



Doc. No. 78-6022-01

Release Notes for CiscoSecure ACS 2.3 for UNIX

November 9, 1998

These release notes provide new information about CiscoSecure Access Control Server (ACS) 2.3 for UNIX that became available after the *CiscoSecure ACS 2.3 for UNIX User Guide* and *CiscoSecure ACS 2.3 for UNIX Reference Guide* were printed. This document includes:

- New Information about CiscoSecure ACS 2.3, page 2
- Existing Issues with CiscoSecure ACS 2.3, page 5
- Corrections to the *CiscoSecure ACS 2.3 for UNIX Reference Guide*, page 9
- Cisco Connection Online, page 12

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Copyright © 1998
Cisco Systems, Inc.
All rights reserved.

New Information about CiscoSecure ACS 2.3

This section provides the latest information about this version of the CiscoSecure ACS 2.3 for UNIX software. Information is updated immediately prior to release of the software. This section discusses the following topics:

- Security Precautions Using the Microsoft Internet Explorer Browser, page 2
- Distributed Session Manager Installations—Avoid Moving or Deleting Active Users, page 2
- Supporting TACACS+ ISDN Multilink Users on Cisco IOS Release 11.3 or Higher, page 3
- Precautions If Enabling or Disabling Max Sessions Control Manually, page 3
- Editing CSU.cfg to Specify a CiscoSecure Software License Key, page 4
- Changing the Username and Password on the Web Server, page 5
- Specifying an Enable Password, page 5

Security Precautions Using the Microsoft Internet Explorer Browser

As a security precaution, administrators who use the Microsoft Internet Explorer (IE) browser to access CiscoSecure ACS Administrator web pages should avoid saving any HTML bookmarks in their browser that might include clear text password strings to those pages.

This precaution is not necessary for administrators who use the Netscape Navigator or Netscape Communicator browser, for which the secure post method of HTML form processing and page retrieval has been enabled.

If absolutely necessary, the post method of HTML form processing and web page retrieval can also be activated for Microsoft IE browsers by running a UNIX script, **IESecure**, from the CiscoSecure `$BASEDIR/utls/bin` directory following successful CiscoSecure ACS installation.

Step 1 Log in as [Root] to the machine on which the CiscoSecure ACS is installed.

Step 2 Change to the `$BASEDIR/utls/bin` directory, and enter:

```
./IESecure
```



Caution Enabling the post method causes the CiscoSecure ACS Administrator web pages to hang within the Microsoft IE browser after a period of inactivity (around 5 minutes). In this situation, the administrator can restart the Microsoft IE browser and log in to the web pages again. [CSCdk27030]

Distributed Session Manager Installations—Avoid Moving or Deleting Active Users

If you have the CiscoSecure Distributed Session Manager (DSM) module licensed and enabled, you must avoid moving or deleting users from groups while those users are running active sessions. When a user who is still running active sessions is deleted or moved from a group, the number of active sessions belonging to that user is *not* decremented from that group's or any parent group's total active session count (as displayed in their Current Value field) until another user logs in to the same NAS through the same port. When the new user logs in, the number of active sessions will be decremented for the user that was moved or deleted. Until the group's active session count is adjusted in this way, it will be higher than it actually is. Consequently, that group could be limited to fewer concurrent sessions than its Group Max Sessions setting actually allots it. [CSCdk11175]

Supporting TACACS+ ISDN Multilink Users on Cisco IOS Release 11.3 or Higher

If your TACACS+ NASes are running Cisco IOS Release 11.3 or higher, and you want to support CiscoSecure authorization of users who are dialing in over multiple ISDN channels, use the Java-based CiscoSecure Administrator advanced configuration program to add the **protocol = multilink** attribute-value to the profiles of the affected groups or users.

