors.

Related Fields

For information about fields that configure devices, see the "Administering Devices and Credentials" section on page 9-8.

Additional References for Device Discovery

For additional information related to device discovery, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide*

Standards

Standards	Title
NETCONF protocol over the Secure Shell (SSH)	RFC 4742

Administering Devices and Credentials

This section describes how to administer NX-OS devices and the credentials that are used by the DCNM server to authenticate itself to the devices.

- Information About Devices and Credentials, page 9-9
- Licensing Requirements for Devices and Credentials, page 9-10
- Prerequisites for Administering Devices and Credentials, page 9-10
- Guidelines and Limitations for Devices and Credentials, page 9-10

Information About Devices and Credentials

This section includes the following topics:

Devices

The Devices and Credentials feature allows you to administer individual devices, which each represent a single VDC on a device running NX-OS. For example, after you have discovered multiple devices using the Device Discovery feature, you have need to retrieve again the running configuration and status information of a single VDC. Rather than performing device discovery for all the VDC on the NX-OS device, you can use the Devices and Credentials feature to rediscover the single device that represents the changed VDC.

Credentials

Devices and Credentials supports the NX-OS ability to secure each VDC with different credentials. DCNM allows you to configure unique credentials for each discovered device or the use of default credentials when you do not configure unique credentials for a device. If some managed devices share the same credentials but others do not, you can configure unique credentials for some devices and configure the default credentials with the credentials that are shared by some of the managed devices.

Devices and Credentials associates a unique set of device credentials with each DCNM server user account. This allows you to accounting logs on managed devices that reflect the actions of each DCNM server user. If you open the DCNM with a user account that does not yet have device credentials configured, the client prompts you to configure device credentials for the user account.

If support for accounting is not important to your organization, you must still configure each DCNM server user with device credentials, even if the credentials specified for each user are the same.

Device Status

The Devices and Credentials feature shows the status each device. The possible status are as follows:

- Managed—DCNM can connect to the device using SSH, configure the running configuration of the device, and retrieve logs and other data from it. This status is possibly only for devices that run a supported release of NX-OS and that are configured properly to support discovery by DCNM. For more information, see the "NX-OS Device Preparation" section on page 9-2.
- Unmanaged—DCNM does not manage the device or monitor the status of the device.

- Unreachable—DCNM cannot connect to the device, which was a managed device prior to becoming unreachable. Common causes for this status are as follows:
  - A network issue is preventing the DCNM server from contacting the device.
  - SSH is disabled on the device.
  - All terminal lines on the device are in use.

Virtualization Support

DCNM treats each virtual device context (VDC) on an NX-OS device as a separate device; therefore, DCNM can maintain unique credentials for each VDC on a device. DCNM tracks the status of each VDC separately, as well.

Licensing Requirements for Devices and Credentials

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	Device and Credentials requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the *Cisco DCNM Licensing Guide*.

Prerequisites for Administering Devices and Credentials

Performing device discovery with the Devices and Credentials feature has the following prerequisites:

- The DCNM server must be able to connect to device that you want to discover.
- The NX-OS device must be running a supported version of NX-OS.
- The NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "NX-OS Device Preparation" section on page 9-2.

Guidelines and Limitations for Devices and Credentials

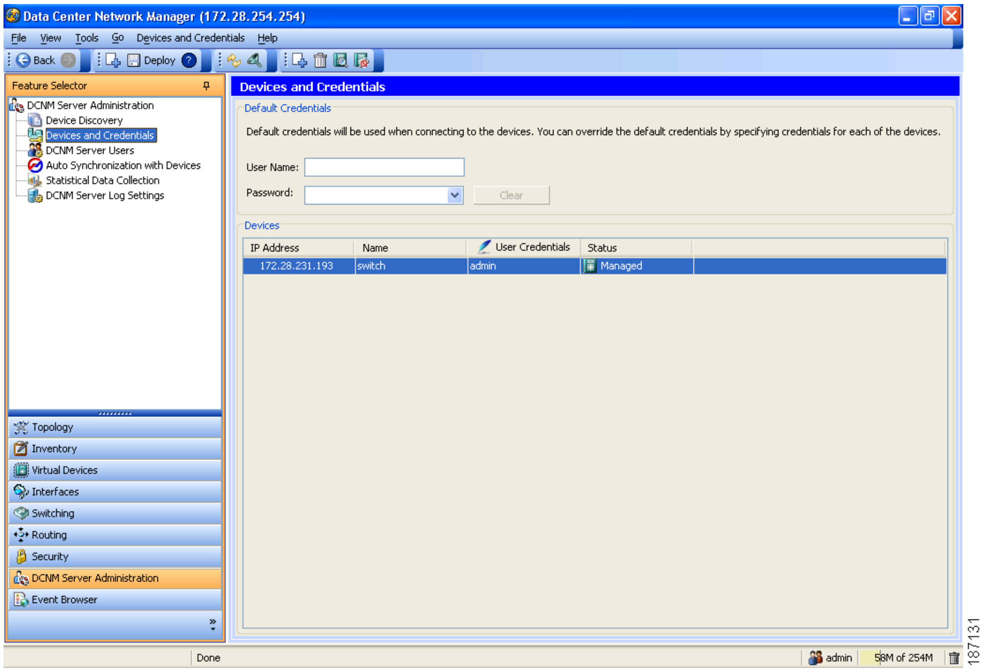
The Devices and Credentials feature has the following configuration guidelines and limitations:

- Discovering a device by using the Devices and Credentials feature does not support CDP-based discovery of neighboring devices. To use CDP-based discovery, see the "Administering Device Discovery" section on page 9-1.
- Be careful when you change the default credentials or device-specific credentials. Incorrect credentials prevent DCNM from managing devices.

Configuring Devices and Credentials

Figure 9-2 shows the Devices and Credentials content pane.

Figure 9-2 Devices and Credentials Content Pane



Default credentials will be used when connecting to the devices. You can override the default credentials by specifying credentials for each of the devices.

User Name:

Password:

IP Address	Name	User Credentials	Status
172.28.231.193	switch	admin	Managed

This section includes the following topics:

- Adding a Device, page 9-11
- Discovering a Device, page 9-12
- Unmanaging a Device, page 9-13
- Deleting a Device, page 9-13
- Configuring Default Device Credentials, page 9-14
- Clearing Default Device Credentials, page 9-15
- Configuring Unique Credentials for a Device, page 9-16
- Clearing Unique Credentials for a Device, page 9-17

Adding a Device

You can add a device. This feature is particularly useful when you need to use DCNM to configure a new VDC on an NX-OS device with which you have already performed device discovery. Rather than rediscovering all VDCs on the device, you can add the one VDC that is new.

After you add a device, you can discover it. For more information, see the "Discovering a Device" section on page 9-12.

BEFORE YOU BEGIN

Determine the IPv4 address for the device.

Determine whether DCNM can communicate with the device using the default device credentials or whether you need to add unique device credentials when you add the device to DCNM.

DETAILED STEPS

To add a device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 From the menu bar, choose **Devices and Credentials > New Device**.

A blank row appears in the Devices area on the Contents pane.

Step 3 In the IP Address column for the new device, enter the IPv4 address that DCNM must use to connect to the device.

Step 4 Press **Enter**.

Step 5 (Optional) If you need to add unique device credentials, in the User Credentials column, double-click the entry for the device that you added, click the down-arrow button, and configure the unique device credentials.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

The status of the new device is Unmanaged.

Discovering a Device

You can discover a device.

Discovering an unmanaged device changes its status to Managed. During the discovery, DCNM retrieves the running configuration of the device.

