



# Configuring TACACS+

---

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

This chapter includes the following sections:

- [About TACACS+, on page 1](#)
- [Prerequisites for TACACS+, on page 5](#)
- [Guidelines and Limitations for TACACS+, on page 5](#)
- [Default Settings for TACACS+, on page 5](#)
- [One-Time Password Support, on page 6](#)
- [Configuring TACACS+, on page 6](#)
- [Monitoring TACACS+ Servers, on page 27](#)
- [Clearing TACACS+ Server Statistics, on page 28](#)
- [Verifying the TACACS+ Configuration, on page 28](#)
- [Configuration Examples for TACACS+, on page 29](#)
- [Where to Go Next , on page 30](#)
- [Additional References for TACACS+, on page 30](#)

## About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to a Cisco 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 Cisco 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.

## TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco 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 a Cisco NX-OS device using TACACS+, the following actions occur:




---

**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 your mother's maiden name.

---

1. When the Cisco NX-OS device establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.
2. The Cisco NX-OS device will eventually receive one of the following responses from the TACACS+ daemon:

### **ACCEPT**

User authentication succeeds and service begins. If the Cisco NX-OS device requires user authorization, authorization begins.

### **REJECT**

User authentication failed. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.

### **ERROR**

An error occurred at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco NX-OS device. If the Cisco NX-OS device receives an ERROR response, the Cisco 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 Cisco NX-OS device. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Cisco 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.

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 Secret Key

You must configure the TACACS+ secret key to authenticate the switch to the TACACS+ server. A secret key is a secret text string shared between the Cisco 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 secret key for all TACACS+ server configurations on the Cisco NX-OS device to use.

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

## Command Authorization Support for TACACS+ Servers

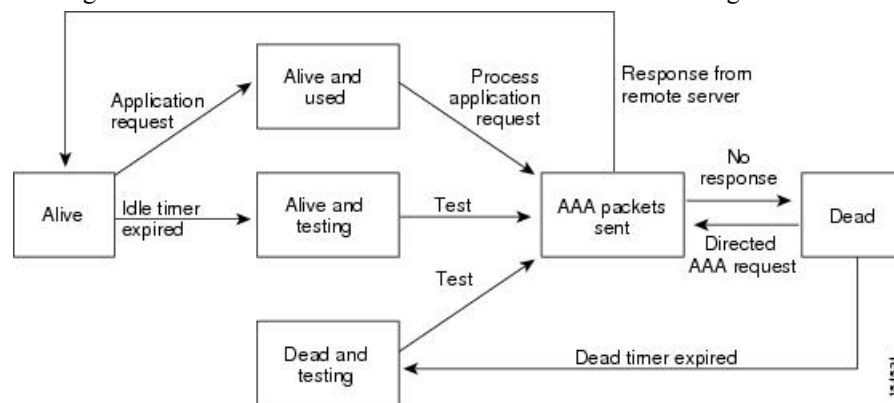
By default, command authorization is done against a local database in the Cisco NX-OS software when an authenticated user enters a command at the command-line interface (CLI). You can also verify authorized commands for authenticated users using TACACS+.

## TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests. A Cisco NX-OS device can periodically monitor a TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco NX-OS device marks unresponsive TACACS+ servers as dead and does not send AAA requests to any dead TACACS+ servers. A Cisco 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 a TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco NX-OS device displays an error message that a failure is taking place before it can impact performance.

**Figure 1: TACACS+ Server States**

This figure shows the server states for TACACS+ server monitoring.



### 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 for TACACS+

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.

