CHAPTER 15

Administering DCNM-LAN Authentication Settings

This chapter describes how to administer Cisco Data Center Network Manager for LAN (DCNM-LAN) authentication settings.

Cisco DCNM authentication settings determine how a Cisco DCNM server authenticates users who attempt to access the server with the Cisco DCNM client. They also determine the user role for the user, which affects what the user can configure in the Cisco DCNM client.

As described in the following table, Cisco DCNM supports two user roles.

Cisco DCNM Role	Description
User	• Cannot change Cisco DCNM authentication mode • Cannot add or delete Cisco DCNM local user accounts • Can change the details of its own local user account • Can use all other features
Administrator	• Has full control of Cisco DCNM authentication settings • Can use all other features

This chapter includes the following sections:

Information About Administering DCNM-LAN Authentication Settings

DCNM-LAN authentication settings determine how a DCNM-LAN server authenticates users who attempt to access the server with the DCNM-LAN client. They also determine the user role for the user, which affects what the user can configure in the DCNM-LAN client.

This section contains the following topics:

Users and User Roles

DCNM-LAN implements user-based access to allow you to control who can access a DCNM-LAN server by using the DCNM-LAN client. User access is secured by a password. DCNM-LAN supports strong passwords.

When you ensure that each person who accesses DCNM-LAN has a unique user account, user-based access allows you to determine what actions are taken by each user.

In addition, DCNM-LAN allows you to assign a role to each user. Roles determine what actions a user can take in the DCNM-LAN client. As described in Table 15-1, DCNM-LAN supports two user roles.

Table 15-1 DCNM-LAN User Roles

DCNM-LAN Role	Description
User	• Cannot change DCNM-LAN authentication mode • Cannot add or delete DCNM-LAN local user accounts • Can change the details of its own local user account • Can use all other features
Administrator	• Has full control of DCNM-LAN authentication settings • Can use all other features

Local Authentication and DCNM-LAN Local Users

The DCNM-LAN database contains any DCNM-LAN local users that you create.

Note DCNM-LAN server users are local to the DCNM-LAN server. Creating, changing, and removing DCNM-LAN server users has no effect on user accounts on managed devices.

A DCNM-LAN server uses local users to grant access in the following cases:

- When the authentication mode is local
- When no authentication server for the current authentication mode is reachable.

You can use local authentication as the primary authentication mode. If you specify RADIUS or TACACS+ as the primary authentication mode, the DCNM-LAN server always falls back to local authentication if no authentication server for the current authentication mode is reachable.

Attribute Setup for External AAA using ACS 5.x

The steps for ACS 5.x TACACS+ are to essentially configure the following under Police Elements / Authorization and Permissions / Device Administration / Shell Profiles / shell profile name

- Attribute: cisco-av-pair
- Requirement: optional
- Value: shell:roles="network-admin"

RADIUS and TACACS+ Authentication

You can configure DCNM-LAN to authenticate users with either the RADIUS or TACACS+ AAA protocol.

DCNM-LAN supports primary, secondary, and tertiary authentication servers for RADIUS and TACACS+. Only a primary server is required. For each authentication server, you can specify the port number that the server listens to for authentication requests.

During authentication, if the primary server for the current authentication mode does not respond to the authentication request, the DCNM-LAN server sends the authentication request to the secondary server. If the secondary server does not respond, DCNM-LAN sends the authentication request to the tertiary server.

If none of the servers configured for the current authentication mode responds to an authentication request, the DCNM-LAN server falls back to local authentication.

User Role Assignment by RADIUS and TACACS+

DCNM-LAN supports the assignment of a user role by the RADIUS or TACACS+ server that grants a user access to the DCNM-LAN client. The user role assigned to a user is in effect for the current session in the DCNM-LAN client only.

To assign a DCNM-LAN user role by RADIUS, configure the RADIUS server to return the RADIUS vendor-specific attribute 26/9/1, which is the Cisco-AV-Pair attribute. To assign a DCNM-LAN user role by TACACS+, the TACACS+ server must return a cisco-av-pair attribute-value pair. If an authentication response does not assign the user role, DCNM-LAN assigns the User role. Table 15-2 shows the supported attribute-value pair values for each DCNM-LAN user role.

