



# Configuring the CSS as a Client of a TACACS+ Server

---

The Terminal Access Controller Access Control System (TACACS+) protocol provides access control for routers, network access servers (NAS), or other devices through one or more daemon servers. TACACS+ encrypts all traffic between the NAS and daemon using TCP communications for reliable delivery.

You can configure the CSS as a client of a TACACS+ server to provide a method for authentication of users, and a method of authorization and accounting of configuration and nonconfiguration commands.

This chapter contains the following major sections:

- [TACACS+ Configuration Quick Start](#)
- [Configuring TACACS+ Server User Accounts for Use with the CSS](#)
- [Configuring Global TACACS+ Attributes](#)
- [Defining a TACACS+ Server](#)
- [Setting TACACS+ Authorization](#)
- [Setting TACACS+ Accounting](#)
- [Showing TACACS+ Server Configuration Information](#)

After you configure the TACACS+ server on the CSS, configure TACACS+ authentication for virtual or console authentication. Refer to [Chapter 1, Controlling CSS Access](#) for details.

# TACACS+ Configuration Quick Start

[Table 4-1](#) provides a quick overview of the steps required to configure the TACACS+ feature on a CSS. Each step includes the CLI command required to complete the task. For a complete description of each feature and all the options associated with the CLI command, see the sections following the table.

**Table 4-1 TACACS+ Configuration Quick Start**

---

## Task and Command Example

---

1. Configure the authentication settings on the Cisco Secure ACS in the Network Configuration section of the Cisco Secure ACS HTML interface, the Add AAA Client page, and complete the following fields:
  - AAA Client Hostname
  - AAA Client IP Address
  - Key
  - Authenticate Using

See the [“Configuring Authentication Settings”](#) section.

---

2. To determine the privilege level of users accessing the CSS, configure the user accounts on the TACACS+ server. See the [“Configuring Authorization Settings”](#) section.
  3. (Optional) If you are configuring global timeout, keepalive frequency, or encryption key attributes for the TACACS+ server, you must configure these parameters before you configure the server. For information on configuring global TACACS+ attributes, see the [“Configuring Global TACACS+ Attributes”](#) section.
- 

4. Use the **tacacs-server** command to define a server. You must provide the IP address and port number for the server. You can optionally define a specific timeout period, encryption key, or keepalive frequency, and designate the server as the primary server. See the [“Defining a TACACS+ Server”](#) section.

```
(config)# tacacs-server 192.168.11.1 12 20 "summary" primary
frequency 10
```

---

**Table 4-1 TACACS+ Configuration Quick Start (continued)****Task and Command Example**

5. Use the **virtual authentication** command to configure the primary, secondary, and tertiary virtual authentication method.

```
#(config) virtual authentication primary tacacs
```

6. (Recommended) Verify your TACACS+ server configuration. See the [“Showing TACACS+ Server Configuration Information”](#) section.

```
(config)# show tacacs-server
```

The following running-configuration example shows the results of entering the commands in [Table 4-1](#).

```
!***** GLOBAL *****
virtual authentication primary tacacs
tacacs-server 192.168.11.1 12 20 6dab4b3gibcbef3e primary frequency 10
```

## Configuring TACACS+ Server User Accounts for Use with the CSS

This section provides background information on the setup of a TACACS+ server. It is intended as a guide to help ensure proper communication with a TACACS+ server and a CSS operating as a TACACS+ client.

The following sections summarize the recommended Cisco Secure Access Control Server (ACS) TACACS+ user authentication and authorization settings.

### Configuring Authentication Settings

To configure the authentication settings on Cisco Secure ACS, go to the Network Configuration section of the Cisco Secure ACS HTML interface, the Add AAA Client page, and complete the following fields:

- AAA Client Hostname - Enter a name you want assigned to the CSS.
- AAA Client IP Address - Enter the IP address of the CSS Ethernet management port or of a CSS circuit (depending on how the CSS is configured to communicate with the Cisco Secure ACS).

- Key - Enter the shared secret that the CSS and Cisco Secure ACS use to authenticate transactions. For correct operation, you must specify the identical shared secret on both the Cisco Secure ACS and the CSS. The key is case-sensitive.
- Authenticate Using - Select **TACACS+ (Cisco IOS)**.

## Configuring Authorization Settings

To determine the privilege level of users accessing the CSS, you must configure the user accounts on the TACACS+ server to permit or deny execution of the **privilege** command. The CSS queries the TACACS+ server for authorization to execute the **privilege** command. If the server allows the **privilege** command, the user is granted privileged (SuperUser and configuration modes) access to the CSS. If the server denies the **privilege** command, the user is granted nonprivileged (User mode) access to the CSS.

To configure the group authorization settings:

1. From the Group Setup section of the Cisco Secure ACS HTML interface, Group Setup Select page, select the group for which you want to configure TACACS+ settings.
2. On the Shell Command Authorization Set page, click the **Per Group Command Authorization** checkbox
3. Under **Unmatched Cisco IOS Commands**, either permit or deny execution of the privilege command:
  - For a group that has SuperUser privileges on the CSS, select **Permit**. A SuperUser can issue any CSS command.
  - For a group that has User privileges on the CSS, select **Deny**. A user can issue CSS commands that does not change the CSS configuration; for example, **show** commands.

An alternative way to configure the group authorization settings is as follows:

1. Select **Shared Profile Components, Shell Command Authorization Sets** page.
2. Click the **Add** button to add a set or to edit an existing set.
3. Enter a name and description.

4. Proceed next to Unmatched Commands, either permit or deny execution of the privilege command:
  - For a user that has SuperUser privileges on the CSS, click **Permit**. A SuperUser can issue any CSS command.
  - For a user that has User privileges on the CSS, click **Deny**. A user can issue CSS commands that do not change the CSS configuration; for example, **show** commands.
5. From the Group Setup section, Group Setup Select page, select the group for which you want to configure TACACS+ settings.
6. On the Shell Command Authorization Set section, select **Assign a Shell Command Authorization Set for any network device**.
7. Select the set from the list.

To add a user to a group, go to the **User Setup** section of the Cisco Secure ACS HTML interface:

- On the User Setup Select page, specify a username.
- On the User Setup Edit page, specify the following:
  - Password Authentication - Select an applicable authentication type from the list.
  - Password - Specify and confirm a password.
  - Group - Select the previously created TACACS+ group to which you want to assign the user.

## Configuring Global TACACS+ Attributes

The TACACS+ timeout period, encryption key, and keepalive frequency have default values that are applied to the TACACS server. During the server configuration, you can configure these attributes to be specific to the server or omit them for the server to accept the default values. You can change the default values for any of these global attributes. The following sections provide information for:

- [Setting the Global CSS TACACS+ Timeout Period](#)
- [Defining a Global Encryption Key](#)
- [Setting the Global TACACS+ Keepalive Frequency](#)

**Note**

---

The timeout, encryption key, or keepalive frequency that you define when you configure a TACACS+ server overrides the global attribute (see the [“Defining a TACACS+ Server”](#) section).

---

## Setting the Global CSS TACACS+ Timeout Period

The CSS allows you to define a global TACACS+ timeout period for use with all configured TACACS+ servers. To determine the availability of the TACACS+ servers, the CSS sends periodic TCP keepalive probes to them. If the server does not respond to the probe within the timeout period, the CSS considers the server unavailable.

If the CSS attempts to contact the server and does not receive a response within the defined timeout value, it uses another server. The next configured server is contacted and the process is repeated. If a second (or third) TACACS+ server has been identified, the CSS selects that server as the active server.

If the CSS cannot reach all three TACACS+ servers, users are not authenticated and cannot log in to the CSS unless TACACS+ is used in combination with a RADIUS or local server, as defined through the **virtual** command or the **console** command. See [Chapter 1, Controlling CSS Access](#) for details about the two commands.

To change the timeout period, use the **tacacs-server timeout** command. Enter a number from 1 to 255. The default is 5 seconds. The CSS dynamically applies the modified global timeout period and the new value automatically takes effect on the next TACACS+ connection.

For example, to set the timeout period to 60 seconds, enter:

```
#(config) tacacs-server timeout 60
```

To reset the timeout period to the default of 5 seconds, enter:

```
#(config) no tacacs-server timeout
```

**Note**

---

The timeout period that you configure when you specify a TACACS+ server overrides the global timeout period (see the [“Defining a TACACS+ Server”](#) section).

---

## Defining a Global Encryption Key

The CSS allows you to define a global encryption key for communications with all configured TACACS+ servers. To encrypt TACACS+ packet transactions between the CSS and the TACACS+ server, you must define an encryption key. If you do not define an encryption key, packets are not encrypted. The key is a shared secret value that is identical to the one on the TACACS+ server. Use the **tacacs-server key** command to specify a shared secret between the CSS and the server.

The shared secret key can be either clear text entered in quotes or the DES-encrypted secret. The clear text key is DES-encrypted before it is placed in the running configuration. Either key type can have a maximum of 100 characters. The CSS dynamically applies the modified key and the new value automatically takes effect on the next TACACS+ connection.

For example, to define the clear text key, enter:

```
#(config) tacacs-server key "market"
```

To define a DES-encrypted key, enter:

```
#(config) tacacs-server key acskefterefesdtx
```

To remove the key, enter:

```
#(config) no tacacs-server key
```

**Note**

---

A shared secret that you configure when you specify a TACACS+ server overrides the global encryption key (see the [“Defining a TACACS+ Server”](#) section).

---

## Setting the Global TACACS+ Keepalive Frequency

The CSS allows you to define a global keepalive frequency for use with all configured TACACS+ servers. To determine the availability of the TACACS+ servers, the CSS sends periodic TCP keepalive probes to them. If the server does not respond to the probe within the configured timeout period, the CSS considers the server unavailable.

When it sends a keepalive to the TACACS+ server, the CSS attempts to use a persistent connection with the server. If the server is not configured for persistence, the CSS opens a new connection each time it sends a keepalive.

To set the global TACACS+ keepalive frequency, use the **tacacs-server frequency** command in global configuration mode. This command has the following syntax:

```
tacacs-server frequency number
```

The *number* variable defines the keepalive frequency in seconds. Enter an integer from 0 to 255. The default is 5 seconds. A setting of 0 disables keepalives. The CSS dynamically applies the modified keepalive frequency and immediately restarts the keepalive with the new value.

For example, to set the global TACACS+ keepalive frequency to 50 seconds, enter:

```
(config)# no tacacs-server frequency 50
```

**Note**

---

A keepalive frequency that you configure when you specify a TACACS+ server overrides the global keepalive frequency (see the [“Defining a TACACS+ Server”](#) section).

---

To reset the global TACACS+ keepalive frequency to the default of 5 seconds, use the **no tacacs-server frequency** command.

For example, enter:

```
(config)# no tacacs-server frequency
```

## Defining a TACACS+ Server

The TACACS+ server contains the TACACS+ authentication, authorization, and accounting databases. You can designate a maximum of three servers on the CSS. However, the CSS uses only one server at a time. The CSS selects the server based upon availability, giving preference to the configured primary server. The CSS sends periodic TCP keepalive probes at a frequency of every five seconds to the TACACS+ server to determine its operational state: Alive, Dying, or Dead. The TCP keepalive frequency is not user-configurable in the CSS.

**Note**

For general guidelines on the recommended setup of a TACACS+ server (the Cisco Secure Access Control Server in this example), see the [“TACACS+ Configuration Quick Start”](#) section.

To apply a TACACS+ global attribute, such as the timeout period, keepalive frequency, or shared secret, to a TACACS+ server, you must configure the global attribute before you configure the server. To apply a modified global attribute to a configured CSS TACACS+ server, remove the server and reconfigure it.

Use the **tacacs-server** command to define a server. You must provide the IP address and port number for the server. You can optionally define the timeout period and encryption key and designate the server as the primary server.

The syntax for this global configuration command is:

```
tacacs-server ip_address port {timeout [“cleartext_key”|des_key]}  
                {primary} {frequency number}
```

The variables and options for this command are as follows:

- *ip\_address* - The IP address of the TACACS+ server. Enter the IP address in dotted-decimal format.
- *port* - The TCP port of TACACS+ server. The default port is 49. You can enter a port number from 1 to 65535.
- *timeout* - (Optional) The amount of time to wait for a response from the server. Enter a number from 1 to 255. The default is 5 seconds. Defining this option overrides the **tacacs-server timeout** command. For more information on the TACACS+ timeout period and setting a global timeout, see the [“Setting the Global CSS TACACS+ Timeout Period”](#) section.
- *“cleartext\_key”|des\_key* - (Optional) The shared secret between the CSS and the server. You must define an encryption key to encrypt TACACS+ packet transactions between the CSS and the TACACS+ server. If you do not define an encryption key, packets are not encrypted.

The shared secret value is identical to the one on the TACACS+ server. The shared secret key can be either clear text entered in quotes or the DES-encrypted secret entered without quotes. The clear text key is DES-encrypted before it is placed in the running configuration. Either key type can have a maximum of 100 characters.

Defining this option overrides the **tacacs-server key** command. For more information on defining a global encryption key, see the “[Defining a Global Encryption Key](#)” section.

- **primary** - (Optional) Assigns the TACACS+ server precedence over the other configured servers. You can specify only one primary server.
- **frequency number** - (Optional) Allows you to set the keepalive frequency for the specified TACACS+ server. The default number variable is 5 seconds. The range for the variable is 0 to 255. A setting of 0 disables keepalives. Defining this option overrides the **tacacs-server frequency** command.



#### Note

If you need to change a timeout period or the shared secret for a specific server, you must delete the server and redefine it with the updated parameter.

For example, to define a primary TACACS+ server at IP address 192.168.11.1 with a default port of 49, a timeout period of 12 seconds, a clear text shared secret of summary, and a keepalive frequency of 10 seconds, enter:

```
#(config) tacacs-server 192.168.11.1 12 20 "summary" primary frequency 10
```

To delete a TACACS+ server at IP address 192.168.11.1 with a default port of 49, enter:

```
#(config) no tacacs-server 192.168.11.1 49
```

After configuring the TACACS+ server, enable TACACS+ authentication for console and virtual logins (if the username and password pair is not in the local user database) through the **virtual authentication** and **console authentication** commands. See [Chapter 1, Controlling CSS Access](#) for information about the two commands.

# Setting TACACS+ Authorization

TACACS+ authorization allows the TACACS+ server to control specific CSS commands that the user can execute. CSS authorization divides the command set into two categories:

- Configuration commands that change the CSS running configuration. For example, all commands in global configuration mode. For a complete list of global configuration mode commands, refer to the *Cisco Content Services Switch Command Reference*.
- Nonconfiguration commands that do not change the running configuration. These commands include, but are not limited to, mode transition, show, and administrative commands. For example, **cls** (clear screen), **endbranch**, **help**, **ping**, **show**, **terminal**, **traceroute**, and so on. For a complete list of nonconfiguration commands, refer to the *Cisco Content Services Switch Command Reference*.

**Note**

---

When you configure TACACS+ on a CSS, the CSS does not authorize scripts through the TACACS+ server. Because the CSS transforms all XML commands into scripts, the CSS also does not authorize XML commands through the TACACS+ server.

---

By default, authorization is disabled. When authorization is enabled, the TACACS+ server is responsible for granting permission or denying all attempts to issue commands.

When you enable authorization, the exchange between the TACACS+ server and the CSS causes a delay in executing the command. Failure of the TACACS+ server results in the failure of all authorization requests and the suspension of user activity unless another server is reachable. To enable users to execute commands in this case, configure a failover authentication method to a local user database. Users must log back in to the CSS.

In releases prior to 7.30.1.05, if you transitioned from one CLI mode to another (for example, from config mode to service mode), and a service already existed regardless of whether TACACS+ authorization was enabled for configuration or nonconfiguration commands, the CSS did not perform authorization on the command. If you were creating a service and authorization for configuration commands was enabled, then the TACACS+ server was queried if you were authorized to perform the command. In software version 7.30.1.05 and later, on a mode transition in an existing service, the CSS sends a command authorization request to the TACACS+ server if nonconfiguration commands are enabled.

Use the **tacacs-server authorize config** command to enable authorization of all commands that change the running configuration. For example:

```
 #(config) tacacs-server authorize config
```

Use the **tacacs-server authorize non-config** command to enable authorization of all commands that do not change the running configuration. For example:

```
 #(config) tacacs-server authorize non-config
```

Use the **no** form of these commands to disable authorization. For example, to disable authorization for commands that affect the running configuration, enter:

```
 #(config) no tacacs-server authorize config
```

To disable authorization for commands that do not affect the running configuration, enter:

```
 #(config) no tacacs-server authorize non-config
```

## Sending Full CSS Commands to the TACACS+ Server

CSS users can send the commands in their abbreviated syntax to the TACACS+ server. By default, the CSS sends the full syntax of the command, even though you enter the command in its abbreviated form. By expanding the syntax, the CSS minimizes TACACS+ authorization command failures resulting from their abbreviations.

Use the **no** form of the command to disable the CSS from sending the full command and instead to send the command as entered by the user. For example, enter:

```
 #(config) no tacacs-server send-full-command
```

To reenable the CSS to send the full command syntax, use the **tacacs-server send-full-command** command. For example:

```
 #(config) tacacs-server send-full-command
```

## Setting TACACS+ Accounting

TACACS+ accounting allows the TACACS+ server to receive an accounting report for commands that the user can execute. CSS accounting divides the command set into two categories:

- Configuration commands that change the CSS running configuration.
- Nonconfiguration commands that do not change the running configuration. These commands include, but are not limited to, mode transition commands, show commands, and administrative commands.

By default, the CSS disables accounting. When you enable accounting, you can account for configuration commands, nonconfiguration commands, or both.



### Note

---

Failure of the TACACS+ server does not result in the suspension of user activity.

---

Use the **tacacs-server account config** command to enable the CSS to send accounting reports to the TACACS+ server for all commands that change the running configuration. For example:

```
 #(config) tacacs-server account config
```

Use the **tacacs-server account non-config** command to enable the CSS to send accounting reports to the TACACS+ server for all commands that do not change the running configuration. For example:

```
 #(config) tacacs-server account non-config
```

Use the **no** form of these commands to disable accounting. For example, to disable accounting for commands that affect the running configuration, enter:

```
 #(config) no tacacs-server account config
```

To disable accounting for commands that do not affect the running configuration, enter:

```
 #(config) no tacacs-server account non-config
```

# Showing TACACS+ Server Configuration Information

Use the **show tacacs-server** command to display the TACACS+ server configuration information. To view this information, enter:

```
(config)# show tacacs-server
```

[Table 4-2](#) describes the fields in the **show tacacs-server** command output.

**Table 4-2** *Field Descriptions for the show tacacs-server Command*

Field	Description
IP/Port	The TACACS+ server IP address and port number
State	The operational state of the server (Alive, Dying, or Dead) determined by the internal TCP Keepalive
Primary	Indicates whether this record is the primary TACACS+ server
Authen	The number of authentication requests made to the TACACS+ server
Author	The number of authorization requests made to the TACACS+ server
Account	The number of accounting requests made to the TACACS+ server
Key	The shared secret configured for the TACACS+ server
Server Timeout	The timeout period that the CSS waits for a response from the TACACS+ server
Server Frequency	The keepalive frequency in seconds for the TACACS+ server
Global Timeout	The global timeout period that the CSS waits for a response from the TACACS+ servers
Global KAL Frequency	The global keepalive frequency in seconds for the TACACS+ servers
Global Key	The global shared secret, used by all TACACS+ servers, unless individually configured for the server

**Table 4-2** *Field Descriptions for the show tacacs-server Command (continued)*

<b>Field</b>	<b>Description</b>
Authorize Config Commands	Indicates whether configuration commands receive authorization
Authorize Non-Config	Indicates whether nonconfiguration commands receive authorization
Account Config Commands	Indicates whether the CSS sends accounting reports to TACACS+ servers for all commands that change the running configuration
Account Non-Config	Indicates whether the CSS sends accounting reports to TACACS+ servers for all commands that cannot change the running configuration

■ Showing TACACS+ Server Configuration Information