

TACACS, Extended TACACS, and TACACS+ Commands

This chapter describes the commands used to configure TACACS, extended TACACS, and TACACS+.

TACACS Command Comparison

There are currently three versions of the TACACS security protocol, each a separate entity. The Cisco IOS software supports the following versions of TACACS:

- TACACS+—Provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.
- Extended TACACS—Provides information about protocol translator and router use. This information is used in UNIX auditing trails and accounting files.
- TACACS—Provides password checking and authentication, and notification of user actions for security and accounting purposes.

Although TACACS+ is enabled through AAA and uses commands specific to AAA, there are some commands that are common to TACACS, extended TACACS, and TACACS+. Table 1 identifies Cisco IOS commands available to the different versions of TACACS.

Table 1 TACACS Command Comparison

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
aaa accounting	–	–	Yes
aaa authentication arap	–	–	Yes
aaa authentication enable default	–	–	Yes
aaa authentication login	–	–	Yes
aaa authentication local override	–	–	Yes
aaa authentication ppp	–	–	Yes
aaa authorization	–	–	Yes
aaa new-model	–	–	Yes
arap authentication	–	–	Yes
arap use-tacacs	Yes	Yes	–
enable last-resort	Yes	Yes	–
enable use-tacacs	Yes	Yes	–

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**Table 1 TACACS Command Comparison (continued)**

Cisco IOS Command	TACACS	Extended TACACS	TACACS+
ip tacacs source-interface	Yes	Yes	Yes
login authentication	–	–	Yes
login tacacs	Yes	Yes	–
ppp authentication	Yes	Yes	Yes
ppp use-tacacs	Yes	Yes	Yes
tacacs-server attempts	Yes	–	–
tacacs-server authenticate	Yes	Yes	–
tacacs-server directed-request	Yes	Yes	Yes
tacacs-server extended	–	Yes	–
tacacs-server host	Yes	Yes	Yes
tacacs-server key	–	–	Yes
tacacs-server last-resort	Yes	Yes	–
tacacs-server notify	Yes	Yes	–
tacacs-server optional-passwords	Yes	Yes	–
tacacs-server retransmit	Yes	Yes	–
tacacs-server timeout	Yes	Yes	–

**Note**

Refer to the “Authentication Commands” chapter, the “Authorization Commands” chapter, and the “Accounting Commands” chapter for information about commands specific to AAA.

For information on how to configure TACACS or extended TACACS, refer to the “Configuring TACACS and Extended TACACS” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “TACACS Configuration Examples” section located at the end of the “Configuring TACACS and Extended TACACS” chapter in the *Security Configuration Guide*.

For information on how to configure TACACS+, refer to the “Configuring TACACS+” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “TACACS+ Configuration Examples” section located at the end of the “Configuring TACACS+” chapter in the *Security Configuration Guide*.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**arap use-tacacs**

To enable TACACS for ARA authentication, use the **arap use-tacacs** line configuration command. Use the **no** form of this command to disable TACACS for ARA authentication.

arap use-tacacs [single-line]

no arap use-tacacs

Syntax Description

single-line (Optional) Accepts the username and password in the username field. If you are using an older version of TACACS (before extended TACACS), you must use this keyword.

Defaults

Disabled

Command Modes

Line configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command only when you have set up an extended TACACS server. This command requires the new extended TACACS server.

**Note**

This command cannot be used with TACACS+. Use the **arap authentication** command instead.

The command specifies that if a username and password are specified in the username, separated by an asterisk (*), then a standard TACACS login query is performed using that username and password. If the username does not contain an asterisk, then normal ARA authentication is performed using TACACS.

This feature is useful when integrating TACACS with other authentication systems that require a clear text version of the user's password. Such systems include one-time passwords, token card systems, and others.

**Caution**

Normal ARA authentications prevent the clear-text password from being transmitted over the link. When you use the single-line keyword, passwords cross the link in the clear, exposing them to anyone looking for such information.

Due to the two-way nature of the ARA authentication, the ARA application requires that a password value be entered in the Password field in the ARA dialog box. This secondary password must be "arap." First enter the username and password in the form *username*password* in the Name field of the dialog box, then enter **arap** in the Password field.

Examples

The following example enables TACACS for ARA authentication:

```
line 3
 arap use-tacacs
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

Related Commands	Command	Description
	arap enable	Enables ARA for a line.
	arap nolog	Prevents Apple Macintosh guests from logging in to the router.
	autoselect	Configures a line to start an ARA, PPP, or SLIP session.
	tacacs-server extended	Enables an extended TACACS mode.
	tacacs-server host	Specifies a TACACS host.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**enable last-resort**

To specify what happens if the TACACS and extended TACACS servers used by the enable command do not respond, use the **enable last-resort** global configuration command. Use the **no** form of this command to restore the default.

