

# Configuring TACACS and Extended TACACS

---

The Terminal Access Controller Access Control System (TACACS) provides a way to centrally validate users attempting to gain access to a router or access server. Basic Cisco TACACS support is modeled after the original Defense Data Network (DDN) application. TACACS services are maintained in a database on a TACACS server running, typically, on a UNIX workstation. You must have access to and must configure a TACACS server before configuring the TACACS features on your Cisco router.

Cisco implements TACACS in the Cisco IOS software to allow centralized control over access to routers and access servers. Authentication can also be provided for Cisco IOS administration tasks on the router and access server user interfaces. With TACACS enabled, the router or access server prompts for a username and password, then verifies the password with a TACACS server.

This chapter describes the TACACS and extended TACACS protocols and the various ways you can use them to secure access to your network.

---

**Note** Both TACACS and extended TACACS are now deprecated by Cisco.

---

For a complete description of the TACACS and extended TACACS commands used in this chapter, refer to the “TACACS, Extended TACACS, and TACACS+ Commands” chapter in the *Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

## TACACS Protocol Description

Cisco IOS software currently supports three versions of the Terminal Access Controller Access Control System (TACACS) security protocol, each one of which is a separate and unique protocol:

- TACACS+—A recent protocol providing 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.
- TACACS—An older access protocol, incompatible with the newer TACACS+ protocol, that is now deprecated by Cisco. It provides password checking and authentication, and notification of user actions for security and accounting purposes.
- Extended TACACS—An extension to the older TACACS protocol, supplying additional functionality to TACACS. Extended TACACS provides information about protocol translator and router use. This information is used in UNIX auditing trails and accounting files. Extended TACACS is incompatible with TACACS+ and is also deprecated.

This chapter discusses how to enable and configure TACACS and extended TACACS. For information about TACACS+, refer to the “Configuring TACACS+” chapter.

Table 14 identifies Cisco IOS commands available to the different versions of TACACS.

**Table 14 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	–
ip tacacs source-interface	Yes	Yes	Yes
login authentication	–	–	Yes
login tacacs	Yes	Yes	–
ppp authentication	Yes	Yes	Yes
ppp use-tacacs	Yes	Yes	No
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	Yes

## TACACS and Extended TACACS Configuration Task List

You can establish TACACS-style password protection on both user and privileged levels of the system EXEC.

The following sections describe the features available with TACACS and extended TACACS. The extended TACACS software is available using the File Transfer Protocol (FTP)—see the README file in the *ftp-eng.cisco.com* directory.

---

**Note** TACACS and extended TACACS commands cannot be used after you have initialized AAA. To identify which commands can be used with the three versions, refer to Table 14 earlier in this chapter.

---

- Set TACACS Password Protection at the User Level
- Disable Password Checking at the User Level
- Set Optional Password Verification
- Set TACACS Password Protection at the Privileged Level
- Disable Password Checking at the Privileged Level
- Set Notification of User Actions
- Set Authentication of User Actions
- Establish the TACACS Server Host
- Set Limits on Login Attempts
- Enable the Extended TACACS Mode
- Enable Extended TACACS for PPP Authentication
- Enable Standard TACACS for ARA Authentication
- Enable Extended TACACS for ARA Authentication
- Enable TACACS to Use a Specific IP Address

---

**Note** If you require additional security using IP access lists, see the “Configuring IP Services” chapter in the *Network Protocols Configuration Guide, Part 1* for more information.

---

For TACACS configuration examples, refer to the “TACACS Configuration Examples” section located at the end of the this chapter.

### Set TACACS Password Protection at the User Level

To enable password checking at login, use the following command in line configuration mode:

Command	Purpose
<code>login tacacs</code>	Set the TACACS-style user ID and password-checking mechanism.

---

**Note** When configuring TACACS, any usernames locally defined on the router will be used. The router will not go to the TACACS server for authentication.

