



## CHAPTER 4

# Configuring TACACS+

---

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on NX-OS devices.

This chapter includes the following sections:

- [Information About TACACS+, page 4-1](#)
- [Licensing Requirements for TACACS+, page 4-5](#)
- [Prerequisites for TACACS+, page 4-6](#)
- [Guidelines and Limitations, page 4-6](#)
- [Configuring TACACS+, page 4-6](#)
- [Displaying TACACS+ Statistics, page 4-19](#)
- [Where to Go Next, page 4-19](#)
- [Field Descriptions for TACACS+ Server Groups and Servers, page 4-19](#)
- [Additional References, page 4-21](#)

## Information About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to an NX-OS device. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure a TACACS+ server before the configured TACACS+ features on your NX-OS device are available.

TACACS+ provides for separate authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The TACACS+ client/server protocol uses TCP (TCP port 49) for transport requirements. Cisco NX-OS devices provide centralized authentication using the TACACS+ protocol.

This section includes the following topics:

- [TACACS+ Advantages, page 4-2](#)
- [TACACS+ Operation for User Login, page 4-2](#)
- [Default TACACS+ Server Encryption Type and Preshared Key, page 4-3](#)

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

- [TACACS+ Server Monitoring](#), page 4-3
- [Vendor-Specific Attributes](#), page 4-4
- [Virtualization Support](#), page 4-5

## TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the NX-OS device can authorize access without authenticating.
- Uses the TCP transport protocol to send data between the AAA client and server, making reliable transfers with a connection-oriented protocol.
- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

## TACACS+ Operation for User Login

When a user attempts a Password Authentication Protocol (PAP) login to an NX-OS device using TACACS+, the following actions occur:

1. When the NX-OS device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.



**Note** TACACS+ allows an arbitrary conversation between the daemon and the user until the daemon receives enough information to authenticate the user. This action is usually done by prompting for a username and password combination, but may include prompts for other items, such as mother's maiden name.

2. The NX-OS device will eventually receive one of the following responses from the TACACS+ daemon:
  - a. **ACCEPT**—User authentication succeeds and service begins. If the NX-OS device requires user authorization, authorization begins.
  - b. **REJECT**—User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.
  - c. **ERROR**—An error occurred at some time during authentication either at the daemon or in the network connection between the daemon and the NX-OS device. If the NX-OS device receives an ERROR response, the NX-OS device tries to use an alternative method for authenticating the user.

After authentication, the user also undergoes an additional authorization phase if authorization has been enabled on the NX-OS device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the NX-OS device again contacts the TACACS+ daemon and it returns an ACCEPT or REJECT authorization response. An ACCEPT response contains attributes that are used to direct the EXEC or NETWORK session for that user and determines the services that the user can access.

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

Services include the following:

- Telnet, rlogin, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services
- Connection parameters, including the host or client IP address (IPv4 or IPv6), access list, and user timeouts

## Default TACACS+ Server Encryption Type and Preshared Key

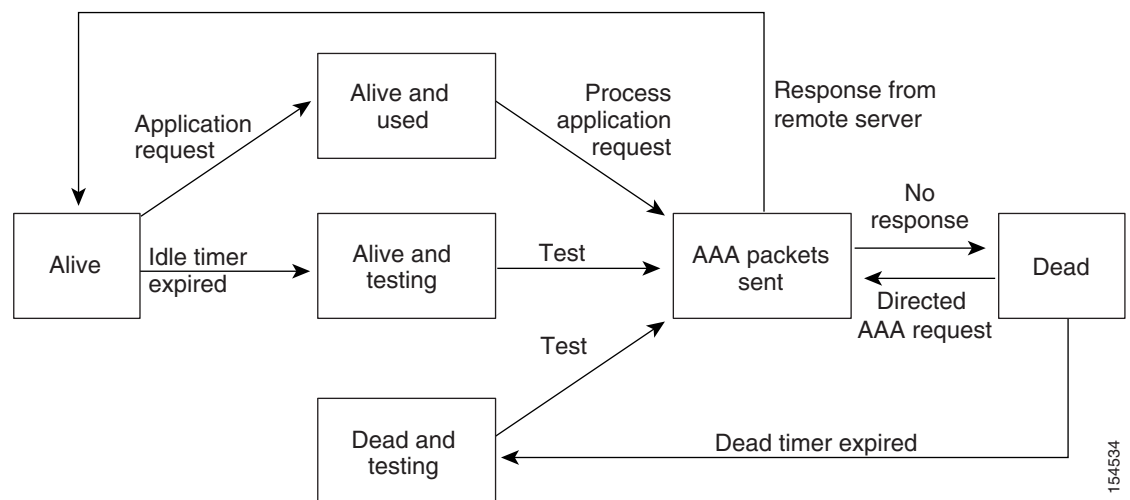
You must configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. A preshared key is a secret text string shared between the NX-OS device and the TACACS+ server host. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global preshared secret key for all TACACS+ server configurations on the NX-OS device to use.