Table 15-2 DCNM-LAN User Role Assignment Values

DCNM-LAN Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell cisco-av-pair Value
User	`shell:roles = "network-operator"`	`cisco-av-pair:shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair:shell:roles="network-admin"`

Fallback to Local Authentication

Local authentication always is the fallback method for RADIUS and TACACS+ authentication modes. If none of the servers configured for the current authentication mode is available, the DCNM-LAN server uses the local database to authenticate login requests. This behavior is designed to help you prevent accidental lockout from DCNM-LAN.

For users who need fallback support, the usernames of their local user accounts must be identical to their usernames on the authentication servers. Also, we recommend that their passwords in the local user accounts should be identical to their passwords on the authentication servers in order to provide transparent fallback support. Because the user cannot determine whether an authentication server or the local database is providing the authentication service, using usernames and passwords on authentication servers that are different than the usernames and passwords in the local database means that the user cannot be certain which username and password should be given.

Password Recovery

If no one can log into the DCNM-LAN client as a user with a DCNM-LAN Administrator role, you can reset passwords by using one of the following scripts:

- For Microsoft Windows, use */user/local/cisco/dcm/fm/bin/adduser.bat*.
- For Linux, use */user/local/cisco/dcm/fm/bin/adduser.sh*.

To reset a password, run the script for the operating system that you are using, and then enter the user ID to be reset and the password to be used for it.

Alternatively, you can reinstall the DCNM-LAN server, which allows you to specify the username and password for a local user account that is assigned the Administrator role. For more information, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

Users and Device Credentials

Each DCNM-LAN server user has unique device credentials, regardless of whether the user authenticates with a local user account or an account on a RADIUS or TACACS+ server. This feature allows you to maintain accounting logs on managed devices that reflect the actions of each DCNM-LAN server user. For more information, see the "Information About Devices and Credentials" section on page 28-1.

Virtualization Support

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

DCNM-LAN server users can configure any managed device.

Licensing Requirements for Administering DCNM-LAN Authentication Settings

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM-LAN	Administering Cisco DCNM-LAN authentication settings requires no license. Any feature not included in a license package is bundled with the Cisco DCNM-LAN and is provided at no charge to you. For information about obtaining and installing a Cisco DCNM-LAN LAN Enterprise license, see the *Cisco DCNM Installation and Licensing Guide, Release 7.1.x*.

Prerequisites for Administering DCNM-LAN Authentication Settings

Administering DCNM-LAN authentication settings has the following prerequisites:

- You must ensure that every authentication server that you want to use with DCNM-LAN is configured to accept authentication requests from the DCNM-LAN server.
- To add, delete, or modify DCNM-LAN local users, you must be logged into the DCNM-LAN client with a user account that is assigned the Administrator DCNM-LAN role.

Guidelines and Limitations for Administering DCNM-LAN Authentication Settings

Administering DCNM-LAN authentication settings has the following configuration guidelines and limitations:

- Create a DCNM-LAN user account for each person who uses the DCNM-LAN client. Do not allow people to share a user account.
- Delete unused DCNM-LAN user accounts.
- Grant an administrator user account only to those who need to perform administrator tasks in the DCNM-LAN 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.

Configuring DCNM-LAN Authentication Settings

This section includes the following topics:

Configuring the Authentication Mode

Does this apply to API sessions, too? Or just the DCNM client?

You can configure the mode that the DCNM-LAN server uses to authenticate DCNM-LAN client users.

BEFORE YOU BEGIN

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

If you want to enable RADIUS or TACACS+ authentication mode, you must configure at least one authentication server for the desired authentication mode.

DETAILED STEPS

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

Step 2 If necessary, expand the Authentication Mode section.

Step 3 Choose the authentication mode.

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

Step 5 Restart the DCNM-LAN server. For more information, see the *Fundamentals Configuration Guide, Cisco DCNM for LAN, Release 7.1.x*.Chapter 25, "Starting and Stopping Cisco DCNM-LAN Servers."

