

Setting Up and Debugging CiscoSecure 2.x TACACS+

Document ID: 13850

Introduction

Prerequisites

Requirements

Conventions

Setting Up Cisco Secure

Setting Up Authentication

Configure

Adding Authorization

Adding Accounting

Adding Dial-up Users

Verify

Troubleshoot

Server

Router

Cisco Secure Users File

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document is intended to assist the first-time Cisco Secure 2.x user in the setup and debugging of a Cisco Secure TACACS+ configuration. It is not an exhaustive description of Cisco Secure capabilities.

Refer to your Cisco Secure documentation for more complete information on server software and user setup. Refer to Cisco IOS Software documentation for the appropriate release for more information on router commands.

Prerequisites

Requirements

The information in this document is based on these software and hardware versions:

- Cisco Secure ACS 2.x and later
- Cisco IOS[®] Software Release 11.3.3 and later

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Setting Up Cisco Secure

Complete these steps:

1. Make sure you use the instructions that came with the software in order to install the Cisco Secure code on the UNIX server.
2. In order to confirm that the product stops and starts, enter `cd to /etc/rc0.d` and as root, execute `./K80Cisco Secure` (to stop the daemons).

Enter `cd to /etc/rc2.d` and as root, execute `./S80Cisco Secure` (to start the daemons).

On startup, you should see messages such as:

```
Cisco Secure starting Processes: Fast Track Admin, FastTrack Server (Delayed Start),
```

Run `$BASE/utils/psg` in order to be sure at least one of each of the individual processes runs, for example, SQLAnywhere or another database engine, Cisco Secure database server process, Netscape Web Server, Netscape Web Admin, Acme Web Server, Cisco Secure AAA process, or Auto restart process.

3. In order to assure you are in the proper directories, set up environmental variables and paths in your shell environment. `c-shell` is used here.

\$BASE is the directory where Cisco Secure is installed, chosen during installation. It contains such directories as DOCS, DBServer, CSU, and so forth.

In this example, installation in `/opt/CSCOacs` is assumed, but this can differ on your system:

```
setenv $BASE /opt/CSCOacs
```

\$SQLANY is the directory where the default Cisco Secure database is installed, chosen during installation. If the default database that comes with the product, SQLAnywhere, was used, it contains such directories as database, doc, and so forth.

In this example, installation in `/opt/CSCOacs/SYBSsa50` is assumed, but this can differ on your system.

```
setenv $SQLANY /opt/CSCOacs/SYBSsa50
```

Add paths in your shell environment to:

```
$BASE/utils
$BASE/bin
$BASE/CSU
$BASE/ns-home/admserv
$BASE/Ns-home/bin/httpd
$SQLANY/bin
```

4. CD to `$BASE/config`

CSU.cfg is the Cisco Secure server control-file. Make a backup copy of this file.

In this file, `LIST config_license_key` shows the license key you received through the licensing process if you purchased the software; if this is a 4-port trial license, you can leave out this line.

The **NAS config_nas_config** section can contain a default network access server (NAS) or router, or the NAS you input during the install. For debugging purposes in this example, you can allow *any* NAS to communicate with the Cisco Secure server *without* a key. For example, remove the name of the NAS and the key from the lines that contain `/* NAS name can go here */` and `/*NAS/Cisco Secure secret key*/`. The only *stanza* in that area reads:

```

NAS config_nas_config = {
  {
    "",          /* NAS name can go here */
    "",          /* NAS/Cisco Secure secret key */
    "",          /* message_catalogue_filename */
    1,           /* username retries */
    2,           /* password retries */
    1            /* trusted NAS for SENDPASS */
  }
};

AUTHEN config_external_authen_symbols = {

```

When you do this, you tell Cisco Secure that it is allowed to talk with all NASs with no exchange of keys.