You can override the global preshared key assignment by explicitly using the **key** option when configuring an individual TACACS+ server.

## TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. An NX-OS device can periodically monitor an TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The NX-OS device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. An NX-OS device periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. This process verifies that a TACACS+ server is in a working state before real AAA requests are sent its way. Whenever an TACACS+ 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 before it can impact performance. See [Figure 4-1](#).

**Figure 4-1** TACACS+ Server States



154534

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


**Note**

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

## Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the TACACS+ server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use.

This section includes the following topics:

- [Cisco VSA Format, page 4-4](#)
- [Cisco TACACS+ Privilege Levels, page 4-5](#)

### Cisco VSA Format

The Cisco TACACS+ implementation supports one vendor-specific option using the format recommended in the IETF 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 TACACS+ servers for authentication on a Cisco NX-OS device, the TACACS+ protocol directs the TACACS+ 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.

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 TACACS+ 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"
```

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



**Note** When you specify a VSA as 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 TACACS+ accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the TACACS+ client on the switch. It can be used only with the accounting protocol data units (PDUs).

## Cisco TACACS+ Privilege Levels

TACACS+ servers support privilege levels for specifying the permissions that users have when logging into an NX-OS device. For the maximum privilege level 15, the Cisco NX-OS software applies the network-admin role in the default VDC or the vdc-admin role for nondefault VDCs. All other privilege levels are translated to the vdc-operator role. For more information on user roles, see [Chapter 5, “Configuring RBAC.”](#)



**Note** If you specify a user role in the cisco-av-pair, that takes precedence over the privilege level.

## Virtualization Support

TACACS+ 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 TACACS+ servers. For more information on VRFs, see the [Cisco DCNM Unicast Routing Configuration Guide, Release 4.0](#).

## Licensing Requirements for TACACS+

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	TACACS+ 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 <a href="#">Cisco DCNM Licensing Guide, Release 4.0</a> .
NX-OS	TACACS+ 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 <a href="#">Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</a> .

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

## Prerequisites for TACACS+

TACACS+ has the following prerequisites:

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

```
switch# configure terminal
switch(config)# logging level tacacs+ 5
```

## Guidelines and Limitations

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ 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 TACACS+

This section includes the following topics:

- [TACACS+ Server Configuration Process, page 4-7](#)
- [Enabling TACACS+, page 4-9](#)
- [Adding TACACS+ Server Hosts, page 4-9](#)
- [Deleting a TACACS+ Server Host, page 4-10](#)
- [Configuring Global Preshared Keys, page 4-11](#)
- [Configuring TACACS+ Server Preshared Keys, page 4-11](#)
- [Adding a TACACS+ Server Group, page 4-12](#)
- [Adding a TACACS+ Server Host to a TACACS+ Server Group, page 4-13](#)
- [Deleting a TACACS+ Server Host from a TACACS+ Server Group, page 4-14](#)
- [Deleting a TACACS+ Server Group, page 4-14](#)
- [Specifying a TACACS+ Server at Login, page 4-14](#)
- [Configuring the Global TACACS+ Timeout Interval, page 4-15](#)
- [Configuring the Timeout Interval for a Server, page 4-16](#)
- [Configuring TCP Ports, page 4-16](#)
- [Configuring Periodic TACACS+ Server Monitoring, page 4-17](#)
- [Configuring the Dead-Time Interval, page 4-18](#)
- [Disabling TACACS+, page 4-18](#)

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

## TACACS+ Server Configuration Process

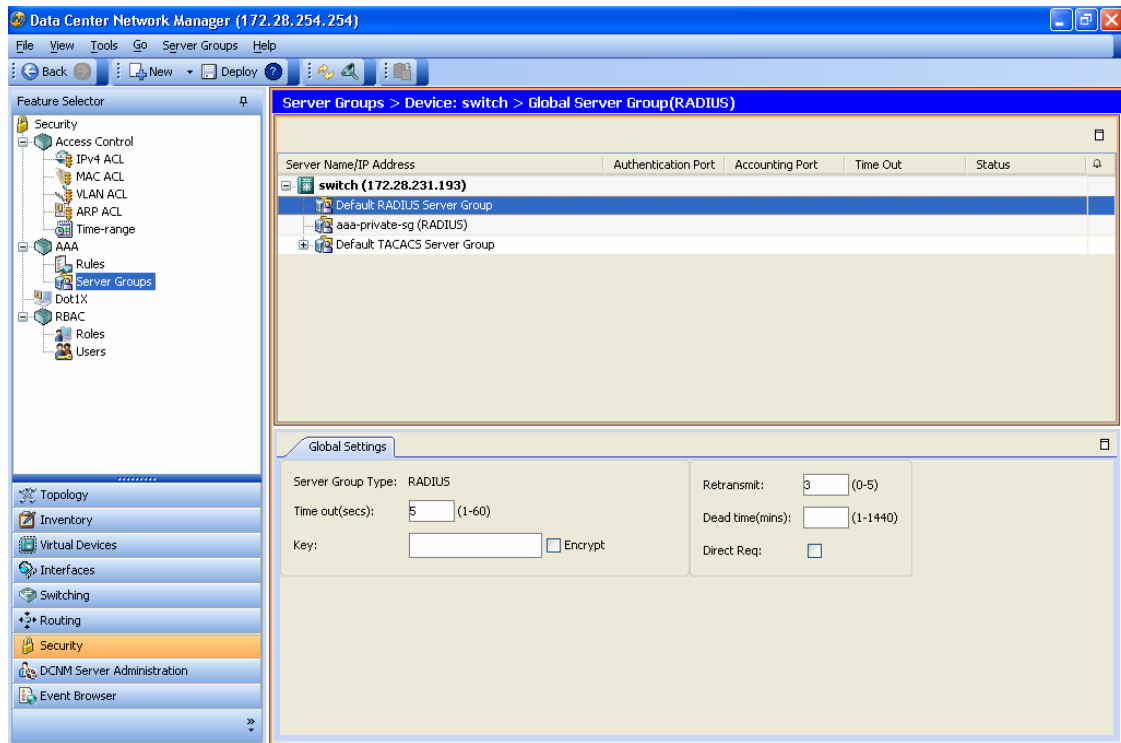
To configure TACACS+ servers, follow these steps:

- 
- Step 1** Enable TACACS+ (see the [“Enabling TACACS+”](#) section on page 4-9).
- Step 2** Establish the TACACS+ server connections to the NX-OS device (see the [“Adding TACACS+ Server Hosts”](#) section on page 4-9).
- Step 3** Configure the preshared secret keys for the TACACS+ servers (see the [“Configuring Global Preshared Keys”](#) section on page 4-11 and the [“Configuring TACACS+ Server Preshared Keys”](#) section on page 4-11).
- Step 4** If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods (see the [“Adding a TACACS+ Server Group”](#) section on page 4-12 and the [“Configuring AAA”](#) section on page 2-7).
- Step 5** If needed, configure any of the following optional parameters:
- Dead-time interval (see the [“Configuring the Dead-Time Interval”](#) section on page 4-18)
  - TACACS+ server specification allowed at user login (see the [“Specifying a TACACS+ Server at Login”](#) section on page 4-14).
  - Timeout interval (see the [“Configuring the Global TACACS+ Timeout Interval”](#) section on page 4-15).
  - TCP port (see the [“Configuring TCP Ports”](#) section on page 4-16).
- Step 6** If needed, configure periodic TACACS+ server monitoring (see the [“Configuring Periodic TACACS+ Server Monitoring”](#) section on page 4-17).
-

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

Figure 4-2 shows the AAA Server Groups pane.

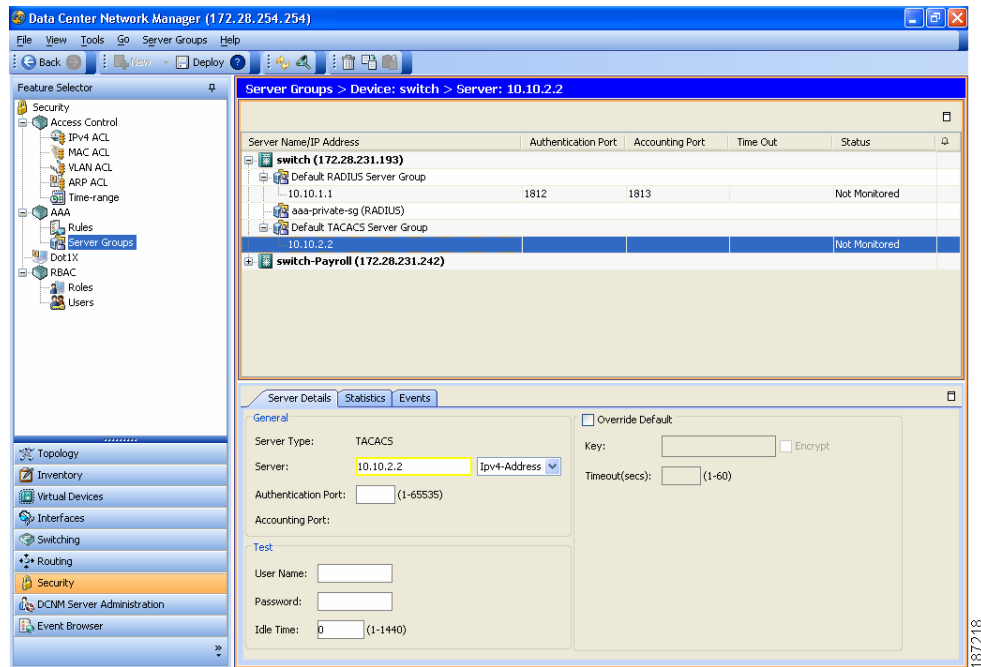
**Figure 4-2 Server Groups Pane**



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

Figure 4-3 shows the Server Details tab.

**Figure 4-3 Server Details Tab**



## Enabling TACACS+

By default, the TACACS+ feature is disabled on the device. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for authentication.

### DETAILED STEPS

To enable TACACS+, 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 > Enable TACACS**.
- Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the device.

## Adding TACACS+ Server Hosts

To access a remote TACACS+ server, you must add the TACACS+ server hosts and configure the IPv4 or IPv6 address or the hostname for the TACACS+ server on the device. All TACACS+ server hosts are added to the default TACACS+ server group. You can add up to 64 TACACS+ servers.

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

If a preshared key is not configured for a configured TACACS+ server, a warning message is issued if a global key is not configured. If a TACACS+ server key is not configured, the global key (if configured) is used for that server (see the “[Configuring Global Preshared Keys](#)” section on page 4-11 and the “[Configuring TACACS+ Server Preshared Keys](#)” section on page 4-11).


### **BEFORE YOU BEGIN**

Enable TACACS+ (see the “[Enabling TACACS+](#)” section on page 4-9).

Obtain the IPv4 or IPv6 addresses or the hostnames for the remote TACACS+ servers.

### **DETAILED STEPS**

To add a TACACS+ 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 TACACS Server Group**.
- Step 4** From the menu bar, choose **Server Groups > Add Server**.  
The Server Details appears in the Details pane.
- Step 5** In the Server field, enter the TACACS+ 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** (Optional) In the Authentication Port field, enter a new TCP port number or clear it to disable authentication.  
The default authentication TCP port is 49.
- Step 8** (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 9** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## **Deleting a TACACS+ Server Host**

You can delete a TACACS+ server host from a server group.

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

## DETAILED STEPS

To delete a TACACS+ 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 TACACS+ server host to delete.
  - Step 5** From the menu bar, choose **Server Groups > Delete Server** and click **Yes** on the confirmation dialog. The TACACS+ 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 device. A preshared key is a shared secret text string between the device and the TACACS+ server hosts. See [Figure 4-2 on page 4-8](#).

### BEFORE YOU BEGIN

Enable TACACS+ (see the “[Enabling TACACS+](#)” section on page 4-9).  
Obtain the preshared key values for the remote TACACS+ 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 TACACS Server Group**.
  - Step 4** From the Details pane, click the **Global TACACS 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 TACACS+ Server Preshared Keys

You can configure preshared keys for a TACACS+ server. A preshared key is a shared secret text string between the device and the TACACS+ server host. See [Figure 4-3 on page 4-9](#).

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

## BEFORE YOU BEGIN

Enable TACACS+ (see the “[Enabling TACACS+](#)” section on page 4-9).

Configure one or more TACACS+ server hosts (see the “[Adding TACACS+ Server Hosts](#)” section on page 4-9).

Obtain the preshared key values for the remote TACACS+ servers.

## DETAILED STEPS

To configure a TACACS+ 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 TACACS Server Group** to display the list of TACACS+ servers.
  - Step 4** Click the desired TACACS+ 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.
  - Step 9** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Adding a TACACS+ 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 TACACS+ 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

Enable TACACS+ (see the “[Enabling TACACS+](#)” section on page 4-9).

Configure one or more TACACS+ server hosts (see the “[Adding TACACS+ Server Hosts](#)” section on page 4-9).

## DETAILED STEPS

To add a TACACS+ 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.

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

- Step 3** From the menu bar, choose **Server Groups > TACACS 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 TACACS+ Server Host to a TACACS+ Server Group

You can add a TACACS+ server host to a TACACS+ server group.

### BEFORE YOU BEGIN

Ensure that you have added the TACACS+ server host to the Default TACACS+ Server Group (see the [“Adding TACACS+ Server Hosts”](#) section on page 4-9).

### DETAILED STEPS

To add a TACACS+ server host to a TACACS+ 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 TACACS+ 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 TACACS+ 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.
-

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

## Deleting a TACACS+ Server Host from a TACACS+ Server Group

You can delete a TACACS+ server host from a TACACS+ server group.

### DETAILED STEPS

To delete a TACACS+ server host from a TACACS+ 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 TACACS+ server host to delete.
  - Step 5** From the menu bar, choose **Server Groups > Delete Server** and click **Yes** on the confirmation dialog. The TACACS+ server host disappears from the list.
  - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Deleting a TACACS+ Server Group

You can delete a TACACS+ server group.

### DETAILED STEPS

To delete a TACACS+ 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 TACACS+ 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.
- 

## Specifying a TACACS+ Server at Login

You can configure the switch to allow the user to specify which TACACS+ server to send the authenticate request by enabling the directed-request option. By default, a device forwards an authentication request based on the default AAA authentication method. 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 TACACS+ server. See [Figure 4-2 on page 4-8](#).

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

**Note**

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

**Note**

User-specified logins are supported only for Telnet sessions.

**BEFORE YOU BEGIN**

Enable TACACS+ (see the [“Enabling TACACS+” section on page 4-9](#)).

**DETAILED STEPS**

To allow users to specify a TACACS+ 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 TACACS Server Group**.
  - Step 4** From the Details pane, click the **Global TACACS Settings** tab.
  - Step 5** Check **Direct Req.**
  - Step 6** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring the Global TACACS+ Timeout Interval

You can set a global timeout interval that the device waits for responses from all TACACS+ servers before declaring a timeout failure. The timeout interval determines how long the device waits for responses from TACACS+ servers before declaring a timeout failure. See [Figure 4-2 on page 4-8](#).

**BEFORE YOU BEGIN**

Enable TACACS+ (see the [“Enabling TACACS+” section on page 4-9](#)).

**DETAILED STEPS**

To configure the global TACACS+ 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 TACACS Server Group**.
  - Step 4** From the Details pane, click the **Global TACACS Settings** tab.
  - Step 5** In the Time out(secs) field, enter the number of seconds for the timeout interval.  
The default is 5 seconds.

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

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

---

## Configuring the Timeout Interval for a Server

You can set a timeout interval that the device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the device waits for responses from a TACACS+ server before declaring a timeout failure. See [Figure 4-3 on page 4-9](#).

Enable TACACS+ (see the [“Enabling TACACS+”](#) section on page 4-9).

Configure one or more TACACS+ server hosts (see the [“Adding TACACS+ Server Hosts”](#) section on page 4-9).

### DETAILED STEPS

To configure the timeout interval for a TACACS+ 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 TACACS Server Group** to display the list of TACACS+ servers.
  - Step 4** Click the desired TACACS+ server.
  - Step 5** From the Details pane, click the **Server Details** tab.
  - Step 6** Check **Override Defaults**.
  - Step 7** In the Timeout(secs) field, enter the number of seconds for the timeout interval.  
The default is 5 seconds.
  - Step 8** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, devices use port 49 for all TACACS+ requests. See [Figure 4-3 on page 4-9](#).

### BEFORE YOU BEGIN

Enable TACACS+ (see the [“Enabling TACACS+”](#) section on page 4-9).

Configure one or more TACACS+ server hosts (see the [“Adding TACACS+ Server Hosts”](#) section on page 4-9).

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

## DETAILED STEPS

To configure the authentication port for TACACS+ 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 TACACS Server Group** to display the list of TACACS+ servers.
  - Step 4** Click the desired TACACS+ server.
  - Step 5** From the Details pane, click the **Server Details** tab.
  - Step 6** In the Authentication Port field, enter a new TCP port number or clear it to disable authentication. The default authentication TCP port is 49.
  - Step 7** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

## Configuring Periodic TACACS+ Server Monitoring

You can monitor the availability of TACACS+ servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test. See [Figure 4-3 on page 4-9](#).



### Note

To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

The test idle timer specifies the interval in which a TACACS+ server receives no requests before the device sends out a test packet.



### Note

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

## BEFORE YOU BEGIN

Enable TACACS+ (see the [“Enabling TACACS+” section on page 4-9](#)).

Configure one or more TACACS+ server hosts (see the [“Adding TACACS+ Server Hosts” section on page 4-9](#)).

## DETAILED STEPS

To configure periodic TACACS+ 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 TACACS Server Group** to display the list of TACACS+ servers.

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

- Step 4** Click the desired TACACS+ 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 TACACS+ servers. The dead-time interval specifies the time that the device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive. See [Figure 4-2 on page 4-8](#).



### Note

When the dead-timer interval is 0 minutes, TACACS+ servers are not marked as dead even if they are not responding. You can configure the dead-timer per group (see the [“Adding a TACACS+ Server Group” section on page 4-12](#)).

---

### BEFORE YOU BEGIN

Enable TACACS+ (see the [“Enabling TACACS+” section on page 4-9](#)).

### DETAILED STEPS

To configure the 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.
  - Step 3** Click **Default TACACS Server Group**.
  - Step 4** From the Details pane, click the **Global TACACS 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.
- 

## Disabling TACACS+

You can disable TACACS+.



### Caution

When you disable TACACS+, all related configurations are automatically discarded.

---

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

## DETAILED STEPS

To disable TACACS+, 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 > Disable TACACS**.
  - Step 4** From the menu bar, choose **File > Deploy** to apply your changes to the device.
- 

# Displaying TACACS+ Statistics

You can display the statistics that the device maintains for TACACS+ activity.

## BEFORE YOU BEGIN

Enable TACACS+ (see the [“Enabling TACACS+”](#) section on page 4-9).

Configure one or more TACACS+ server hosts (see the [“Adding TACACS+ Server Hosts”](#) section on page 4-9).

## DETAILED STEPS

To display TACACS+ 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 TACACS Server Group** to display the list of TACACS+ servers.
  - Step 4** Click the desired TACACS+ server.
  - Step 5** From the Details pane, click the **Statistics** tab.
- 

## Where to Go Next

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

# Field Descriptions for TACACS+ Server Groups and Servers

This section includes the following topics:

- [Security: AAA: Server Groups: Summary Pane, page 4-20](#)
- [Security: AAA: Server Groups: device: Default TACACS Server Group: Global TACACS Settings Tab, page 4-20](#)

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

- [Security: AAA: Server Groups: device: Default TACACS Server Group: server: Server Details Tab, page 4-20](#)
- [Security: AAA: Server Groups: device: server group: Details Tab, page 4-21](#)

## Security: AAA: Server Groups: Summary Pane

**Table 4-1** Security: AAA: Server Groups: Summary Pane

Fields	Description
Authentication Port	TCP port number for authentication traffic for the servers. The default is 49.
Accounting Port	TCP port used for accounting for the RADIUS servers. The TACACS+ servers to use this field.
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 TACACS Server Group: Global TACACS Settings Tab

**Table 4-2** Security: AAA: Server Groups: server group: Default TACACS Server Group: Global TACACS Settings Tab

Field	Description
Server Group Type	TACACS+ for the server group type.
Time out(secs)	Number of seconds for the timeout interval. The default is 5 seconds.
Key	Preshared global key.
Dead time(mins)	Number of minutes for the dead time interface. The default is 0 minutes.
Direct Req	Users can specify a TACACS+ server at login.

## Security: AAA: Server Groups: device: Default TACACS Server Group: server: Server Details Tab

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

Fields	Description
<b>General</b>	
Server Type	TACACS+ for the server type.
Server	Server IPv4 address, IPv6 address, or alphanumeric name and the server name type.
Authentication Port	TCP port number for authentication traffic. The default is 49.

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

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

Fields	Description
Accounting Port	TCP port used for accounting.
<b>Test</b>	
User Name	Username for periodic monitoring of the TACACS+ server.
Password	Password for periodic monitoring of the TACACS+ server.
Idle Time	Number of minutes for the idle time interval for periodic monitoring of the TACACS+ server. The default is 0, which disables periodic monitoring.
Override Default	Global values that you can override and configure for the TACACS+ server. The default is to use the global values.
Key	Preshared server key for the TACACS+ 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.

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

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

Fields	Description
Type	TACACS+ server group type.
Server Group Name	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 TACACS+, see the following sections:

- [Related Documents, page 4-21](#)
- [Standards, page 4-22](#)
- [MIBs, page 4-22](#)

## Related Documents

Related Topic	Document Title
NX-OS Licensing	<a href="#">Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0</a>
DCNM Licensing	<a href="#">Cisco DCNM Licensing Guide, Release 4.0</a>
VRF configuration	<a href="#">Cisco DCNM Unicast Routing Configuration Guide, Release 4.0</a>

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

## 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"> <li>CISCO-AAA-SERVER-MIB</li> <li>CISCO-AAA-SERVER-EXT-MIB</li> </ul>	To locate and download MIBs, go to the following URL: <a href="http://www.cisco.com/public/sw-center/enigmatic/cant/mibs.shtml">http://www.cisco.com/public/sw-center/enigmatic/cant/mibs.shtml</a>