



T Commands

This chapter describes the Cisco Nexus Cloud Services Platform commands that begin with the letter T.

tacacs+ enable

To enable TACACS+, use the **tacacs+ enable** command. To disable TACACS+, use the **no** form of this command.

tacacs+ enable

no tacacs+ enable

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to enable TACACS+:

```
n1010(config)# tacacs+ enable
n1010(config)#
```

This example shows how to disable TACACS+:

```
n1010(config)# no tacacs+ enable
```

■ tacacs+ enable

Send document comments to nexus1k-docfeedback@cisco.com.

```
n1010(config)#
```

Related Commands	Command	Description
	show tacacs-server	Displays the TACACS+ server configuration.
	tacacs-server host	Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host.
	tacacs-server key	Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts.

Send document comments to nexus1k-docfeedback@cisco.com.

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>	Time interval in minutes. The range is from 1 to 1440.
Defaults	0 minutes	
Command Modes	Global configuration (config)	
SupportedUserRoles	network-admin	
Command History	Release	Modification
	4.0(4)SP1(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.

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.

In global configuration mode, you must first enable the TACACS+ feature, using the **tacacs+ enable** command, before you can use any of the other TACACS+ commands to configure the feature.

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

```
n1010# configure terminal
n1010(config)# tacacs-server deadtime 10
```

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

```
n1010# configure terminal
n1010(config)# no tacacs-server deadtime 10
```

Send document comments to nexus1k-docfeedback@cisco.com.

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

Send document comments to nexus1k-docfeedback@cisco.com.

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **tacacs-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 Disabled

Command Modes Global configuration (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Usage Guidelines In global configuration mode, you must first enable the TACACS+ feature, using the **tacacs+ enable** command, before you can use any of the other TACACS+ commands to configure the feature.

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.

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

```
n1010# configure terminal
n1010(config)# tacacs-server directed-request
```

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

```
n1010# configure terminal
n1010(config)# no tacacs-server directed-request
```

Send document comments to nexus1k-docfeedback@cisco.com.

Related Commands	Command	Description
	show tacacs-server	Displays the TACACS+ server configuration.
	tacacs+ enable	Enables TACACS+.

Send document comments to nexus1k-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 username 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

Parameter	Default
Idle-time	disabled

Send document comments to nexus1k-docfeedback@cisco.com.

Server monitoring	disabled
Timeout	1 seconds
Test username	test
Test password	test

Command Modes Global configuration (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Usage Guidelines You must use the **tacacs+ enable** command before you configure TACACS+.
When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

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

```
n1010# configure terminal
n1010(config)# tacacs-server host 10.10.2.3 key HostKey
n1010(config)# tacacs-server host tacacs2 key 0 abcd
n1010(config)# tacacs-server host tacacs3 key 7 1234
n1010(config)# tacacs-server host 10.10.2.3 test idle-time 10
n1010(config)# tacacs-server host 10.10.2.3 test username tester
n1010(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

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

Send document comments to nexus1k-docfeedback@cisco.com.

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To remove 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 (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Usage Guidelines You must configure the TACACS+ preshared key to authenticate the device on 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 **tacacs+ enable** command before you configure TACACS+.

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

```
n1010# configure terminal
n1010(config)# tacacs-server key AnyWord
n1010(config)# tacacs-server key 0 AnyWord
n1010(config)# tacacs-server key 7 public
```

Send document comments to nexus1k-docfeedback@cisco.com.

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

Send document comments to nexus1k-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	5 seconds	
Command Modes	Global configuration (config)	
Supported User Roles	network-admin	
Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.
Usage Guidelines	You must use the tacacs+ enable command before you configure TACACS+.	
Examples	<p>This example shows how to configure the TACACS+ server timeout value:</p> <pre>n1010# configure terminal n1010(config)# tacacs-server timeout 3</pre> <p>This example shows how to revert to the default TACACS+ server timeout value:</p> <pre>n1010# configure terminal n1010(config)# no tacacs-server timeout 3</pre>	
Related Commands	Command	Description
	show tacacs-server	Displays TACACS+ server information.
	tacacs+ enable	Enables TACACS+.

Send document comments to nexus1k-docfeedback@cisco.com.

tail

To display the last lines of a file, use the **tail** command.

