Doc. No. 78-2854-02

CiscoSecure UNIX Server User Guide Release Notes 1.0

This document provides additional information and describes known problems in CiscoSecure UNIX Server software. Use this document to complement information contained in the *CiscoSecure UNIX Server User Guide*.

This document contains the following sections:

Operating Environment

CiscoSecure UNIX Server software is supported on SunOS 4.1.3 or 4.1.4. Note that SunOS 4.1.2 is *not* supported.

CiscoSecure UNIX Server Software Files

The CiscoSecure UNIX Server software bin directory contains the CiscoSecure executable files, and a “samples” directory, that you can use or modify for your own needs. The samples directory contains the files specified in Table 1.

Table 1 Samples Directory Files

File	Description
control.file	CiscoSecure master control file.
aa.database	User AA database, referenced by control.file.

File	Description
msg_cat.1	Very simple message catalog file, referenced by control.file.
left.cfg	Local router configuration file that uses CiscoSecure UNIX Server software.
right.cfg	Remote router configuration file that is standalone. In other words, it doesn't use the TACACS+[1] protocol.

1. TACACS+ = Terminal Access Controller Access System +

These files have been used together in a Cisco Systems lab for some simple tests and are a good place to begin your examination of CiscoSecure UNIX Server software. The router configuration files represent two routers connected to each other by a single serial link. The router, "left," shares an ethernet segment with the CiscoSecure server. While the name of the router is "left," its config file is named left.cfg.

Note Left and right are merely test names and do not imply location.

Four Free Ports When Installing CiscoSecure UNIX Server Software

As a bonus, when you run CiscoSecure UNIX Server software, four additional ports beyond the number of ports your license agreement stipulates, are allowed. For example, if you purchased a license to use 16 ports, CiscoSecure UNIX Server software will indicate that you are licensed to use 20 ports.

Complete installation information and examples are included in the *CiscoSecure UNIX Server User Guide*. However, for your convenience, the following information is provided to help you install CiscoSecure UNIX Server software, and to start and stop the server using the files contained in the samples directory. For more information, see the chapter "Configuring CiscoSecure UNIX Server Software" in the *CiscoSecure UNIX Server User Guide*.

CiscoSecure UNIX Server software Version 1.0 includes the binary image, CiscoSecure. You can install this program anywhere within the file system. However, for best results, install the CiscoSecure binary image in the directory /usr/local/etc. In order to perform its function, CiscoSecure UNIX Server software must be run with superuser privileges.

Take the following steps to install CiscoSecure UNIX Server software:

Step 1 Become superuser.

Step 2 Select a directory into which to install the CiscoSecure software. Normally, this would be a system directory such as /usr/etc/ciscosecure or /usr/local/etc/ciscosecure. Create this directory if it does not already exist and make it your current directory. For example:

```
% su
Password:
# mkdir /usr/local/etc/ciscosecure
# cd /usr/local/etc/ciscosecure
```

Step 3 Extract the distribution into the selected directory. The installation disks contain a compressed tar file:

```
# bar xvZf /dev/rfd0
```

Step 4 Edit the /etc/services file to include a definition for the TACACS+ protocol port number, if this is not already present. The protocol port number definition is as follows:

```
tacacs          49/tcp          TACACS+
```

Step 5 Enter the **hostid** command to obtain the host ID of the system host.

```
# hostid
55412315
```

Step 6 Fill out the "CiscoSecure Software Key Fax-Back Form," including the host ID of the primary and backup CiscoSecure server systems, and fax it to the number on the form. Your software key will be returned within two business days. (For details, refer to the section "Licensing" in the chapter "Using CiscoSecure UNIX Server Software" of the *CiscoSecure UNIX Server User Guide*.)

Step 7 Edit the control file in /usr/local/etc/ciscosecure. At the beginning of the file, locate "LIST config_license_key" and enter the software key that was returned to you when you completed Step 6.

Step 8 Add the binary image, CiscoSecure, to the /etc/rc.local startup file if it is to be restarted automatically on system reboot.

When installation is complete, the CiscoSecure UNIX Server software control file and Authentication and Authorization (AA) database must be properly configured before starting the server. (See the chapters "Configuring CiscoSecure UNIX Server Software," and "The AA Database" in the *CiscoSecure UNIX Server User Guide*.)

User Guide Corrections

This section addresses errors in the *CiscoSecure UNIX Server User Guide*.

