



CHAPTER 3

Configuring RADIUS

This chapter describes how to configure Remote Access Dial-In User Service (RADIUS) protocol on NX-OS devices.

This chapter includes the following sections:

- [Information About RADIUS, page 3-1](#)
- [Licensing Requirements for RADIUS, page 3-4](#)
- [Prerequisites for RADIUS, page 3-5](#)
- [Guidelines and Limitations, page 3-5](#)
- [Configuring RADIUS Servers, page 3-5](#)
- [Displaying RADIUS Server Statistics, page 3-17](#)
- [Where to Go Next, page 3-18](#)
- [Field Descriptions for RADIUS Server Groups and Servers, page 3-18](#)
- [Additional References, page 3-20](#)

Information About RADIUS

The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco NX-OS devices and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

This section includes the following topics:

- [RADIUS Network Environments, page 3-1](#)
- [RADIUS Operation, page 3-2](#)
- [Vendor-Specific Attributes, page 3-3](#)
- [Virtualization Support, page 3-4](#)

RADIUS Network Environments

RADIUS can be implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Send document comments to nexus7k-docfeedback@cisco.com.

You can use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor network devices, each supporting RADIUS. For example, network devices from several vendors can use a single RADIUS server-based security database.
- Networks already using RADIUS. You can add a Cisco NX-OS device with RADIUS to the network. This action might be the first step when you make a transition to a AAA server.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of the RADIUS access control and accounting software to meet special security and billing needs.
- Networks that support authentication profiles. Using the RADIUS server in your network, you can configure AAA authentication and set up per-user profiles. Per-user profiles enable the NX-OS device to better manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

RADIUS Operation

When a user attempts to log in and authenticate to an NX-OS device using RADIUS, the following process occurs:

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
 - ACCEPT—The user is authenticated.
 - REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
 - CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
 - CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

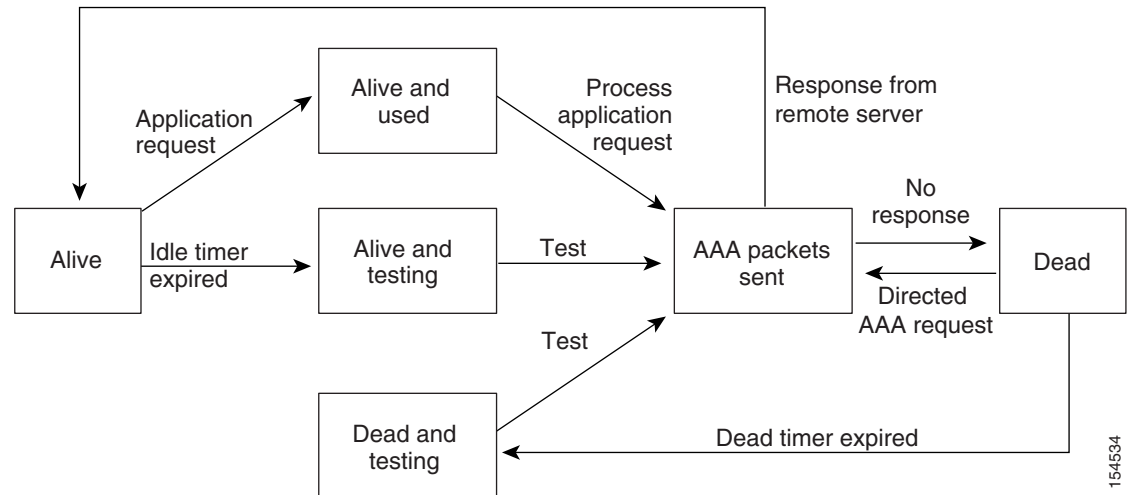
RADIUS Server Monitoring

An unresponsive RADIUS server can cause a delay in processing AAA requests. You can configure the NX-OS device to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The NX-OS device marks unresponsive RADIUS servers as dead and does not send AAA requests to any dead RADIUS servers. The NX-OS device periodically monitors the dead RADIUS servers and brings them to the alive state once they respond. This monitoring process

Send document comments to nexus7k-docfeedback@cisco.com.

verifies that a RADIUS server is in a working state before real AAA requests are sent its way. Whenever a RADIUS server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the NX-OS device displays an error message that a failure is taking place. See Figure 3-1.