If you are rediscovering a device, the configuration data that DCNM retrieves replaces any existing configuration data for the device. Whenever the configuration data that DCNM has for the device is not accurate, such as when a device administrator has used the command-line interface to change the running configuration, you can use this procedure to update the configuration data that DCNM has for the device. This feature is particularly useful when the device is a VDC whose resource allocation was changed, such as changes to the interfaces assigned to the VDC.

Note Discovering a device does not affect the running configuration of the device.

BEFORE YOU BEGIN

Ensure that you have either configured the device entry with unique device credentials or that DCNM can use the default device credentials to connect to the device. For more information, see the "Configuring Default Device Credentials" section on page 9-14.

DETAILED STEPS

To discover a device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 Click the device that you want to discover.

Step 3 From the menu bar, choose **Devices and Credentials > Discover**.

The device discovery begins. The status of the device changes to Discovering.

Step 4 Wait for the status to change to Managed.

Typically, the device discovery occurs in less than 5 minutes. After the status changes to Managed, you can use DCNM to configure the device.

You do not need to save your changes.

Unmanaging a Device

You can change the status of a device to unmanaged.

BEFORE YOU BEGIN

Ensure that you are changing the status of the correct device. DCNM cannot control the running configuration of an unmanaged device.

DETAILED STEPS

To change the status of a device to unmanaged, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 Click the device whose status you want to change to unmanaged.

Step 3 From the menu bar, choose **Devices and Credentials > Unmanage**.

After a short delay, the status of the device changes to Unmanaged.

You do not need to save your changes.

Deleting a Device

You can delete a device. When you delete a device, you delete all configuration data about the device from DCNM.

You should consider deleting devices that you do not intend to manage with DCNM. Additionally, when a device administrator has deleted a VDC by using the command-line interface of the device, you should delete the device from DCNM.

Note Deleting a device does not affect the running configuration of the device.

BEFORE YOU BEGIN

Ensure that you are deleting the correct device.

DETAILED STEPS

To delete a device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 Click the device that you want to delete.

Step 3 From the menu bar, choose **Devices and Credentials > Delete**.

The device disappears from the Devices area.

You do not need to save your changes.

Configuring Default Device Credentials

You can configure the default credentials, which DCNM uses to authenticate itself when it connects to discovered NX-OS devices. DCNM uses the default device credentials to communicate with each discovered device that you have not configured with unique device credentials.

Note Device credentials are unique for each DCNM server user account.

BEFORE YOU BEGIN

Determine what the default device credentials should be. All NX-OS devices that DCNM uses the default credentials to communicate with must have a network administrator account configured with a username and password that are identical to the default credentials that you configure in DCNM.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

To configure default device credentials, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The Default Credentials area appears in the Contents pane, above the Devices area, which lists the discovered devices.

Step 2 In the User Name field, enter the username for the default credentials. A valid username can be 1 to 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Note NX-OS supports usernames that are a maximum of 28 characters.

Step 3 To the right of the Password field, click the down-arrow button.

Step 4 In the Password field and the Confirm Password field, enter the password for the default credentials. Valid passwords are numbers, symbols, and case-sensitive letters.

Note NX-OS supports passwords that are a maximum of 64 characters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Clearing Default Device Credentials

You can clear the default device credentials.

Note If you clear the default device credentials, DCNM can connect to discovered devices only if you have configured unique credentials for each managed device.

BEFORE YOU BEGIN

If you intend to operate DCNM without default device credentials, you should ensure that DCNM is configured with unique device credentials for each discovered device before you perform this procedure. For more information, see the "Configuring Unique Credentials for a Device" section on page 9-16.

DETAILED STEPS

To configure default device credentials, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The Default Credentials area appears in the Contents pane, above the Devices area, which lists the discovered devices.

Step 2 In the Default Credentials area, click **Clear**.

The User Name field and the Password field clear.

Step 3 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Configuring Unique Credentials for a Device

You can configure credentials that are unique to a discovered device. When unique credentials exist for a discovered device, DCNM uses them when it connects to the device rather than using the default device credentials.

Note Device credentials are unique for each DCNM server user account.

BEFORE YOU BEGIN

Determine the username and password for a network administrator user account on the discovered device.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

To configure unique credentials for a discovered device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The discovered devices appear in the Devices area of the Contents pane.

Step 2 In the User Credentials column for the device, double-click the entry and then click the down-arrow button.

Step 3 In the User Name field, enter the username. Valid usernames are between 1 and 32 characters. Valid characters are numbers, symbols, and case-sensitive letters.

Note NX-OS supports usernames that are a maximum of 28 characters.

Step 4 In the Password field and the Confirm Password field, enter the password. Valid passwords are numbers, symbols, and case-sensitive letters.

Note NX-OS supports passwords that are a maximum of 64 characters.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Clearing Unique Credentials for a Device

You can clear unique credentials for a discovered device.

Note If you clear the unique credentials for a discovered device, DCNM uses the default credentials to connect to the device.

BEFORE YOU BEGIN

If you intend to operate DCNM without unique credentials for the device, you should ensure that DCNM is configured with default device credentials before you perform this procedure. For more information, see the "Configuring Default Device Credentials" section on page 9-14.

DETAILED STEPS

To clear unique credentials from a discovered device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

Discovered devices appear in the Devices area of the Contents pane.

Step 2 In the User Credentials column for the device, double-click the entry and then click the down-arrow button.

Step 3 In the User Name field, delete all text.

Step 4 In the Password field, delete all text.

Step 5 In the Confirm Password field, delete all text.

Step 6 Click **OK**.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Viewing Device Credentials and Status

To view the status of device discovery tasks, from the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

The default credentials appears in the Default Credentials area in the Contents pane. Information about devices, including credentials and status, appear in the Devices area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Devices and Credentials" section on page 9-18.

Field Descriptions for Devices and Credentials

This section includes the following field descriptions for Devices and Credentials:

- Device and Credentials Content Pane, page 9-18

Device and Credentials Content Pane

Table 9-2 Device and Credentials Content Pane

Field	Description
Default Credentials	
User Name	Name of the NX-OS device user account that the DCNM server uses to access any device that it is discovering or that it is managing. The user account must be assigned to the network-admin or vdc-admin role on the device. By default, this field is blank. **Note** The information in the User Credentials field in the Devices area overrides the information in the Default Credentials section.
Password	Password for the NX-OS device user account specified in the User Name field. By default, this field is blank.
Devices	
IP Address	*Display only.* The IPv4 address of the NX-OS device.
Name	*Display only.* Name of the NX-OS device.
User Credentials	The NX-OS user account that DCNM uses to connect to the NX-OS device. **Note** If you configure this field, DCNM uses the user account that you configure when it connects to the device. If this field is blank, DCNM uses the user account specified in the Default Credentials area. By default, this field is blank.
Status	*Display only.* Whether the DCNM server can connect to and configure the device. Valid values are as follows: • Managed—The DCNM server can configure the device. • Unmanaged—The DCNM server cannot configure the device. • Unreachable—The DCNM server cannot reach the device.

Additional References for Devices and Credentials

For additional information related to the Devices and Credentials feature, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide*

Standards

Standards	Title
NETCONF protocol over the Secure Shell (SSH)	RFC 4742

Administering DCNM Licensed Devices

In Cisco DCNM Release 4.0(2) and later releases, the DCNM Licensed Devices feature allows you to control which physical devices are covered by DCNM Enterprise LAN licenses that you have installed. This section describes how to use DCNM Licensed Devices.

This section includes the following topics:

- Information About DCNM Licensed Devices, page 9-19
- Licensing Requirements for Administering DCNM Licensed Devices, page 9-20
- Prerequisites for Administering DCNM Licensed Devices, page 9-20
- Guidelines and Limitations for Administering DCNM Licensed Devices, page 9-20
- Configuring DCNM Licensed Devices, page 9-21
- Viewing DCNM Licensed Devices, page 9-23
- Field Descriptions for DCNM Licensed Devices, page 9-23
- Additional References, page 9-23

Information About DCNM Licensed Devices

The DCNM Licensed Devices feature allows you to control which physical devices you can manage with licensed DCNM features. The feature maintains a list of licensed devices. If a device is on this list, you can manage licensed DCNM features on the device.