5. If you wish to have debugging information go to /var/log/csuslog, you need to have a line in the top section of CSU.cfg, which tells the server how much debugging to do. 0x7FFFFFFF adds all possible debugging. Add or modify this line accordingly:

```
NUMBER config_logging_configuration = 0x7FFFFFFF;
```

This additional line sends the debugging information to local0:

```
NUMBER config_system_logging_level = 0x80;
```

Also, add this entry in order to modify the /etc/syslog.conf file:

```
local0.debug /var/log/csuslog
```

Then recycle the syslogd to re-read:

```
kill -HUP `cat /etc/syslog.pid`
```

Recycle the Cisco Secure server:

```
/etc/rc0.d/K80Cisco Secure
/etc/rc2.d/S80Cisco Secure
```

It should still start.

6. You may want to use the browser to add users, groups, and so on, or the CSimport utility. The sample users in the flat file at the end of this document can easily be moved into the database using CSimport. These users will work for test purposes and you may delete them once you get your own users in. Once imported you can see the imported users through the GUI.

If you decide to use CSimport:

```
CD $BASE/utils
```

Put the user and group profiles at the end of this document in a file such as anywhere on the system, then from the \$BASE/utils directory, with the daemons running, for example, /etc/rc2.d/S80Cisco Secure, and as user root, run CSimport with the test (-t) option:

```
./CSimport -t -p <path_to_file> -s <name_of_file>
```

This tests syntax for the users; you should receive messages such as:

```
Secure config home directory is: /opt/CSCOacs/config/CSConfig.ini
hostname = berry and port = 9900 and clientid = 100
```

```
/home/ddunlap/csecure/upgrade.log exists, do you want to write over 'yes' or 'no' ?
yes
Sorting profiles...
Done sorting 21 profiles!
Running the database import test...
```

You should *not* receive messages such as:

```
Error at line 2: password = "adminusr"
Couldn't repair and continue parse
```

Whether or not there were errors, examine the upgrade.log in order to make sure profiles checked out. Once errors are corrected, from the \$BASE/utls directory, with the daemons running (/etc/rc2.d/S80Cisco Secure), and as user root, run CSimport with the commit (-c) option to move the users into the database:

```
./CSimport -c -p <path_to_file> -s <name_of_file>
```

Again, there should not be errors on the screen or in the upgrade.log.

7. Supported browsers are listed in the Cisco Secure Compatibility technical tip. From your PC browser, point to the Cisco Secure/Solaris box **http://#.#.#.#/cs** where #.#.#.# is the IP of the Cisco Secure/Solaris server.

On the screen that appears, for the user enter **superuser** and for the password, enter **changeme**. Do not change the password at this point. You should see the users/groups added if you use the CSimport in the previous step or you can click the browse block **off** and manually add users and groups through the GUI.

Setting Up Authentication

Note: This router configuration was developed on a router that runs Cisco IOS Software Release 11.3.3. Cisco IOS Software Release 12.0.5.T and later shows **group tacacs** instead of **tacacs**.

At this point, configure the router.

1. Kill Cisco Secure while you configure the router.

```
/etc/rc0.d/K80Cisco Secure to stop the daemons.
```

2. On the router, start to configure TACACS+. Enter enable mode and type `conf t` before the command set. This syntax ensures that you are not locked out of the router *initially* providing Cisco Secure is not running. Enter `ps -ef | grep Secure` in order to check to make sure Cisco Secure is not running, and kill -9 the process if it is:

```
!--- Turn on TACACS+
```

```
aaa new-model
enable password whatever
```

```
!--- These are lists of authentication methods,
!--- that is, vty method and con method are
!--- names of lists, and the methods listed on the
!--- same lines are the methods in the order to be
!--- tried. As used here, if authentication
!--- fails due to Cisco Secure not being started,
!--- the enable password is accepted
!--- because it is in each list.
```

```

aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable

!--- Point the router to the server, that is,
!--- #.#.#.# is the server IP address.

tacacs-server host #.#.#.#
line con 0
    password whatever

!--- No time-out to prevent being locked out
!--- during debugging.

    exec-timeout 0 0
    login authentication conmethod
line vty 0 4
    password whatever

!--- No time-out to prevent being locked out
!--- during debugging.

    exec-timeout 0 0
    login authentication vtymethod

```

3. Test to be sure you can still access the router with Telnet and through the console port before you continue. Because Cisco Secure is not running, the enable password should be accepted.



