



## T Commands

---

This chapter covers the following commands:

- [tacacs-server host](#), page 16-2
- [tacacs-server key](#), page 16-4
- [tacacs-server timeout](#), page 16-6
- [telnet enable](#), page 16-8

# tacacs-server host

To specify a TACACS+ server to be used for AAA authentication services, use the **tacacs-server host** command. Use the **no** form of this command to delete the specified host.

**tacacs-server host** *ip-address* [**auth-port** *port-number*] [**timeout** *seconds*] [**key** *key-string*]

**no tacacs-server host** *ip-address* [**auth-port** *nn*]

## Syntax Description

<i>ip-address</i>	The IP address of the TACACS+ server.
<b>auth-port</b> <i>port-number</i>	(Optional) The server port number. Valid port numbers range from 1 to 65535. If unspecified, the port number defaults to 49.
<b>timeout</b> <i>seconds</i>	(Optional) The amount of time the storage router should wait for a reply from a TACACS+ server before timing out. This setting overrides the global setting of the <b>tacacs-server timeout</b> command. If no timeout value is specified, the global value is used.
<b>key</b> <i>key-string</i>	(Optional) The authentication and encryption key for all TACACS+ communication between the storage router and this TACACS+ server. The character string must match the key used by the TACACS+ daemon. This key overrides the global setting of the <b>tacacs-server key</b> command. If no key string is specified, the global value is used. If spaces are part of the key string, enclose the string in quotation marks.

## Defaults

No TACACS+ server is specified.

## Command Modes

Administrator.

## Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

## Usage Guidelines

AAA authentication services are used to provide iSCSI authentication for IP hosts requesting access to storage resources.

- You can use multiple **tacacs-server host** commands to specify multiple TACACS+ servers. The software searches for servers in the order in which you specify them.
- If no server-specific timeout or key values are specified, the global values apply to each TACACS+ server.
- If you use spaces in the key, enclose the key in quotation marks.

Use the **aaa group server tacacs+ server** command to add a TACACS+ server to a server group. If you delete a TACACS+ server, delete the server from the TACACS+ server using the **no aaa group server tacacs+ server** command.

**Note**

Verification of IP addresses in a server group occurs only at runtime. If a TACACS+ server group contains an IP address that is not defined as a TACACS+ server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

**Examples**

The following example specifies the server with IP address 172.29.39.46 as the TACACS+ server and uses the default port for authentication:

```
[SN5428-2A]# tacacs-server host 172.29.39.46
```

The following example specifies port 52 as the destination port for authentication requests on the TACACS+ server 172.29.39.46:

```
[SN5428-2A]# tacacs-server host 172.29.39.46 auth-port 52
```

The following example specifies the server with IP address 172.29.39.46 as the TACACS server, uses ports 52 as the authorization port, sets the timeout value to 6, and sets *tac123* as the encryption key, matching the key on the TACACS+ server:

```
[SN5428-2A]# tacacs-server host 172.29.39.46 auth-port 52 timeout 6 key tac123
```

**Related Commands**

Command	Description
<a href="#">aaa authentication enable</a>	Configure AAA authentication services for Administrator mode access to the storage router via the CLI <b>enable</b> command.
<a href="#">aaa authentication iscsi</a>	Configure the AAA authentication services to be used for iSCSI authentication.
<a href="#">aaa authentication login</a>	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
<a href="#">aaa group server tacacs+</a>	Create a named group of TACACS+ servers for AAA authentication services.
<a href="#">aaa test authentication</a>	Enable testing of the specified AAA authentication list.
<a href="#">debug aaa</a>	Enable debugging for the AAA authentication services.
<a href="#">ip tacacs sourceinterface</a>	Specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers.
<a href="#">radius-server host</a>	Configure remote RADIUS servers for AAA authentication services.
<a href="#">restore aaa</a>	Restore AAA authentication services from the named configuration file.
<a href="#">save aaa</a>	Save the current AAA configuration information.
<a href="#">scsirouter authentication</a>	Enable iSCSI authentication for the named SCSI routing instance.
<a href="#">show aaa</a>	Display AAA configuration information.
<a href="#">tacacs-server key</a>	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.
<a href="#">tacacs-server timeout</a>	Sets the interval the storage router waits for a TACACS+ server to reply.

## tacacs-server key

To set the authentication and encryption key used for all TACACS+ communications between the storage router and the TACACS+ daemon, use the **tacacs-server key** command. To disable the key, use the **no** form of this command.

**tacacs-server key** *key-string*

**no tacacs-server key**

<b>Syntax Description</b>	<i>key-string</i>	The authentication and encryption key string to be used for all TACACS+ communications, in unencrypted text. If spaces are part of the key string, enclose the string in quotation marks.
<b>Defaults</b>	None.	
<b>Command Modes</b>	Administrator.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.2.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

**Usage Guidelines**

After using the **aaa authentication iscsi** command to configure the iSCSI authentication list to use TACACS+ authentication services, use the **tacacs-server key** command to set the global authentication and encryption key. The key entered as part of the command must match the key used on the TACACS+ daemon. If spaces are part of the key string, enclose the key string in quotation marks.

To override the global key for a specific TACACS+ server, use the **tacacs-server host** command with the **key** keyword.

**Examples**

The following example sets the global authentication and encryption key to *my TACACS key string*:

```
[SN5428-2A]# radius-server key "my TACACS key string"
```

Related Commands	Command	Description
	<b>aaa authentication enable</b>	Configure AAA authentication services for Administrator mode access to the storage router via the CLI <b>enable</b> command.
	<b>aaa authentication iscsi</b>	Configure the AAA authentication services to be used for iSCSI authentication.
	<b>aaa authentication login</b>	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
	<b>aaa group server tacacs+</b>	Create a named group of TACACS+ servers for AAA authentication services.
	<b>aaa test authentication</b>	Enable testing of the specified AAA authentication list.
	<b>debug aaa</b>	Enable debugging for the AAA authentication services.
	<b>ip tacacs sourceinterface</b>	Specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers.
	<b>radius-server host</b>	Configure remote RADIUS servers for AAA authentication services.
	<b>restore aaa</b>	Restore AAA authentication services from the named configuration file.
	<b>save aaa</b>	Save the current AAA configuration information.
	<b>scsirouter authentication</b>	Enable iSCSI authentication for the named SCSI routing instance.
	<b>show aaa</b>	Display AAA configuration information.
	<b>tacacs-server host</b>	Configure remote TACACS+ servers for AAA authentication services.
	<b>tacacs-server timeout</b>	Sets the interval the storage router waits for a TACACS+ server to reply.

# tacacs-server timeout

To set the global interval that the storage router waits for a TACACS+ server to reply, use the **tacacs-server timeout** command. To restore the default, use the **no** form of this command.

**tacacs-server timeout** *seconds*

**no tacacs-server timeout**

<b>Syntax Description</b>	<i>seconds</i>	The global timeout value, in seconds. Enter a value in the range of 1 to 1000. The default is 5.
---------------------------	----------------	--

**Defaults** The timeout value defaults to five seconds.

**Command Modes** Administrator.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.2.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

**Usage Guidelines** Use this command to set the number of seconds the storage router waits for a TACACS+ server to reply before timing out.

To override the global timeout value for a specific TACACS+ server, use the **tacacs-server host** command with the **timeout** keyword.

**Examples** The following example sets the global timeout value to 10. You may want to increase the timeout value if you have network problems or if TACACS+ servers are slow to respond, causing persistent timeouts when a lower timeout value is used.

```
[SN5428-2A]# tacacs-server timeout 10
```

Related Commands	Command	Description
	<b>aaa authentication enable</b>	Configure AAA authentication services for Administrator mode access to the storage router via the CLI <b>enable</b> command.
	<b>aaa authentication iscsi</b>	Configure the AAA authentication services to be used for iSCSI authentication.
	<b>aaa authentication login</b>	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
	<b>aaa group server tacacs+</b>	Create a named group of TACACS+ servers for AAA authentication services.
	<b>aaa test authentication</b>	Enable testing of the specified AAA authentication list.
	<b>debug aaa</b>	Enable debugging for the AAA authentication services.
	<b>ip tacacs sourceinterface</b>	Specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers.
	<b>radius-server host</b>	Configure remote RADIUS servers for AAA authentication services.
	<b>restore aaa</b>	Restore AAA authentication services from the named configuration file.
	<b>save aaa</b>	Save the current AAA configuration information.
	<b>scsirouter authentication</b>	Enable iSCSI authentication for the named SCSI routing instance.
	<b>show aaa</b>	Display AAA configuration information.
	<b>tacacs-server host</b>	Configure remote TACACS+ servers for AAA authentication services.
	<b>tacacs-server key</b>	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.

# telnet enable

To enable Telnet for the storage router and to start the Telnet server, use the **telnet enable** command. To disable Telnet and stop the Telnet server, use the **no** form of this command.

**telnet enable**

**no telnet enable**

**Syntax Description** This command has no arguments or keywords.

**Defaults** Telnet is enabled and the Telnet server is started by default.

**Command Modes** Administrator.

Command History	Release	Modification
	2.5.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

**Usage Guidelines** Use this command to enable Telnet for the storage router and start the Telnet server. If Telnet is enabled and the Telnet server is running, you can still restrict Telnet access to the storage router for specific interfaces by using the **restrict** command.

**Examples** The following example disables Telnet and stops the Telnet server:

```
[SN5428-2A]# no telnet enable
```

The following example enables Telnet and starts the Telnet server:

```
[SN5428-2A]# telnet enable
```

Related Commands	Command	Description
	<a href="#">restrict</a>	Secure access to storage router interfaces by communications protocols and services.
	<a href="#">show telnet</a>	Display the status of the Telnet server.