You can add as many devices to licenses as your licenses support. For example, if you install two LAN Enterprise licenses that each support five devices, you can add a total of 10 devices to the list of licensed devices.

You can also remove devices from the list of licensed devices and replace them with other devices.

When you try to use a DCNM licensed feature to configure a device that you have not added to the list of licensed devices, the client does not allow you to use the feature to configure the unlicensed device.

Licensing Requirements for Administering DCNM Licensed Devices

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	DCNM Licensed Devices requires an Enterprise LAN license. For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the *Cisco DCNM Licensing Guide.*

Prerequisites for Administering DCNM Licensed Devices

Administering DCNM Licensed Devices has the following prerequisites:

- You must install one or more LAN Enterprise licenses. For more information, see the "Installing Licenses" section on page 2-11.
- You must discover the devices that you want to add to the list of DCNM-licensed devices. For more information, see the "Discovering Devices" section on page 9-4.

Guidelines and Limitations for Administering DCNM Licensed Devices

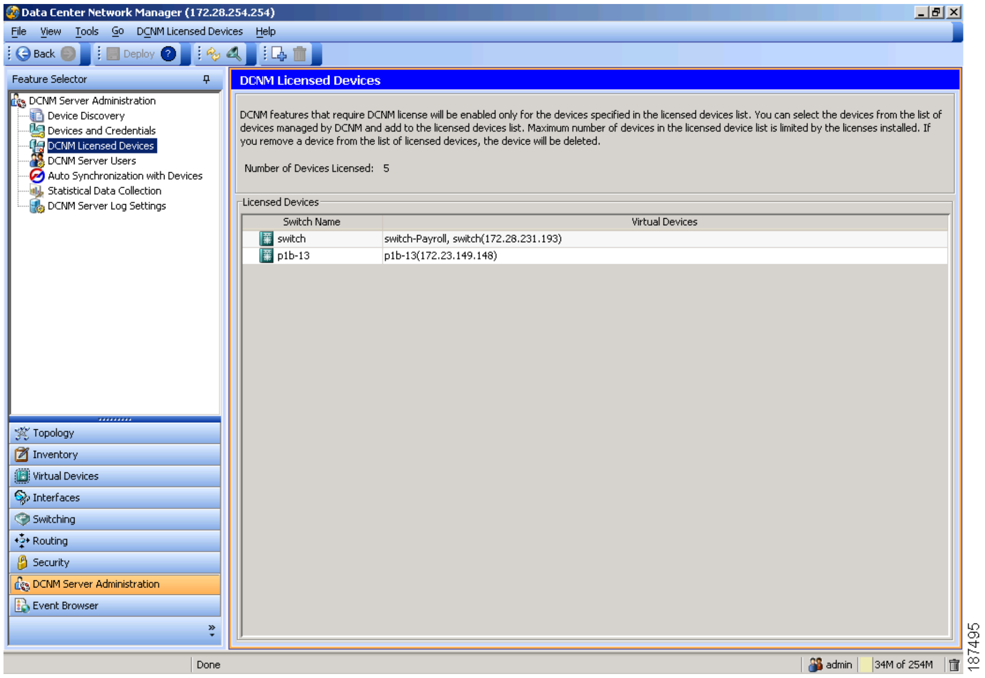
Administering DCNM Licensed Devices has the following configuration guidelines and limitations:

- You can add only managed devices to the list of licensed devices.
- You can add to the list of licensed devices only as many devices as permitted by all of the LAN Enterprise licenses that you have installed.
- When you remove a device from the list of licensed devices, the device and all of its VDCs are removed from DCNM. To continue managing the device, you must discover the device. For more information, see the "Discovering Devices" section on page 9-4.

Configuring DCNM Licensed Devices

Figure 9-3 shows the DCNM Licensed Devices content pane.

Figure 9-3 DCNM Licensed Devices Content Pane



DCNM features that require DCNM license will be enabled only for the devices specified in the licensed devices list. You can select the devices from the list of devices managed by DCNM and add to the licensed devices list. Maximum number of devices in the licensed device list is limited by the licenses installed. If you remove a device from the list of licensed devices, the device will be deleted.

Number of Devices Licensed: 5

Licensed Devices

Switch Name	Virtual Devices
switch	switch-Payroll, switch(172.28.231.193)
p1b-13	p1b-13(172.23.149.148)

This section includes the following topics:

- Adding Devices to the Licensed Devices List, page 9-21
- Removing Devices from the Licensed Devices List, page 9-22

Adding Devices to the Licensed Devices List

You can add managed devices to the list of DCNM-licensed devices.

BEFORE YOU BEGIN

You must have installed at least one DCNM Enterprise LAN license. For more information, see the "Installing Licenses" section on page 2-11.

If you have already added as many devices as the maximum number of devices allowed by your licenses, you must remove one or more devices from the list of licensed devices before you can add other devices to the list. For more information, see the "Removing Devices from the Licensed Devices List" section on page 9-22.

DETAILED STEPS

To add a device to the list of licensed devices, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration** > **DCNM Licensed Devices**.

The Contents pane displays the list of licensed devices.

Step 2 From the menu bar, choose **DCNM Licensed Devices > New**.

The client adds a row to the list and the Available Devices dialog box lists available and selected physical devices.

Step 3 From the Available Devices list, choose the physical devices that you want to add to the license and then click **Add**.

Step 4 Click **OK**.

The Contents pane displays a list of licensed devices, including the devices that you added.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

You can begin using licensed DCNM features when you manage the device.

Removing Devices from the Licensed Devices List

You can remove one or more physical devices from the list of DCNM-licensed devices when you no longer need to use licensed DCNM features to manage the devices.

Note When you remove a physical device from the list of licensed devices, the device and all of its VDCs are removed from DCNM. To continue managing the device, you must discover the device. For more information, see the "Discovering Devices" section on page 9-4.

DETAILED STEPS

To remove devices from the list of licensed devices, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration** > **DCNM Licensed Devices**.

The Contents pane displays the list of licensed devices.

Step 2 For each device that you want to remove from the list of licensed devices, follow these steps:

a. Choose the device that you want to remove from the list of licensed devices.

b. From the menu bar, choose **DCNM Licensed Devices > Delete**.

The client displays a confirmation dialog box.

c. Click **Yes**.

The client removes the device from the list of licensed devices.

Note Devices that you remove from the list of licensed devices are no longer managed by DCNM.

Step 3 (Optional) To continue managing devices that you removed from the list of licensed devices, discover the devices. For more information, see the "Discovering Devices" section on page 9-4.

Viewing DCNM Licensed Devices

To view the list of DCNM-licensed devices, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Licensed Devices**.

The list of DCNM-licensed devices appears in the Contents pane. For information about the fields that appear, see the "Field Descriptions for DCNM Licensed Devices" section on page 9-23.

Field Descriptions for DCNM Licensed Devices

This section includes the following field descriptions for DCNM Licensed Devices:

- DCNM Licensed Devices Content Pane, page 9-23

DCNM Licensed Devices Content Pane

Table 9-3 DCNM Licensed Devices Content Pane

Field	Description
Number of Devices Licensed	*Display only.* Sum of devices licensed by all DCNM Enterprise LAN licenses installed. For example, if you installed two licenses that each support 5 devices, this field would display 10.
Switch Name	*Display only.* Name of a licensed physical device. You can use licensed DCNM features on the device.
Virtual Devices	*Display only.* Each virtual device context (VDC) that is configured on the physical device.