Figure 3-1 RADIUS Server States



Note

The monitoring interval for alive servers and dead servers are different and can be configured by the user. The RADIUS server monitoring is performed by sending a test authentication request to the RADIUS server.

Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating VSAs between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named `cisco-av-pair`. The value is a string with the following format:

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use RADIUS servers for authentication on a Cisco NX-OS device, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Cisco NX-OS software:

- Shell—Protocol used in access-accept packets to provide user profile information.
- Accounting—Protocol used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

Send document comments to nexus7k-docfeedback@cisco.com.

The Cisco NX-OS software supports the following attributes:

- **roles**—Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space. For example, if the user belongs to roles `network-operator` and `vdc-admin`, the value field would be `"network-operator vdc-admin."` This subattribute, which the RADIUS server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute as supported by Cisco ACS:

```
shell:roles="network-operator vdc-admin"
```

```
shell:roles*"network-operator vdc-admin"
```

The following examples show the roles attribute as supported by FreeRADIUS:

```
Cisco-AVPair = "shell:roles=\"network-operator vdc-admin\""
```

```
Cisco-AVPair = "shell:roles*\"network-operator vdc-admin\""
```



Note

When you specify a VSA as `shell:roles*"network-operator vdc-admin"` or `"shell:roles*\"network-operator vdc-admin\""`, this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

- **accountinginfo**—Stores accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the switch. It can be used only with the accounting protocol data units (PDUs).

Virtualization Support

RADIUS configuration and operation are local to the virtual device context (VDC). For more information on VDCs, see the [Cisco DCNM Virtual Device Context Configuration Guide, Release 4.0](#).

The NX-OS device uses virtual routing and forwarding instances (VRFs) to access the RADIUS servers. For more information on VRFs, see the [Cisco DCNM Unicast Routing Configuration Guide, Release 4.0](#).

Licensing Requirements for RADIUS

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	RADIUS 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, Release 4.0 .
NX-OS	RADIUS requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0 .

Send document comments to nexus7k-docfeedback@cisco.com.

Prerequisites for RADIUS

RADIUS has the following prerequisites:

- Obtain IPv4 or IPv6 addresses or hostnames for the RADIUS servers.
- Obtain preshared keys from the RADIUS servers.
- Ensure that the NX-OS device is configured as a RADIUS client of the AAA servers.
- Ensure that the logging level for RADIUS in the NX-OS software is set to 5 using the command-line interface (CLI).

```
switch# configure terminal
switch(config)# logging level radius 5
```

Guidelines and Limitations

RADIUS has the following guidelines and limitations:

- You can configure a maximum of 64 RADIUS servers on the NX-OS device.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Configuring RADIUS Servers

This section includes the following topics:

- [RADIUS Server Configuration Process, page 3-6](#)
- [Adding RADIUS Server Hosts, page 3-8](#)
- [Deleting a RADIUS Server Host, page 3-9](#)
- [Configuring Global Preshared Keys, page 3-9](#)
- [Configuring RADIUS Server Preshared Keys, page 3-10](#)
- [Adding a RADIUS Server Group, page 3-11](#)
- [Adding a RADIUS Server Host to a RADIUS Server Group, page 3-11](#)
- [Deleting a RADIUS Server Host from a RADIUS Server Group, page 3-12](#)
- [Deleting a RADIUS Server Group, page 3-13](#)
- [Allowing Users to Specify a RADIUS Server at Login, page 3-13](#)
- [Configuring the Global RADIUS Transmission Retry Count and Timeout Interval, page 3-14](#)
- [Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server, page 3-14](#)
- [Configuring Accounting and Authentication Attributes for RADIUS Servers, page 3-15](#)
- [Configuring Periodic RADIUS Server Monitoring, page 3-15](#)
- [Configuring the Dead-Time Interval, page 3-16](#)
- [Deleting a RADIUS Server Host, page 3-17](#)

Send document comments to nexus7k-docfeedback@cisco.com.