Precautions If Enabling or Disabling Max Sessions Control Manually

Cisco strongly recommends using the Max Sessions Enabled field in the CiscoSecure Administrator AAA General web page to enable or disable the various types of max sessions control as described in the chapter “Limiting Sessions Per User, Group, or VPDN” in the *CiscoSecure ACS 2.3 for UNIX User Guide*.

Alternatively, if you do not have access to a web browser, you can enable or disable max sessions control by editing the CSU.cfg and CSConfig.ini configuration files.

Step 1 In the \$BASEDIR/config directory of your ACS server, edit your CSU.cfg and CSConfig.ini files as specified in Table 1 to enable the DSM or other supported types of max sessions control.



Caution If you edit the CSU.cfg and CSConfig.ini files, make sure that when you *enable* one type of max sessions control that you also *disable* all other types of max sessions control. Enabling the settings for one type of max sessions control in Table 1 *without* disabling the settings for the other types of max sessions control can cause extremely slow authentication performance and out-of-memory errors.

Table 1 Max Sessions Enabling or Disabling CSU.cfg and CSConfig.ini Settings

Enabling this Type of Max Sessions:	Requires These CSU.cfg Settings:	And Requires These CSConfig.ini Settings:
None (all max sessions control disabled)	• config_maxsessions_enable= 0 • config_distmaxsessions_enable=0 These settings disable AAA server and DSM max sessions control.	• ProcessInMemoryMaxSessionInfo = disable • ArchiveMaxSessionInfoToDB = disable These settings disable DBServer-based max sessions control.
Distributed Session Manager (DSM) ¹	• config_maxsessions_enable= 0 • config_distmaxsessions_enable=1 These settings disable AAA server-based max sessions control and enable the DSM.	• ProcessInMemoryMaxSessionInfo = disable • ArchiveMaxSessionInfoToDB = disable These settings disable DBServer-based max sessions control.
DBServer-based max sessions control (default setting)	• config_maxsessions_enable= 0 • config_distmaxsessions_enable=0 These settings disable AAA server-based max sessions control and the DSM.	• ProcessInMemoryMaxSessionInfo = enable • ArchiveMaxSessionInfoToDB = enable These settings enable DBServer-based max sessions control.

Table 1 Max Sessions Enabling or Disabling CSU.cfg and CSConfig.ini Settings

Enabling this Type of Max Sessions:	Requires These CSU.cfg Settings:	And Requires These CSConfig.ini Settings:
AAA server-based max sessions control	• config_maxsessions_enable= 1 • config_distmaxsessions_enable=0 These settings enable AAA server-based max sessions control and disable the DSM.	• ProcessInMemoryMaxSessionInfo = disable • ArchiveMaxSessionInfoToDB = disable These settings disable DBServer-based max sessions control.

1. DSM-based session control can only take effect if the optional DSM module has been licensed for this installation of CiscoSecure ACS 2.3 for UNIX.

- Step 2** After making the above settings, stop and restart the CiscoSecure ACS to make sure that all the above settings take effect.
- Log in as [Root] to the UltraSPARC workstation where you installed CiscoSecure ACS. To stop the CiscoSecure ACS enter:

```
# /etc/rc0.d/K80CiscoSecure
```
 - To restart the CiscoSecure ACS, enter:

```
# /etc/rc2.d/S80CiscoSecure
```

Note All forms of max sessions control require that the AAA accounting functions be enabled in the client NASes.

Editing CSU.cfg to Specify a CiscoSecure Software License Key

If you want to specify a software license key after installing CiscoSecure ACS, or if you want to modify the software license key for an existing CiscoSecure ACS 2.3 UNIX installation because you have obtained a new key to enable the optional DSM module, you can use the CiscoSecure License Key field in the CiscoSecure Administrator AAA General web page.