```
enable last-resort {password | succeed}
```

```
no enable last-resort {password | succeed}
```

Syntax Description

password	Allows you to enter enable mode by entering the privileged command level password. A password must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
succeed	Allows you to enter enable mode without further question.

Defaults

Access to enable mode is denied.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This secondary authentication is used only if the first attempt fails.

**Note**

This command is not used with TACACS+, which uses the **aaa authentication** suite of commands instead.

Examples

In the following example, if the TACACS servers do not respond to the enable command, the user can enable by entering the privileged level password:

```
enable last-resort password
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**enable use-tacacs**

To enable the use of TACACS to determine whether a user can access the privileged command level, use the **enable use-tacacs** global configuration command. Use the **no** form of this command to disable TACACS verification.

enable use-tacacs

no enable use-tacacs

**Caution**

If you use the **enable use-tacacs** command, you must also use the **tacacs-server authenticate enable** command or you will be locked out of the privileged command level.

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When you add this command to the configuration file, the EXEC enable command prompts for a new username and password pair. This pair is then passed to the TACACS server for authentication. If you are using extended TACACS, it also passes any existing UNIX user identification code to the server.

**Note**

This command initializes TACACS. Use the **tacacs server-extended** command to initialize extended TACACS or use the **aaa new-model** command to initialize AAA and TACACS+.

Examples

The following example sets TACACS verification on the privileged EXEC-level login sequence:

```
enable use-tacacs
tacacs-server authenticate enable
```

Related Commands

Command	Description
tacacs-server authenticate	Configures the Cisco IOS software to indicate whether users can perform an attempted action under TACACS and extended TACACS.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**ip tacacs source-interface**

To use the IP address of a specified interface for all outgoing TACACS packets, use the **ip tacacs source-interface** global configuration command. Use the **no** form of this command to disable use of the specified interface IP address.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Syntax Description

subinterface-name Name of the interface that TACACS uses for all of its outgoing packets.

Defaults

This command has no factory-assigned default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command to set a subinterface's IP address for all outgoing TACACS packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have an IP address or is in a *down* state, TACACS reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the *up* state.

Examples

The following example makes TACACS use the IP address of subinterface s2 for all outgoing TACACS (TACACS, extended TACACS, or TACACS+) packets:

```
ip tacacs source-interface s2
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server attempts**

To control the number of login attempts that can be made on a line set up for TACACS verification, use the **tacacs-server attempts** global configuration command. Use the **no** form of this command to restore the default.

tacacs-server attempts *count*

no tacacs-server attempts

Syntax Description	<i>count</i>	Integer that sets the number of attempts. The default is 3 attempts.
--------------------	--------------	--

Defaults	Three attempts
----------	----------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	None.
------------------	-------

Examples	The following example allows only one login attempt:
----------	--

```
tacacs-server attempts 1
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server authenticate**

To configure the Cisco IOS software to indicate whether users can perform an attempted action under TACACS and extended TACACS, use the **tacacs-server authenticate** global configuration command. Use the **no** form of this command to remove authentication.

```
tacacs-server authenticate { connection [always] enable | slip [always] [access-lists] }
```

```
no tacacs-server authenticate
```

Syntax Description

connection	Configures a required response when a user makes a TCP connection.
always	(Optional) Performs authentication even when a user is not logged in.
enable	Configures a required response when a user enters the enable command.
slip	Configures a required response when a user starts a SLIP or PPP session.
access-lists	(Optional) Requests and installs access lists. This option only applies to the slip keyword.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords were added to this command: { connection [always] enable slip [always] [access-lists] }.

Usage Guidelines

Enter one of the keywords to specify the action (when a user enters enable mode, for example).

Before you use the **tacacs-server authenticate** command, you must enable the **tacacs-server extended** command.

**Note**

This command is not used in TACACS+. It has been replaced by the **aaa authorization** command.

Examples

The following example configures TACACS logins that authenticate users to use Telnet or rlogin:

```
tacacs-server authenticate connect
```

Related Commands

Command	Description
enable secret	Specifies an additional layer of security over the enable password command.
enable use-tacacs	Enables the use of TACACS to determine whether a user can access the privileged command level.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server directed-request**

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request** global configuration command. Use the **no** form of this command to send the entire string to the TACACS server.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command sends only the portion of the username before the “@” symbol to the host specified after the “@” symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the “@” symbol, to be sent to the default TACACS server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS servers can be specified by the user after the “@” symbol. If the host name specified by the user does not match the IP address of a TACACS server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS servers and to cause the entire string to be passed to the default server.

Examples

The following example enables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS server:

```
no tacacs-server directed-request
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server extended**

To enable an extended TACACS mode, use the **tacacs-server extended** global configuration command. Use the **no** form of this command to disable the mode.

tacacs-server extended

no tacacs-server extended

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command initializes extended TACACS.

Examples

The following example enables extended TACACS mode:

```
tacacs-server extended
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server host**

To specify a TACACS host, use the **tacacs-server host** global configuration command. Use the **no** form of this command to delete the specified name or address.

```
tacacs-server host hostname [single-connection] [port integer] [timeout integer] [key string]  
no tacacs-server host hostname
```

Syntax Description

<i>hostname</i>	Name or IP address of the host.
single-connection	(Optional) Specify that the router maintain a single open connection for confirmation from a AAA/TACACS+ server (CiscoSecure Release 1.0.1 or later). This command contains no autodetect and fails if the specified host is not running a CiscoSecure daemon.
port	(Optional) Specify a server port number. This option overrides the default, which is port 49.
<i>integer</i>	(Optional) Port number of the server. Valid port numbers range from 1 to 65535.
timeout	(Optional) Specify a timeout value. This overrides the global timeout value set with the tacacs-server timeout command for this server only.
<i>integer</i>	(Optional) Integer value, in seconds, of the timeout interval.
key	(Optional) Specify an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only.
<i>string</i>	(Optional) Character string specifying authentication and encryption key.