RADIUS Server Configuration Process

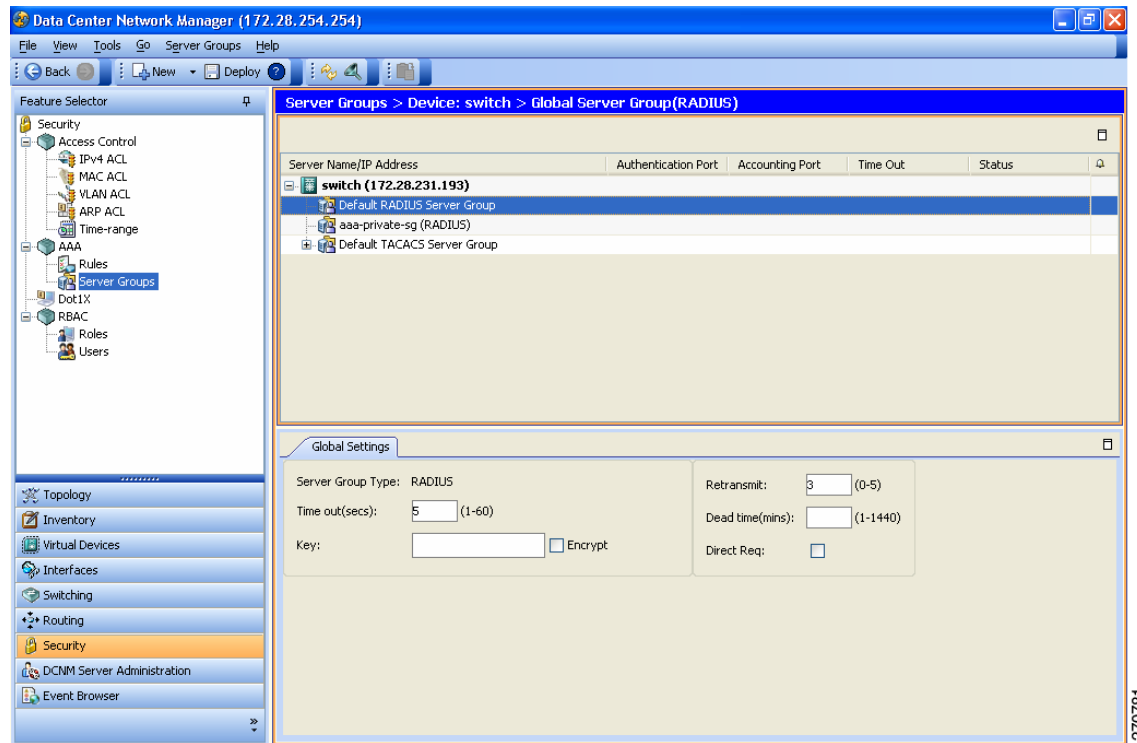
Follow these steps to configure RADIUS servers:

-
- Step 1** Establish the RADIUS server connections to the NX-OS device (see the [“Adding RADIUS Server Hosts” section on page 3-8](#)).
- Step 2** Configure the preshared secret keys for the RADIUS servers (see the [“Configuring Global Preshared Keys” section on page 3-9](#)).
- Step 3** If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods (see the [“Allowing Users to Specify a RADIUS Server at Login” section on page 3-13](#) and the [“Configuring AAA” section on page 2-7](#)).
- Step 4** If needed, configure any of the following optional parameters:
- Dead-time interval (see the [“Configuring the Dead-Time Interval” section on page 3-16](#)).
 - Allow specification of a RADIUS server at login (see the [“Allowing Users to Specify a RADIUS Server at Login” section on page 3-13](#)).
 - Transmission retry count and timeout interval (see the [“Configuring the Global RADIUS Transmission Retry Count and Timeout Interval” section on page 3-14](#)).
 - Accounting and authentication attributes (see the [“Configuring Accounting and Authentication Attributes for RADIUS Servers” section on page 3-15](#)).
- Step 5** If needed, configure periodic RADIUS server monitoring (see the [“Configuring Periodic RADIUS Server Monitoring” section on page 3-15](#)).
-

Send document comments to nexus7k-docfeedback@cisco.com.