Alternatively, you can manually edit the config_license_key variable in the CSU.cfg file:

- Step 1** Open the file \$BASEDIR/config/CSU.cfg.
- \$BASEDIR is the install directory for CiscoSecure that you specified at the time of installation.
- Step 2** Find the config_license_key variable and enter or modify the value for software license key number. For example:
- ```
LIST config_license_key = {"a9505ad08a77f927afa4"};
```
- Step 3** After changing the software license key, stop and restart the CiscoSecure ACS for your changes to the CSU.cfg file to take effect.
- Log in as [Root] to the UltraSPARC workstation where you installed CiscoSecure ACS. To stop the CiscoSecure ACS enter:  

```
/etc/rc0.d/K80CiscoSecure
```
  - To restart the CiscoSecure ACS, enter:  

```
/etc/rc2.d/S80CiscoSecure
```

## Changing the Username and Password on the Web Server

To change the username and password on your FastTrack Server, perform the following steps:

- Step 1** Log in to FastTrack as the administrator using a web browser installed on the same machine:

**http://name of your CiscoSecure Server:64000**

You see a screen requesting your username and password.

- Step 2** Enter your administrator username and password to gain access to the Web Server Administration section.

---

**Note** The default username is admin and the default password is password.

---

- Step 3** Click the **Configure Administration** box.

- Step 4** Click the **Access Control** line.

Editable fields for username and password display.

- Step 5** Replace the username and password as necessary.

## Specifying an Enable Password

An enable password will allow a user to carry out expanded system administrator-level EXEC operations. To specify an enable password for a given user:

- Step 1** In the CiscoSecure Administrator advanced configuration program, click the icon for the user profile in the tree that is displayed in the Navigator pane of the tabbed Members page.

- Step 2** Click the **Profile** icon to expand it.

- Step 3** Click the **Privilege - Clear** icon.

- Step 4** In the Attribute window, enter the privilege level (1-15) and the enable password.

- Step 5** Click **Apply**.

- Step 6** Click **Submit**.

On the NAS, enter the following command:

```
aaa authen enable tacacs+ enable
```

## Existing Issues with CiscoSecure ACS 2.3

This section identifies issues with CiscoSecure ACS 2.3 and related information. Some of these issues will be addressed in a subsequent release.

### Database Polling and Database Replication Synchronization Issues

The DBPollInterval parameter in the [ProfileCaching] section of the \$BASEDIR/config/CSConfig.ini file specifies the interval between updating of the cache for database entries that were made directly by a third party application, such as Oracle or Sybase replication. If this interval is less than the database replication time specified in Oracle or Sybase,

there might be a period of time when the cache and the database are not the same. To avoid this situation, you can set the DBPollInterval parameter to as little as 1 second. However, frequent polling can affect ACS performance. For more information on modifying the profile caching interval, see “Tuning Profile Caching” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide*. [CSCdk38740]

### Invalid Port Range Displayed

When using the CiscoSecure Administrator GUI to create or edit a DSM authority, you can enter a TCP port for DSM and Graphical User Interface (GUI). If you enter an invalid port number for either of these fields, an error message is displayed. The associated help file for TCP port incorrectly shows the valid port range as 1-165535. The port range should be 1-65535. [CSCdk44369]

### Remote DSM Authority Performance Issues

If you are planning to limit and track sessions using the optional DSM module, for optimum performance, Cisco recommends that the DSM authority you assign to manage sessions is on a machine that is at least as fast as the machines from which it will be receiving session information and requests. [CSCdk46412]

### Restricting sessions by Point of Presence Group Issues

When CiscoSecure ACS receives AAA information through a CiscoSecure Global Roaming Server (GRS), the session count for a point-of-presence (PoP) group might be inaccurate. Because the CiscoSecure GRS specifies itself as the NAS in all requests it sends, all NASes going through a given CiscoSecure GRS would be seen as one NAS. This renders the session count for a PoP group inaccurate. [CSCdk29120]

### Security Socket Layer Feature Issues

If the Security Socket Layer (SSL) feature is enabled on your web browser, the performance of the CiscoSecure Administrator GUI will be significantly slower because of the additional processing involved with SSL. [CSCdk41887]