Caution: Keep the console port session active and remain in enable mode; this session should not time out. You start to limit access to the router at this point and you need to be able to make configuration changes without locking yourself out.

Issue these commands in order to see server-to-router interaction at the router:

```

terminal monitor
debug aaa authentication

```

4. As root, start Cisco Secure on the server:

```

/etc/rc2.d/S80Cisco Secure

```

This starts the processes, but you want to enable more debugging than is configured in S80Cisco Secure, so:

```

ps -ef | grep Cisco Secure
kill -9 <pid_of CS_process>

```

```

CD $BASE/CSU

```

```

./Cisco Secure -cx -f $BASE/config/CSU.cfg to start the Cisco Secure process with de

```

With `-x` option, Cisco Secure runs in the foreground so router to server interaction can be observed. You should not see error messages. The Cisco Secure process should start and hang there due to the `-x` option.

5. From another window, check to be sure Cisco Secure started. Enter `ps -ef` and look for the Cisco Secure process.
6. Telnet (vty) users should now have to authenticate through Cisco Secure. With debug on the router, Telnet into the router from another part of the network. The router should produce a username and password prompt. You should be able to access the router with these user-id/password combinations:

```

adminusr/adminusr
operator/oper
desusr/encrypt

```

Watch the server and the router where you should see the interaction, that is, what is sent where, responses, and requests, and so forth. Correct any problems before you continue.

7. If you also want for your users to authenticate through Cisco Secure to get into enable mode, make sure your console port session is still active and add this command to the router:

```
!--- For enable mode, list 'default' looks to Cisco Secure  
!--- then enable password if Cisco Secure is not running.
```

```
aaa authentication enable default tacacs+ enable
```

8. You should now have to **enable** through Cisco Secure. With debug on the router, Telnet into the router from another part of the network. When the router asks for username/password respond with operator/oper.

When user operator tries to enter enable mode (privilege level 15), the password "cisco" is required. Other users will not be able to enter enable mode without the privilege level statement (or the Cisco Secure daemon down).

Watch the server and the router where you should see the Cisco Secure interaction, for instance, what is being sent where, responses, and requests, and so on. Correct any problems before continuing.

9. Bring down the Cisco Secure process on the server while still connected to the console port to be sure that your users can still access the router if Cisco Secure is down:

```
'ps -ef' and look for Cisco Secure process  
kill -9 pid_of_Cisco Secure
```

Repeat the Telnet and enable of the previous step. The router should realize that the Cisco Secure process does not respond and allow users to login and enable with the default enable passwords.

10. Bring up the Cisco Secure server again and establish a Telnet session to the router, which should authenticate through Cisco Secure, with userid/password **operator/oper** in order to check for authentication of your console port users through Cisco Secure. Remain telnetted into the router and in enable mode until you are sure you can login to the router through the console port, for example, log out of your original connection to the router through the console port, then reconnect to the console port. Console port authentication to login with the use of the the previous userid/password combinations should now be through Cisco Secure. For example, userid/password **operator/oper** then password **cisco** has to be used in order to **enable**.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Adding Authorization

Adding authorization is optional.

By default, there are three command-levels on the router:

- Privilege level 0 which includes disable, enable exit, help, and logout
- Privilege level 1 normal level on a Telnet and prompt says router>
- Privilege level 15 enable level and prompt says router#

Since commands available depend on the Cisco IOS feature set, Cisco IOS software release, model of router, and so forth, there is no comprehensive list of all commands at levels 1 and 15. For example, **show ipx route** is not present in an IP only feature set, **show ip nat trans** is not in Cisco IOS Software Release 10.2.X code because NAT was not introduced at the time, and **show environment** is not present in router models without power supply and temperature monitoring.

Commands available in a particular router at a particular level can be found by entering a **?** at the prompt in the router when at that privilege level.