Figure 3-2 shows the AAA Server Groups pane.

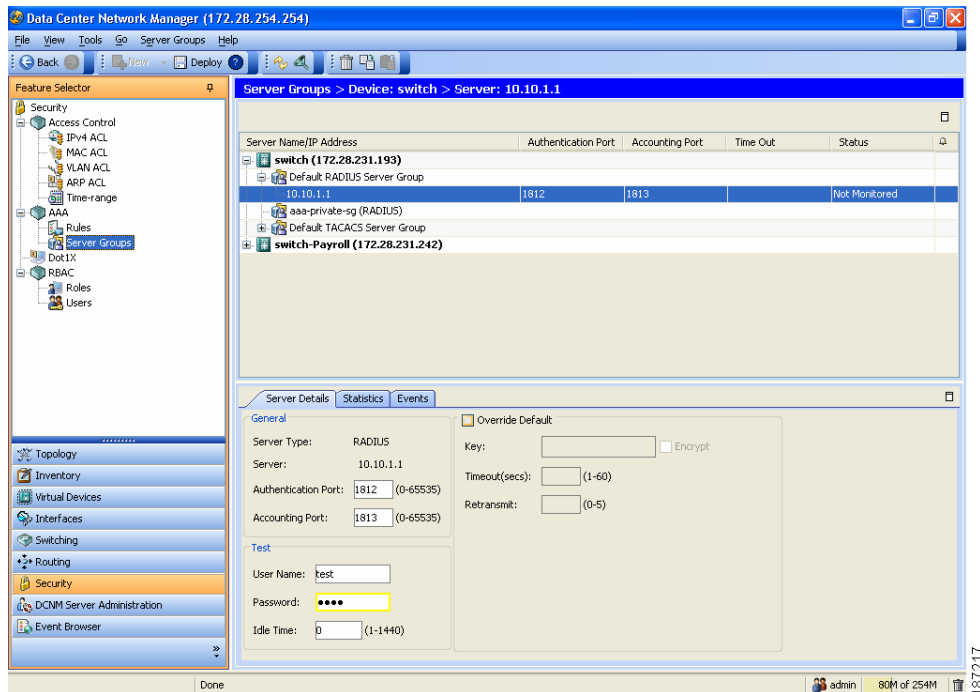
Figure 3-2 Server Groups Pane



Send document comments to nexus7k-docfeedback@cisco.com.

Figure 3-3 shows the Server Details tab.

Figure 3-3 Server Details Tab



Adding RADIUS Server Hosts

You must add the RADIUS server hosts and configure the IPv4 or IPv6 address or the hostname for each RADIUS server that you want to use for authentication. All RADIUS server hosts are added to the default RADIUS server group. You can add up to 64 RADIUS servers. See [Figure 3-3 on page 3-8](#).

DETAILED STEPS

To add a RADIUS server host, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
- Step 2** From the Summary pane, double-click the device to display the server groups.
- Step 3** Click **Default RADIUS Server Group**.
- Step 4** From the menu bar, choose **Server Groups > Add Server**.
The Server Details appear in the Details pane.
- Step 5** In the Server field, enter the RADIUS server IPv4 address, IPv6 address, or hostname in the Server field.
- Step 6** From the Server drop-down list, choose either the IPv4 address, IPv6 address, or hostname as the correct server identifier type.

Send document comments to nexus7k-docfeedback@cisco.com.

**Note**

If the server identifier format matches the identifier type selected, DCNM outlines the Server field in yellow to indicate that it is correct. If the server identifier format does not match the identifier type, DCNM outlines the Server field in red to indicate an error. Change the address or the address type to correct this problem.