### Internet Explorer 4.0 Issues

The Microsoft Internet Explorer 4.0 browser does not support the long URL syntax necessary to carry out all CiscoSecure Administrative web page functions. If you experience this problem, use Netscape Navigator 3.04 or 4.05. [CSCdj46466]

### Internet Explorer 3.02 Issues

The following issues have been reported when administering CiscoSecure ACS through the Microsoft Internet Explorer 3.02 web browser. To remedy the following issues, upgrade to Microsoft Internet Explorer 4.01 or use Netscape Navigator 3.04 or 4.04.

- Focus—After you click **OK** in a dialog box in Internet Explorer 3.02, the focus will temporarily shift somewhere else, then shift back to Internet Explorer.
- Scrolling the Members tab tree—In the Members tab of the Java-based CiscoSecure Administrator advanced configuration program, when you click the gray area of the scroll bar for the tree (the area that contains neither the arrows nor the scroll button), portions of the tree momentarily flash on the screen. Additionally, the scrolling goes very slowly.

- Dictionary scrolls 6 items at a time—In the Dictionaries tab of the Java-based CiscoSecure Administrator advanced configuration program, clicking on the gray area of the scroll bar should take the user up or down one full screen. IE scrolls more than a single screen with each click. To view all the data, you must click the arrows on the scroll bar or drag the slider.

## Navigator 4 for Solaris and the SSL Feature

The SSL feature of the Navigator 4 for Solaris browser does not support the Java-based CiscoSecure Administrator advanced configuration program. To access the CiscoSecure Administrator using the SSL feature, do so through Netscape Navigator or Netscape Communicator for Windows 95 or Windows NT. [CSCdj68773]

## SDI-Based Authentications Can Experience Server Malfunctions

The authentication methodology used by the one-time password (OTP) cards from Security Dynamics, Inc. (SDI) differs somewhat from that used by the CiscoSecure ACS. Whereas SDI authentication uses a single process, CiscoSecure ACS employs a multithreaded approach for improved performance. Although not seen in either a laboratory or a beta site, a large volume of simultaneous SDI-based authentications can theoretically generate unexpected failures. In this case, the authentication might fail even though the username and password are correct. If users encounter this issue, advise them to wait a few moments, and then retry the operation. [CSCdj01541]

## Working with Slow GUI Performance

Depending on the size of your database and the number of client/server transactions taking place, you might experience some processing delays, such as waiting a long time for GUI screens to refresh. Although these GUI performance issues can be annoying, they do not result in system malfunction or loss of data.

Unlike other GUI-based applications that run locally on a given computer, CiscoSecure ACS is a network-based application and is therefore dependent on external data-transfer rates, such as that provided by local telephone services. In addition, CiscoSecure ACS is a client/server product that includes a full relational database management system, so you might experience wait time as profiles are written to and from the database.

## Problems Updating the Same CiscoSecure User Profile at Different CiscoSecure ACS Sites

In cases where Oracle Master-to-Master or Sybase Peer-to-Peer database replication has been implemented, the CiscoSecure system administrators must avoid updating the same CiscoSecure user profile at two or more different CiscoSecure ACS profile database sites during the same time period between database replication processes.

If the same user profile is updated at two different sites within the same time period between replications, the user profile edits at both sites will neither be replicated nor reconciled. The user profile will remain with unreconciled settings at both sites.

For more information, see “Oracle Database Replication Setup Following CiscoSecure Installation” or “Sybase Database Replication Setup Following CiscoSecure Installation” in the *CiscoSecure ACS 2.3 for UNIX Installation Guide* or “Setting Up Database Replication Among CiscoSecure ACSes” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide*. [CSCdj79568]

### Problems With Failed User Logins at Two or More Sites

In cases where Oracle Master-to-Master (or Master-to-Updateable-Snapshot) database replication has been implemented, precautions need to be taken to minimize the chance of a CiscoSecure user attempting a failed login at 2 or more different CiscoSecure ACS profile database sites during the same interval between database replication processes.