Console port authorization was not added as a feature until CSCdi82030 was implemented. Console port authorization is off by default to lessen the likelihood of accidentally being locked out of the router. If a user has physical access to the router through the console, console port authorization is not extremely effective. But, console port authorization can be turned on under the **line con 0** command in a Cisco IOS image in which CSCdi82030 was implemented with the **authorization exec default|WORD** command.

Complete these steps:

1. The router can be configured to authorize commands through Cisco Secure at all or some levels. This router configuration allows all users to have per-command authorization set up on the server. You can authorize all commands through Cisco Secure but if the server is down, no authorization is necessary, hence the **none**.

With the Cisco Secure server down, enter these commands:

Enter this command in order to remove the requirement that enable authentication be done through Cisco Secure:

```
no aaa authentication enable default tacacs+ none
```

Enter these commands in order to require that commands authorization be done through Cisco Secure:

```
aaa authorization commands 0 default tacacs+ none
aaa authorization commands 1 default tacacs+ none
aaa authorization commands 15 default tacacs+ none
```

2. While the Cisco Secure server runs, Telnet into the router with **userid/password loneusr/lonepwd**. This user should not be able to do any commands other than:

```
show version
ping <anything>
logout
```

The previous users, **adminusr/adminusr**, **operator/oper**, **desusr/encrypt**, should still be able to do all commands by virtue of their **default service = permit**. If there are problems with the process, enter enable mode on the router and turn on authorization debugging with this command:

```
terminal monitor
debug aaa authorization
```

Watch the server and the router where you should see the Cisco Secure interaction, for instance, what is sent where, responses, and requests, and so forth. Correct any problems before you continue.

3. The router can be configured to authorize exec sessions through Cisco Secure. The **aaa authorization exec default tacacs+ none** command institutes TACACS+ authorization for exec sessions.

If you apply this, it affects users **time/time**, **telnet/telnet**, **todam/todam**, **todpm/todpm** and **somerouters/somerouters**. After you add this command to the router and Telnet to the router as user **time/time**, an exec session remains open for one minute (set **timeout = 1**). User **telnet/telnet** enters

the router but is immediately sent to the other address (set autocomd = "telnet 171.68.118.102"). It is possible that users **todam/todam** and **todpm/todpm** are or are not able to access the router, which depends on what time of day it is during the testing. User **somerouters** is only able to Telnet into the router koala.rtp.cisco.com from network 10.31.1.x. Cisco Secure tries to resolve the name of the router. If you use the IP address 10.31.1.5, it is valid if resolution does not take place, and if you use the name koala, it is valid if resolution is through.

Adding Accounting

Adding accounting is optional.

1. Accounting does not take place unless configured in the router, if the the router runs Cisco IOS software release later than Cisco IOS Software Release 11.0. You can enable accounting on the router:

```
aaa accounting exec default start-stop tacacs+
aaa accounting connection default start-stop tacacs+
aaa accounting network default start-stop tacacs+
aaa accounting system default start-stop tacacs+
```

Note: Command-accounting was broken, in Cisco bug ID CSCdi44140, but if you use an image in which this is fixed, command-accounting can also be enabled.

2. Add accounting record debugging on the router:

```
terminal monitor
debug aaa accounting
```

3. Debug on the console should show accounting records entering the server as users log in.

4. In order to retrieve accounting records, as root:

```
CD $BASE/utils/bin
./AcctExport <filename> no_truncate
```

no_truncate means the data is retained in the database.