- Step 7** (Optional) In the Authentication Port field, enter a new UDP port number or clear the field to disable authentication.
- The default authentication UDP port is 1812.
- Step 8** (Optional) In the Accounting Port field, enter a new UDP port number or clear the field to disable accounting.
- The default accounting UDP port is 1813.
- Step 9** (Optional) In the Test area, you can enter a username, password, and idle time interval in minutes for periodic server host monitoring.
- The default username is test, the default password is test, and the default idle time interval is 0 minutes, which disables periodic monitoring.
- Step 10** From the menu bar, choose **File > Deploy** to apply your changes to the device.

Deleting a RADIUS Server Host

You can delete a RADIUS server host from a server group.

DETAILED STEPS

To delete a RADIUS server host, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
- Step 2** From the Summary pane, double-click the device to display the server groups.
- Step 3** Double-click the server group to display the list of server hosts.
- Step 4** Click the RADIUS server host to delete.
- Step 5** From the menu bar, choose **Server Groups > Delete Server** and click **Yes** on the confirmation dialog.
- The RADIUS server host disappears from the list.
- Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring Global Preshared Keys

You can configure preshared keys at the global level for all servers used by the NX-OS device. A preshared key is a shared secret text string between the NX-OS device and the RADIUS server hosts. See [Figure 3-2 on page 3-7](#).

Send document comments to nexus7k-docfeedback@cisisco.com.

BEFORE YOU BEGIN

Obtain the preshared key values for the remote RADIUS servers.

DETAILED STEPS

To configure a global preshared key, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Click **Default RADIUS Server Group**.
 - Step 4** From the Details pane, click the **Global RADIUS Settings** tab.
 - Step 5** In the Key field, enter the preshared key.
 - Step 6** (Optional) Check **Encrypt** to encrypt the key.
The default is clear text.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring RADIUS Server Preshared Keys

You can configure preshared keys for a RADIUS server. A preshared key is a shared secret text string between the NX-OS device and the RADIUS server host. See [Figure 3-3 on page 3-8](#).

BEFORE YOU BEGIN

Configure one or more RADIUS server hosts (see the “[Adding RADIUS Server Hosts](#)” section on [page 3-8](#)).

Obtain the preshared key values for the remote RADIUS servers.

DETAILED STEPS

To configure a RADIUS server preshared key, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
 - Step 4** Click the desired RADIUS server.
 - Step 5** From the Details pane, click the **Server Details** tab.
 - Step 6** Check **Override Defaults**.
 - Step 7** In the Key field, enter the preshared key.
The default is the global preshared key.
 - Step 8** (Optional) Check **Encrypt** to encrypt the key.
The default is clear text.

Send document comments to nexus7k-docfeedback@cisco.com.

Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Adding a RADIUS Server Group

You can reference one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the RADIUS protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service. For information on AAA services, see the [“Remote AAA Services” section on page 2-2](#).

BEFORE YOU BEGIN

Configure one or more RADIUS server hosts (see the [“Adding RADIUS Server Hosts” section on page 3-8](#)).

DETAILED STEPS

To add a RADIUS server group, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.

Step 2 From the Summary pane, click the device.

Step 3 From the menu bar, choose **Server Groups > RADIUS Server Group**.

A new line appears at the end of the server group list for the device and the Details tab appears in the Details pane.

Step 4 In the Server Group Name field, enter the name and press the **Enter** key.

The server group name is a case-sensitive alphanumeric string with a maximum length of 127 characters.

Step 5 (Optional) In the Dead time(mins) field, enter the number of minutes for the dead-time interval.

The default dead-time interval is 0 minutes.

Step 6 In the VRF Name field, click the down arrow to display the VRF Name dialog and click a VRF. Click **OK**.

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

Adding a RADIUS Server Host to a RADIUS Server Group

You can add a RADIUS server host to a RADIUS server group.

BEFORE YOU BEGIN

Ensure that you have added the RADIUS server host to the Default RADIUS Server Group (see the [“Adding RADIUS Server Hosts” section on page 3-8](#)).

Send document comments to nexus7k-docfeedback@cisco.com.