Additional References

For additional information related to administering DCNM Licensed Devices, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
Installing a DCNM Enterprise LAN license	*Installing Licenses, page 2-11*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Administering DCNM Server Users

This section describes how to administer DCNM server user accounts.

This section includes the following topics:

- Information About Administering DCNM Server Users, page 9-24
- Licensing Requirements for Administering DCNM Server Users, page 9-25
- Prerequisites for Administering DCNM Server Users, page 9-25
- Guidelines and Limitations for Administering DCNM Server Users, page 9-25
- Configuring DCNM Server Users, page 9-26
- Viewing DCNM Server Users, page 9-29
- Field Descriptions for DCNM Server Users, page 9-29
- Additional References, page 9-30

Information About Administering DCNM Server Users

DCNM server users are user accounts that allow people to access the DCMM client. User access is secured by password, and DCNM supports strong passwords.

DCNM server users are local to the DCNM server; creating, changing, and removing DCNM server users has no effect on user accounts on NX-OS devices.

As described in Table 9-4, DCNM supports two user roles.

Table 9-4 DCNM Server User Roles

DCNM Role	Description
User	• Cannot add or delete DCNM server user accounts • Can change the password only for its own account • Can use all other features
Admin	• Has full control of DCNM server user accounts • Can use all other features

Users and Device Credentials

Each DCNM server user has unique device credentials. This allows you to accounting logs on managed devices that reflect the actions of each DCNM server user. For more information, see the "Information About Devices and Credentials" section on page 9-9.

Virtualization Support

NX-OS support for virtual device contexts has no effect on DCNM server users.

DCNM server users can configure any managed device.

Licensing Requirements for Administering DCNM Server Users

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	Administering DCNM server users requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the *Cisco DCNM Licensing Guide*.

Prerequisites for Administering DCNM Server Users

Administering DCNM server users has the following prerequisites:

- To add, delete, or modify DCNM server users, you must be logged into the DCNM client with a user account that is assigned the Administrator DCNM role.

Guidelines and Limitations for Administering DCNM Server Users

Administering DCNM server users has the following configuration guidelines and limitations:

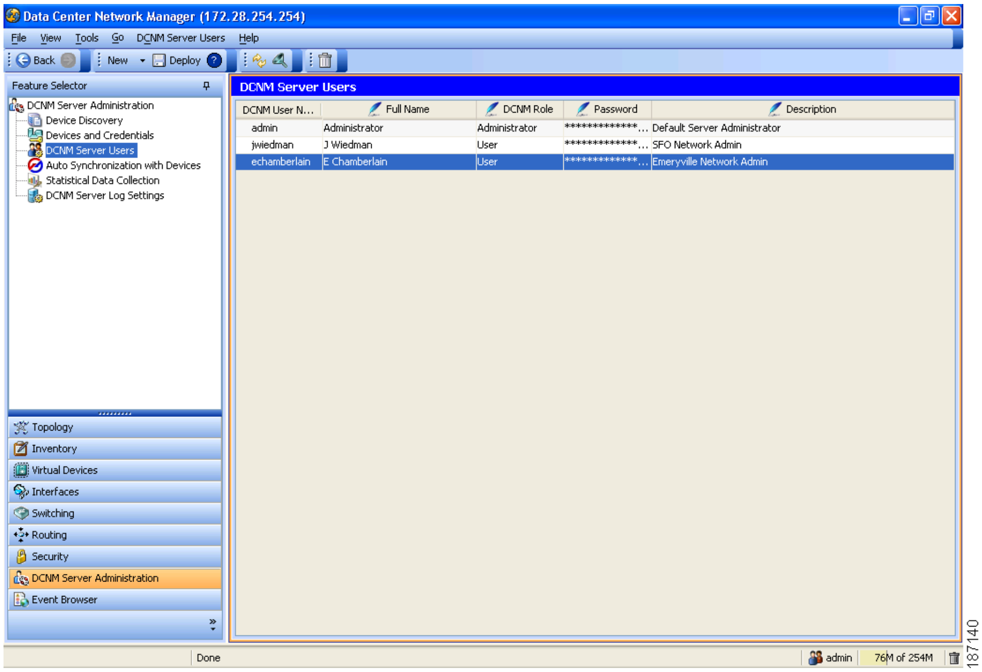
- Create a DCNM user account for each person who uses the DCNM client.
- Delete unused DCNM user accounts.
- Grant an admin user account only to those who need to perform administrator tasks in the DCNM client.
- We recommend that you use strong passwords. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

Send document comments to nexus7k-docfeedback@cisco.com

Configuring DCNM Server Users

Figure 9-4 shows the DCNM Server Users content pane.

Figure 9-4 DCNM Server Users Content Pane



DCNM User N...	Full Name	DCNM Role	Password	Description
admin	Administrator	Administrator	*************...	Default Server Administrator
jwiedman	J Wiedman	User	*************...	SFO Network Admin
echamberlain	E Chamberlain	User	*************...	Emeryville Network Admin

This section includes the following topics:

- Adding a DCNM Server User, page 9-26
- Changing the Password of a DCNM Server User, page 9-27
- Changing the Full Name, Role, or Description of a DCNM Server User, page 9-28
- Deleting a DCNM Server User, page 9-29

Adding a DCNM Server User

You can add a DCNM server user account.

Note Adding a DCNM server user account does not affect the user account configuration on any NX-OS device.

BEFORE YOU BEGIN

Log into the DCNM client with a user account that has the Administrator user role.

Determine the username and password for the new DCNM server user account.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

To add a DCNM server user, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Users**.

A table of DCNM server users appear in the Contents pane.

Step 2 From the menu bar, choose **DCNM Server Users > Add User**.

A new row appears at the bottom of the list of users. By default, all fields in the new row are blank.

Step 3 In the User Name column of the new row, enter the username. The username can be 1 to 198 characters. Entries can contain case-sensitive letters, numbers, and symbols.

Step 4 (Optional) In the Full Name column, double-click the entry and add a name. For example, enter the real name of the person who will use the DCNM server user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 5 In the DCNM Role column, double-click the entry and choose the role. By default, the role is User.

Step 6 In the Password column, double-click the entry and then click the down-arrow button.

Step 7 In the Password field and the Confirm Password field, enter the password. The password can be 1 to 255 characters. Entries can contain case-sensitive letters, numbers, and symbols.

Step 8 Click **OK**.

Step 9 (Optional) In the Description column, double-click the entry and add a description of the user account. For example, you could use this entry to provide e-mail and telephone contact details of the person who will be using this DCNM server user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 10 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Changing the Password of a DCNM Server User

You can change the password of a DCNM server user.

BEFORE YOU BEGIN

An Administrator role is required if you want to change the password of a user account other than the account that you use to log into the DCNM client. If your user account has the User role, you can change the password of your account only.

Determine what the new password should be.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

DETAILED STEPS

To change the password of a DCNM server user, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Users**.

A table of DCNM server users appear in the Contents pane.

Step 2 In the User Name column, click the username for the user account that you want to change.

The row of the username that you clicked is highlighted.

Step 3 In the Password column, double-click the entry and then click the down-arrow button.

Step 4 In the Password field and the Confirm Password field, enter the new password. The password can be 1 to 255 characters. Entries can contain case-sensitive letters, numbers, and symbols.

Step 5 Click **OK**.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Changing the Full Name, Role, or Description of a DCNM Server User

You can change the full name, role, or description of a DCNM server user.

Note You cannot change the username. Instead, add a user account with the desired username and remove the user account with the unwanted username.

BEFORE YOU BEGIN

Determine what the new full name or description should be.

An Administrator role is required if you want to change the full name, role, or description of a user account other than the account that you use to log into the DCNM client. If your user account has the User role, you can change these items for your account only.

DETAILED STEPS

To change the full name or description of a DCNM server user, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Users**.