### Cisco VSA Format for TACACS+

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, the 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 `network-admin`, the value field would be `network-operator network-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 network-admin
```

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




---

**Note** When you specify a VSA as `shell:roles*"network-operator network-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).

## Prerequisites for TACACS+

TACACS+ has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the TACACS+ servers.
- Obtain the secret keys from the TACACS+ servers, if any.
- Ensure that the Cisco NX-OS device is configured as a TACACS+ client of the AAA servers.

## Guidelines and Limitations for TACACS+

TACACS+ has the following guidelines and limitations:

- You can configure a maximum of 64 TACACS+ servers on the Cisco 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.
- Cisco recommends that you configure the dead-time interval if more than six servers are configured in a group. If you must configure more than six servers, make sure to set the dead-time interval to a value greater than 0 and enable dead server monitoring by configuring the test username and test password.
- Command authorization on TACACS+ servers is available for console sessions.
- For N9K-X9636C-R and N9K-X9636Q-R line cards and the N9K-C9508-FM-R fabric module, TACACS+ authentication fails for usernames with special characters.

## Default Settings for TACACS+

This table lists the default settings for TACACS+ parameters.

**Table 1: Default TACACS+ Parameters Settings**

Parameters	Default
TACACS+	Disabled
Dead timer interval	0 minutes
Timeout interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test

Parameters	Default
Periodic server monitoring password	test
Privilege level support for TACACS+ authorization	Disabled

## One-Time Password Support

A one-time password (OTP) is a password that is valid for a single login session or a transaction. OTPs avoid multiple disadvantages that are associated with the static passwords. OTPs are not at risk to replay attacks. If an intruder manages to record an OTP that was already used to log into a service or to conduct an operation, it cannot be misused because it is no longer valid.

OTPs are applicable only to the RADIUS and TACACS+ protocol daemons. For a RADIUS protocol daemon, you must ensure that you disable the ASCII authentication mode. For a TACACS+ protocol daemon, you must enable the ASCII authentication mode. To enable the ASCII authentication mode, use the **aaa authentication login ascii-authentication** command.

## Configuring TACACS+

This section describes how to configure TACACS+ on a Cisco NX-OS device.



**Note** If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

## TACACS+ Server Configuration Process

### Procedure

- Step 1** Enable TACACS+.
- Step 2** Establish the TACACS+ server connections to the Cisco NX-OS device.
- Step 3** Configure the secret keys for the TACACS+ servers.
- Step 4** If needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods.
- Step 5** (Optional) Configure the TCP port.
- Step 6** (Optional) If needed, configure periodic TACACS+ server monitoring.
- Step 7** (Optional) If TACACS+ distribution is enabled, commit the TACACS+ configuration to the fabric.

### Related Topics

[Enabling TACACS+](#) , on page 7

## Enabling TACACS+

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

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>feature tacacs+</b>  <b>Example:</b> switch(config)# <b>feature tacacs+</b>	Enables TACACS+.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	Exits configuration mode.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

## Configuring TACACS+ Server Hosts

To access a remote TACACS+ server, you must configure the IP address or the hostname for the TACACS+ server on the Cisco NX-OS device. You can configure up to 64 TACACS+ servers.



**Note** By default, when you configure a TACACS+ server IP address or hostname on the Cisco NX-OS device, the TACACS+ server is added to the default TACACS+ server group. You can also add the TACACS+ server to another TACACS+ server group.

### Before you begin

Enable TACACS+.

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

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> }  <b>Example:</b> switch(config)# <b>tacacs-server host</b> <b>10.10.2.2</b>	Specifies the IPv4 or IPv6 address or hostname for a TACACS+ server.
<b>Step 3</b>	(Optional) <b>show tacacs+</b> { <b>pending</b>   <b>pending-diff</b> }  <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	Displays the TACACS+ configuration pending for distribution.
<b>Step 4</b>	(Optional) <b>tacacs+ commit</b>  <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	Exits configuration mode.