DETAILED STEPS

To add a RADIUS server host to a RADIUS server group, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Click a RADIUS server group.
 - Step 4** From the menu bar, choose **Server Groups > Add Server**.
The Server Details appear in the Details pane.
 - Step 5** In the Server field, enter the RADIUS server IPv4 address, IPv6 address, or hostname in the Server field.
 - Step 6** From the Server drop-down list, choose either the IPv4 address, IPv6 address, or hostname as the correct server identifier type.



Note If the server identifier format matches the identifier type selected, DCNM outlines the Server field in yellow to indicate that it is correct. If the server identifier format does not match the identifier type, DCNM outlines the Server field in red to indicate an error. Change the address or the address type to correct this problem.

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

Deleting a RADIUS Server Host from a RADIUS Server Group

You can delete a RADIUS server host from a RADIUS server group.

DETAILED STEPS

To delete a RADIUS server host from a RADIUS server group, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Double-click the server group to display the list of server hosts.
 - Step 4** Click the RADIUS server host to delete.
 - Step 5** From the menu bar, choose **Server Groups > Delete Server** and click **Yes** on the confirmation dialog.
The RADIUS server host disappears from the list.
 - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to nexus7k-docfeedback@cisco.com.

Deleting a RADIUS Server Group

You can delete a RADIUS server group.

DETAILED STEPS

To delete a RADIUS server group, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the list of server groups.
 - Step 3** Click the RADIUS server group to delete.
 - Step 4** From the menu bar, choose **Server Groups > Delete Server Group** and click **Yes** in the confirmation dialog.
The server group disappears from the server group list.
 - Step 5** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Allowing Users to Specify a RADIUS Server at Login

By default, the NX-OS device forwards an authentication request based on the default AAA authentication method. You can configure the NX-OS device to allow the user to specify a VRF and RADIUS server to send the authenticate request by enabling the directed-request option. If you enable this option, the user can log in as *username@vrfname:hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured RADIUS server. See [Figure 3-2 on page 3-7](#).

**Note**

If you enable the directed-request option, the device uses only the RADIUS method for authentication and not the default local method.

**Note**

User-specified logins are supported only for Telnet sessions.

DETAILED STEPS

To allow users to specify a RADIUS server at login, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Click **Default RADIUS Server Group**.
 - Step 4** From the Details pane, click the **Global RADIUS Settings** tab.
 - Step 5** Click **Direct Req**.
 - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring the Global RADIUS Transmission Retry Count and Timeout Interval

You can configure a global retransmission retry count and timeout interval for all RADIUS servers. By default, a switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. The timeout interval determines how long the NX-OS device waits for responses from RADIUS servers before declaring a timeout failure. See [Figure 3-2 on page 3-7](#).

DETAILED STEPS

To configure the global RADIUS transmission retry count and timeout interval, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Click **Default RADIUS Server Group**.
 - Step 4** From the Details pane, click the **Global RADIUS Settings** tab.
 - Step 5** In the Retransmit field, enter a number of retransmit attempts.
The default is 1.
 - Step 6** In the Time out(secs) field, enter the number of seconds for the timeout interval.
The default is 5 seconds.
 - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server

By default, an NX-OS device retries a transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also set a timeout interval that the NX-OS device waits for responses from RADIUS servers before declaring a timeout failure. See [Figure 3-3 on page 3-8](#).

Configure one or more RADIUS server hosts (see the [“Adding RADIUS Server Hosts” section on page 3-8](#)).

DETAILED STEPS

To configure the transmission retry count and timeout interval for a RADIUS server, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
 - Step 4** Click the desired RADIUS server.
 - Step 5** From the Details pane, click the **Server Details** tab.
 - Step 6** Check **Override Defaults**.

Send document comments to nexus7k-docfeedback@cisco.com.

- Step 7** In the Retransmit field, enter the number of retransmit attempts.
The default is 1.
- Step 8** In the Timeout(secs) field, enter the number of seconds for the retransmission interval.
The default is 5 seconds.
- Step 9** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring Accounting and Authentication Attributes for RADIUS Servers

You can specify that a RADIUS server is to be used only for accounting purposes or only for authentication purposes. By default, RADIUS servers are used for both accounting and authentication. You can also specify the destination UDP port numbers where RADIUS accounting and authentication messages should be sent if there is a conflict with the default port. See [Figure 3-3 on page 3-8](#).