RELATED TOPICS

- Adding a DCNM-LAN Local User, page 15-6
- Adding Authentication Servers, page 15-10

Adding a DCNM-LAN Local User

You can add a DCNM-LAN local user account.

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

BEFORE YOU BEGIN

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

Determine the username and password for the new DCNM-LAN local 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

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

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the Cisco DCNM Local Users section.

Step 3 From the menu bar, choose **Actions > 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 4 In the DCNM 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 5 (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-LAN local user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 6 In the DCNM Role column, double-click the entry and choose the role. By default, the role is User.

Step 7 In the Password column, double-click the entry and then click the down-arrow button.

Step 8 In the New 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 9 Click **OK**.

Step 10 (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-LAN server user account. The maximum length is 255 case-sensitive letters, numbers, and symbols.

Step 11 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.

RELATED TOPICS

- Changing the Password of a DCNM-LAN Local User, page 15-8
- Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8
- Deleting a DCNM-LAN Server User, page 15-9

Changing the Password of a DCNM-LAN Local User

You can change the password of a DCNM-LAN local user.

BEFORE YOU BEGIN

An Administrator role is required if you want to change the password of a local user account other than the account that you use to log into the DCNM-LAN client. If your user account is a local user account and it 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

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

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the DCNM Local Users section.

Step 3 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 4 In the Password column, double-click the entry and then click the down-arrow button.

Step 5 In the New 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 6 Click **OK**.

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

RELATED TOPICS

- Adding a DCNM-LAN Local User, page 15-6
- Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8
- Deleting a DCNM-LAN Server User, page 15-9

Changing the Full Name, Role, or Description of a DCNM-LAN Local User

You can change the full name, role, or description of a DCNM-LAN local user.

Note You cannot change the username. Instead, add a local user account with the desired username and remove the local 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 local user account other than the local user account that you use to log into the DCNM-LAN client. If your user account is a local user account and it has the User role, you can change the full name and description for your account only.

DETAILED STEPS

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

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the Cisco DCNM Local Users section.

Step 3 In the User Name column, click the username of the local user account that you want to change.

The row of the username that you clicked is highlighted.

Step 4 (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 5 (Optional) In the DCNM Role column, double-click the entry and choose the new role. You can choose Administrator or User.

Step 6 (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 7 From the menu bar, choose **File > Deploy** to apply your changes to the DCNM-LAN server.

RELATED TOPICS

- Adding a DCNM-LAN Local User, page 15-6
- Changing the Password of a DCNM-LAN Local User, page 15-8
- Deleting a DCNM-LAN Server User, page 15-9

Deleting a DCNM-LAN Server User

You can remove a DCNM-LAN local user account.

BEFORE YOU BEGIN

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

Ensure that you are removing the correct DCNM-LAN local user account.

DETAILED STEPS

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

Step 2 If necessary, expand the **DCNM Local Users** section.

A table of users appears in the DCNM Local Users section.

Step 3 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 4 From the menu bar, choose **Actions > Delete User**.

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

RELATED TOPICS

- Adding a DCNM-LAN Local User, page 15-6
- Changing the Password of a DCNM-LAN Local User, page 15-8
- Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8

Adding Authentication Servers

You can add RADIUS and TACACS+ servers to the DCNM-LAN authentication settings.

BEFORE YOU BEGIN

Note You must ensure that every authentication server that you want to use with DCNM-LAN is configured to accept authentication requests from the DCNM-LAN server.

Ensure that you have the following information about each authentication server that you want to add:

- AAA protocol: RADIUS or TACACS+
- Server IPv4 address or DNS name that can be resolved by the DCNM-LAN server.
- Secret key.
- Port number on which the server accepts authentication requests.
- (RADIUS only) Port number on which the server accepts accounting messages.
- Authentication protocol: PAP, CHAP, MSCHAP, or ASCII.
- (Optional) Username and password of a valid user account on the server for server verification.

Determine whether the server should be a primary, secondary, or tertiary server, which depends upon your authentication server failover strategy.

DETAILED STEPS

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

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 If necessary, expand the **RADIUS** or **TACACS+** server rows.

Step 4 For each authentication server that you want to add, follow these steps:

a. Choose the row in which you want to add the server.