A table of DCNM server users appear in the Contents pane.

Step 2 In the User Name column, click the username of the user account that you want to change.

The row of the username that you clicked is highlighted.

Step 3 (Optional) In the Full Name column, double-click the entry and enter the new name. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 4 (Optional) In the DCNM Role column, double-click the entry and choose the new role. You can choose Administrator or User.

Step 5 (Optional) In the Description column, double-click the entry and enter the new description of the user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Deleting a DCNM Server User

You can remove a DCNM server user account.

BEFORE YOU BEGIN

Ensure that you are removing the correct DCNM server user account.

DETAILED STEPS

To delete a DCNM server user account, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Users**.

A table of DCNM server users appear in the Contents pane.

Step 2 In the User Name column, click the username of the user account that you want to remove.

The row of the username that you clicked is highlighted.

Step 3 From the menu bar, choose **DCNM Server Administration > Delete User**.

Step 4 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Viewing DCNM Server Users

To view DCNM server user accounts, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Users**.

DCNM server user accounts, including usernames and descriptions, appear in the Contents pane. Passwords appear masked for security. For information about the fields that appear, see the "Field Descriptions for DCNM Server Users" section on page 9-29.

Field Descriptions for DCNM Server Users

This section includes the following field descriptions for DCNM server users:

- DCNM Server Users Content Pane, page 9-30

DCNM Server Users Content Pane

Table 9-5 DCNM Server Users Content Pane

Field	Description
DCNM User Name	*Display only.* Name of the DCNM server user account. This name can be used to log into the DCNM client. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. Minimum length is 1 character. Maximum length is 198 characters.
Full Name	Other name for the user account, such as the name of the person who uses the DCNM server user account. This name cannot be used to log into the DCNM client. Valid characters are all letters, numbers, and symbols. Maximum length is 255 characters. This field is blank by default.
DCNM Role	Role of the user account. Valid values are User and Administrator. For more information, see Table 9-4. By default, a DCNM server user account is assigned the role of User.
Password	Password for the DCNM server user. This field is always masked for security. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. Minimum length is 1 character. Maximum length is 255 characters.
Description	Description of the DCNM server user. Valid characters are all letters, numbers, and symbols. Maximum length is 255 characters. This field is blank by default.

Additional References

For additional information related to administering DCNM server users, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
Logging into the DCNM client	*Opening the DCNM Client, page 4-7*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Administering Auto-Synchronization with Devices

This section describes how to administer the Auto-Synchronization with Devices feature.

This section includes the following topics:

Information About Auto-Synchronization with Devices

Automatically synchronizing with devices ensures that the DCNM server has current configuration and status information about managed devices. The DCNM server creates one poller process for each device to retrieve the system and accounting logs that this feature requires.

When you choose Auto Synchronization with Devices on the Feature Selector, the content pane shows information about each poller process and allows you to control them. You can also use this feature to purge old data from the events database.

You can configure the length of time that DCNM waits before polling a device again. By default, DCNM polls each managed device every 60 seconds. You can increase the length of time to a maximum of 300 seconds. For more information, see the "Configuring the Polling Interval" section on page 9-33.

DCNM polls devices concurrently; however, to avoid polling all devices simultaneously, DCNM begins polling devices in alphabetical device-name order and delays each polling process by a short, random amount of time.

Virtualization Support

DCNM treats each virtual device context (VDC) on an NX-OS device as a separate device. DCNM creates one poller process per device.

Licensing Requirements for Auto-Synchronization with Devices

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	Auto-synchronization with devices requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the *Cisco DCNM Licensing Guide*.

Prerequisites for Auto-Synchronization with Devices

The Auto-Synchronization with Devices feature has the following prerequisites:

- The DCNM server must be able to connect to the devices.
- The NX-OS device must be running a supported version of NX-OS.
- The NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "NX-OS Device Preparation" section on page 9-2.

Guidelines and Limitations for Auto-Synchronization with Devices

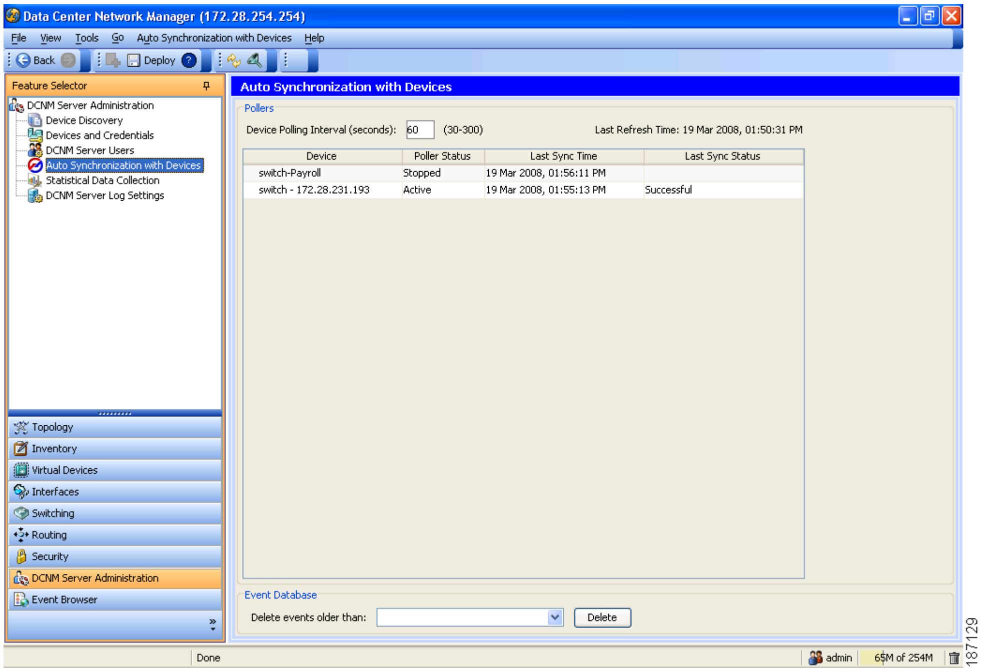
Auto-synchronization with devices has the following configuration guidelines and limitations:

- We recommend that you use the default device polling interval unless you encounter issues with synchronization due to slow response from devices or to managing many devices. For more information, see the "Configuring the Polling Interval" section on page 9-33.
- For the Auto-Synchronization with Devices feature, the client does not automatically update the information shown in the Summary pane. To ensure that you are viewing current information, from the menu bar, choose **View > Refresh**.

Configuring Device Auto-Synchronization

Figure 9-5 shows the Auto-Synchronization with Devices content pane.

Figure 9-5 Auto-Synchronization with Devices Content Pane



Device Polling Interval (seconds): 60 (30-300)

Last Refresh Time: 19 Mar 2008, 01:50:31 PM

Device	Poller Status	Last Sync Time	Last Sync Status
switch-Payroll	Stopped	19 Mar 2008, 01:56:11 PM	
switch - 172.28.231.193	Active	19 Mar 2008, 01:55:13 PM	Successful

Delete events older than:

This section includes the following topics:

Starting and Stopping a Poller

You can start and stop a poller for a device. When a poller is stopped, auto-synchronization for the device does not occur.

DETAILED STEPS

To start or stop a poller, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

A table of pollers appears in the Contents pane. Each row corresponds to a poller for a particular device. Devices are listed alphabetically. The Poller Status field displays messages about whether the poller is running or is stopped.

Step 2 Click the poller that you want to start or stop.

Step 3 Do one of the following:

- To start a poller, from the menu bar, choose **Auto Synchronization with Devices > Start Poller**. The Poller Status field changes to Running.
- To stop a poller, from the menu bar, choose **Auto Synchronization with Devices > Stop Poller**. The Poller Status field changes to Stopped.