---

## Disable Password Checking at the User Level

If a TACACS server does not respond to a login request, the Cisco IOS software denies the request by default. However, you can prevent that login failure in one of the following two ways:

- Allow a user to access privileged EXEC mode if that user enters the password set by the **enable** command.
- Allow the user to access the privileged EXEC mode without further question.

To specify one of these features, use either of the following commands in global configuration mode:

Command	Purpose
<b>tacacs-server last-resort password</b>	Allow a user to access privileged EXEC mode.
<b>tacacs-server last-resort succeed</b>	Set last resort options for logins.

## Set Optional Password Verification

You can specify that the first TACACS request to a TACACS server is made without password verification. To do so, use the following command in global configuration mode:

Command	Purpose
<b>tacacs-server optional-passwords</b>	Set TACACS password as optional.

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 is completed. If the TACACS server refuses this request, the terminal server 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.

## Set TACACS Password Protection at the Privileged Level

You can set the TACACS protocol to determine whether a user can access the privileged EXEC level. To do so, use the following command in global configuration mode:

Command	Purpose
<b>enable use-tacacs</b>	Set the TACACS-style user ID and password-checking mechanism at the privileged EXEC level.

When you set TACACS password protection at the privileged EXEC level, the EXEC **enable** command will ask for both a new username and a password. This information is then passed to the TACACS server for authentication. If you are using the extended TACACS, it also passes any existing UNIX user identification code to the server.



**Caution** If you use the **enable use-tacacs** command, you must also specify **tacacs-server authenticate enable**; otherwise, you will be locked out.

---

**Note** When used without extended TACACS, this task allows anyone with a valid username and password to access the privileged command level, creating a potential security problem. This is because the TACACS query resulting from entering the **enable** command is indistinguishable from an attempt to log in without extended TACACS.

---

## Disable Password Checking at the Privileged Level

You can specify a last resort if the TACACS servers used by the **enable** command do not respond. To invoke this “last resort” login feature, use either of the following commands in global configuration mode:

Command	Purpose
<b>enable last-resort password</b>	Allow user to enable by asking for the privileged EXEC-level password.
<b>enable last-resort succeed</b>	Allow user to enable without further questions.

## Set Notification of User Actions

The **tacacs-server notify** command allows you to configure the TACACS server to send a message when a user does the following:

- Makes a TCP connection
- Enters the **enable** command
- Logs out

To specify that the TACACS server send notification, use the following command in global configuration mode:

Command	Purpose
<b>tacacs-server notify</b> { <b>connection</b> [ <b>always</b> ]   <b>enable</b>   <b>logout</b> [ <b>always</b> ]   <b>slip</b> [ <b>always</b> ]}	Set server notification of user actions.

The retransmission of the message is performed by a background process for up to five minutes. The terminal user, however, receives an immediate response, allowing access to the terminal.

The **tacacs-server notify** command is available only if you have set up an extended TACACS server using the latest Cisco extended TACACS server software, available via FTP. (See the README file in the *ftp-eng.cisco.com* directory.)

## Set Authentication of User Actions

For a SLIP or PPP session, you can specify that if a user tries to start a session, the TACACS software requires a response (either from the TACACS server host or the router) indicating whether the user can start the session. You can specify that the TACACS software perform authentication even when a user is not logged in; you can also request that the TACACS software install access lists.

If a user issues the **enable** command, the TACACS software must respond indicating whether the user can give the command. You can also specify authentication when a user enters the **enable** command.

To configure any of these scenarios, use the following command in global configuration mode:

Command	Purpose
<b>tacacs-server authenticate</b> {connection[always] enable   slip [always] [access-lists]}	Set server authentication of user actions.

The **tacacs-server authenticate** command is available only when you have set up an extended TACACS server using the latest Cisco extended TACACS server software, which is available via FTP. (See the README file in the *ftp.cisco.com* directory).

## Establish the TACACS Server Host

The **tacacs-server host** command allows you to specify the names of the IP host or hosts maintaining a TACACS server. Because the TACACS software searches for the hosts in the order specified, this feature can be useful for setting up a list of preferred servers.