If failed logins under the same user profile occur at 2 different sites within the same interval between replications, the next time replication is run, Oracle shows a Unique Constraint error due to both profiles having the same name but different profile IDs.

When the same user subsequently attempts to log in, that user will fail due to the user account being locked.

The database administrator must delete one of the user's conflicting profiles at one of the sites and force replication before the user account can be reset.

To minimize the possibility of failed login of the same user at two or more sites within the same interval between replications:

- Schedule replications as frequently as practical. The shorter the interval between replications, the less likely that two failed logins at different CiscoSecure ACS sites by the same user will occur.
- Arrange, as much as possible, for a single CiscoSecure ACS to oversee the NAS sites that any one user is likely to dial-in to within the period of time between replications. For example, a single CiscoSecure ACS server overseeing all the access numbers within a given area code. [CSCdj89491]

### Scaling Limitations of the SQLAnywhere Database Option

Cisco does *not* recommend that large enterprise or large ISP customers, who anticipate rapid growth and scaling up operations in the number of users, use the default SQLAnywhere CiscoSecure installation option as the RDBMS engine to support your users. Please note the following limitations of the SQLAnywhere RDBMS engine:

- SQLAnywhere does not support more than 5,000 users.
- SQLAnywhere does not support database fault tolerance or replication functions.

For customers who plan to carry out large scale database growth and update operations, we recommend use of the Oracle Enterprise or Sybase Enterprise RDBMS engines.

### Problems with Oracle 7.3.3 and Earlier Client Modules

CiscoSecure ACS installations using versions 7.3.3 and 7.3.2 of the Oracle client modules SQL\*Net and TCP/IP protocol adapter sometimes experience profile retrieval and DBServer module failure problems under heavy usage. To forestall these problems, install the SQL\*Net and TCP/IP protocol adapter client modules that come with Oracle 7.3.4 or higher.

The Oracle 7.3.4 upgrade is available free to all customers with a valid support contract. [CSCdj78312] [CSCdj86330]

## Problems with Failed Accounting Record Updates

Failure to maintain sufficient available disk space on the SQLAnywhere, Oracle, or Sybase database server storing records for the CiscoSecure ACS can result in a general warning message and a failure to update CiscoSecure accounting records. To prevent such failures, the system administrator should:

- Ensure that sufficient disk space exists to record and update all login transactions.

A typical example of heavy accounting disk space requirements might be those of an ISP's ACS, running TACACS+ protocol, receiving about 200,000 login requests per day, and configured to send Start, Update, and Stop accounting records (approximately 200 bytes each) for each login.

To calculate the accounting-related database disk space requirements for the above example, you would multiply 200,000 (logins per day) x 3 (accounting records per login) x 200 (bytes per record). The result indicates that 120 MB of disk space per day on the SQLAnywhere, Oracle, or Sybase database server would be required to accommodate the daily accounting data in the above example.

- Periodically run the CiscoSecure AcctExport tool to export the accounting records from the SQLAnywhere, Oracle, or Sybase RDBMS to a flatfile. [CSCdj87504]

## Problems with Oracle Core Data Dumps

When the Oracle trace file exceeds 5 MB (as might happen under frequent and heavy loads), the Oracle server might occasionally dump core data and abort. This is a known Oracle problem (ID Number: 510778) that is remedied with Oracle version 8.0.4.

