CHAPTER 6

Using CiscoSecure UNIX Server Software

This chapter contains functional and administrative information about using CiscoSecure UNIX Server software, and includes the following sections:

- Starting CiscoSecure UNIX Server
- Using Invocation Options
- Controlling and Shutting Down CiscoSecure UNIX Server Software
- System Logging Functions
- Changing Passwords
- Licensing

Starting CiscoSecure UNIX Server

CiscoSecure UNIX Server software normally runs in the background as a daemon process, but can also be run as a foreground process. To start the CiscoSecure server, you must specify the name of the control file on the command line, as follows:

```
# /usr/local/etc/ciscosecure/CiscoSecure -f /usr/local/etc/ciscosecure/control.file
```

Internally, the CiscoSecure server goes through the following initialization steps:

1. The administration process is created.
2. The administration process parses the server control file for server configuration including protocols, authentication, and encryption methods to be supported.

3 The administration process parses the AA database to create the shared user data set.

The CiscoSecure server is now operational.

Using Invocation Options

When you start up the CiscoSecure UNIX Server software, you can use several flags to invoke different options. (See Table 6-1.)

Table 6-1 CiscoSecure UNIX Server Invocation Options

Flag	Option
-v	Displays the CiscoSecure UNIX Server software version information
-c	Instructs CiscoSecure to display its logging output on *stderr*. Normally, all output is logged using the syslog facility
-d	Produces a verbose log while parsing the user database
-p	Causes CiscoSecure to read and verify that the control file and referenced user database files are correct.
-u	Instructs CiscoSecure to verify and update its configuration based on passwords which have been changed by users
-x	CiscoSecure will not divorce itself from the controlling terminal and will stay in the foreground
-f *controlfile*	Identifies the control file

To use these options enter the following UNIX command line:

```
# CiscoSecure [-v] [-c] [-d] [-p] [-u] [-x] -f controlfile
```

Flags in brackets are optional.

Controlling and Shutting Down CiscoSecure UNIX Server Software

When the CiscoSecure UNIX Server software is running, you can control its operation and shutdown by using UNIX signals, which are sent with the UNIX **kill** command:

- SIGHUP—Reloads the CiscoSecure server and rereads the control and AA database files. Enter the following command:

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

While reloading, the CiscoSecure server continues to service user requests using the currently loaded control and AA database files. When the new files are properly parsed, the server switches to the new data set and frees the previous dataset from memory. System logging levels (see the next section, “System Logging Functions”) are changed by modifying the server control file variable *config_system_logging_level* and reloading the server.

- SIGINT—Stops the CiscoSecure server, closing all open connections. To stop the server in this manner, enter the following command:

  ```
  # kill -INT ‘cat /etc/CiscoSecure.pid‘
  ```

- SIGUSR1—Applies all collected user updates (such as password changes) to the database. To apply all collected user updates in this manner, enter the following command:

  ```
  # kill -SIGUSR1 ‘cat /etc/CiscoSecure.pid‘
  ```

Note In these three command lines, the process ID of the CiscoSecure UNIX Server software is taken from the file /etc/CiscoSecure.pid, which is created when the CiscoSecure server starts. The grave accents and cat /etc/CiscoSecure.pid are replaced with the process ID contained in the file. This avoids the necessity of using the **ps** command to look up the process ID before sending the process the appropriate signal.

System Logging Functions

CiscoSecure UNIX Server software makes use of the system logging (syslog) facilities. You can use syslog to determine which information is immediately displayed on the console or retained for later use.

Events that can be logged by the CiscoSecure server include the following:

- Server start, restart, stop, and crash events
- Fatal internal errors
- Serious internal errors resulting in limitation of server operation
- TCP/IP connection resets
- Unexpected accounting transactions (indicating probable error recovery)
- Failed authentication and authorization requests
- Successful enable requests
- Packet-level information

Controlling CiscoSecure UNIX Server Logging

Logging is controlled through the *config_logging_configuration* variable in the control file. These variables are bitmasks consisting of the logical OR of each of the desired settings; setting a bit indicates that the associated information is to be displayed. The meaning of each bit (shown in hexadecimal notation) is listed in Table 6-2, Table 6-3, Table 6-4 and Table 6-5.

The bitmasks that correspond to general errors and messages are shown in Table 6-2.

Table 6-2 General Errors and Messages

Value	Meaning
0x01	Information
0x02	Notices
0x04	Warnings

Value	Meaning
0x08	Errors
0x10	Critical events
0x80	Normal server events

The bitmasks that correspond to authentication information are shown in Table 6-3.