With TACACS and extended TACACS, the **tacacs-server retransmit** command allows you to modify the number of times the system software searches the list of TACACS servers (from the default of two times) and the interval it waits for a reply (from the default of five seconds).

To define the number of times the Cisco IOS software searches the list of servers, and how long the server waits for a reply, use the following commands as needed for your system configuration in global configuration mode:

Step	Command	Purpose
1	<b>tacacs-server host</b> <i>name</i>	Specify a TACACS host.
2	<b>tacacs-server retransmit</b> <i>retries</i>	Specify the number of times the server will search the list of TACACS and extended TACACS server hosts before giving up.
3	<b>tacacs-server timeout</b> <i>seconds</i>	Set the interval the server waits for a TACACS and extended TACACS server host to reply.

## Set Limits on Login Attempts

The **tacacs-server attempts** command allows you to specify the number of login attempts that can be made on a line set up for TACACS. Use the following command in global configuration mode to limit login attempts:

Command	Purpose
<b>tacacs-server attempts</b> <i>count</i>	Control the number of login attempts that can be made on a line set for TACACS verification.

## Enable the Extended TACACS Mode

While standard TACACS provides only username and password information, extended TACACS mode provides information about the terminal requests to help set up UNIX auditing trails and accounting files for tracking the use of protocol translators, access servers, and routers. The information includes responses from these network devices and validation of user requests.

An unsupported, extended TACACS server is available via FTP for UNIX users who want to create the auditing programs (see the README file in the *ftp-eng.cisco.com* directory).

To enable extended TACACS mode, use the following command in global configuration mode:

Command	Purpose
<code>tacacs-server extended</code>	Enable an extended TACACS mode.

---

**Note** When configuring extended TACACS, any usernames locally defined on the router will be used. The router will not go to the TACACS server for authentication.

---

## Enable Extended TACACS for PPP Authentication

You can use extended TACACS for authentication within PPP sessions. To do so, use the following commands in interface configuration mode:

Step	Command	Purpose
1	<code>ppp authentication {chap   chap pap   pap chap   pap} [if-needed] [list-name   default] [callin]</code>	Enable CHAP or PAP.
2	<code>ppp use-tacacs [single-line]</code>	Enable Extended TACACS under PPP.

For more information on PPP, refer to the “Configuring Media-Independent PPP and Multilink PPP” chapter in the *Dial Solutions Configuration Guide*. For an example of enabling TACACS for PPP protocol authentication, see the “TACACS Configuration Examples” section at the end of this chapter.

## Enable Standard TACACS for ARA Authentication

You can use the standard TACACS protocol for authentication within AppleTalk Remote Access (ARA) protocol sessions. To do so, use the following commands starting in line configuration mode:

Step	Command	Purpose
1	<b>arap use-tacacs single-line</b>	Enable standard TACACS under the ARA protocol.
2	<b>autoselect arap</b>	Enable autoselection of ARA.
3	<b>autoselect during-login</b>	(Optional) Have the ARA session start automatically at user login.

The **arap use-tacacs single-line** command 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.

By using the optional **during-login** argument with the **autoselect** command, you can display the username or password prompt without pressing the **Return** key. While the username or password name is displayed, you can choose to answer these prompts or to start sending packets from an autoselected protocol.

The remote user logs in through ARA as follows:

- Step 1** When prompted for a username by the ARA application, the remote user enters *username\*password* and presses **Return**.
- Step 2** When prompted for password by the ARA application, the remote user enters **arap** and presses **Return**.

For more information on the ARA protocol, refer to the "Configuring AppleTalk Remote Access" chapter in the *Dial Solutions Configuration Guide*. For examples of enabling TACACS for ARA protocol authentication, see the "TACACS Configuration Examples" section at the end of this chapter.