If this condition is causing problems, Oracle recommends that you disable Oracle tracing as follows:

- Step 1** Go to the `$ORACLE_HOME/otrace/admin` directory of your Oracle server.
- Step 2** Delete the existing `process.dat` and `regid.dat` files and recreate them to the default size:  

```
% otrccef
```
- Step 3** Edit the Oracle user's shell startup file. For Bourne or Korn shell users, the settings to add or edit are:  

```
EPC_DISABLED=TRUE; export EPC_DISABLED
```
- Step 4** Stop and restart the Oracle server. [CSCdj85981]

## Corrections to the *CiscoSecure ACS 2.3 for UNIX Reference Guide*

This section addresses errors in the *CiscoSecure ACS 2.3 for UNIX Reference Guide* and information that was not available before the reference guide was printed.

- Chapter 4—Tuning CiscoSecure ACS Performance and Configuration, “Message Catalog Format,” (page 4-24)

The list of default message IDs, message names, and message strings at the end of this section should be replaced with the following list:

---

**Note** Only messages 0 through 18 can be customized by the system administrator.

---

```

0 AUTHEN_CLIENT_LOGIN_PROMPT, "\nUser Access Verification\n"
1 AUTHEN_CLIENT_USERNAME_PROMPT, "Username:"
2 AUTHEN_CLIENT_PASSWORD_PROMPT, "Password:"
3 AUTHEN_CLIENT_SIGN_ON_MESSAGE, ""
4 AUTHEN_CLIENT_CHANGEPASS_INTRO, "Change password sequence"
5 AUTHEN_CLIENT_PASSWORDS_IDENTICAL, "Error - passwords the same"
6 AUTHEN_CLIENT_PASSWORD_EXPIRED, "Your password has expired"
7 AUTHEN_CLIENT_TOO_MANY_TRIES_FOR_USERNAME, "Too many tries for username"
8 AUTHEN_CLIENT_TOO_MANY_TRIES_FOR_PASSWORD, "Too many tries for password"
9 AUTHEN_CLIENT_NEW_PASSWORD1, "New password:"
10 AUTHEN_CLIENT_NEW_PASSWORD2, "New password again:"
11 AUTHEN_CLIENT_PASSWORDS_DIFFERENT, "The passwords are different"
12 AUTHEN_CLIENT_BAD_PASSWORD, "Bad password"
13 AUTHEN_CLIENT_CANT_CHANGE_PASSWORD, "You cannot change your password"
14 AUTHEN_CLIENT_ACCOUNT_EXPIRY_WARNING, "Your account will expire in %d days"
15 AUTHEN_CLIENT_PASSWORD_EXPIRY_WARNING, "Your password will expire in %d days"
16 AUTHEN_CLIENT_NEW_PASSWORD_CRITERIA, "A password must be between 6 and 13 characters
long, containing at least one alphabetic and one numeric character."
17 AUTHEN_CLIENT_DATABASE_ERROR, "Unable to save your changes in the database"
18 AUTHEN_CLIENT_ACCOUNT_DISABLED, "Your account is currently disabled."
19 MAX_CLIENT_MESSAGE_CODE, "Dummy"
20 AUTHEN_USER_NOT_FOUND "Authentication - User not found"
21 AUTHEN_BAD_METHOD_FOR_USER "Authentication - Bad method for user"
22 AUTHEN_BAD_TYPE "Authentication - Bad type"
23 AUTHEN_NO_USERNAME "Authentication - No username specified"
24 AUTHEN_INSUFFICIENT_PRIVILEGE "Authentication - Insufficient privilege"
25 AUTHEN_UNEXPECTED_DATA "Authentication - Unexpected data"
26 AUTHEN_UNEXPECTED_RESERVED_DATA "Authentication - Unexpected reserved data"
27 AUTHEN_INCORRECT_PASSWORD "Authentication - Incorrect password"
28 AUTHEN_ABORTED_SEQUENCE "Authentication - Aborted sequence"
29 AUTHEN_FILEHANDLING_ERROR "Authentication - File handling error"
30 AUTHEN_UNKNOWN_PASSWORD_TYPE "Authentication - Unknown password type"
31 AUTHEN_USER_NOT_IN_FILE "Authentication - User not in file"
32 AUTHEN_ERROR_IN_EXTERNAL_FN "Authentication - Error in external function"
33 AUTHEN_BAD_SERVICE "Authentication - Bad service"
34 AUTHEN_BAD_ACTION "Authentication - Bad action"
35 AUTHEN_BAD_PASSWORD "Authentication - Bad password"
36 AUTHEN_NO_TOKEN_PASSCODE "Authentication - No token passcode received"
37 AUTHEN_SENDPASS_SUCCESSFUL "Authentication - SENDPASS successful"
38 AUTHEN_SENDPASS_FAIL "Authentication - SENDPASS failed"
39 AUTHEN_LOGIN_SUCCESSFUL "Authentication - LOGIN successful"
40 AUTHEN_ENABLE_SUCCESSFUL "Authentication - ENABLE successful"
41 AUTHEN_CHPASS_SUCCESSFUL "Authentication - CHPASS successful"
42 AUTHEN_SENDAUTH_SUCCESSFUL "Authentication - SENDAUTH successful"
43 AUTHEN_SENDAUTH_FAIL "Authentication - SENDAUTH failed"
44 AUTHEN_TOO_MANY_TRIES "Authentication - Too many tries"
45 AUTHEN_CANT_CHANGE_PASSWORD "Authentication - Cant change password"
46 AUTHEN_CHANGE_PASSWORD_FAILED "Authentication - Change password failed"
47 AUTHEN_ACCOUNT_DISABLED "Authentication - Account disabled"
48 AUTHEN_MAX_SESSIONS "Authentication - Maximum session exceeded"
49 PROTOCOL_USERNAME_TOO_LONG "Protocol - Username too long"
50 PROTOCOL_TOKENCODE_TOO_LONG "Protocol - Token passcode too long"
51 PROTOCOL_NASNAME_TOO_LONG "Protocol - NAS name too long"
52 PROTOCOL_NASPORT_TOO_LONG "Protocol - NAS port name too long"
53 PROTOCOL_NACADDR_TOO_LONG "Protocol - NAC address too long"
54 PROTOCOL_BAD_PRIVILEGE "Protocol - Invalid privilege field"
55 PROTOCOL_ACTIVE_SESSION "Protocol - Session id in use"
56 PROTOCOL_NO_SESSION "Protocol - No session found"
57 PROTOCOL_INCORRECT_TYPE "Protocol - Incorrect type"
58 PROTOCOL_INCORRECT_SESSION "Protocol - Incorrect session"
59 PROTOCOL_INCORRECT_SEQUENCE "Protocol - Incorrect sequence"
60 PROTOCOL_INCORRECT_VERSION "Protocol - Incorrect version"
61 PROTOCOL_GARBLED "Protocol - Garbled message"
62 PROTOCOL_READ_TIMEOUT "Protocol - Read timeout"
63 PROTOCOL_CONNECTION_CLOSED "Protocol - Connection closed"