Adding Dial-up Users

Complete these steps:

1. Make sure that the other functions of Cisco Secure work before you add dial-up users. If the Cisco Secure server and the modem did not work before this point, they do not work after this point.
2. Add this command to the router configuration:

```
aaa authentication ppp default if-needed tacacs+
aaa authentication login default tacacs+ enable
aaa authorization network default tacacs+
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
```

The interface configurations differ, which depends on how authentication is done, but dial-in lines are used in this example, with these configurations:

```
interface Ethernet 0
ip address 10.6.1.200 255.255.255.0

!
!--- CHAP/PPP authentication user:

interface Async1
```

```
ip unnumbered Ethernet0
encapsulation ppp
async mode dedicated
peer default ip address pool async
no cdp enable
ppp authentication chap
```

```
!  
!--- PAP/PPP authentication user:
```

```
interface Async2
ip unnumbered Ethernet0
encapsulation ppp
async mode dedicated
peer default ip address pool async
no cdp enable
ppp authentication pap
```

```
!  
!--- login authentication user with autocommand PPP:
```

```
interface Async3
ip unnumbered Ethernet0
encapsulation ppp
async mode interactive
peer default ip address pool async
no cdp enable
```

```
ip local pool async 10.6.100.101 10.6.100.103
```

```
line 1
session-timeout 20
exec-timeout 120 0
autoselect during-login
script startup default
script reset default
modem Dialin
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
```

```
!
```

```
line 2
session-timeout 20
exec-timeout 120 0
autoselect during-login
script startup default
script reset default
modem Dialin
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
```

```
!
```

```
line 3
session-timeout 20
exec-timeout 120 0
autoselect during-login
autoselect ppp
script startup default
```

```
script reset default
modem Dialin
autocommand ppp
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
```

!

```
access-list 101 deny icmp any any
```

3. From user file of the Cisco Secure:

- ◆ chapuser CHAP/PPP user dials in on line 1; address is assigned by **peer default ip address pool async and ip local pool async 10.6.100.101 10.6.100.103** on the router
- ◆ chapaddr CHAP/PPP user dials in on line 1; address 10.29.1.99 is assigned by server
- ◆ chapacl CHAP/PPP user dials in on line 1; address 10.29.1.100 is assigned by server and inbound access list 101 is applied (which must be defined on the router)
- ◆ papuser PAP/PPP user dials in on line 2; address is assigned by **peer default ip address pool async and ip local pool async 10.6.100.101 10.6.100.103** on the router
- ◆ papaddr PAP/PPP user dials in on line 2; address 10.29.1.98 is assigned by server
- ◆ papacl PAP/PPP user dials in on line 2; address 10.29.1.100 is assigned by server and inbound access list 101 is applied, which must be defined on the router
- ◆ loginauto user dials in on line 3; login authentication with autocommand on line forces user to PPP connection and assigns address from the pool

4. Microsoft Windows setup for all users except user loginauto

- a. Choose **Start > Programs > Accessories > Dial-Up Networking**.
- b. Choose **Connections > Make New Connection**. Type a name for your connection.
- c. Enter your modem-specific information. In **Configure > General**, choose the highest speed of your modem, but do not check the box below this.
- d. In **Configure > Connection**, use 8 data bits, no parity, and 1 stop bit. Call preferences are **Wait for dial tone before dialing** and **Cancel the call if not connected after 200 seconds**.
- e. In Advanced, choose only **Hardware Flow Control** and **Modulation Type Standard**.
- f. In **Configure > Options**, nothing should be checked except under status control. Click **OK**.
- g. On the Next window, enter the telephone number of the destination, then click **Next**, and then click **Finish**.
- h. Once the new connection icon appears, right-click it and choose **Properties**, and then click **Server Type**.
- i. Choose **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** and do not check any advanced options.
- j. In Allowed network protocols, check at least **TCP/IP**.
- k. Under TCP/IP settings, choose **Server assigned IP address, Server assigned name server addresses**, and **Use default gateway on remote network**. Click **OK**.
- l. When you double-click the icon to bring up the Connect To window in order to dial, you must fill in the User name and Password fields, and then click the **Connect**.

5. Microsoft Windows 95 Setup for User loginauto

- a. Configuration for user loginauto, authentication user with autocommand PPP, is the same as for other users except on the **Configure > Options** window. Check **Bring up terminal window after dialing**.
- b. When you double-clicks the icon to bring up the Connect To window to dial, you do not fill in the User name and Password fields. Click **Connect** and after the connection to the router is made, type in the username and password in the black window that appears.
- c. After authentication, click **Continue(F7)**.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Server

```
./Cisco Secure -cx -f $BASE/CSU $BASE/config/CSU.cfg
```

Router

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands. For more information about specific commands, please see Cisco IOS Debug Command Reference.