Note The DCNM-LAN client does not allow you to add a secondary server if you have not added a primary server. In addition, you cannot add a tertiary server if you have not added a secondary server.

b. Double-click the **Server Name** field and enter the server IPv4 address or DNS hostname.

Note If you enter a hostname that the DCNM-LAN server cannot resolve, the Server Name field is highlighted in red.

c. Double-click the **Secret Key** field and enter the secret key (sometimes called a shared secret) of the authentication server.

d. (Optional) If you need to change the default Authentication Port or Accounting Port (RADIUS only), double-click the applicable port field and enter the new port number.

e. Double-click the **Authentication Method** field and choose the authentication protocol that DCNM-LAN must use when sending authentication requests to the authentication server.

Step 5 (Optional) If you want to verify that the DCNM-LAN server can authenticate a user with a new authentication server, follow these steps:

a. To the right of the row for the authentication server that you want to verify, click **Verify**.

A Verification dialog box appears.

b. Enter a username and password for a valid user account on the authentication server.

c. Click **Verify**.

The DCNM-LAN client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

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

RELATED TOPICS

- Configuring the Authentication Mode, page 15-6
- Changing Authentication Server Settings, page 15-11
- Removing an Authentication Server, page 15-12
- Verifying Authentication Server Settings, page 15-13

Changing Authentication Server Settings

You can change the settings for authentication servers that you have already configured in the DCNM-LAN client. If you have more than one RADIUS or TACACS+ server, you can change which server is primary, secondary, or tertiary.

DETAILED STEPS

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

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 If necessary, expand the **RADIUS** or **TACACS+** server rows.

Step 4 (Optional) If you want to change the settings of an authentication server, double-click each field that you need to change and enter the changes.

Step 5 (Optional) If you want to reorder RADIUS or TACACS+ servers, right-click a server and choose **Move Up** or **Move Down**, as needed.

Step 6 (Optional) If you want to verify that the DCNM-LAN server can authenticate a user with an authentication server, follow these steps:

a. To the right of the row for the authentication server that you want to verify, click **Verify**.

A Verification dialog box appears.

b. Enter a username and password for a valid user account on the authentication server.

c. Click **Verify**.

The DCNM-LAN client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

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

RELATED TOPICS

- Configuring the Authentication Mode, page 15-6
- Adding Authentication Servers, page 15-10
- Removing an Authentication Server, page 15-12
- Verifying Authentication Server Settings, page 15-13

Removing an Authentication Server

You can remove a RADIUS or TACACS+ authentication server from the DCNM-LAN authentication settings.

BEFORE YOU BEGIN

You cannot remove all authentication servers for the current authentication mode. Instead, change the authentication mode first and then remove all the authentication servers.

DETAILED STEPS

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

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 If necessary, expand the **RADIUS** or **TACACS+** server rows.

Step 4 Right-click the authentication server that you want to remove and choose **Remove Server**.

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

RELATED TOPICS

- Configuring the Authentication Mode, page 15-6
- Adding Authentication Servers, page 15-10
- Changing Authentication Server Settings, page 15-11
- Verifying Authentication Server Settings, page 15-13

Viewing DCNM-LAN Local Users

To view DCNM-LAN server user accounts, from the Feature Selector pane, choose **DCNM Server Administration > DCNM Authentication Settings** and then, if necessary, expand the Cisco DCNM Local Users section.

DCNM-LAN 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-LAN Authentication Settings" section on page 15-14.

RELATED TOPICS

- Adding a DCNM-LAN Local User, page 15-6
- Changing the Password of a DCNM-LAN Local User, page 15-8
- Changing the Full Name, Role, or Description of a DCNM-LAN Local User, page 15-8
- Deleting a DCNM-LAN Server User, page 15-9

Verifying Authentication Server Settings

You can verify that the DCNM-LAN server can authenticate a user with a particular authentication server that you have configured.

DETAILED STEPS

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

Step 2 If necessary, expand the **Authentication Servers** section.

The Authentication Server Settings table shows RADIUS and TACACS+ server settings.

Step 3 Click **Verify**.

