CHAPTER 3

Configuring CiscoSecure UNIX Server Software

This chapter describes how to configure and use the CiscoSecure UNIX Server software. It contains the following sections:

- Server Control File
- Message Catalogs

To configure and use CiscoSecure UNIX Server software, you need the following files:

- Server control file—Defines global parameters and identifies the name of the Authentication and Authorization (AA) database file.
- Message catalog—Contains all messages that should be returned to the user during transactions with the network access server and the CiscoSecure server, allowing support for multiple languages (including French, German, and English) without changing the CiscoSecure server.
- AA (Authentication and Authorization) database file—Contains user-specific information for authentication and authorization, such as each user’s password
- Accounting database—Contains information that enables you to track start and stop times for users, as well as the name of the network access server, and other information
- Password log file—Stores changes to user passwords

Server Control File

The server control file is the main file required for setting up CiscoSecure UNIX Server software. This file includes basic configuration parameters for each network access server that is to be serviced, and specifies the following information:

- License key(s) that enable CiscoSecure UNIX Server software

- Filename(s) of the AA database
- Filename to use for recording accounting information
- Default logging levels to be used while the CiscoSecure server is running
- How often to write accounting records to the accounting file
- Network access server-specific configuration parameters

The Network Access Server-specific parameters are as follows:

- Name of the network access server to which the parameters are to be applied
- Encryption key shared between the CiscoSecure server and the selected network access server.
- The message catalog filename for the specified network access server
- Maximum time (in seconds) after sending a response to wait for a client to continue a transaction
- Maximum number of attempts to get username and password before the operation is cancelled.
- Maximum period of inactivity (in seconds) before an open accounting session is timed out and closed
- Duration of the warning period for expiring passwords and services
- List of network access servers that are authorized to use SENDPASS as an authentication method

The syntax of the server control file is similar to that of C language syntax. Each statement or grouping is terminated by a semicolon. Comments begin with the characters “/*” and end with the characters “*/”. Lines may be continued on a successive line by ending them with a back-slash (\). A sample server control file follows:

```
/*
 * CiscoSecure UNIX Server example control file
 */

/* The license for this server. Multiple license keys may
 * be specified, each separated by a comma.
 */
```

```
LIST config_license_key = {"061db8afcf66db981f3c", \
     "7f4f9db4d7ce8ed85b69" }; /* */

/* The pathname of the Configuration Database */
LIST config_aa_database_filename = {"./configuration.database"};

/*
 * The pathname of the accounting log file - if this
 * variable is not specified then accounting information is not recorded.
 */
STRING config_accounting_database_filename = "/tmp/acct";

/* Default logging configuration - basic information is logged */
NUMBER config_logging_configuration = 0x7e;

/*
 * The maximum number of seconds to hold accounting information before
 * writing it to the accounting file (if specified).
 */
NUMBER config_accounting_write_frequency = 5;

/*
 * Per-NAS configuration records. The default encryption key is "arachnid"
 * for all NAS except 'boggle', which is using "heliotrope".
 */
NAS config_nas_config = {
  {
    "",     /* NAS name */
    "arachnid",/* secret key */
    "cat_1",/* message_catalogue_filename */
    1,      /* Authentication: username retries */
    3,      /* Authentication: password retries */
    1,      /* is default NAS configuration */
    1,      /* trusted NAS for SENDPASS */
    30      /* Password expiry period in days */
  },
  {
    "boggle",/* NAS name */
    "heliotrope",/* secret key */
    "",     /* message_catalogue_filename */
    2,      /* Authentication: username retries */
    2,      /* Authentication: password retries */
    0,      /* is not the default NAS configuration */
    0,      /* not a trusted NAS for SENDPASS */
    10      /* Password expiry period in days */
    }
  };
```

The variables shown in Table 3-1 are valid in CiscoSecure UNIX Server software control files:

Table 3-1 `Variables in Software Control Files`

Type	Name	Default	Description	Example
List	config_aa_database_filename	None	A list of the names of the AA databases to load.	`LIST config_aa_database_filename = { "./db.1", "./db.2" };`
List	config_license_key	None	A list of the license keys used to enable the product.	`LIST config_license_key = {"061db8afcf66db981f3c",\ "7f4f9db4d7ce8ed85b69" };`
String	config_accounting_database_filename	None	The name of the accounting database.	`STRING config_accounting_database_filename = "./accounting";`
String	config_update_log_filename	None	The name of the file that keeps the results of password changes, etc.	`STRING config_update_log_filename = "./updates";`
Number	config_accounting_write_frequency	10 (seconds)	How often to slave the accounting data to disk, in seconds.	`NUMBER config_accounting_write_frequency = 20;`
Number	config_delay_on_blocking	100000 (0.1 (seconds))	How long to let the connection 'sleep' when EWOULDBLOCK is returned, in usec.	`NUMBER config_delay_on_blocking = 200000;`
Number	config_expiry_period	30 (days)	How long, in days, before a (new) password changed via CHPASS expires.	`NUMBER config_expiry_period = 30;`

Type	Name	Default	Description	Example
Number	config_warning_period	10 (days)	The period, in days, before a password expires during which the user is warned that her password will expire soon.	`NUMBER config_warning_period = 10;`
Number	config_get_names_from_dns	1 (true)	Decide if server should perform IP address to hostname lookups.	`NUMBER config_get_names_from_dns = 0;`
Number	config_limit_for_idle_connection	300 (seconds)	Maximal time to hold an idle NAS connection open, in seconds.	`NUMBER config_limit_for_idle_connection = 300;`
Number	config_nodelay_for_tcp	1 (on)	Decide whether to TCP_NODELAY on TCP sockets, and thus turn off the Nagel algorithm. Should be left ON for performance reasons.	`NUMBER config_nodelay_for_tcp = 1;`
Number	config_priv_level_for_own_CHPASS	1	Privilege level at which a user may change his/her own password.	`NUMBER config_priv_level_for_own_CHPASS = 1;`
Number	config_receive_buffer_size	16384 (16KB)	Buffer size to allocate for receive for each TCP connection.	`NUMBER config_receive_buffer_size = 8192;`
Number	config_send_buffer_size	16384 (16KB)	Buffer size to allocate for send for each TCconnection.	`NUMBER config_send_buffer_size = 8192;`

Type	Name	Default	Description	Example
Number	config_system_logging_level	0x80 (LOG_LOCAL0)	Syslog facility under which to log.	`NUMBER config_system_logging_level 0x80;`
Number	config_system_priority_level	-4	System priority ('nice' value) to assign the ciscoSecure daemon.	`NUMBER config_system_priority_level = -4;`
Number	config_use_keepalives	1 (on)	Decide if SO_KEEPALIVE on TCP sockets should be set, and thus be informed (more) quit the event of a network or NAS failure.	`NUMBER config_use_keepalives = 1;`
Number	config_logging_configuration	0x7E	Configure logging parameters.The default (0x7E) turns on all the standard logging levels. Additional details and protocol debugging info can be obtained by the logical OR of the values as described in the Table 3-2.	`NUMBER config_logging_configuration = 0x7E`

The logging levels are listed in Table 3-2.

Table 3-2 Logging levels

Name	Value	Description
LOG_DEBUG	0x2	Debug messages
LOG_INFO	0x4	Informational messages
LOG_NOTICE	0x8	Notices
LOG_WARNING	0x10	Warnings
LOG_ERROR	0x20	Errors
LOG_ALERT	0x40	Alerts

Authentication information is listed in Table 3-3.