<b>Step 6</b>	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	Displays the TACACS+ server configuration.
<b>Step 7</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config</b> <b>startup-config</b>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#) , on page 7

[Configuring TACACS+ Server Groups](#), on page 11

## Configuring Global TACACS+ Keys

You can configure secret TACACS+ keys at the global level for all servers used by the Cisco NX-OS device. A secret key is a shared secret text string between the Cisco NX-OS device and the TACACS+ server hosts.



**Before you begin**

Enable TACACS+.

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

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server key [0   6   7] key-value</b>  <b>Example:</b> <pre>switch(config)# tacacs-server key 0 QsEfThUkO</pre> <b>Example:</b> <pre>switch(config)# tacacs-server key 7 "fewhg"</pre>	<p>Specifies a TACACS+ key for all TACACS+ server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters.</p> <p>By default, no secret key is configured.</p> <p><b>Note</b> If you already configured a shared secret using the <b>generate type7_encrypted_secret</b> command, enter it in quotation marks, as shown in the second example. For more information, see <a href="#">Configuring the Shared Secret for RADIUS or TACACS+</a>.</p>
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
<b>Step 4</b>	(Optional) <b>show tacacs-server</b>  <b>Example:</b> <pre>switch# show tacacs-server</pre>	<p>Displays the TACACS+ server configuration.</p> <p><b>Note</b> The secret keys are saved in encrypted form in the running configuration. Use the <b>show running-config</b> command to display the encrypted secret keys.</p>
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#) , on page 7

[About AES Password Encryption and Primary Encryption Keys](#)

## Configuring a Key for a Specific TACACS+ Server

You can configure secret keys for a TACACS+ server. A secret key is a shared secret text string between the Cisco NX-OS device and the TACACS+ server host.

**Before you begin**

Enable TACACS+.

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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>key</b> [0   6   7] <i>key-value</i>  <b>Example:</b> <pre>switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg</pre> <b>Example:</b> <pre>switch(config)# tacacs-server host 10.10.1.1 key 7 "fewhg"</pre>	<p>Specifies a secret key for a specific TACACS+ server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters.</p> <p>This secret key is used instead of the global secret key.</p> <p><b>Note</b> If you already configured a shared secret using the <b>generate type7_encrypted_secret</b> command, enter it in quotation marks, as shown in the second example. For more information, see <a href="#">Configuring the Shared Secret for RADIUS or TACACS+</a>.</p>
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
<b>Step 4</b>	(Optional) <b>show tacacs-server</b>	Displays the TACACS+ server configuration.

	Command or Action	Purpose
	<b>Example:</b> <pre>switch# show tacacs-server</pre>	<b>Note</b> The secret keys are saved in encrypted form in the running configuration. Use the <b>show running-config</b> command to display the encrypted secret keys.
<b>Step 5</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

**Related Topics**

[About AES Password Encryption and Primary Encryption Keys](#)

## Configuring TACACS+ Server Groups

You can specify 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.

**Before you begin**

Enable TACACS+.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>aaa group server tacacs+ group-name</b>  <b>Example:</b> <pre>switch(config)# aaa group server tacacs+ TacServer switch(config-tacacs)#</pre>	Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.
<b>Step 3</b>	<b>server {ipv4-address   ipv6-address   hostname}</b>  <b>Example:</b> <pre>switch(config-tacacs)# server 10.10.2.2</pre>	Configures the TACACS+ server as a member of the TACACS+ server group.  If the specified TACACS+ server is not found, configure it using the <b>tacacs-server host</b> command and retry this command.

	Command or Action	Purpose
<b>Step 4</b>	<b>exit</b> <b>Example:</b> switch(config-tacacs+) # <b>exit</b> switch(config) #	Exits TACACS+ server group configuration mode.
<b>Step 5</b>	(Optional) <b>show tacacs-server groups</b> <b>Example:</b> switch(config) # <b>show tacacs-server groups</b>	Displays the TACACS+ server group configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config) # <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#) , on page 7

[Remote AAA Services](#)

[Configuring TACACS+ Server Hosts](#), on page 7

[Configuring the TACACS+ Dead-Time Interval](#), on page 20

