



T Commands

This chapter describes the Cisco NX-OS security commands that begin with T.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description	<i>time</i>	Specifies the time interval in minutes. The range is from 1 to 1440.
Defaults	0 minutes	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.	

Send document comments to nexus7k-docfeedback@cisco.com

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

You must use the **feature tacacs+** command before you configure TACACS+.

This command does not require a license.

Examples

This example shows how to configure the dead-time interval and enable periodic monitoring:

```
switch# config terminal
switch(config)# tacacs-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch# config terminal
switch(config)# no tacacs-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

Send document comments to nexus7k-docfeedback@cisco.com

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Sends the authentication request to the configured TACACS+ server groups

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use the **feature tacacs+** command before you configure TACACS+.

The user can specify the *username@vrfname:hostname* during login, where *vrfname* is the virtual routing and forwarding (VRF) name to use and *hostname* is the name of a configured TACACS+ server. The username is sent to the server name for authentication.



Note

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

This command does not require a license.

Examples

This example shows how to allow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch# config terminal
switch(config)# tacacs-server directed-request
```

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to disallow users to send authentication requests to a specific TACACS+ server when logging in:

```
switch# config terminal  
switch(config)# no tacacs-server directed-request
```

Related Commands

Command	Description
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.
feature tacacs+	Enables TACACS+.

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

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command in configuration mode. To revert to the defaults, use the **no** form of this command.

```
tacacs-server host {hostname | ipv4-address | ipv6-address}
  [key [0 | 7] shared-secret] [port port-number]
  [test {idle-time time | password password | username name}]
  [timeout seconds]
```

```
no tacacs-server host {hostname | ipv4-address | ipv6-address}
  [key [0 | 7] shared-secret] [port port-number]
  [test {idle-time time | password password | username name}]
  [timeout seconds]
```

Syntax Description

<i>hostname</i>	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
<i>ipv4-address</i>	TACACS+ server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	TACACS+ server IPv6 address in the <i>X:X:X::X</i> format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
<i>shared-secret</i>	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port <i>port-number</i>	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time <i>time</i>	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password <i>password</i>	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username <i>name</i>	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout <i>seconds</i>	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Defaults

Idle time: disabled
Server monitoring: disabled

Send document comments to nexus7k-docfeedback@cisco.com

Timeout: 1 second.

Test username: test

Test password: test

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines You must use the **feature tacacs+** command before you configure TACACS+.

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

This command does not require a license.

Examples This example shows how to configure TACACS+ server host parameters:

```
switch# config terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands	Command	Description
	show tacacs-server	Displays TACACS+ server information.
	feature tacacs+	Enables TACACS+.

Send document comments to nexus7k-docfeedback@cisco.com

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To removed a configured shared secret, use the **no** form of this command.

```
tacacs-server key [0 | 7] shared-secret
```

```
no tacacs-server key [0 | 7] shared-secret
```

Syntax Description	0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
	7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
	<i>shared-secret</i>	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Defaults None

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines You must configure the TACACS+ preshared key to authenticate the device to the TACACS+ server. 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 key to be used for all TACACS+ server configurations on the device. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

You must use the **feature tacacs+** command before you configure TACACS+.

This command does not require a license.

Examples The following example shows how to configure TACACS+ server shared keys:

```
switch# config terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	show tacacs-server	Displays TACACS+ server information.
	feature tacacs+	Enables TACACS+.

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

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description	<i>seconds</i>	Seconds between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.
---------------------------	----------------	---

Defaults	1 second
-----------------	----------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	You must use the feature tacacs+ command before you configure TACACS+. This command does not require a license.
-------------------------	---

Examples	This example shows how to configure the TACACS+ server timeout value:
-----------------	---

```
switch# config terminal
switch(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch# config terminal
switch(config)# no tacacs-server timeout 3
```

Related Commands	Command	Description
	show tacacs-server	Displays TACACS+ server information.
	feature tacacs+	Enables TACACS+.

Send document comments to nexus7k-docfeedback@cisco.com

telnet

To create a Telnet session using IPv4 on the NX-OS device, use the **telnet** command.

```
telnet {ipv4-address | hostname} [port-number] [vrf vrf-name]
```

Syntax Description		
	<i>ipv4-address</i>	IPv4 address of the remote device.
	<i>hostname</i>	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
	<i>port-number</i>	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
	vrf <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Defaults

Port 23

Default VRF

Command Modes

Any command mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **telnet server enable** command.

To create a Telnet session with IPv6 addressing, use the **telnet6** command.

This command does not require a license.

Examples

This example shows how to start a Telnet session using an IPv4 address:

```
switch# telnet 10.10.1.1 vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.
telnet6	Creates a Telnet session using IPv6 addressing.
telnet server enable	Enables the Telnet server.

Send document comments to nexus7k-docfeedback@cisco.com

telnet server enable

To enable the Telnet server for a virtual device context (VDC), use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines This command does not require a license.

Examples This example shows how to enable the Telnet server:

```
switch# config t
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch# config t
switch(config)# no telnet server enable
XML interface to system may become unavailable since ssh is disabled
```

Related Commands	Command	Description
	show telnet server	Displays the SSH server key information.

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

telnet6

To create a Telnet session using IPv6 on the NX-OS device, use the **telnet6** command.

```
telnet6 {ipv6-address | hostname} [port-number] [vrf vrf-name]
```

Syntax Description		
	<i>ipv6-address</i>	IPv6 address of the remote device.
	<i>hostname</i>	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
	<i>port-number</i>	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
	vrf <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Defaults	
	Port 23
	Default VRF

Command Modes	
	Any command mode

Supported User Roles	
	network-admin vdc-admin

Command History	Release	Modification
	4.0(2)	This command was introduced.

Usage Guidelines	
	To use this command, you must enable the Telnet server using the telnet server enable command.
	To create a Telnet session with IPv4 addressing, use the telnet command.
	This command does not require a license.

Examples	
	This example shows how to start a Telnet session using an IPv6 address:
	<pre>switch# telnet6 2001:0DB8:0:0:E000::F vrf management</pre>

Related Commands	Command	Description
	clear line	Clears Telnet sessions.
	telnet	Creates a Telnet session using IPv4 addressing.
	telnet server enable	Enables the Telnet server.

Send document comments to nexus7k-docfeedback@cisco.com

time-range

To configure a time range, use the **time-range** command. To remove a time range, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description	<i>time-range-name</i> Name of the time range, which can be up to 64 alphanumeric, case-sensitive characters.
---------------------------	---

Defaults	None
-----------------	------

Command Modes	Global configuration
----------------------	----------------------

SupportedUserRoles	network-admin vdc-admin
---------------------------	----------------------------

Command History	Release	Modification
	4.0(1)	This command was introduced.

Usage Guidelines	This command does not require a license. You can use a time range in permit and deny commands for IPv4 ACLs.
-------------------------	---

Examples	This example shows how to use the time-range command and enter time range configuration mode:
-----------------	--

```
switch# config t
switch(config)# time-range workweek-vpn-access
switch(config-time-range)#
```

Related Commands	Command	Description
	absolute	Specifies a time range that has a specific start date and time.
	deny (IPv4)	Configures an IPv4 deny rule.
	periodic	Specifies a time range that is active one or more times per week.
	permit (IPv4)	Configures an IPv4 permit rule.

time-range

Send document comments to nexus7k-docfeedback@cisco.com