One Installation Disk

CiscoSecure UNIX Server software is provided on one disk. The documentation incorrectly references two disks.

Accounting Record Format

In the chapter "CiscoSecure UNIX Server Accounting," in the "Accounting Database" section, the accounting record format is incorrect. The correct format of the accounting record is structured as follows:

```
char    nas_name[]      /* NAS name */
char    user_name[]     /* username */
char    port_name[]     /* port the connection is on */
char    remote_address[]        /* where the user connected from */
char    record_type[]   /* (start, update, stop etc) */
char    server[]        /* hostname of the server, as an AV pair */
char    time[]          /* time of this record, as an AV pair */
char    date[]          /* date of this record, as an AV pair */
char    attribute_value_pairs[] /* there are an arbitrary number of these */
```

Message Catalogs

The message catalog in the appendix “CiscoSecure UNIX Server File Formats and Syntax” is incorrect. The following list identifies the correct default message IDs, message names, and message strings used by CiscoSecure UNIX Server software:

```
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 six and thirteen
characters, containing at least one alphabetic and numeric character.”

18 AUTHEN_USER_NOT_FOUND        “Authentication - User not found”
19 AUTHEN_BAD_METHOD_FOR_USER   “Authentication - Bad method for user”
20 AUTHEN_BAD_TYPE              “Authentication - Bad type”
21 AUTHEN_NO_USERNAME           “Authentication - No username specified”
22 AUTHEN_INSUFFICIENT_PRIVILEGE  “Authentication - Insufficient privilege”
23 AUTHEN_UNEXPECTED_DATA       “Authentication - Unexpected data”
24 AUTHEN_UNEXPECTED_RESERVED_DATA  “Authentication - Unexpected reserved data”
25 AUTHEN_INCORRECT_PASSWORD    “Authentication - Incorrect password”
26 AUTHEN_ABORTED_SEQUENCE      “Authentication - Aborted sequence”
27 AUTHEN_FILEHANDLING_ERROR    “Authentication - File handling error”
28 AUTHEN_UNKNOWN_PASSWORD_TYPE  “Authen - Unknown password type”
29 AUTHEN_USER_NOT_IN_FILE      “Authentication - User not in file”
30 AUTHEN_ERROR_IN_EXTERNAL_FN,”Authentication - Error in external function”
31 AUTHEN_BAD_SERVICE           “Authentication - Bad Service”
32 AUTHEN_BAD_ACTION            “Authentication - Bad Action”
33 AUTHEN_SENDPASS_OK           “Authentication - SENDPASS (ok)”
34 AUTHEN_SENDPASS_FAIL         “Authentication - SENDPASS (fail)”

35 PROTOCOL_USERNAME_TOO_LONG   “Protocol - Username too long”
36 PROTOCOL_NASNAME_TOO_LONG    “Protocol - NAS name too long”
37 PROTOCOL_NASPORT_TOO_LONG    “Protocol - NAS port name too long”
38 PROTOCOL_NACADDR_TOO_LONG    “Protocol - NAC address too long”
39 PROTOCOL_BAD_PRIVILEGE       “Protocol - Invalid privilege field”
40 PROTOCOL_ACTIVE_SESSION      “Protocol - Session id in use”
41 PROTOCOL_NO_SESSION          “Protocol - No session found”
42 PROTOCOL_INCORRECT_TYPE      “Protocol - Incorrect type”
43 PROTOCOL_INCORRECT_SESSION   “Protocol - Incorrect session”
44 PROTOCOL_INCORRECT_SEQUENCE  “Protocol - Incorrect sequence”
45 PROTOCOL_INCORRECT_VERSION   “Protocol - Incorrect version”
46 PROTOCOL_GARBLED             “Protocol - Garbled message”
47 PROTOCOL_READ_TIMEOUT        “Protocol - Read timeout”
48 PROTOCOL_CONNECTION_CLOSED   “Protocol - Connection closed”
49 PROTOCOL_BAD_TYPE            “Protocol - Bad type”
50 PROTOCOL_MAX_USERS_EXCEEDED  “Maximum number of users exceeded”
51 PROTOCOL_ENCRYPTION_MISMATCH  “Mismatched encryption”

52 AUTHOR_NO_SERVICE            “Authorization - No service specified”
53 AUTHOR_FAILED_MANDATORY_ARG  “Authorization - Failed mandatory argument”
54 AUTHOR_FAILED_COMMAND_LINE   “Authorization - Failed command line”
55 AUTHOR_FAILED_SERVICE        “Authorization - Failed service”
```

```
56 AUTHOR_FAILED_TIME           “Authorization - Failed time qualification”
57 AUTHOR_BAD_ARGUMENT          “Authorization - Bad argument”
58 AUTHOR_NO_COMMAND            “Authorization - No command specified”
59 AUTHOR_FAILED_CMD            “Authorization - Failed command”
60 AUTHOR_NO_PROTOCOL           “Authorization - No protocol”
61 AUTHOR_UNKNOWN_USER          “Authorization - Unknown user”
62 AUTHOR_INVALID_NAS_OR_PORT   “Authorization - Unauthorized NAS or PORT”
63 AUTHOR_COMMAND_AUTHORIZED    “Authorization - Command authorized”
```

Late-Breaking News on the GUI and CiscoSecure Server

This section contains information that became available after the *CiscoSecure UNIX Server User Guide* was printed.

Working With S/Key Authentication

The S/Key one-time password system, from Bellcore, provides secure authentication over networks that are subject to eavesdropping. S/Key distinguishes itself from other one-time or multi-use authentication systems by preventing the user's secret password from ever crossing the network during login.

A Scenario of Using S/Key

To help you better understand the benefits of using S/Key with CiscoSecure UNIX Server software, consider the following example of a hypothetical user, Sue, who authenticates to the CiscoSecure network access server by means of the S/Key system.

1. Upon the standard prompt for authentication, Sue identifies herself to the network access server by her login name.

   ```
   User Access Verification
   Username: sue
   s/key 97 fr09072
   Password:
   ```

   The CiscoSecure server observes that Sue needs to supply an S/Key password.

2. The CiscoSecure server then issues a challenge including the sequence number of the one-time password expected and a “seed.” The seed is a special value used by the S/Key algorithm as the starting point for the creation of an S/Key password. This seed will also allow Sue to securely use a single secret password.

   Based on the verification display, the CiscoSecure server instructed the network access server to display the sequence number, 97, and a seed, fr09072, which will be used by a separate program to initiate the encryption process leading to an S/Key password.

   Sue notes the sequence number and seed, then pauses from her interaction with the network access server in order to generate a password. She will generate the password by entering the sequence number and seed, along with her secret password, into an S/Key calculator program.

3. Sue enters 97 and fr09072 into her S/Key calculator program at the UNIX prompt, as shown in the example display. (On UNIX, the S/Key calculator program is called key.)

   ```
   % key 97 fr09072
   Enter secret password: secret password
   ```

   The secret password is any string of at least 10 alphanumeric characters generated by Sue, for Sue, and known only by Sue.

4 The secret password triggers the creation of a second password, as follows:

```
CRAG BAKE MOLT JEAN JIBE OFT
```

The one-time S/Key password is always expressed as a sequence of six short English words. Note how the one-time password is generated without any secret information crossing the network.

This second password will be used to authenticate Sue to the CiscoSecure server. Sue now returns to her interaction with the network access server. She enters the S/Key password and is authenticated, as follows:

```
Password: CRAG BAKE MOLT JEAN JIBE OFT
```

Sue correctly enters the six short words; however, they are not displayed.

5 The next time Sue attempts network access, she will be prompted for the one-time password sequence number, 96.

The sequence number is one less than what was used for the previous authentication. In the case of Sue, her last sequence number was 97, so the next required sequence number will be 96. When the sequence number reaches 0, Sue will not be able to log in without reinitializing the S/Key system.

Sue's account could also be configured so that she is required to use S/Key when she enables on the router. In this case, the AA database would be modified to display something like the following:

```
user = sue {
        password = skey
        privilege = skey 15
}
```

In this case, Sue would be required to give a different S/Key password every time she logs in and every time she enables at level 15.

Preparing to Install S/KEY

Take the following steps to prepare for S/Key installation and use:

Step 1 Modify your CiscoSecure UNIX Server AA database file to set up each S/Key user. For example, to set up a hypothetical user named Sue, you would modify the CiscoSecure server AA database file as follows:

```
user = sue {
password = skey
}
```

Step 2 Restart the CiscoSecure server by entering the UNIX command as follows:

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

Note After modifying the AA database, instruct S/Key users that they will have to run the keyinit program on the CiscoSecure server. The keyinit program initializes the S/Key system for that user. You should also inform users that when they run keyinit, they will be prompted for two passwords. The first is the UNIX login password. The second is the secret password used with S/Key. For security purposes, the UNIX password and the secret password should not be the same. Also note that the secret password must be at least 10 characters.

Installing and Getting Ready to Use S/Key

Take the following steps to install the S/Key system on a CiscoSecure server:

Step 1 Log in to the CiscoSecure web site at the following location and download the S/Key one-time password system prebuilt distribution:

ftp://*userid*@**www.cisco.com/cisco/netmgmt/ciscosecure/sunos**

Step 2 Unpack the skey-cs.tar file, as follows:

```
# tar -xvf skey-cs.tar
```

Step 3 Run the enclosed INSTALL.S_Key script, as follows.

```
# INSTALL.S_Key
```

In the next step, each S/Key user will run the keyinit program to initialize the S/Key system for that user. (For the purpose of example, a hypothetical user, Sue, will run the keyinit program to initialize the S/Key system. This process enables Sue to use S/Key authentication.)

Step 4 Have CiscoSecure users who will use S/Key run keyinit at the UNIX prompt as follows:

```
% keyinit
Password: UNIX password
[Adding sue]
Enter secret password: secret password
```

When the keyinit program asks Sue for a secret password, she is free to supply any mix of 10 or more alphanumeric characters.

```
Again secret password: secret password


ID sue s/key is 99 fr05065
Next login password: SKI INCA HONE NEE MESS LEAF
```

Now Sue is ready to use S/Key with CiscoSecure UNIX Server software.

S/Key also accounts for previous iterations of keyinit, providing assurance for the user that someone has not altered the system. As a result, the next time that Sue runs keyinit, she will see a display similar to the following:

```
% keyinit
Password: Unix password
[Updating sue]
Old key: fr05064
Enter secret password: secret password


Again secret password: secret password


ID sue s/key is 99 fr05065
Next login password: SKI INCA HONE NEE MESS LEAF
```

Note Remember that when Sue enters her secret password, she is entering a personal identification number in order to generate another password. The secret password could be the same as her UNIX password, or it might be any string of characters. This secret password does not change. Sue, as an S/Key user, must remember her S/Key password in order to generate the second password used for S/Key authentication to the CiscoSecure UNIX server.

CiscoSecure UNIX Server Graphical User Interface

This section provides additional information about the graphical user interface (GUI) and authorizing commands from a logged-in user.

Understanding Default and Unknown User

The "default" entry in the AA database has been renamed "unknown_user." If you have a preliminary version of CiscoSecure UNIX Server software, your AA database probably contains the entry for "default," which was assigned in cases where an unknown username was passed from the network access server to the CiscoSecure server. To reflect this change, you need to replace occurrences of "default" in your AA database with "unknown_user."

The AA database will handle the occurrence of either "default" or "unknown_user" for a period of time but "default" will be deleted in a subsequent release of CiscoSecure UNIX Server software.

Assigning the Same Name to a Group and User

The GUI does not acknowledge the difference between a group and user with the same name. This will be fixed in a subsequent release of CiscoSecure UNIX Server.

Deleting a User

Although this feature is not documented in the user guide, you can delete a user by taking the following steps:

Step 1 Select the name of the group in which the user you want to delete resides.

Step 2 Select **Open User List** from the View menu.

Step 3 Select the name of the user you want to delete.

Step 4 Select **Delete User** from the Users menu.

Protocol Services

Support for IP, IPX, LCP, ARA protocol, and Exec have been added to the list of service attributes in the GUI.

Specifying the Date

CiscoSecure enables you to specify a date on which authentication or authorization attributes become available or unavailable. The following is an example of the correct format:

```
21 Mar 96
```

This format is required by the CiscoSecure server. Although the CiscoSecure GUI does not place any restrictions on the values you enter in the date field, if you enter the date incorrectly, the CiscoSecure server will not recognize it.

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content 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, 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, Internet e-mail, and fax download options, and 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`.
- Telnet: `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 baud rates up to 14.4 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact `cco-help@cisco.com`. For additional information, contact `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`. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or `cs-rep@cisco.com`.

This document is to be used in conjunction with the *CiscoSecure UNIX Server User Guide* publication.