You do not need to save your changes.

Configuring the Polling Interval

You can configure how often DCNM automatically synchronizes with managed devices.

BEFORE YOU BEGIN

The default polling interval is 60 seconds.

Determine how often you want DCNM to perform auto-synchronization with managed devices. In general, consider the following:

- How often device configurations are changed by means other than DCNM, such as using the command-line interface of a device. If changes by means other than DCNM are common, consider using a short polling interval.
- How important it is to your organization that DCNM be up to date with managed device configurations. If up-to-date configuration information is important to your organization, consider using a short polling interval.

DETAILED STEPS

To configure the polling interval, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The device polling interval appears in the Contents pane, above the table of pollers.

Step 2 In the Device Polling Interval field, enter the number of seconds between auto-synchronizations for all devices. The default interval is 60 seconds. You can specify an interval between 30 and 300 seconds.

Step 3 From the menu bar, choose **File > Deploy** to save the polling interval.

Synchronizing with a Device

You can make DCNM synchronize with a device manually when you do not want to wait for the next auto-synchronization to occur.

Note If many configuration changes have occurred on the device since the last successful synchronization, consider performing device discovery instead of synchronization. For more information, see "Discovering a Device" section on page 9-12.

BEFORE YOU BEGIN

Ensure that you have either configured the device entry with unique device credentials or that DCNM can use the default device credentials to connect to the device. For more information, see the "Configuring Default Device Credentials" section on page 9-14.

DETAILED STEPS

To synchronize with a device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

A table of pollers appears in the Contents pane. Each row corresponds to a poller for a particular device. Devices are listed alphabetically.

Step 2 Click the device that you want DCNM to synchronize with.

Step 3 From the menu bar, choose **Auto Synchronization with Devices > Synchronize with Device**.

Synchronization begins.

To determine when the synchronization has finished, watch the Last Sync Status column. Typically, synchronization with a device occurs in less than 5 minutes.

You do not need to save your changes.

Deleting Data from the Events Database

You can delete data from the events database.

Note Events that you delete can no longer appear in the Events Browser or on a feature-specific Events tab.

BEFORE YOU BEGIN

Determine the date and time of the newest events data that you want to delete. When you follow the steps in this procedure, DCNM deletes all events that are older than the date and time that you select.

DETAILED STEPS

To delete data from the events database, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

The Events Database area appears in the Contents pane, below the table of pollers.

Step 2 From the Delete events older than drop-down list, choose the date and time of the newest event that you want to delete and click **OK**.

Step 3 Click **Delete**.

DCNM deletes all events older than the date and time that you specified.

Viewing the Status of Auto-Synchronization Pollers

To view the status of an auto-synchronization poller, from the Feature Selector pane, choose **DCNM Server Administration > Auto Synchronization with Devices**.

Poller status and information about the synchronization time and status appear in the Pollers area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Auto Synchronization with Devices" section on page 9-35.s

Field Descriptions for Auto Synchronization with Devices

This section includes the following field descriptions for the Auto Synchronization with Devices feature:

- Auto Synchronization with Devices Content Pane, page 9-36

Auto Synchronization with Devices Content Pane

Table 9-6 Auto Synchronization with Devices Content Pane

Field	Description
Pollers	
Device Polling Interval	Number of seconds that all pollers wait before the next attempt to synchronize with a device. The default value is 60 seconds. Valid values are from 30 to 300 seconds.
Last Refresh Time	*Display only.* Date and time that the client updated information shown on the Content pane.
Device	*Display only.* Name and IP address of the device for the corresponding poller.
Poller Status	*Display only.* Shows whether the poller is running or stopped. A running poller attempts to synchronize with the configuration and status information from its device at the frequency specified by the Device Polling Interval field.
Last Sync Time	*Display only.* Date and time that the poller last retrieved system and accounting log data from the device.
Last Sync Status	*Display only.* Shows whether the most recent synchronization attempt succeeded or failed. If synchronization failed, determine why DCNM failed to connect to the device. If necessary, rediscover the device.
Event Database	
Delete events older than	Specifies the date and time of the newest event to be deleted from the events database. There is no default value for this field.

Additional References

For additional information related to administering auto-synchronization with devices, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
Events	*Chapter 7, "Managing Events"*
Device discovery	*Administering Device Discovery, page 9-1*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Administering Statistical Data Collection

This section describes how to administer statistical data collection.

This section includes the following topics:

Information About Statistical Data Collection

You can use the Statistical Data Collection feature to control the statistics monitoring processes that you have created for one of the many device configuration features that support statistics. You can also use the Statistical Data Collection feature to delete unwanted statistical data.

When you choose Statistical Data Collection on the Feature Selector, the content pane shows information about each statistical collection and allows you to control them. You can also use this feature to purge old data from the statistical database.

You can configure the length of time that DCNM waits before retrieving statistical data from devices that it is monitoring. By default, DCNM retrieves statistical data from monitored device every 30 seconds. You can increase the length of time to a maximum of 4 minutes. For more information, see the "Configuring the Default Frequency of Statistical Data Retrieval" section on page 4-15.

Virtualization Support

DCNM treats each virtual device context (VDC) on an NX-OS device as a separate device. Statistical data collections contain statistics from objects within devices.

Licensing Requirements for Statistical Data Collection

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	Real-time monitoring requires no license. DCNM requires a LAN Enterprise license for the following features: • Maintaining a history of statistical data • Using overview charts For a complete explanation of the DCNM licensing scheme and how to obtain and apply licenses, see the *Cisco DCNM Licensing Guide*.

Prerequisites for Statistical Data Collection

Statistical data collection has the following prerequisites:

- The DCNM server must be able to connect to the devices.
- The NX-OS device must be running a supported version of NX-OS.
- The NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "NX-OS Device Preparation" section on page 9-2.

Guidelines and Limitations for Statistical Data Collection

Statistical data collection has the following configuration guidelines and limitations:

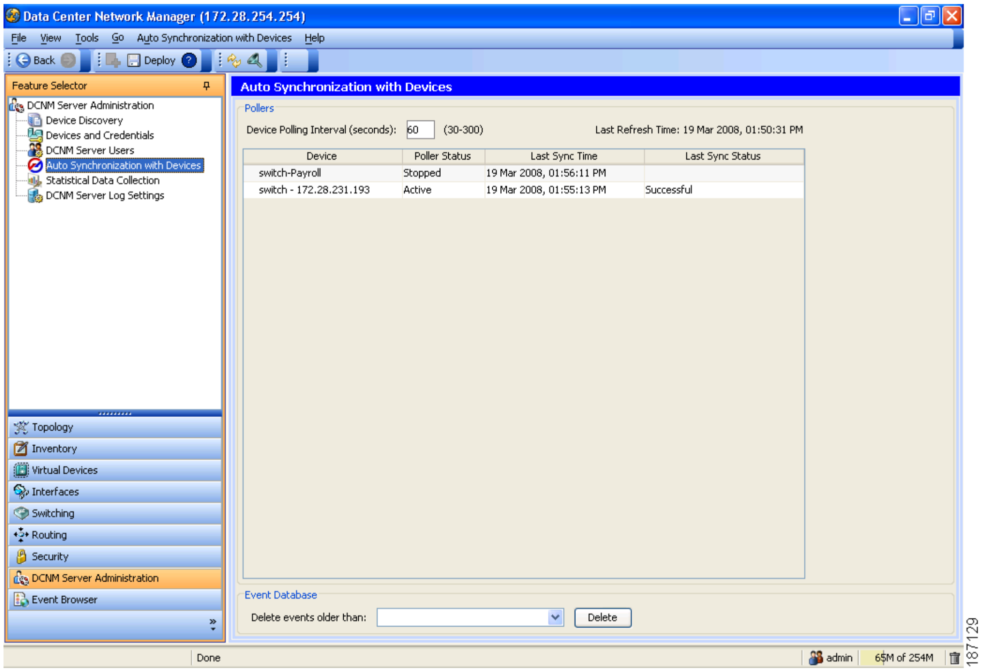
- Collections are created by starting monitoring for a new chart. For more information, see the "Starting Statistical Monitoring for a Chart" section on page 4-11.
- For the Statistical Data Collection feature, the DCNM client does not automatically update the information shown in the Summary pane. To ensure that you are viewing current information, from the menu bar, choose **View > Refresh**.
- When you start statistical monitoring for one or more charts and then close the DCNM client, a dialog box prompts you to decide whether to stop the collections or let them run. We recommend that you stop any unnecessary collections when you log out of the client. This conserves database space and decreases server load.