## Configuring the Global Source Interface for TACACS+ Server Groups

You can configure a global source interface for TACACS+ server groups to use when accessing TACACS+ servers. You can also configure a different source interface for a specific TACACS+ server group. By default, the Cisco NX-OS software uses any available interface.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> switch(config)	Enters global configuration mode.
<b>Step 2</b>	<b>ip tacacs source-interface interface</b> <b>Example:</b> switch(config) # <b>ip tacacs source-interface mgmt 0</b>	Configures the global source interface for all TACACS+ server groups configured on the device.
<b>Step 3</b>	<b>exit</b> <b>Example:</b> switch(config) # <b>exit</b> switch#	Exits configuration mode.

	Command or Action	Purpose
<b>Step 4</b>	(Optional) <b>show tacacs-server</b> <b>Example:</b> switch# <b>show tacacs-server</b>	Displays the TACACS+ server configuration information.
<b>Step 5</b>	(Optional) <b>copy running-config startup config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#), on page 7

[Configuring TACACS+ Server Groups](#), on page 11

## Allowing Users to Specify a TACACS+ Server at Login

You can configure the switch to allow the user to specify which TACACS+ server to send the authentication request by enabling the directed-request option. By default, a Cisco NX-OS 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.



**Note** If you enable the directed-request option, the Cisco NX-OS 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+.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>tacacs-server directed-request</b> <b>Example:</b> <code>switch(config)# tacacs-server directed-request</code>	Allows users to specify a TACACS+ server to send the authentication request when logging in. The default is disabled.
<b>Step 3</b>	(Optional) <b>show tacacs+ {pending   pending-diff}</b> <b>Example:</b> <code>switch(config)# show tacacs+ pending</code>	Displays the pending TACACS+ configuration.
<b>Step 4</b>	(Optional) <b>tacacs+ commit</b> <b>Example:</b> <code>switch(config)# tacacs+ commit</code>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> <code>switch(config)# exit</code> <code>switch#</code>	Exits configuration mode.
<b>Step 6</b>	(Optional) <b>show tacacs-server directed-request</b> <b>Example:</b> <code>switch# show tacacs-server directed-request</code>	Displays the TACACS+ directed request configuration.
<b>Step 7</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#) , on page 7

## Configuring the Timeout Interval for a TACACS+ Server

You can set a timeout interval that the Cisco NX-OS device waits for responses from a TACACS+ server before declaring a timeout failure. The timeout interval determines how long the Cisco NX-OS device waits for responses from a TACACS+ server before declaring a timeout failure.

**Before you begin**

Enable TACACS+.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>timeout</b> <i>seconds</i> <b>Example:</b> switch(config)# <b>tacacs-server host</b> <b>server1 timeout 10</b>	Specifies the timeout interval for a specific server. The default is the global value. <b>Note</b> The timeout interval value specified for a TACACS+ server overrides the global timeout interval value specified for all TACACS+ servers.
<b>Step 3</b>	(Optional) <b>show tacacs+</b> { <b>pending</b>   <b>pending-diff</b> } <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	Displays the TACACS+ configuration pending for distribution.
<b>Step 4</b>	(Optional) <b>tacacs+ commit</b> <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	Exits configuration mode.
<b>Step 6</b>	(Optional) <b>show tacacs-server</b> <b>Example:</b> switch# <b>show tacacs-server</b>	Displays the TACACS+ server configuration.
<b>Step 7</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config</b> <b>startup-config</b>	Copies the running configuration to the startup configuration.

## Related Topics

[Enabling TACACS+](#), on page 7

## Configuring TCP Ports

You can configure another TCP port for the TACACS+ servers if there are conflicts with another application. By default, Cisco NX-OS devices use port 49 for all TACACS+ requests.

**Before you begin**

Enable TACACS+.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>port</b> <i>tcp-port</i> <b>Example:</b> <pre>switch(config)# tacacs-server host 10.10.1.1 port 2</pre>	Specifies the TCP port to use for TACACS+ messages to the server. The default TCP port is 49. The range is from 1 to 65535.
<b>Step 3</b>	(Optional) <b>show tacacs+</b> { <b>pending</b>   <b>pending-diff</b> } <b>Example:</b> <pre>switch(config)# show tacacs+ distribution pending</pre>	Displays the TACACS+ configuration pending for distribution.
<b>Step 4</b>	(Optional) <b>tacacs+ commit</b> <b>Example:</b> <pre>switch(config)# tacacs+ commit</pre>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
