CHAPTER 6

Administering Devices and Credentials

This chapter describes how to administer Cisco NX-OS devices and the credentials that are used by the Cisco Data Center Network Manager (DCNM) server to authenticate itself to the devices.

This chapter includes the following sections:

- Information About Devices and Credentials, page 6-1
- Licensing Requirements for Devices and Credentials, page 6-2
- Prerequisites for Administering Devices and Credentials, page 6-3
- Guidelines and Limitations for Devices and Credentials, page 6-3
- Configuring Devices and Credentials, page 6-3
- Viewing Device Credentials and Status, page 6-9
- Field Descriptions for Devices and Credentials, page 6-10
- Additional References for Devices and Credentials, page 6-11
- Feature History for Devices and Credentials, page 6-11

Information About Devices and Credentials

This section includes the following topics:

- Devices, page 6-1
- Credentials, page 6-2
- Device Status, page 6-2
- VDC Support, page 6-2

Devices

The Devices and Credentials feature allows you to administer the management state of devices. If the managed physical device supports virtual device contexts (VDCs), Cisco DCNM represents each VDC as a device. If you need to retrieve the running configuration and status information of a single VDC on a physical device with multiple VDCs, rather than performing device discovery for all the VDCs on the physical 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 ability to secure each managed device with different credentials. Cisco DCNM allows you to configure unique credentials for each discovered device or use 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 Cisco DCNM server user which means that the accounting logs on managed devices reflect the actions of each Cisco DCNM server user. If you log into the Cisco DCNM client as a user who does not have device credentials configured, the Cisco DCNM 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 Cisco 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—Cisco 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 possible only for devices that run a supported release of Cisco NX-OS and that are configured properly to support discovery by Cisco DCNM. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.
- Unmanaged—Cisco DCNM does not manage the device or monitor the status of the device.
- Unreachable—Cisco 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 Cisco DCNM server from contacting the device.
  - SSH is disabled on the device.
  - All terminal lines on the device are in use.

VDC Support

For devices that support VDCs, Cisco DCNM treats each VDC on a physical device as a separate device; therefore, Cisco DCNM can maintain unique credentials for each VDC on a device. Cisco 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
Cisco 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 information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.

Prerequisites for Administering Devices and Credentials

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

- The Cisco DCNM server must be able to connect to a device that you want to discover.
- Cisco NX-OS devices must be running a supported release of Cisco NX-OS. For information about supported releases of Cisco NX-OS, see the *Cisco DCNM Release Notes, Release 5.x*.
- The Cisco NX-OS device must have the minimal configuration that is required to enable device discovery to succeed. For more information, see the "Verifying the Discovery Readiness of a Cisco NX-OS Device" section on page 5-7.

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 5-1.
- Be careful when you change the default credentials or device-specific credentials. Incorrect credentials prevent Cisco DCNM from managing devices.

Configuring Devices and Credentials

This section includes the following topics:

- Adding a Device, page 6-3
- Discovering a Device, page 6-4
- Unmanaging a Device, page 6-5
- Deleting a Device, page 6-5
- Configuring Default Device Credentials, page 6-6
- Clearing Default Device Credentials, page 6-7
- Configuring Unique Credentials for a Device, page 6-7
- Clearing Unique Credentials for a Device, page 6-8

Adding a Device

You can add a device. After you add a device, you can discover it. For more information, see the "Discovering a Device" section on page 6-4.

BEFORE YOU BEGIN

Determine the IPv4 address for the device.

Determine whether Cisco 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 Cisco DCNM.

DETAILED 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 **Actions > 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 Cisco 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 Cisco 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, Cisco DCNM retrieves the running configuration of the device.

If you are rediscovering a device, the configuration data that Cisco DCNM retrieves replaces any existing configuration data for the device. Whenever the configuration data that Cisco 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 Cisco DCNM has for the device.

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 Cisco DCNM can use the default device credentials to connect to the device. For more information, see the "Configuring Default Device Credentials" section on page 6-6.

DETAILED 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 **Actions > 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 Cisco 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. Cisco DCNM cannot control the running configuration of an unmanaged device.

DETAILED 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 **Actions > 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 Cisco DCNM.

You should consider deleting devices that you do not intend to manage with Cisco DCNM. Additionally, if a network administrator of a device that supports VDCs uses the command-line interface of the device to delete a VDC, you should delete from Cisco DCNM the device that represented the VDC.

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

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 **Actions > 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 Cisco DCNM uses to authenticate itself when it connects to discovered Cisco NX-OS devices. Cisco 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 Cisco DCNM server user.