Send document comments to nexus7k-docfeedback@cisco.com

Configuring Statistical Data Collection

Figure 9-6 shows the Statistical Data Collection content pane.

Figure 9-6 Statistical Data Collection Content Pane



Device Polling Interval (seconds): 60 (30-300)

Last Refresh Time: 19 Mar 2008, 01:50:31 PM

Device	Poller Status	Last Sync Time	Last Sync Status
switch-Payroll	Stopped	19 Mar 2008, 01:56:11 PM	
switch - 172.28.231.193	Active	19 Mar 2008, 01:55:13 PM	Successful

Delete events older than:

This section includes the following topics:

- Starting and Stopping Statistical Data Collection, page 9-39
- Deleting Statistical Data from a Collection, page 9-40
- Deleting a Collection, page 9-40
- Deleting Data from the Statistics Database, page 9-41

Starting and Stopping Statistical Data Collection

You can use the Statistical Data Collection feature to start and stop a statistical data collection process. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

DETAILED STEPS

To start or stop a collection process, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

A table of statistical data collectors appears in the Contents pane. Each row corresponds to a collector for a particular device. The Status field displays whether the collector is running or is stopped.

Step 2 Click the collector that you want to start or stop.

Step 3 Do one of the following:

- To start a collector, from the menu bar, choose **Statistical Data Collection > Start Collection**. The Status field changes to Running.
- To stop a collector, from the menu bar, choose **Statistical Data Collection > Stop Collection**. The Status field changes to Stopped.

You do not need to save your changes.

Deleting Statistical Data from a Collection

You can delete statistical data from a collection. This feature allows you to delete all the data from a collection without affecting data from other collections and without deleting the collection itself. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

DETAILED STEPS

To delete statistical data from a collection, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

A table of statistical data collectors appears in the Contents pane. Each row corresponds to a collector for a particular device. Devices are listed alphabetically. The Status field displays whether the collector is running or is stopped.

Step 2 Right-click the collection.

Step 3 From the menu bar, choose **Statistical Data Collection > Delete Statistical Data**.

DCNM deletes all statistical data from the collection.

Deleting a Collection

You can delete a collection of statistical data from a specific device. Each collection process represents a statistical monitoring process that you created by starting monitoring for a device configuration feature.

Note If you want to delete all data from a collections rather than deleting the collection itself, perform the steps in the "Deleting Statistical Data from a Collection" section on page 9-40.

BEFORE YOU BEGIN

Determine which collection of data you want to delete.

DETAILED STEPS

To delete a collection of statistical data from a device, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

A table of statistical data collectors appears in the Contents pane. Devices are listed alphabetically. Each row corresponds to a collection of statistical data for a particular device.

Step 2 Click the collection of data that you want to delete.

Step 3 From the menu bar, choose **Statistical Data Collection > Delete Collection**.

The collection is deleted.

You do not need to save your changes.

Deleting Data from the Statistics Database

You can delete statistical data from the statistics database.

Note If you want to delete all data from a specific collection rather than deleting old data from all collections, perform the steps in the "Deleting a Collection" section on page 9-40.

BEFORE YOU BEGIN

Determine the date and time of the newest statistical data that you want to delete. When you follow the steps in this procedure, DCNM deletes all statistics that are older than the date and time that you select.

DETAILED STEPS

To delete data from the statistics database, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

The Statistics Database area appears in the Contents pane, below the table of statistical data collectors.

Step 2 From the Delete statistical data older than drop-down list, select the date and time of the newest statistics that you want to delete and click **OK**.

Step 3 Click **Delete**.

DCNM deletes all statistics older than the date and time that you specified.

Viewing the Status of Statistical Data Collectors

To view the status of statistical data collectors, from the Feature Selector pane, choose **DCNM Server Administration > Statistical Data Collection**.

Collector status and other information appear in the Statistical Data Collectors area in the Contents pane. For information about the fields that appear, see the "Field Descriptions for Statistical Data Collection" section on page 9-42.

Field Descriptions for Statistical Data Collection

This section includes the following field descriptions for the Statistical Data Collection feature:

- Statistical Data Collection Content Pane, page 9-42

Statistical Data Collection Content Pane

Table 9-7 Statistical Data Collection Content Pane

Field	Description
Statistical Data Collectors	
Last Refresh Time	*Display only.* Date and time that the client updated information shown on the Content pane.
Collector ID	*Display only.* Name and IP address of the device for the corresponding poller.
Owner	*Display only.* Username of the DCNM user who started monitoring for the chart that corresponds to the collection.
Device	*Display only.* Name and IP address of the device that is providing the statistical data in the collection.
Objects	*Display only.* Description of the entity on the device that is providing the statistical data in the collection. For example, if the collection has statistical data for a rule that is assigned the sequence number 10 and is in an IPv4 ACL named acl-01, this field displays acl-01,seqNo=10. If the collection has data for the Ethernet 1/5 port, this field displays Ethernet1/5.
Collected Statistics	*Display only.* Type of statistical data in the collection. For example, if the collection has statistical data for a rule in an IPv4 ACL, this field displays IpAclAceMatchStatistics.
Status	*Display only.* Shows whether the collector is started or stopped.
Statistics Database	
Delete statistical data older than	Specifies the date and time of the newest statistical data to be deleted from the statistics database. There is no default value for this field.

Additional References

For additional information related to administering statistical data collection, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
Device discovery	*Administering Device Discovery, page 9-1*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Administering DCNM Server Log Settings

This section describes how to administer DCNM server log settings.

This section includes the following topics:

Information About Administering DCNM Server Log Settings

The DCNM server maintains a log file of its operations. The log file contains information from DCNM features and server components.

Note The DCNM Server Log Settings feature does not affect logging levels of NX-OS devices. DCNM does not support the configuration of device logging levels.

Logging Levels

The DCNM server supports a hierarchy of logging levels, ordered by severity of log messages. Each level includes messages for that level in addition to all log messages from levels of higher severity. The logging levels, in order from highest to lowest severity, are as follows:

- Fatal Errors
- Errors
- Warnings

- Information
- Debugging
- Verbose

Log File and Location

The DCNM server writes server log messages to the sys.pipe file at the following location:

INSTALL_DIR\log

By default, when you install the DCNM server on Microsoft Windows Server 2003, INSTALL_DIR is C:\Program Files\Cisco Systems\DCNM.

Virtualization Support

DCNM server logs do not contain log messages from NX-OS devices; therefore, this feature has no effect on virtualization support.

Licensing Requirements for Administering DCNM Server Log Settings

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	DCNM server logging requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the *Cisco DCNM Licensing Guide*.

Prerequisites for Administering DCNM Server Log Settings

Administering DCNM server log settings has the following prerequisites:

- You should be familiar with a DCNM feature before you configure server log settings for it.