```

|    |                                |                                             |
|----|--------------------------------|---------------------------------------------|
| 64 | PROTOCOL_BAD_TYPE              | "Protocol - Bad type"                       |
| 65 | PROTOCOL_MAX_USERS_EXCEEDED    | "Maximum number of users exceeded"          |
| 66 | PROTOCOL_MISMATCHED_ENCRYPTION | "Protocol - mismatched encryption"          |
| 67 | PROTOCOL_MISMATCHED_KEYS       | "Protocol - mismatched encryption keys"     |
| 68 | AUTHOR_NO_SERVICE              | "Authorization - No service specified"      |
| 69 | AUTHOR_FAILED_MANDATORY_ARG    | "Authorization - Failed mandatory argument" |
| 70 | AUTHOR_FAILED_COMMAND_LINE     | "Authorization - Failed command line"       |
| 71 | AUTHOR_FAILED_SERVICE          | "Authorization - Failed service"            |
| 72 | AUTHOR_FAILED_TIME             | "Authorization - Failed time qualification" |
| 73 | AUTHOR_BAD_ARGUMENT            | "Authorization - Bad argument"              |
| 74 | AUTHOR_NO_COMMAND              | "Authorization - No command specified"      |
| 75 | AUTHOR_FAILED_CMD              | "Authorization - Failed command"            |
| 76 | AUTHOR_NO_PROTOCOL             | "Authorization - No protocol"               |
| 77 | AUTHOR_UNKNOWN_USER            | "Authorization - Unknown user"              |
| 78 | AUTHOR_INVALID_NAS_OR_PORT     | "Authorization - Unauthorized NAS or PORT"  |
| 79 | AUTHOR_COMMAND_AUTHORIZED      | "Authorization - Request authorized"        |
| 80 | AUTHOR_MAX_SESSIONS            | "Authorization - Maximum sessions exceeded" |
| 81 | RADIUS_DEBUG_MSG               | "RADIUS"                                    |
| 82 | MSS_DEBUG_MSG                  | "DMS"                                       |