Configure one or more RADIUS server hosts (see the [“Adding RADIUS Server Hosts” section on page 3-8](#)).

DETAILED STEPS

To configure the authentication and accounting attributes for RADIUS servers, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
- Step 2** From the Summary pane, double-click the device to display the server groups.
- Step 3** Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
- Step 4** Click the desired RADIUS server.
- Step 5** From the Details pane, click the **Server Details** tab.
- Step 6** (Optional) In the Authentication Port field, enter a new UDP port number or clear the field to disable authentication.
The default authentication UDP port is 1812.
- Step 7** (Optional) In the Accounting Port field, enter a new UDP port number or clear the field to disable accounting.
The default accounting UDP port is 1813.
- Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring Periodic RADIUS Server Monitoring

You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the NX-OS device sends out a test packet. You can configure this option to test servers periodically. See [Figure 3-3 on page 3-8](#).

Send document comments to nexus7k-docfeedback@cisco.com.

**Note**

For security reasons, we recommend that you do not configure a test username that is the same as an existing user in the RADIUS database.

The test idle timer specifies the interval during which a RADIUS server receives no requests before the NX-OS device sends out a test packet.

**Note**

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the NX-OS device does not perform periodic RADIUS server monitoring.

Add one or more RADIUS server hosts (see the [“Adding RADIUS Server Hosts”](#) section on page 3-8).

DETAILED STEPS

To configure periodic RADIUS server monitoring, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
 - Step 4** Click the desired RADIUS server.
 - Step 5** From the Details pane, click the **Server Details** tab.
 - Step 6** In the User Name field, enter a username.
 - Step 7** In the Password field, enter a password.
 - Step 8** In the Idle Time field, enter the number of minutes for periodic monitoring.
 - Step 9** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Configuring the Dead-Time Interval

You can configure the dead-time interval for all RADIUS servers. The dead-time interval specifies the time that the NX-OS device waits after declaring a RADIUS server is dead, before sending out a test packet to determine if the server is now alive. The default value is 0 minutes. See [Figure 3-2 on page 3-7](#).

**Note**

When the dead-time interval is 0 minutes, RADIUS servers are not marked as dead even if they are not responding. You can configure the dead-time interval for a RADIUS server group (see the [“Adding a RADIUS Server Group”](#) section on page 3-11).

DETAILED STEPS

To configure the RADIUS dead-time interval, follow these steps:

-
- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.

Send document comments to nexus7k-docfeedback@cisco.com.

- Step 3** Click **Default RADIUS Server Group**.
 - Step 4** From the Details pane, click the **Global RADIUS Settings** tab.
 - Step 5** In the Dead time(mins) field, enter the number of minutes.
The default is 0 minutes.
 - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Deleting a RADIUS Server Host

You can delete a RADIUS server host from a RADIUS server group. See [Figure 3-3 on page 3-8](#).

BEFORE YOU BEGIN

Add one or more RADIUS server hosts (see the [“Adding RADIUS Server Hosts”](#) section on page 3-8).

DETAILED STEPS

To delete a RADIUS server host, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
 - Step 2** From the Summary pane, double-click the device to display the server groups.
 - Step 3** Click **Default RADIUS Server Group**.
 - Step 4** Click the desired RADIUS server.
 - Step 5** From the menu bar, choose **Server Groups > Delete Server**.
The RADIUS server disappears from the list of servers.
 - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
-

Displaying RADIUS Server Statistics

You can display the statistics that the NX-OS device maintains for RADIUS server activity.

Configure one or more RADIUS server hosts (see the [“Adding RADIUS Server Hosts”](#) section on page 3-8).

DETAILED STEPS

To display RADIUS server statistics, follow these steps:

- Step 1** From the Feature Selector pane, choose **Security > AAA > Server Groups**.
- Step 2** From the Summary pane, double-click the device to display the server groups.
- Step 3** Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
- Step 4** Click the desired RADIUS server.