BEFORE YOU BEGIN

Determine what the default device credentials should be. All Cisco NX-OS devices that Cisco 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 Cisco 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

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 Cisco 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 Cisco 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 Cisco DCNM server.

Clearing Default Device Credentials

You can clear the default device credentials.

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

BEFORE YOU BEGIN

If you intend to use Cisco DCNM without default device credentials, you should ensure that Cisco 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 6-7.

DETAILED 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 Cisco 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, Cisco DCNM uses them when it connects to the device rather than using the default device credentials.

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

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

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 Cisco 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 Cisco 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 Cisco 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, Cisco DCNM uses the default credentials to connect to the device.

BEFORE YOU BEGIN

If you intend to operate Cisco DCNM without unique credentials for the device, you should ensure that Cisco DCNM is configured with default device credentials before you perform this procedure. For more information, see the "Configuring Default Device Credentials" section on page 6-6.

DETAILED 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 Cisco DCNM server.

Viewing Device Credentials and Status

To view the status for devices and whether credentials are configured for the device, 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.

The Reason field provides a brief message that explains the device status. The following table provides information about how to resolve the issue indicated by the message.

Reason	Resolution
Success	Not applicable. Cisco DCNM is managing the device.
Authentication failure	Ensure that the credentials are correct for the device. Ensure that Cisco DCNM can reach the device.
Unsupported platform	Verify that the device is a supported platform and that it is running a supported release of Cisco NX-OS. For information about supported platforms and Cisco NX-OS releases, see the *Cisco DCNM Release Notes, Release 5.x*.
Device sync up failure	Cisco Nexus 7000 Series devices only. The sequence numbers of accounting and system message log messages are not in a proper format. Clear the log files on the device and discover the device again.
Unmanaged manually	A Cisco DCNM user changed the device status to Unmanaged. Discover the device again.
Error when executing database query	Discover the device again. If the error reoccurs, clean the Cisco DCNM database. For more information about cleaning the database, see Chapter 17, “Maintaining the Cisco DCNM Database.”
Auto synchronization for device is disabled by user	Discover the device again.
Logging levels required by DCNM are not configured on the device	Discover the device again. For more information, see the “Automatic Logging-Level Configuration Support” section on page 5-4.

Reason	Resolution
Error in SSH connection	Ensure that SSH is enabled on the device and that it is functioning properly. Discover the device again.
Unreachable	Ensure that you specify the correct IP address for the device. Ensure that Cisco DCNM can contact the device. Discover the device again.
Discovery failed because server node stopped/crashed	Discover the device again.
Syslog messages logging disabled on device	Discover the device again.

For information about the fields that appear, see the "Field Descriptions for Devices and Credentials" section on page 6-10.

Field Descriptions for Devices and Credentials

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

- Device and Credentials Content Pane, page 6-10

Device and Credentials Content Pane

Table 6-1 Device and Credentials Content Pane

Field	Description
Default Credentials	
User Name	Name of the Cisco NX-OS device user account that the Cisco DCNM server uses to access any device that it is discovering or that it is managing. On the device, the user account must be assigned to the network-admin or vdc-admin role. 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 Cisco NX-OS device user account specified in the User Name field. By default, this field is blank.
Devices	
IP Address	*Display only.* IPv4 address of the Cisco NX-OS device.
Name	*Display only.* Name of the Cisco NX-OS device.
User Credentials	The Cisco NX-OS user account that Cisco DCNM uses to connect to the Cisco NX-OS device. **Note** If you configure this field, Cisco DCNM uses the user account that you configure when it connects to the device. If this field is blank, Cisco DCNM uses the user account specified in the Default Credentials area. By default, this field is blank.

Table 6-1 Device and Credentials Content Pane (continued)

Field	Description
Status	*Display only.* Whether the Cisco DCNM server can connect to and configure the device. Valid values are as follows: • Managed—The Cisco DCNM server can configure the device. • Unmanaged—The Cisco DCNM server cannot configure the device. • Unreachable—The Cisco DCNM server cannot reach the device.
Reason	*Display only.* Provides a brief explanation for the device status. For more information, see the "Viewing Device Credentials and Status" section on page 6-9.

Additional References for Devices and Credentials

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

- Related Documents, page 6-11
- Standards, page 6-11

Related Documents

Related Topic	Document Title
Cisco NX-OS XML management interface	*Cisco NX-OS XML Management Interface User Guide, Release 5.x*

Standards

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

Feature History for Devices and Credentials

Table 6-2 lists the release history for this feature.

Table 6-2 Feature History for Devices and Credentials

Feature Name	Releases	Feature Information
Reason field	5.0(2)	The Reason field was added to the Devices and Credentials feature.