- **terminal monitor** Display **debug** command output and system error messages for the current terminal and session.
- **debug ppp negotiation** Display PPP packets transmitted during PPP startup, where PPP options are negotiated.
- **debug ppp packet** Display PPP packets that are sent and received. This command displays low-level packet dumps.
- **debug ppp chap** Display information on traffic and exchanges in an internetwork implementing Challenge Authentication Protocol (CHAP).
- **debug aaa authentication** See what methods of authentication are being used and what the results of these methods are.
- **debug aaa authorization** See what methods of authorization are being used and what the results of these methods are.

Cisco Secure Users File

```
group = admin {
    password = clear "adminpwd"
    service = shell {
        default cmd = permit
        default attribute = permit
    }
}

group = oper {
    password = clear "oper"
    privilege = clear "cisco" 15
    service = shell {
        default cmd = permit
        default attribute = permit
    }
}

user = adminusr {
    password = clear "adminusr"
    default service = permit
}
```

```

user = desusr {
    password = des "QjnXYd1kd7ePk"
    default service = permit
}

user = operator {
    member = oper
    default service = permit
}

user = time {
    default service = permit
    password = clear "time"
    service = shell {
        set timeout = 1
        default cmd = permit
        default attribute = permit
    }
}

user = todam {
    password = clear "todam"
    service = shell {
        default cmd = permit
        default attribute = permit
        time = Any 0600 - 1200
    }
}

user = todpm {
    password = clear "todpm"
    service = shell {
        default cmd = permit
        default attribute = permit
        time = Any 1200 - 2359
    }
}

user = telnet {
    password = clear "telnet"
    service = shell {
        set autocmd = "telnet 171.68.118.102"
    }
}

user = limit_lifetime {
    password = clear "cisco" from
    "2 may 2001" until
    "4 may 2001"
}

user = loneusr {
    password = clear "lonepwd"
    service = shell {
        cmd = show {
            permit "ver"
        }
        cmd = ping {
            permit "."
        }
        cmd = logout {
            permit "."
        }
    }
}

```

```

user = chapuser {
    default service = permit
    password = chap "chapuser"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
        }
    }
}

user = chapaddr {
    password = chap "chapaddr"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
            set addr = 10.29.1.99
        }
    }
}

user = chapacl {
    default service = permit
    password = chap "chapacl"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
            set inacl = 101
            set addr = 10.29.1.100
        }
    }
}

user = papuser {
    default service = permit
    password = pap "papuser"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
        }
    }
}

user = papaddr {
    default service = permit
    password = pap "papaddr"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
            set addr = 10.29.1.98
        }
    }
}

user = papacl {
    default service = permit
    password = chap "papacl"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
        }
    }
}

```

```

        set inacl = 101
        set addr = 10.29.1.100
    }
}

user = loginauto {
    default service = permit
    password = clear "loginauto"
    service = ppp {
        protocol = lcp {
        }
        protocol = ip {
        }
    }
}

user = somerouters {
    password = clear "somerouters"
    allow koala ".*" "10\.31\.1\.*"
    allow koala.rtp.cisco.com ".*" "10\.31\.1\.*"
    allow 10.31.1.5 ".*" "10\.31\.1\.*"
    refuse ".*" ".*" ".*"
    service=shell {
        default cmd=permit
        default attribute=permit
    }
}

```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Documentation for CiscoSecure ACS for UNIX](#)
- [Security Products Field Notices \(including Cisco Secure UNIX\)](#)
- [Cisco Secure UNIX Product Support Page](#)
- [RADIUS in IOS Documentation](#)
- [RADIUS Technology Support Page](#)
- [Requests for Comments \(RFCs\)](#)
- [TACACS+ in IOS Documentation](#)
- [TACACS+ Technology Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