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

Step 5 From the Details pane, click the **Statistics** tab.

Where to Go Next

You can now configure AAA authentication methods to include the RADIUS server groups (see [Chapter 2, “Configuring AAA”](#)).

Field Descriptions for RADIUS Server Groups and Servers

This section includes the following topics:

- [Security: AAA: Server Groups: Summary Pane, page 3-18](#)
- [Security: AAA: Server Groups: device: Default RADIUS Server Group: Global RADIUS Settings Tab, page 3-18](#)
- [Security: AAA: Server Groups: device: Default RADIUS Server Group: server: Server Details Tab, page 3-19](#)
- [Security: AAA: Server Groups: device: server group: Details Tab, page 3-19](#)

Security: AAA: Server Groups: Summary Pane

Table 3-1 *Security: AAA: Server Groups: Summary Pane*

Fields	Description
Authentication Port	UDP port number for authentication traffic for the servers. The default is 49.
Accounting Port	UDP port used for accounting for the servers.
Timeout	Number of seconds for the timeout interval for the servers. The default is 5 seconds.
Status	Status of the servers.

Security: AAA: Server Groups: device: Default RADIUS Server Group: Global RADIUS Settings Tab

Table 3-2 *Security: AAA: Server Groups: device: Default RADIUS Server Group: Global RADIUS Settings Tab*

Field	Description
Server Group Type	Server group type.
Time out(secs)	Number of seconds for the timeout interval. The default is 5 seconds.
Key	Preshared global key.
Retransmit	Number of retransmissions when the server does not respond.

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

Table 3-2 *Security: AAA: Server Groups: device: Default RADIUS Server Group: Global RADIUS Settings Tab (continued)*

Field	Description
Dead time(mins)	Number of minutes for the dead time interval. The default is 0 minutes.
Direct Req	Users can specify a RADIUS server at login.

Security: AAA: Server Groups: device: Default RADIUS Server Group: server: Server Details Tab

Table 3-3 *Security: AAA: Server Groups: device: Default RADIUS Server Group: Server: Server Details Tab*

Fields	Description
General	
Server Type	Server type.
Server	Server IPv4 address, IPv6 address, or alphanumeric name and the server name type.
Authentication Port	UDP port number for authentication traffic. The default is 1812.
Accounting Port	UDP port number for accounting traffic. The default is 1813.
Test	
User Name	Username for periodic monitoring of the RADIUS server.
Password	Password for periodic monitoring of the RADIUS server.
Idle Time	Number of minutes for the idle time interval for periodic monitoring of the RADIUS server. The default is 0, which disables periodic monitoring.
Override Default	Global values that you can override and configure for the RADIUS server. The default is to use the global values.
Key	Preshared server key for the RADIUS server.
Encrypt	Preshared server key encryption status. The default is clear text.
Timeout(secs)	Number of seconds for the timeout interval. The default is 5 seconds.
Retransmit	Number of retransmissions when the server does not respond. The default is 3.

Security: AAA: Server Groups: device: server group: Details Tab

Table 3-4 *Security: AAA: Server Groups: device: Default TACACS Server Group: server: Server Details Tab*

Fields	Description
Type	Displays RADIUS for the server group type.

Send document comments to nexus7k-docfeedback@cisco.com.

Table 3-4 Security: AAA: Server Groups: device: Default TACACS Server Group: server: Server Details Tab (continued)

Fields	Description
Server Group Name	Displays the server group name.
Dead time(mins)	Number of minutes for the dead-time interval for the server group. The default is 0 minutes.

Additional References

For additional information related to implementing RADIUS, see the following sections:

- [Related Documents, page 3-20](#)
- [Standards, page 3-20](#)
- [MIBs, page 3-20](#)

Related Documents

Related Topic	Document Title
NX-OS Licensing	Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0
DCNM Licensing	Cisco DCNM Licensing Guide, Release 4.0
VRF configuration	Cisco DCNM Unicast Routing Configuration Guide, Release 4.0

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.	—

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB 	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml