



Configuring TACACS+

This chapter describes how to configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router).

This chapter includes the following sections:

- [Information About TACACS+, page 3-1](#)
- [Prerequisites for TACACS+, page 3-5](#)
- [Guidelines and Limitations, page 3-5](#)
- [Default Settings, page 3-5](#)
- [Configuring TACACS+, page 3-6](#)
- [Monitoring TACACS+ Statistics, page 3-17](#)
- [Verifying TACACS+ Configuration, page 3-18](#)
- [Configuration Example, page 3-18](#)
- [Where to Go Next, page 3-18](#)

Information About TACACS+

The TACACS+ security protocol provides centralized validation of users attempting to gain access to the Cisco CG-OS router. 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 you can configure and employ the TACACS+ features on your Cisco CG-OS router.

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. The Cisco CG-OS router provides centralized authentication using the TACACS+ protocol.

This section includes the following topics:

- [TACACS+ Advantages, page 3-2](#)
- [TACACS+ Operation for User Login, page 3-2](#)

- [Default TACACS+ Server Encryption Type and Secret Key, page 3-3](#)
- [TACACS+ Server Monitoring, page 3-3](#)
- [Vendor-Specific Attributes, page 3-4](#)

TACACS+ Advantages

TACACS+ has the following advantages over RADIUS authentication:

- Provides independent AAA facilities. For example, the Cisco CG-OS router 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 Cisco CG-OS router 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 CG-OS router using TACACS+, the following actions occur:

1. When the Cisco CG-OS router establishes a connection, it contacts the TACACS+ daemon to obtain the username and password.



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 the maiden name of your mother.

2. The Cisco CG-OS router will eventually receive one of the following responses from the TACACS+ daemon:
 - a. **ACCEPT**—User authentication succeeds and service begins. When the Cisco CG-OS router requires user authorization, authorization begins.
 - b. **REJECT**—User authentication fails. The TACACS+ daemon either denies further access to the user or prompts the user to retry the login sequence.
 - c. **ERROR**—An error occurs at some time during authentication either at the daemon or in the network connection between the daemon and the Cisco CG-OS router. When the Cisco CG-OS router receives an **ERROR** response, the Cisco CG-OS router tries to use an alternative method for authenticating the user.

After authentication, the user also undergoes an additional authorization phase when authorization is enabled on the Cisco CG-OS router. Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the Cisco CG-OS router 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 Cisco CG-OS router to the TACACS+ server. A secret key is a secret text string shared between the Cisco CG-OS router 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 CG-OS router to use.

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

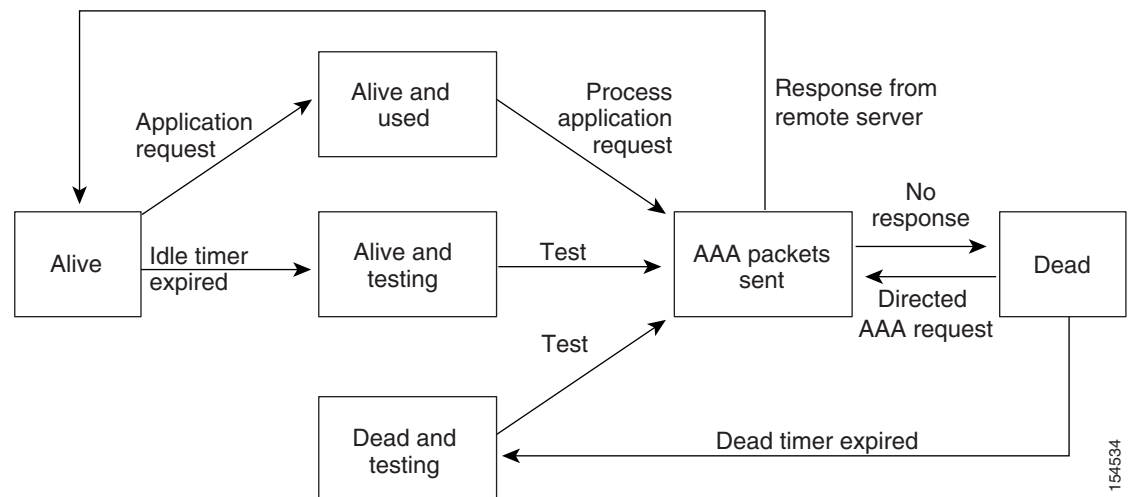
TACACS+ Server Monitoring

An unresponsive TACACS+ server can delay the processing of AAA requests.

A Cisco CG-OS router periodically monitors a TACACS+ server to check whether it is responding (or alive) to save time in processing AAA requests. The router marks an unresponsive TACACS+ server as dead and does not continue to send AAA requests to that dead TACACS+ server.

A Cisco CG-OS router periodically monitors dead TACACS+ servers and brings them to the alive state once they are responding. Continual monitoring ensures that a TACACS+ server is in a working state before it receives real AAA requests. Whenever a TACACS+ server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco CG-OS router displays an error message that a failure is taking place before it can impact performance. (See [Figure 3-1](#).)

Figure 3-1 TACACS+ Server States



Note

The Cisco CG-OS router initiates TACACS+ server monitoring by sending a test authentication request to the TACACS+ server.

Vendor-Specific Attributes

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.

This section includes the following topics:

- [Cisco VSA Format, page 3-4](#)
- [Cisco TACACS+ Privilege Levels, page 3-5](#)

Cisco VSA Format

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, separator is an equal sign (=) for mandatory attributes, and an asterisk (*) indicates optional attributes.

When you use TACACS+ servers for authentication on a Cisco CG-OS router, 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 Cisco CG-OS software supports the following VSA protocol options:

- **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, enclose the value within double quotation marks.

The Cisco CG-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 `vdc-admin`, the value field would be “`network-operator vdc-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 vdc-admin"
```

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



Note

When you specify a VSA as `shell:roles*"network-operator vdc-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 the standard TACACS+ accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the TACACS+ client on the Cisco CG-OS router. It can be used only with the accounting protocol data units (PDUs).

Cisco TACACS+ Privilege Levels

TACACS+ servers support privilege levels for specifying the permissions that users have when logging onto a Cisco CG-OS router. For the maximum privilege level 15, the Cisco CG-OS software applies the network-admin role in the default VDC or the vdc-admin role for non-default VDCs. All other privilege levels are translated to the vdc-operator role. For more information on user roles, see [Chapter 7, “Configuring User Accounts and RBAC.”](#)


Note

When you specify a user role in the cisco-av-pair, that takes precedence over the privilege level.


Note

Although references to a default VDC might be seen in CLI displays, the Cisco CG-OS router does not support the configuration of more than one VDC. The Cisco CG-OS router only supports a default VDC.

Prerequisites for TACACS+

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 CG-OS router is recognized as a TACACS+ client on the AAA servers.

Guidelines and Limitations

Configure a maximum of 64 TACACS+ servers on the Cisco CG-OS router.

When you have a user account configured on the local Cisco CG-OS router that has the same name as a remote user account on an AAA server, the Cisco CG-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Default Settings

[Table 3-1](#) lists the default settings for TACACS+ parameters.

Table 3-1 *Default TACACS+ Parameters*

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

Configuring TACACS+

This section includes the following topics:

- [TACACS+ Server Configuration Process, page 3-6](#)
- [Enabling TACACS+, page 3-7](#)
- [Configuring TACACS+ Server Hosts, page 3-7](#)
- [Configuring Global TACACS+ Keys, page 3-8](#)
- [Configuring a Key for a Specific TACACS+ Server, page 3-9](#)
- [Configuring TACACS+ Server Groups, page 3-10](#)
- [Configuring the Global Source Interface for TACACS+ Server Groups, page 3-11](#)
- [Configuring the Global TACACS+ Timeout Interval, page 3-12](#)
- [Configuring the Timeout Interval for a Server, page 3-12](#)
- [Configuring TCP Ports, page 3-13](#)
- [Configuring Periodic TACACS+ Server Monitoring, page 3-14](#)
- [Configuring the Dead-Time Interval, page 3-15](#)
- [Enabling ASCII Authentication, page 3-15](#)
- [Manually Monitoring TACACS+ Servers or Groups, page 3-16](#)
- [Disabling TACACS+, page 3-17](#)

TACACS+ Server Configuration Process

To configure TACACS+ servers, follow these steps:

-
- Step 1** Enable TACACS+. (See [Enabling TACACS+, page 3-7.](#))
- Step 2** Establish the TACACS+ server connections to the Cisco CG-OS router. (See [Configuring TACACS+ Server Hosts, page 3-7.](#))
- Step 3** Configure the secret keys for the TACACS+ servers. (See [Configuring Global TACACS+ Keys, page 3-8](#) and [Configuring a Key for a Specific TACACS+ Server, page 3-9.](#))
- Step 4** When needed, configure TACACS+ server groups with subsets of the TACACS+ servers for AAA authentication methods. (See [Configuring TACACS+ Server Groups, page 3-10](#) and [Configuring AAA, page 4-6.](#))
- Step 5** When needed, configure any of the following optional parameters:
- Dead-time interval (See [Configuring the Dead-Time Interval, page 3-15.](#))
 - TACACS+ server specification allowed at user login (See [Configuring the Global TACACS+ Timeout Interval, page 3-12.](#))
 - Timeout interval (See [Configuring the Global TACACS+ Timeout Interval, page 3-12.](#))
 - TCP port (See [Configuring TCP Ports, page 3-13.](#))
- Step 6** When needed, configure periodic TACACS+ server monitoring. (See [Configuring Periodic TACACS+ Server Monitoring, page 3-14.](#))
-

Enabling TACACS+

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

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>feature tacacs+</code>	Enables TACACS+.
Step 3	<code>show feature</code>	(Optional) Displays the enabled status of the feature.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable the TACACS+ feature on the Cisco CG-OS router before configuring commands that support authentication.

```
router# configure terminal
router(config)# feature tacacs+
router(config)# copy running-config startup-config
```

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 CG-OS router. You can configure up to 64 TACACS+ servers.



Note

By default, when you configure a TACACS+ server IP address or hostname on the Cisco CG-OS router, the TACACS+ server is added to the default TACACS+ server group. You can also add the TACACS+ server to another TACACS+ server group. For information about creating TACACS+ server groups, see [Configuring TACACS+ Server Groups, page 3-10](#).

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+, page 3-7](#).)

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

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	tacacs-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i> }	Specifies the IPv4 or IPv6 address or hostname for a TACACS+ server.
Step 3	show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 4	copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure an IP address for the TACACS+ server on the Cisco CG-OS router.

```
router# configure terminal
router(config)# tacacs-server host 10.10.2.2
router(config)# copy running-config startup-config
```

Configuring Global TACACS+ Keys

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

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

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

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	tacacs-server key [0 7] <i>key-value</i>	Specifies a TACACS+ key for all TACACS+ server. You can specify that the <i>key-value</i> is in clear text (0) format or is encrypted (7). The Cisco CG-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. By default, no secret key is configured.

	Command	Purpose
Step 3	<code>show tacacs-server</code>	(Optional) Displays the TACACS+ server configuration. Note The Cisco CG-OS router saves the secret keys in an encrypted form in the running configuration. Use the show running-config command to display the encrypted secret keys.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a global TACACS+ key for the Cisco CG-OS router.

```
router# configure terminal
router(config)# tacacs-server key 0 QsEfThUk0
router(config)# copy running-config startup-config
```

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 CG-OS router and the TACACS+ server host to allow secure communication.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

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

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>tacacs-server host {ipv4-address ipv6-address host-name} key [0 7] key-value</code>	Specifies a secret key for a specific TACACS+ server. You can specify that the <i>key-value</i> is in clear text (0) format or is encrypted (7). Cisco CG-OS software encrypts a clear text key before saving it to the running configuration. The maximum length is 63 characters. The default format is clear text. When a secret key is configured, it supersedes the global secret key.

	Command	Purpose
Step 3	<code>show tacacs-server</code>	(Optional) Displays the TACACS+ server configuration. Note The secret keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted secret keys.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a key for a specific TACACS+ server.

```
router# configure terminal
router(config)# tacacs-server host 10.10.1.1 key 0 P1IjUHYg
router(config)# copy running-config startup-config
```

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 use the TACACS+ protocol. The Cisco CG-OS router attempts access to the servers 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. For information on AAA services, see [Remote AAA Services, page 4-2](#).

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+, page 3-7](#).)

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>aaa group server tacacs+ <i>group-name</i></code>	Creates a TACACS+ server group and enters the TACACS+ server group configuration mode for that group.
Step 3	<code>server {<i>ipv4-address</i> <i>ipv6-address</i> <i>host-name</i>}</code>	Configures the TACACS+ server as a member of the TACACS+ server group. Tip If the specified TACACS+ server is not found, configure it using the tacacs-server host command and retry this command.

	Command	Purpose
Step 4	<code>deadtime minutes</code>	Configures the monitoring dead time. The range is from 1 through 1440. The default is 0 minutes. Note The recommended value is one (1) minute. A value greater than one incurs greater delay in authentication with the external AAA server. Note When the dead-time interval for a TACACS+ server group is greater than zero (0), that value takes precedence over the global dead-time value. (See Configuring the Dead-Time Interval , page 3-15.)
Step 5	<code>source-interface interface</code>	(Optional) Configures a source interface to access the TACACS+ servers in the server group. You can use Ethernet interfaces, loopback interfaces, or the management interface (mgmt 0). The default is the global source interface.
Step 6	<code>show tacacs-server groups</code>	(Optional) Displays the TACACS+ server group configuration.
Step 7	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a TACACS+ server group for authentication.

```
router# configure terminal
router(config)# aaa group server tacacs+ TacServer
router(config-tacacs)# server 10.10.2.2
router(config-tacacs)# deadtime 1
router(config-tacacs)# copy running-config startup-config
```

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. To configure a different source interface for a specific TACACS+ server group, see [Configuring TACACS+ Server Groups](#), page 3-10. By default, the Cisco CG-OS software uses any available interface.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>ip tacacs source-interface interface</code>	Configures the global source interface for all TACACS+ server groups configured on the device.

	Command	Purpose
Step 3	<code>show tacacs-server</code>	(Optional) Displays the TACACS+ server configuration information.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a global source interface for TACACS+ server groups.

```
router# configure terminal
router(config)# ip tacacs source-interface mgmt 0
router(config)# copy running-config startup-config
```

Configuring the Global TACACS+ Timeout Interval

You can set a global timeout interval for all TACACS+ servers. The timeout interval determines how long the Cisco CG-OS router waits for responses from TACACS+ servers before declaring a timeout failure.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>tacacs-server timeout seconds</code>	Specifies the timeout interval for TACACS+ servers. The range is from 1 to 60 seconds. The default timeout interval is 5 seconds.
Step 3	<code>show tacacs-server</code>	(Optional) Displays the TACACS+ server configuration.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a global TACACS+ timeout interval for the Cisco CG-OS router.

```
router# configure terminal
router(config)# tacacs-server timeout 10
router(config)# copy running-config startup-config
```

Configuring the Timeout Interval for a Server

The timeout interval determines how long the Cisco CG-OS router waits for responses from a TACACS+ server before declaring a timeout failure.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+, page 3-7.](#))

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>tacacs-server host { ipv4-address ipv6-address host-name } timeout seconds</code>	Specifies the timeout interval for a specific server. The default is the global value. Note When you configure a timeout interval value for a TACACS+ server, that value overrides any global timeout interval value configured for all TACACS+ servers.
Step 3	<code>show tacacs-server</code>	(Optional) Displays the TACACS+ server configuration.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure a timeout for a TACACS+ server.

```
router# configure terminal
router(config)# tacacs-server host server1 timeout 10
router(config)# copy running-config startup-config
```

Configuring TCP Ports

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

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+, page 3-7.](#))

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>tacacs-server host { ipv4-address ipv6-address host-name } port tcp-port</code>	Specifies the TCP port to use for TACACS+ messages to the server. The range is from 1 to 65535. The default TCP port is 49.
Step 3	<code>show tacacs-server</code>	(Optional) Displays the TACACS+ server configuration.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

```
router# configure terminal
router(config)# tacacs-server host 10.10.1.1 port 2
router(config)# copy running-config startup-config
```

Configuring Periodic TACACS+ Server Monitoring

You can monitor the availability of TACACS+ servers. The monitoring 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 CG-OS router sends out a test packet. You can configure this option to test servers periodically, or you can run a one-time only test.

**Note**

To protect network security, Cisco recommends 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, the Cisco CG-OS router does not perform periodic TACACS+ server monitoring.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

DETAILED STEPS

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

EXAMPLE

This example shows how to configure a dead time interval to monitor the availability of a TACACS+ server and how to configure a unique monitoring username and password.

```
router(config)# configure terminal
router(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
router(config)# tacacs-server deadtime 5
router(config)# copy running-config startup-config
```

Configuring the Dead-Time Interval

You can configure a global dead-time interval for all TACACS+ servers. The dead-time interval specifies the time that the Cisco CG-OS router 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 server group. (See [Configuring TACACS+ Server Groups](#), page 3-10.)

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	tacacs-server deadtime <i>minutes</i>	Configures the global dead time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes
Step 3	show tacacs-server	(Optional) Displays the TACACS+ server configuration.
Step 4	copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to deliver a global deadtime interval that applies to all TACACS+ servers.

```
router(config)# configure terminal
router(config)# tacacs-server deadtime 5
router(config)# copy running-config startup-config
```

Enabling ASCII Authentication

You can enable ASCII authentication on the TACACS+ server.

**Note**

Only TACACS+ servers support ASCII authentication.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+, page 3-7.](#))

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	aaa authentication login ascii-authentication	Enables ASCII authentication. The default is disabled.
Step 3	show aaa authentication login ascii-authentication	(Optional) Displays the TACACS+ ASCII authentication configuration.
Step 4	copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable ASCII authentication on the TACACS+ server.

```
router# configure terminal
router(config)# aaa authentication login ascii-authentication
router(config)# copy running-config startup-config
```

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+. (See [Enabling TACACS+, page 3-7.](#))

DETAILED STEPS

Enter one or both of the commands below as applicable.

Command	Purpose
test aaa server tacacs+ {ipv4-address ipv6-address host-name} username password	Sends a test message to a TACACS+ server to confirm availability.
test aaa group group-name username password	Sends a test message to a TACACS+ server group to confirm availability.

EXAMPLE

This example shows how to configure a command to send a manual test of a TACACS+ server.


```
router# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
```

This example shows how to configure a command to send a manual test of a TACACS+ server group.

```
router# test aaa group TacGroup user2 As3He3CI
```

Disabling TACACS+

You can disable TACACS+.



Caution

When you disable TACACS+, the Cisco CG-OS router automatically discards all related running configurations.

BEFORE YOU BEGIN

Ensure that an alternate TACACS+ server resource is available for those devices that are authenticated by the server before it is taken out of service.

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>no feature tacacs+</code>	Disables TACACS+.
Step 3	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to disable a TACACS+ server.

```
router# configure terminal
router(config)# no feature tacacs+
router(config)# copy running-config startup-config
```

Monitoring TACACS+ Statistics

You can display the statistics that the Cisco CG-OS router maintains for TACACS+ activity by using the command in the table below.

BEFORE YOU BEGIN

Enable TACACS+. (See [Enabling TACACS+](#), page 3-7.)

Command	Purpose
<code>show tacacs-server statistics {hostname ipv4-address ipv6-address}</code>	Displays the TACACS+ statistics.

Verifying TACACS+ Configuration

To display TACACS+ configuration information, enter any or all of the following commands:

Command	Purpose
<code>show feature</code>	Displays the enabled status of the feature.
<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] [groups sorted statistics]</code>	<p>Displays all configured TACACS+ server parameters.</p> <p>Note The Cisco CG-OS router does not support the directed-response option of this command and it is not shown in the command.</p>

Configuration Example

The following example shows how to configure TACACS+:

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

Where to Go Next

You can now configure AAA authentication methods to include the TACACS+ server groups. (See [Chapter 4, “Configuring AAA”](#).)