A Verification dialog box appears.

Step 4 Enter a username and password for a valid user account on the authentication server.

Step 5 To the right of the row for the authentication server that you want to verify, click **Verify**.

The DCNM-LAN client displays a message indicating whether the verification attempt succeeded or failed. A verification failure may mean that the authentication server is unavailable or that the authentication settings are incorrect.

RELATED TOPICS

- Adding Authentication Servers, page 15-10
- Removing an Authentication Server, page 15-12
- Verifying Authentication Server Settings, page 15-13

Field Descriptions for DCNM-LAN Authentication Settings

This section includes the following field descriptions for the DCNM-LAN Authentication Settings feature:

- Authentication Mode Section, page 15-14
- DCNM-LAN Local Users Section, page 15-15
- Authentication Servers Section, page 15-15

Authentication Mode Section

Table 15-3 Authentication Mode Section

Field	Description
Local	Whether DCNM-LAN authenticates users with the local user database only.
RADIUS	Whether DCNM-LAN authenticates users with a RADIUS server. When no configured RADIUS server is reachable, DCNM-LAN falls back to using the local database for user authentication.
TACACS+	Whether DCNM-LAN authenticates users with a TACACS+ server. When no configured TACACS+ server is reachable, DCNM-LAN falls back to using the local database for user authentication.

DCNM-LAN Local Users Section

Table 15-4 DCNM-LAN Local Users Section

Field	Description
DCNM-LAN User Name	*Display only.* Name of the DCNM-LAN server user account. This name can be used to log into the DCNM-LAN client when the authentication mode is local or when no authentication server for the current authentication mode is reachable. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. The minimum length is 1 character. The maximum length is 198 characters.
Full Name	Other name for the user account, such as the name of the person who uses the DCNM-LAN server user account. This name cannot be used to log into the DCNM-LAN client. Valid characters are all letters, numbers, and symbols. The maximum length is 255 characters. This field is blank by default.
DCNM-LAN Role	Role of the user account. Valid values are User and Administrator. For more information, see Table 15-1. By default, a DCNM-LAN server user account is assigned the role of User.
Password	Password for the DCNM-LAN server user. This field is always masked for security. Entries are case sensitive. Valid characters are all letters, numbers, and symbols. The minimum length is 1 character. The maximum length is 255 characters.
Description	Description of the DCNM-LAN server user. Valid characters are all letters, numbers, and symbols. The maximum length is 255 characters. This field is blank by default.

Authentication Servers Section

Table 15-5 Authentication Servers Section

Field	Description
Server Name	DNS name or IPv4 address of the authentication server. • DNS name—If you specify a DNS name, the DCNM-LAN server must be able to resolve the IP address of the server. Valid DNS names characters are alphanumeric. • IPv4 address—If you specify an IP address, valid entries are in dotted decimal format.
Secret Key	Shared secret of the authentication server. Valid entries are case-sensitive letters, numbers, and symbols.
Authentication Port	TCP or UDP port number that the authentication server listens to for authentication requests. By default, the authentication port for a RADIUS server is UDP port 1812 and the authentication port for a TACACS+ server is TCP port 49.

Table 15-5 Authentication Servers Section (continued)

Field	Description
Accounting Port	UDP port number that the RADIUS authentication server listens to for authentication requests. By default, the accounting port for a RADIUS server is UDP port 1813.
Authentication Method	Authentication protocol that the DCNM-LAN server uses in authentication requests to the authentication server. Supported authentication methods are as follows: • PAP • CHAP • MSCHAP • ASCII

Additional References

For additional information related to administering DCNM-LAN authentication settings, see the following sections:

- Related Documents, page 15-16
- Standards, page 15-16

Related Documents

Related Topic	Document Title
Logging into the DCNM-LAN client	*Opening the DCNM-LAN Client, page 14-8*

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.	—

Feature History for DCNM-LAN Authentication Settings

Table 15-6 lists the release history for this feature.

Table 15-6 Feature History for DCNM-LAN Server Users

Feature Name	Releases	Feature Information
DCNM-LAN Authentication Settings	5.0(2)	No change from Release 4.2.