Table 6-3 Authentication Value Information

Value	Meaning
0x0200	Normal authentication information
0x0400	Failed authentication information
0x0800	Error authentication information
0x2000	Authentication information sent to the NAS (client)

The bitmasks that correspond to authorization information are shown in Table 6-4

Table 6-4 Authorization Value Information

Value	Meaning
0x020000	Normal authorization information
0x040000	Authorization commands failed for bad command lines
0x080000	Authorization commands failed for bad arguments
0x100000	Authorization commands failed for other reasons
0x200000	Authorization errors

The bitmasks that correspond to protocol errors are shown in Table 6-5.

Table 6-5 Protocol Errors

Value	Meaning
0x40000000	TACACS+ protocol errors
0x80000000	Display all TACACS+ packets

A standard setting results in error conditions being reported on the log output. You should use other logging configuration options during investigative or troubleshooting operations. The default setting is as follows:

```
NUMBER config_logging_configuration = 0x7E;
```

UNIX Syslog Configuration

To help ensure proper database operation, verify that the UNIX system is properly configured for recording the CiscoSecure UNIX server logging information. This information is typically logged into a file. Significant events are logged to the system console.

The default syslog facility is LOG_LOCAL0. (Refer to your UNIX system documentation for more information about syslog.) You can change this by changing the value of the CiscoSecure UNIX Server software control file variable *config_system_logging_level*.

To maintain a centralized database of messages, modify the configuration of syslog to log all CiscoSecure messages.

- To cause all informational messages to be sent to the named file, add the following line to /etc/syslog.conf:

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

- To cause syslogd to reread its configuration file, enter the following command:

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

Changing Passwords

Users can change their passwords when they log in.

Passwords should be between 6 and 13 characters and contain at least one numeric and one alphabetic character. CiscoSecure UNIX Server software checks passwords when they are changed to make sure that easily guessed or deciphered passwords are not used.

Take the following steps to change a password when logging in:

Step 1 Connect to the network access server.

Step 2 Enter your username at the UNIX prompt.

Step 3 Press **Return** at the prompt requesting you to enter a password.

Step 4 Enter **yes** at the prompt asking if you want to change your password.

Step 5 Enter your existing password at the prompt.

Step 6 Enter your new password at the prompt.

Step 7 Enter your new password a second time to verify that it is correct.

The password retries variable specifies the number of NULL returns a user can make to the password prompt before being faulted. The password retries variable is configured per network access server and is located in the control file. This variable must be set to a number greater than 1 for the change password function to work. You can only change the password if you enter a NULL return at the prompt. If the retry-count is set to 1, then you are stopped at that point. In addition, the config_priv_level_for_own_CHPASS variable in the control file should be set to 1. This number is the privilege level at which a user can change his or her own password. When someone logs into a router, that user's default level is 1, so if this variable is not set to 1, the user will not be able to change his or her password.

Licensing

CiscoSecure UNIX Server software is licensed according to the number of network access server ports that are served by the software. Each license is encoded with the number of ports you purchased. To license additional ports, you need to purchase an additional license. Any number of licenses can be combined to accommodate the required number of port licenses needed by a site.

For details on setting up licensing on your CiscoSecure server, see the section “Installing CiscoSecure UNIX Server Software” in the chapter “Getting Started with CiscoSecure UNIX Server Software.”

CiscoSecure Operation

CiscoSecure UNIX Server software monitors the licensed ports by recording those that have been used since the CiscoSecure server was started. When the licensed number of ports is reached, the CiscoSecure server will refuse authentication requests on any ports that have not already been used.

For example, a site that is licensed for 16 ports has two Cisco 2509 network access servers (the Cisco 2509 has eight asynchronous ports), NAS1 and NAS2. A primary and backup CiscoSecure server are configured with license keys for each, using the host ID from each system. When the CiscoSecure server is started, it has an empty port table. As users connect to the network, the port from which they are connecting is recorded in the port table within the CiscoSecure server. With this configuration, users connect to NAS1 and NAS2 and, as they do, the CiscoSecure UNIX Server software records the name of the network access server and the port number on which the user connected. Eventually, the CiscoSecure UNIX Server software has recorded NAS1 ports 1 through 8 and NAS2 ports 1 through 8.

Now, assume that the site adds another Cisco 2509, called NAS3. At this point, all the licensed CiscoSecure server ports have been allocated. Any user connecting to NAS3 on any port will be denied because the CiscoSecure server license table is full.

In case of hardware failure, the licensing scheme allows you to replace a faulty network access server with one that functions properly. The only requirement is that the new network access server must have the same configuration as the one that was removed from service. This guarantees that it has the same name and IP address and therefore will not be viewed within the Cisco Secure server as a different device that is trying to obtain service without being licensed.