## Updated Copyright Information

The following information supplements the copyright information in the *CiscoSecure ACS 2.3 for UNIX User Guide*:

- CiscoSecure ACS software is derived in part from software of J-Lex. Permission by J-Lex; Copyright © 1996 by Elliot Joel Berk. Elliot Joel Berk disclaims all warranties with regard to this software, including all implied warranties of merchantability and fitness. In no event shall Elliot Joel Berk be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data, or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of this software.
- CiscoSecure ACS software is derived in part from the Generic Library Release Version 2.0 ("JGL"). Permission by ObjectSpace, Inc. Copyright © 1996.
- CiscoSecure ACS software is derived in part from the SUN Java JDK software from Sun Java Microsystems. CiscoSecure also uses JDBC-ODBC Bridges from Sun Java Microsystems. Copyright © 1992-1996. All rights reserved.
- CiscoSecure ACS software is derived in part from the SSLava Toolkit. The SSLava Toolkit is used strictly for the support of SSL. SSLava is a trademark of Phaos Technology Corporation. Copyright© 1996, 1997, Phaos Technology Corporation. All Rights Reserved.

## Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

---

**Note** If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or [tac@cisco.com](mailto:tac@cisco.com). To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or [cs-rep@cisco.com](mailto:cs-rep@cisco.com)

---

---

This document is to be used in conjunction with the *CiscoSecure ACS 2.3 for UNIX User Guide* and *CiscoSecure ACS 2.3 for UNIX Reference Guide*.

AccessPath, AtmDirector, the CCIE logo, CD-PAC, Centri, Centri Bronze, Centri Gold, Centri Security Manager, Centri Silver, the Cisco Capital logo, Cisco IOS, the Cisco IOS logo, CiscoLink, the Cisco Powered Network logo, the Cisco Press logo, ClickStart, ControlStream, Fast Step, FragmentFree, IGX, JumpStart, Kernel Proxy, LAN<sup>2</sup>LAN Enterprise, LAN<sup>2</sup>LAN Remote Office, MICA, Natural Network Viewer, NetBeyond, Netsys Technologies, Packet, PIX, Point and Click Internetworking, Policy Builder, RouteStream, Secure Script, SMARTnet, StrataSphere, StrataSphere BILdler, StrataSphere Connection Manager, StrataSphere Modeler, StrataSphere Optimizer, Stratm, StreamView, SwitchProbe, *The Cell*, TrafficDirector, VirtualStream, VlanDirector, Workgroup Director, Workgroup Stack, and XCI are trademarks; Empowering the Internet Generation and The Network Works. No Excuses. are service marks; and BPX, Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, EtherChannel, FastHub, FastPacket, ForeSight, IPX, LightStream, OptiClass, Phase/IP, StrataCom, and StrataView Plus are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.

Copyright © 1998, Cisco Systems, Inc.  
All rights reserved. Printed in USA.  
9810R