Defaults

No TACACS host is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **single-connection**, **port**, **timeout**, and **key** options only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**Examples**

The following example specifies a TACACS host named Sea_Change:

```
tacacs-server host Sea_Change
```

The following example specifies that, for AAA confirmation, the router consult the CiscoSecure TACACS+ host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
tacacs-server host Sea_Cure single-connection port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
login tacacs	Configures your router to use TACACS user authentication.
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.
tacacs-server timeout	Sets the interval that the server waits for a server host to reply.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server key**

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

tacacs-server key *key*

no tacacs-server key [*key*]

Syntax Description

key Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

After enabling AAA with the **aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
tacacs-server key dare to go
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
tacacs-server host	Specifies a TACACS host.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server last-resort**

To cause the network access server to request the privileged password as verification, or to allow successful login without further input from the user, use the **tacacs-server last-resort** global configuration command. Use the **no** form of this command to deny requests when the server does not respond.

tacacs-server last-resort {password | succeed }

no tacacs-server last-resort {password | succeed }

Syntax Description

password Allows the user to access the EXEC command mode by entering the password set by the **enable** command.

succeed Allows the user to access the EXEC command mode without further question.

Defaults

If, when running the TACACS server, the TACACS server does not respond, the default action is to deny the request.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **tacacs-server last-resort** command to be sure that login can occur; for example, when a systems administrator needs to log in to troubleshoot TACACS servers that might be down.

**Note**

This command is not used in TACACS+.

Examples

The following example forces successful login:

```
tacacs-server last-resort succeed
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
login (EXEC)	Enables or changes a login username.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL

tacacs-server login-timeout

The **timeout login response** command replaces this command. Refer to the description of the **timeout login response** command for more information.

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server notify**

To cause a message to be transmitted to the TACACS server, with retransmission being performed by a background process for up to five minutes, use the **tacacs-server notify** global configuration command. Use the **no** form of this command to disable notification.

```
tacacs-server notify {connection [always] | enable | logout [always] | slip [always]}
```

```
no tacacs-server notify
```

Syntax Description

connection	Specifies that a message be transmitted when a user makes a TCP connection.
always	(Optional) Sends a message even when a user is not logged in. This option applies only to SLIP or PPP sessions and can be used with the logout or slip keywords.
enable	Specifies that a message be transmitted when a user enters the enable command.
logout	Specifies that a message be transmitted when a user logs out.
slip	Specifies that a message be transmitted when a user starts a SLIP or PPP session.

Defaults

No message is transmitted to the TACACS server.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The keywords always and slip were added to this command.

Usage Guidelines

The terminal user receives an immediate response, allowing access to the feature specified. Enter one of the keywords to specify notification of the TACACS server upon receipt of the corresponding action (when a user logs out, for example).



This command is not used in TACACS+. It has been replaced by the **aaa accounting** suite of commands.

Examples

The following example sets up notification of the TACACS server when a user logs out:

```
tacacs-server notify logout
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server optional-passwords**

To specify that the first TACACS request to a TACACS server be made *without* password verification, use the **tacacs-server optional-passwords** global configuration command. Use the **no** form of this command to restore the default.

tacacs-server optional-passwords

no tacacs-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the TACACS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The TACACS server must support authentication for users without passwords to make use of this feature. This feature supports all TACACS requests, such as login, SLIP, and enable.

**Note**

This command is not used by TACACS+.

Examples

The following example configures the first login to not require TACACS verification:

```
tacacs-server optional-passwords
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server retransmit**

To specify the number of times the Cisco IOS software searches the list of TACACS server hosts before giving up, use the **tacacs-server retransmit** global configuration command. Use the **no** form of this command to disable retransmission.

tacacs-server retransmit *retries*

no tacacs-server retransmit

Syntax Description *retries* Integer that specifies the retransmit count.

Defaults Two retries

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines The Cisco IOS software will try all servers, allowing each one to time out before increasing the retransmit count.

Examples The following example specifies a retransmit counter value of five times:

```
tacacs-server retransmit 5
```

(DRAFT LABEL) ALPHA DRAFT - CISCO CONFIDENTIAL**tacacs-server timeout**

To set the interval that the server waits for a server host to reply, use the **tacacs-server timeout** global configuration command. Use the **no** form of this command to restore the default.

tacacs-server timeout *seconds*

no tacacs-server timeout

Syntax Description

seconds Integer that specifies the timeout interval in seconds (between 1 and 300).
The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example changes the interval timer to 10 seconds:

```
tacacs-server timeout 10
```

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS host.