```
tail [filesystem:[//module/]][directory/]filename lines
```

Syntax Description	
<i>filesystem:</i>	(Optional) Name of a file system. The name is case sensitive.
<i>//module/</i>	(Optional) Identifier for a supervisor module. Valid values are sup-active , sup-local , sup-remote , or sup-standby . The identifiers are case sensitive.
<i>directory/</i>	(Optional) Name of a directory. The name is case sensitive.
<i>filename</i>	Name of the command file. The name is case sensitive.
<i>lines</i>	(Optional) Number of lines to display. The range is from 0 to 80.

Defaults	
	10 lines

Command Modes	
	Any command mode

SupportedUserRoles	
	network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to display the last 10 lines of a file:

```
n1010# tail bootflash:startup.cfg
ip arp inspection filter marp vlan 9
ip dhcp snooping vlan 13
ip arp inspection vlan 13
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
logging level dhcp_snoop 6
logging level eth_port_channel 6
```

This example shows how to display the last 20 lines of a file:

```
n1010# tail bootflash:startup.cfg 20
area 99 virtual-link 1.2.3.4
router rip Enterprise
router rip foo
    address-family ipv4 unicast
router bgp 33.33
event manager applet sdtest
monitor session 1
monitor session 2
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip arp inspection filter marp vlan 9
ip dhcp snooping vlan 13
ip arp inspection vlan 13
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
logging level dhcp_snoop 6
logging level eth_port_channel 6
```

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Copies files.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

Send document comments to nexus1k-docfeedback@cisco.com.

telnet

To create a Telnet session, 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

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

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

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

```
n1010# telnet 10.10.1.1 vrf management
```

Related Commands	Command	Description
	clear line	Clears Telnet sessions.
	telnet server enable	Enables the Telnet server.

Send document comments to nexus1k-docfeedback@cisco.com.

telnet server enable

To enable the Telnet server, 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 (config)

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to enable the Telnet server:

```
n1010# configure terminal
n1010(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
n1010# configure terminal
n1010(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 Telnet server configuration.
	telnet	Creates a Telnet session.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal event-manager bypass

To bypass the CLI event manager, use the **terminal event-manager bypass** command.

terminal event-manager bypass

Syntax Description This command has no arguments or keywords.

Defaults Event manager is enabled.

Command Modes Any command mode

SupportedUserRoles network-admin
network-operator

Syntax Description	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to disable the CLI event manager:

```
n1010# terminal event-manager bypass
n1010#
```

Related Commands	Command	Description
	show terminal	Displays terminal configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal length

To set the number of lines that appear on the screen, use the **terminal length** command.

terminal length *number*

Syntax Description	<i>number</i>	Number of lines. The range is from 0 to 511.
---------------------------	---------------	--

Defaults	28 lines
-----------------	----------

Command Modes	Any command mode
----------------------	------------------

SupportedUserRoles	network-admin network-operator
---------------------------	-----------------------------------

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Usage Guidelines	Set <i>number</i> to 0 to disable pausing.
-------------------------	--

Examples	This example shows how to set the number of lines that appear on the screen:
-----------------	--

```
n1010# terminal length 60
n1010#
```

Related Commands	Command	Description
	show terminal	Displays the terminal configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal monitor

To enable logging for Telnet or Secure Shell (SSH), use the **terminal monitor** command.

terminal monitor

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to enable logging for Telnet or SSH:

```
n1010# terminal monitor
n1010#
```

Related Commands	Command	Description
	show terminal	Displays the terminal configuration.
	terminal length	Sets the number of lines that appear on the screen.
	terminal session-timeout	Sets the session timeout.
	terminal terminal-type	Specifies the terminal type.
	terminal width	Sets the terminal width.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal session-timeout

To set a session timeout, use the **terminal session-timeout** command.

terminal session-timeout *time*

Syntax Description	<i>time</i>
	Timeout time, in seconds. The range is from 0 to 525600.