Table 3-3 Authentication Information

Name	Value	Description
AUTHEN_OK	0x100	Successful authentication operations
AUTHEN_FAIL	0x200	Failed authentication operations
AUTHEN_ERROR	0x400	Authentication operations that result in an error
AUTHEN_OUTPUT	0x800	All authentication information

Authorization information is listed in Table 3-4

Table 3-4 Authorization Information

Name	Value	Description
AUTHOR_OK	0x1000	Successful authorization operations
AUTHOR_FAIL_CMD	0x2000	Authorization failed for command
AUTHOR_FAIL_ARG	0x4000	Authorization failed—bad arguments
AUTHOR_FAIL_OTHER	0x8000	Authorization failed for other reasons

Name	Value	Description
AUTHOR_ERROR	0x10000	Authorization errors

Accounting information is listed in Table 3-5.

Table 3-5 Accounting Information

Name	Value	Description
ACCOUNT_OK	0x100000	Successful accounting operations
ACCOUNT_FAIL	0x200000	Failed accounting operations
ACCOUNT_ERROR	0x400000	Errors in accounting operations

Protocol logging information is listed in Table 3-6.

Table 3-6 Protocol Logging

Name	Value	Description
ERRNO_INFO	0x10000000	Many types of protocol and operational errors
SERVICE_INFO	0x20000000	Major protocol operations
PROTOCOL_ERROR	0x40000000	TACACS+ protocol errors
PACKET_INFO	0x80000000	Display TACACS+ protocol packets
NAS config_nas_config	`NONE`	A list of NAS configuration records. Each record must contain the values in the order that follows:

Order of Values in the NAS Configuration Records

Each value in a NAS Configuration record should be listed in the following order:

1. Network access server name

2 Encryption key

3 Message catalog filename

4 Number of username retries allowed

5 Number of password retries allowed

6 Value of nonzero if this record is the default network access server description

7 A value which is nonzero if the network access server is trusted to send replies to SENDPASS

8 Number of days during which users are warned of a pending password expiration

An example Configuration file follows:

```
Example:
               NAS config_nas_config = {
                 {
                   "", /* any NAS name */
                   "zeotrope", /* secret encryption key */
                   "./cat_1", /* message_catalogue_filename */
                   1, /* username retries */
                   3, /* password retries */
                   1, /* this record is the default for any NAS not
                       specifically listed */
                   1, /* trusted NAS for SENDPASS */
                   5 /* password expiration period, in days */
                 }
               };
```

Message Catalogs

A catalog of messages forms part of the configurable data of the CiscoSecure server. A message catalog contains all messages that should be returned to users during transactions with the network access server and the CiscoSecure UNIX Server software, allowing multiple languages (such as French, German, and English) to be supported by the CiscoSecure UNIX Server software without having to change any major configuration in the CiscoSecure server.

CiscoSecure UNIX Server sends these messages to the network access server in the native language of the users. CiscoSecure UNIX Server software does this by referencing all user messages with a message ID. These message IDs identify a particular message that should be sent to the network access server for display to the user. CiscoSecure UNIX Server software does not use the actual message stored in the message catalog, thus providing language independence. By configuring different message catalogs, the software can support multiple network access servers, each with different user communities based on language. A message catalog is associated with a particular network access server by configuration statements in the server control file. Each network access server can have a different message catalog assigned to it if necessary.

Messages in the message catalog are returned to the network access server in response to specific transactions between users and the servers.

Message Catalog Format

The format of the message catalog is *message_number message_string*

For example:

```
3 “Hello\040there”
2 “ok, what’s your password\012”
```

The formatting and display of messages is determined by the network access server. By convention, however, the Return-Linefeed sequence in the message catalog is represented by a newline (\n) character. You enter special characters using escaped octal notation in which the first character is a backslash (\) and is followed by three octal digits representing the ASCII value of the character. For example, a Return is represented by the value *\010* and a Linefeed is represented by the value *\012*. Extended character sets may contain null values, which are acceptable because each message is stored with an associated length field and is not null terminated.

See the section “Message Catalogs” in the appendix “CiscoSecure UNIX Server File Formats and Syntax” for a full list of messages and their message IDs.