Guidelines and Limitations for Administering DCNM Server Log Settings

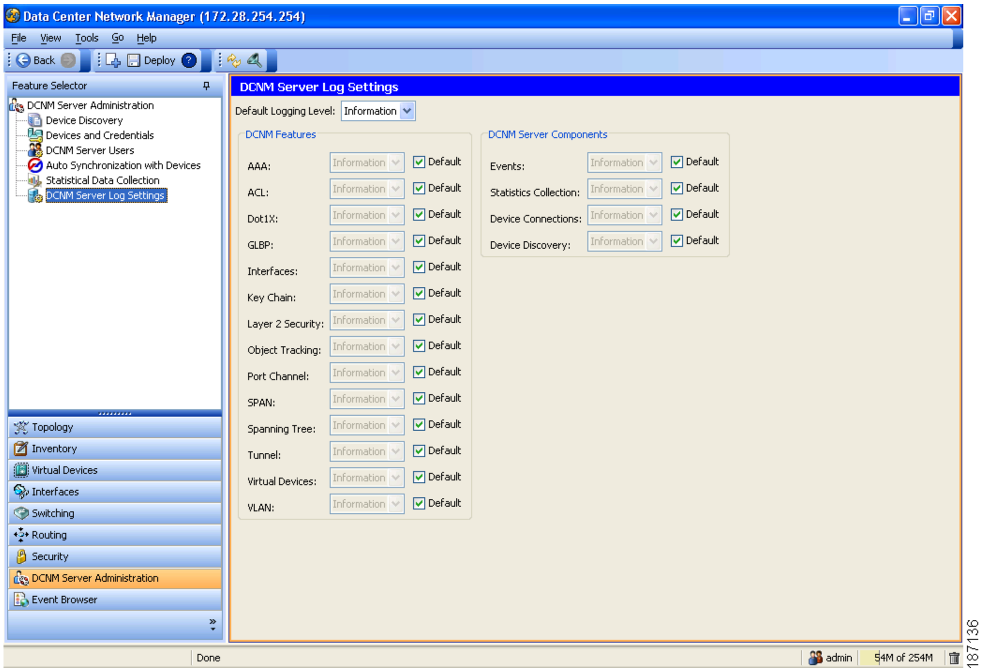
Administering DCNM server log settings has the following configuration guidelines and limitations:

- Setting a logging level to a lower severity results in more messages in the log file.
- We recommend using the default logging settings unless you are troubleshooting an issue.
- When you are troubleshooting an issue, consider lowering the logging level severity of the affected feature or server component.
- After you resolve an issue, consider restoring the logging level of the affected feature or server component to a higher severity.

Configuring DCNM Server Log Settings

Figure 9-7 shows the DCNM Server Log Settings content pane.

Figure 9-7 DCNM Server Log Settings Content Pane



DCNM Server Log Settings

Default Logging Level: Information

DCNM Features

AAA: Information ☑ Default
ACL: Information ☑ Default
Dot1X: Information ☑ Default
GLBP: Information ☑ Default
Interfaces: Information ☑ Default
Key Chain: Information ☑ Default
Layer 2 Security: Information ☑ Default
Object Tracking: Information ☑ Default
Port Channel: Information ☑ Default
SPAN: Information ☑ Default
Spanning Tree: Information ☑ Default
Tunnel: Information ☑ Default
Virtual Devices: Information ☑ Default
VLAN: Information ☑ Default

DCNM Server Components

Events: Information ☑ Default
Statistics Collection: Information ☑ Default
Device Connections: Information ☑ Default
Device Discovery: Information ☑ Default

This section includes the following topics:

- Configuring the Default Logging Level, page 9-45
- Configuring a Unique Logging Level for a Feature or Server Component, page 9-46

Configuring the Default Logging Level

You can configure the default logging level for all DCNM features and server components.

BEFORE YOU BEGIN

Determine what the default logging level should be. For more information, see the "Logging Levels" section on page 9-43.

DETAILED STEPS

To configure the default logging level for all DCNM features and server components, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The log settings appear in the Contents pane.

Step 2 From the Default Logging Level drop-down list, choose the logging level.

Step 3 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Configuring a Unique Logging Level for a Feature or Server Component

You can configure a logging level of a feature or server component that is independent of the default logging level.

BEFORE YOU BEGIN

Determine what the logging level of the feature or service should be. For more information, see the "Logging Levels" section on page 9-43.

DETAILED STEPS

To configure a unique logging level for a feature or server component, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The log settings appear in the Contents pane.

Step 2 Find the feature or server component that you want to configure with a unique logging level.

Step 3 Uncheck **Default** to the right of the feature or server component.

The logging level drop-down list for the feature or server component becomes available.

Step 4 From the logging level drop-down list, choose the logging level. For more information, see the "Logging Levels" section on page 9-43.

Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Configuring a Feature or Server Component to Use the Default Logging Level

You can configure a feature or server component to use the default logging level.

BEFORE YOU BEGIN

Ensure that the default logging level is appropriate for the feature or service. For more information, see the "Logging Levels" section on page 9-43.

DETAILED STEPS

To configure a feature or server component to use the default logging level, follow these steps:

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The log settings appear in the Contents pane.

Step 2 Find the feature or server component that you want to use the default logging level.

Step 3 Check **Default** to the right of the feature or service.

The logging level drop-down list for the feature or server component becomes unavailable.

Step 4 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM server.

Viewing DCNM Server Log Settings

To view DCNM server user accounts, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Server Log Settings**.

The default logging level, feature logging settings, and server component logging settings appear in the Contents pane. For information about the fields that appear, see the "Field Descriptions for DCNM Server Log Settings" section on page 9-47.

Field Descriptions for DCNM Server Log Settings

This section includes the following field descriptions for DCNM server log settings:

- DCNM Server Log Settings Content Pane, page 9-47

DCNM Server Log Settings Content Pane

Table 9-8 DCNM Server Log Settings Content Pane

Field	Description
Default Logging Level	Logging level for the features or server components whose Default check box is checked. The default value for this list is Informational. For more information about logging levels, see the "Logging Levels" section on page 9-43.
DCNM Features	
Default	Whether logging for the corresponding feature uses the default logging level or the logging level specified for the feature. When a Default check box is checked, the logging level list for the corresponding feature is unavailable. By default, these check boxes are unchecked.
AAA	Logging level for the AAA feature.
ACL	Logging level for the access control list feature.
Dot1X	Logging level for the 802.1x feature.
GLBP	Logging level for the Gateway Load-Balancing Protocol feature.
Interfaces	Logging level for the Interfaces feature.
Key Chain	Logging level for the keychain management feature.

Table 9-8 DCNM Server Log Settings Content Pane (continued)

Field	Description
Layer2 Security	Logging level for the layer 2 security feature, which are as follows: • Dynamic ARP inspection • Port security • DHCP snooping • IP Source Guard • Traffic storm control
Object Tracking	Logging level for the object tracking feature.
Port Channel	Logging level for the port security feature.
SPAN	Logging level for the SPAN feature.
Spanning Tree	Logging level for the STP feature.
Tunnel	Logging level for tunnel interface management feature.
Virtual Devices	Logging level for the virtual device context feature.
VLAN	Logging level for the VLAN feature.
DCNM Server Components	
Default	Whether logging for the corresponding server component uses the default logging level or the logging level specified for the component. When a Default check box is checked, the logging level list for the corresponding component is unavailable. By default, these check boxes are unchecked.
Event	Logging level for the event component, which includes messages about how DCNM processes the system and accounting logs it retrieves from devices and also events generated by DCNM.
Statistics Collection	Logging level for the statistical data collection component.
Device Connections	Logging level for the component that connects the DCNM server to devices.
Device Discovery	Logging level for the component that performs device discovery.

Additional References

For additional information related to administering DCNM server log settings, see the following sections:

- Related Documents, page 9-8
- Standards, page 9-8

Related Documents

Related Topic	Document Title
Troubleshooting DCNM	*Chapter 10, "Troubleshooting DCNM"*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—