<b>Step 6</b>	(Optional) <b>show tacacs-server</b> <b>Example:</b> <pre>switch# show tacacs-server</pre>	Displays the TACACS+ server configuration.
<b>Step 7</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#) , on page 7



## Configuring Global Periodic TACACS+ Server Monitoring

You can monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.



**Note** Test parameters that are configured for individual servers take precedence over global test parameters.

The global configuration parameters include the username and password to use for the servers and an idle timer. The idle timer specifies the interval in which a TACACS+ server receives no requests before the Cisco NX-OS device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.



**Note** The test parameters are distributed across switches. If even one switch in the fabric is running an older release, the test parameters are not distributed to any switch in the fabric.



**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.



**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+.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server test</b> { <i>idle-time minutes</i>   <i>password password</i> [ <i>idle-time minutes</i> ]   <i>username name</i> [ <i>password password</i> [ <i>idle-time minutes</i> ]]}  <b>Example:</b>	Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.

	Command or Action	Purpose
	<code>switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3</code>	<b>Note</b> For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
<b>Step 3</b>	<b>tacacs-server dead-time</b> <i>minutes</i>  <b>Example:</b> <code>switch(config)# tacacs-server dead-time 5</code>	Specifies the number of minutes before the Cisco NX-OS device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> <code>switch(config)# exit switch#</code>	Exits configuration mode.
<b>Step 5</b>	(Optional) <b>show tacacs-server</b>  <b>Example:</b> <code>switch# show tacacs-server</code>	Displays the TACACS+ server configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

**Related Topics**

[Configuring Periodic TACACS+ Server Monitoring on Individual Servers](#), on page 18

## Configuring Periodic TACACS+ Server Monitoring on Individual Servers

You can monitor the availability of individual TACACS+ servers. The configuration 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 Cisco NX-OS device sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.



**Note** Test parameters that are configured for individual servers take precedence over global test parameters.



**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.



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



**Note** The test parameters are distributed across switches. The test parameters are not distributed to any switch in the fabric.

### Before you begin

Enable TACACS+.

Add one or more TACACS+ server hosts.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>test</b> { <b>idle-time</b> <i>minutes</i>   <b>password</b> <i>password</i> [ <b>idle-time</b> <i>minutes</i> ]   <b>username</b> <i>name</i> [ <b>password</b> <i>password</i> [ <b>idle-time</b> <i>minutes</i> ]]}  <b>Example:</b> switch(config)# <b>tacacs-server host</b> 10.10.1.1 <b>test</b> <b>username</b> user1 <b>password</b> Ur2Gd2BH <b>idle-time</b> 3	Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes.  <b>Note</b> For periodic TACACS+ server monitoring, the idle timer value must be greater than 0.
<b>Step 3</b>	<b>tacacs-server dead-time</b> <i>minutes</i>  <b>Example:</b> switch(config)# <b>tacacs-server dead-time</b> 5	Specifies the number of minutes before the Cisco NX-OS device checks a TACACS+ server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	Exits configuration mode.
<b>Step 5</b>	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	Displays the TACACS+ server configuration.
<b>Step 6</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	Copies the running configuration to the startup configuration.

**Related Topics**

[Configuring TACACS+ Server Hosts](#), on page 7

[Configuring Global Periodic TACACS+ Server Monitoring](#), on page 17

## Configuring the TACACS+ Dead-Time Interval

You can configure the dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Cisco NX-OS device waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.



**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.

**Before you begin**

Enable TACACS+.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> switch(config)#	Enters global configuration mode.
<b>Step 2</b>	<b>tacacs-server deadtime</b> <i>minutes</i>  <b>Example:</b> switch(config)# <b>tacacs-server deadtime</b> 5	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.
<b>Step 3</b>	(Optional) <b>show tacacs+ {pending   pending-diff}</b>  <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	Displays the pending TACACS+ configuration.
<b>Step 4</b>	(Optional) <b>tacacs+ commit</b>  <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	Exits configuration mode.

	Command or Action	Purpose
<b>Step 6</b>	(Optional) <code>show tacacs-server</code> <b>Example:</b> <code>switch# show tacacs-server</code>	Displays the TACACS+ server configuration.
<b>Step 7</b>	(Optional) <code>copy running-config startup-config</code> <b>Example:</b> <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Configuring ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

### Before you begin

Enable TACACS+.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<code>configure terminal</code> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<code>aaa authentication login ascii-authentication</code> <b>Example:</b> <code>switch(config)# aaa authentication login</code> <code>ascii-authentication</code>	Enables ASCII authentication. The default is disabled.
<b>Step 3</b>	(Optional) <code>show tacacs+ {pending   pending-diff}</code> <b>Example:</b> <code>switch(config)# show tacacs+ pending</code>	Displays the pending TACACS+ configuration.
<b>Step 4</b>	(Optional) <code>tacacs+ commit</code> <b>Example:</b> <code>switch(config)# tacacs+ commit</code>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<code>exit</code> <b>Example:</b> <code>switch(config)# exit</code> <code>switch#</code>	Exits configuration mode.

	Command or Action	Purpose
<b>Step 6</b>	(Optional) <code>show tacacs-server</code> <b>Example:</b> <code>switch# show tacacs-server</code>	Displays the TACACS+ server configuration.
<b>Step 7</b>	(Optional) <code>copy running-config startup-config</code> <b>Example:</b> <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

## Configuring Command Authorization on TACACS+ Servers

You can configure authorization for commands on TACACS+ servers.



**Caution** Command authorization disables user role-based authorization control (RBAC), including the default roles.



**Note** If you use a console to login to the server, command authorization is disabled. Authorization is available for both non-console and console sessions. By default, command authorization is disabled for console sessions even if it is configured for default (non-console) sessions. You must explicitly configure a AAA group for the console to enable command authorization for console sessions.



**Note** By default, context sensitive help and command tab completion show only the commands supported for a user as defined by the assigned roles. When you enable command authorization, the Cisco NX-OS software displays all commands in the context sensitive help and in tab completion, regardless of the role assigned to the user.

### Before you begin

Enable TACACS+.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<code>configure terminal</code> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.
<b>Step 2</b>	<code>aaa authorization {commands   config-commands} {console   default} {group group-list [local]   local}</code>	Configures the command authorization method for specific roles on a TACACS+ server.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>switch(config)# aaa authorization commands default group TacGroup Per command authorization will disable RBAC for all users. Proceed (y/n)?</pre>	<p>The <b>commands</b> keyword configures authorization sources for all EXEC commands, and the <b>config-commands</b> keyword configures authorization sources for all configuration commands.</p> <p>The <b>console</b> keyword configures command authorization for a console session, and the <b>default</b> keyword configures command authorization for a non-console session.</p> <p>The <i>group-list</i> argument consists of a space-delimited list of TACACS+ server group names. Servers belonging to this group are contacted for command authorization. The <b>local</b> method uses the local role-based database for authorization.</p> <p>The <b>local</b> method is used only if all the configured server groups fail to respond and you have configured <b>local</b> as the fallback method. The default method is <b>local</b>.</p> <p>If you have not configured a fallback method after the TACACS+ server group method, authorization fails if all server groups fail to respond.</p> <p>If you press <b>Enter</b> at the confirmation prompt, the default action is <b>n</b>.</p>
<b>Step 3</b>	<p>(Optional) <b>show tacacs+ {pending   pending-diff}</b></p> <p><b>Example:</b></p> <pre>switch(config)# show tacacs+ pending</pre>	Displays the pending TACACS+ configuration.
<b>Step 4</b>	<p>(Optional) <b>tacacs+ commit</b></p> <p><b>Example:</b></p> <pre>switch(config)# tacacs+ commit</pre>	Applies the TACACS+ configuration changes in the temporary database to the running configuration.
<b>Step 5</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	Exits global configuration mode.
<b>Step 6</b>	<p>(Optional) <b>show aaa authorization [all]</b></p> <p><b>Example:</b></p> <pre>switch(config)# show aaa authorization</pre>	Displays the AAA authorization configuration. The <b>all</b> keyword displays the default values.

	Command or Action	Purpose
<b>Step 7</b>	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

**Related Topics**

[Enabling TACACS+](#) , on page 7

[Testing Command Authorization on TACACS+ Servers](#), on page 24

## Testing Command Authorization on TACACS+ Servers

You can test the command authorization for a user on the TACACS+ servers.



**Note** You must send correct commands for authorization or else the results may not be reliable.



**Note** The **test** command uses the default (non-console) method for authorization, not the console method.

**Before you begin**

Enable TACACS+.

Ensure that you have configured command authorization for the TACACS+ servers.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>test aaa authorization command-type {commands   config-commands} user username command command-string</b>  <b>Example:</b> <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	Tests a user's authorization for a command on the TACACS+ servers.  The <b>commands</b> keyword specifies only EXEC commands and the <b>config-commands</b> keyword specifies only configuration commands.  <b>Note</b> Put double quotes (") before and after the <i>command-string</i> argument if it contains spaces.

**Related Topics**

[Enabling TACACS+](#) , on page 7

[Configuring Command Authorization on TACACS+ Servers](#), on page 22

[Configuring User Accounts and RBAC](#)



## Enabling and Disabling Command Authorization Verification

You can enable and disable command authorization verification on the command-line interface (CLI) for the default user session or for another username.



**Note** The commands do not execute when you enable authorization verification.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal verify-only</b> [username <i>username</i> ] <b>Example:</b> switch# terminal verify-only	Enables command authorization verification. After you enter this command, the Cisco NX-OS software indicates whether the commands you enter are authorized or not.
<b>Step 2</b>	<b>terminal no verify-only</b> [username <i>username</i> ] <b>Example:</b> switch# terminal no verify-only	Disables command authorization verification.

## Permitting or Denying Commands for Users of Privilege Roles

As a network administrator, you can modify the privilege roles to permit users to execute specific commands or to prevent users from running those commands.

You must follow these guidelines when changing the rules of privilege roles:

- You cannot modify the priv-14 and priv-15 roles.
- You can add deny rules only to the priv-0 role.
- These commands are always permitted for the priv-0 role: **configure**, **copy**, **dir**, **enable**, **ping**, **show**, **ssh**, **telnet**, **terminal**, **traceroute**, **end**, and **exit**.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	Enters global configuration mode.
<b>Step 2</b>	[no] <b>role name priv-<i>n</i></b> <b>Example:</b> switch(config)# role name priv-5 switch(config-role)#	Enables or disables a privilege role and enters role configuration mode. The <i>n</i> argument specifies the privilege level and is a number between 0 and 13.

	Command or Action	Purpose
<b>Step 3</b>	<p><b>rule</b> <i>number</i> {deny   permit} <b>command</b> <i>command-string</i></p> <p><b>Example:</b></p> <pre>switch(config-role)# rule 2 permit command pwd</pre>	<p>Configures a command rule for users of privilege roles. These rules permit or deny users to execute specific commands. You can configure up to 256 rules for each role. The rule number determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.</p> <p>The <i>command-string</i> argument can contain spaces.</p> <p><b>Note</b> Repeat this command for as many rules as needed.</p>
<b>Step 4</b>	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-role)# exit switch(config)#</pre>	Exits role configuration mode.
<b>Step 5</b>	<p>(Optional) <b>copy running-config</b> <b>startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

**Related Topics**

[Creating User Roles and Rules](#)

## Manually Monitoring TACACS+ Servers or Groups

You can manually issue a test message to a TACACS+ server or to a server group.

**Before you begin**

Enable TACACS+.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<p><b>test aaa server tacacs+</b> {<i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i>} [<b>vrf</b> <i>vrf-name</i>] <i>username password</i></p> <p><b>Example:</b></p> <pre>switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH</pre>	Sends a test message to a TACACS+ server to confirm availability.