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

Command Modes	Any command mode
---------------	------------------

SupportedUserRoles	network-admin network-operator
--------------------	-----------------------------------

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Usage Guidelines	Set <i>time</i> to 0 to disable timeout.
------------------	--

Examples	This example shows how to set a session timeout:
----------	--

```
n1010# terminal session-timeout 100
n1010#
```

Related Commands	Command	Description
	show terminal	Displays the terminal configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal terminal-type

To specify the terminal type, use the **terminal terminal-type** command.

terminal terminal-type *type*

Syntax Description	<i>type</i>	Terminal type.
Defaults	None	
Command Modes	Any command mode	
SupportedUserRoles	network-admin network-operator	
Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.
Examples	This example shows how to specify the terminal type: n1010# terminal terminal-type vt100 n1010#	
Related Commands	Command	Description
	show terminal	Displays the terminal configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal tree-update

To update the main parse tree, use the **terminal tree-update** command.

terminal tree-update

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any command mode

SupportedUserRoles network-admin
network-operator

Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.

Examples This example shows how to update the main parse tree:

```
n1010# terminal tree-update
n1010#
```

Related Commands	Command	Description
	show terminal	Displays the terminal configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

terminal width

To set the terminal width, use the **terminal width** command.

terminal width *number*

Syntax Description	<i>number</i>	Number of characters on a single line. The range is from 24 to 511.
Defaults	102 columns	
Command Modes	Any command mode	
Supported User Roles	network-admin network-operator	
Command History	Release	Modification
	4.0(4)SP1(1)	This command was introduced.
Examples	This example shows how to set the terminal width: n1010# terminal width 60 n1010#	
Related Commands	Command	Description
	show terminal	Displays the terminal configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

traceroute

To discover the routes that packets take when traveling to an IPv4 address, use the **traceroute** command.

```
traceroute {dest-ipv4-addr | hostname} [vrf vrf-name] [show-mpls-hops] [source src-ipv4-addr]
```

Syntax	Description
<i>dest-ipv4-addr</i>	IPv4 address of the destination device. The format is <i>A.B.C.D</i> .
<i>hostname</i>	Name of the destination device. The name is case sensitive.
vrf <i>vrf-name</i>	(Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive.
show-mpls-hops	(Optional) Displays the Multiprotocol Label Switching (MPLS) hops.
source <i>src-ipv4-addr</i>	(Optional) Specifies a source IPv4 address. The format is <i>A.B.C.D</i> .

Defaults

Uses the default VRF.
Does not show the MPLS hops.
Uses the management IPv4 address for the source address.

Command Modes

Any command mode

Supported User Roles

network-admin

Command History

Release	Modification
4.0(4)SP1(1)	This command was introduced.

Usage Guidelines

To use IPv6 addressing for discovering the route to a device, use the **traceroute6** command.

Examples

This example shows how to discover a route to a device:

```
n1010# traceroute 172.28.255.18 vrf management
traceroute to 172.28.255.18 (172.28.255.18), 30 hops max, 40 byte packets
 1 172.28.230.1 (172.28.230.1) 0.746 ms 0.595 ms 0.479 ms
 2 172.24.114.213 (172.24.114.213) 0.592 ms 0.51 ms 0.486 ms
 3 172.20.147.50 (172.20.147.50) 0.701 ms 0.58 ms 0.486 ms
 4 172.28.255.18 (172.28.255.18) 0.495 ms 0.43 ms 0.482 ms
```

Related Commands

Command	Description
ping	Determines the network connectivity to another device using IPv4 addressing

Send document comments to nexus1k-docfeedback@cisco.com.