## Enable Extended TACACS for ARA Authentication

You can use extended TACACS for authentication within AppleTalk Remote Access (ARA) protocol sessions. The extended TACACS server software is available via FTP (see the README file in the *ftp.cisco.com* directory).

---

**Note** Before entering the commands listed in the following task table, you must edit the file called "Makefile" in the extended TACACS server software to use ARA. To do this, you must uncomment the lines that enable ARA support and recompile the file.

---

After installing an extended TACACS server with ARA support, use the following commands in line configuration mode on each line:

Step	Command	Purpose
1	<b>arap use-tacacs</b>	Enable extended TACACS under the ARA protocol on each line.
2	<b>autoselect arap</b>	(Optional) Enable autoselection of ARA.
3	<b>autoselect during-login</b>	(Optional) Have the ARA session start automatically at user login.

By using the optional **during-login** argument with the **autoselect** command, you can display the username or password prompt without pressing the Return key. While the Username or Password name is being presented, you can choose to answer these prompts, or to start sending packets from an autoselected protocol.

For more information on the ARA protocol, refer to the “Configuring AppleTalk Remote Access” chapter in the *Dial Solutions Configuration Guide*.

## Enable TACACS to Use a Specific IP Address

You can designate a fixed source IP address for all outgoing TACACS packets. The feature enables TACACS to use the IP address of a specified interface for all outgoing TACACS packets. This is especially useful if the router has many interfaces, and you want to make sure that all TACACS packets from a particular router have the same IP address.

To enable TACACS to use the address of a specified interface for all outgoing TACACS packets, use the following command in configuration mode:

Command	Purpose
<b>ip tacacs source-interface</b> <i>subinterface-name</i>	Enable TACACS to use the IP address of a specified interface for all outgoing TACACS packets.

## TACACS Configuration Examples

The following example shows TACACS enabled for PPP authentication:

```
int async 1
  ppp authentication chap
  ppp use-tacacs
```

The following example shows TACACS enabled for ARA authentication:

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

The following example shows a complete TACACS configuration for the Cisco AS5200 using Cisco IOS Release 11.1:

```
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname isdn-14
!
enable password ww
!
username cisco password lab
isdn switch-type primary-5ess
!
controller T1 1
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
interface Loopback20
 no ip address
!
interface Ethernet0
 ip address 172.16.25.15 255.255.255.224
!
interface Serial0
 no ip address
 shutdown
!
interface Serial1
 no ip address
 shutdown
 no cdp enable
!
interface Serial1:23
 ip address 150.150.150.2 255.255.255.0
 no ip mroute-cache
 encapsulation ppp
 isdn incoming-voice modem
 no peer default ip address pool
 dialer idle-timeout 1
 dialer map ip 150.150.150.1 name isdn-5 broadcast 1234
 dialer-group 1
 no fair-queue
 ppp multilink
 ppp authentication pap
 ppp pap sent-username isdn-14 password 7 05080F1C2243
!
interface Group-Async1
 ip unnumbered Ethernet0
 encapsulation ppp
 async mode interactive
 peer default ip address pool default
 no cdp enable
 ppp authentication chap
 ppp use-tacacs
 group-range 1 24
!
ip local pool default 171.68.187.1 171.68.187.8
no ip classless
ip route 0.0.0.0 0.0.0.0 172.16.25.1
ip route 192.100.0.12 255.255.255.255 Serial1:23
tacacs-server host 171.68.186.35
tacacs-server last-resort succeed
```

```
tacacs-server extended
tacacs-server authenticate slip access-lists
tacacs-server notify connections always
tacacs-server notify logout always
tacacs-server notify slip always
!
dialer-list 1 protocol ip permit
!
line con 0
line 1 24
  session-timeout 30 output
  exec-timeout 1 0
  no activation-character
  autoselect during-login
  autoselect ppp
  no vacant-message
  modem InOut
  modem autoconfigure type microcom_hdms
  transport input all
  speed 115200
line aux 0
line vty 0 4
  password ww
  login
end
```