	Command or Action	Purpose
<b>Step 2</b>	<b>test aaa group</b> <i>group-name username password</i> <b>Example:</b> <pre>switch# test aaa group TacGroup user2 As3He3CI</pre>	Sends a test message to a TACACS+ server group to confirm availability.

**Related Topics**

[Configuring TACACS+ Server Hosts](#), on page 7

[Configuring TACACS+ Server Groups](#), on page 11

## Disabling TACACS+

You can disable TACACS+.



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

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>no feature tacacs+</b> <b>Example:</b> <pre>switch(config)# no feature tacacs+</pre>	Disables TACACS+.
<b>Step 3</b>	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
<b>Step 4</b>	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

## Monitoring TACACS+ Servers

You can monitor the statistics that the Cisco NX-OS device maintains for TACACS+ server activity.

**Before you begin**

Configure TACACS+ servers on the Cisco NX-OS device.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>show tacacs-server statistics</b> { <i>hostname</i>   <i>ipv4-address</i>   <i>ipv6-address</i> }  <b>Example:</b> <pre>switch# show tacacs-server statistics 10.10.1.1</pre>	Displays the TACACS+ statistics.

**Related Topics**

[Configuring TACACS+ Server Hosts](#), on page 7

[Clearing TACACS+ Server Statistics](#), on page 28

## Clearing TACACS+ Server Statistics

You can display the statistics that the Cisco NX-OS device maintains for TACACS+ server activity.

**Before you begin**

Configure TACACS+ servers on the Cisco NX-OS device.

**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	(Optional) <b>show tacacs-server statistics</b> { <i>hostname</i>   <i>ipv4-address</i>   <i>ipv6-address</i> }  <b>Example:</b> <pre>switch# show tacacs-server statistics 10.10.1.1</pre>	Displays the TACACS+ server statistics on the Cisco NX-OS device.
<b>Step 2</b>	<b>clear tacacs-server statistics</b> { <i>hostname</i>   <i>ipv4-address</i>   <i>ipv6-address</i> }  <b>Example:</b> <pre>switch# clear tacacs-server statistics 10.10.1.1</pre>	Clears the TACACS+ server statistics.

**Related Topics**

[Configuring TACACS+ Server Hosts](#), on page 7

## Verifying the TACACS+ Configuration

To display the TACACS+ configuration, perform one of the following tasks:

Command	Purpose
<code>show tacacs+ { status   pending   pending-diff }</code>	Displays the TACACS+ Cisco Fabric Services distribution status and other details.
<code>show running-config tacacs [all]</code>	Displays the TACACS+ configuration in the running configuration.
<code>show startup-config tacacs</code>	Displays the TACACS+ configuration in the startup configuration.
<code>show tacacs-server [host-name   ipv4-address   ipv6-address] [directed-request   groups   sorted   statistics]</code>	Displays all configured TACACS+ server parameters.

## Configuration Examples for TACACS+

The following example shows how to configure a TACACS+ server host and server group:

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhT1"
aaa group server tacacs+ TacServer
    server 10.10.2.2
```

The following example shows how to configure and use command authorization verification:

```
switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief
```

```
-----
Ethernet      VLAN   Type Mode   Status Reason          Speed   Port
Interface
-----
Eth7/2        1      eth  access down   SFP not inserted  auto(D) --
```

The following example shows how to permit all users with roles priv-5 and above to execute the **pwd** command:

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd
```

The following example shows how to deny the **show running-config** command to all users with roles below priv-5. First, you must remove the permission to execute this command from the priv-0 role; then you must permit the command at role priv-5 so that users with roles priv-5 and above have permission to run the command.

```

switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-config
switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-config
switch(config-role)# exit

```

## Where to Go Next

You can now configure AAA authentication methods to include the server groups.

## Additional References for TACACS+

This section includes additional information related to implementing TACACS+.

### Related Documents

Related Topic	Document Title
Cisco NX-OS licensing	<i>Cisco NX-OS Licensing Guide</i>
VRF configuration	<i>Cisco NX-OS 9000 Series NX-OS Unicast Routing Configuration Guide</i>

### 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
MIBs related to TACACS+	To locate and download supported MIBs, go to the following URL: <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>