CHAPTER 1

Introducing the CLI Configuration Guide

This chapter describes how to use the IPS CLI, and contains the following sections:

- Purpose of the CLI Configuration Guide, page 1-1
- Sensor Configuration Sequence, page 1-1
- User Roles, page 1-3
- CLI Behavior, page 1-4
- Command Line Editing, page 1-6
- IPS Command Modes, page 1-7
- Regular Expression Syntax, page 1-7
- Generic CLI Commands, page 1-9
- CLI Keywords, page 1-10

Purpose of the CLI Configuration Guide

This guide is a task-based configuration guide for the Cisco IPS 6.1 CLI. The term "sensor" is used throughout this guide to refer to all sensor models, unless a procedure refers to a specific appliance or to one of the modules, such as the AIM IPS, AIP SSM, IDSM2, or NME IPS.

For an alphabetical list of all IPS commands, refer to *Command Reference for Cisco Intrusion Prevention System 6.1*. For information on locating all IPS 6.1 documents on Cisco.com, refer to *Documentation Roadmap for Cisco Intrusion Prevention System 6.1*.

You can also use an IPS manager to configure your sensor. For information on how to access documentation that describes how to use IPS managers, refer to *Documentation Roadmap for Cisco Intrusion Prevention System 6.1*.

Sensor Configuration Sequence

Perform the following tasks to configure the sensor:

1. Log in to the sensor.
2. Initialize the sensor.

   Run the **setup** command to initialize the sensor.
3. Verify the sensor initialization.

4. Create the service account.

   A service account is needed for special debug situations directed by TAC.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a new password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

5. License the sensor.
6. Perform the other initial tasks, such as adding users and trusted hosts, and so forth.
7. Make changes to the interface configuration if necessary.

   You configure the interfaces during initialization.
8. Add or delete virtual sensors as necessary.

   You configure the virtual sensors during initialization.
9. Configure event action rules.
10. Configure the signatures for intrusion prevention.
11. Configure anomaly detection.

    You can run anomaly detection using the default values or you can tailor it to suit your network needs.
12. Set up any external product interfaces.

    CSA MC is the only external product supported by Cisco IPS 6.1.
13. Configure IP Logging.
14. Configure blocking.
15. Configure SNMP if you are going to use it.
16. Perform miscellaneous tasks to keep your sensor running smoothly.
17. Upgrade the IPS software with new signature updates and service packs.
18. Reimage the application partition and the maintenance partition when needed.

For More Information

- For the procedure for logging in to your sensor, see Chapter 2, “Logging In to the Sensor.”
- For the procedure for using the **setup** command to initialize your sensor, see Chapter 3, “Initializing the Sensor.”
- For the procedure for verifying sensor initialization, see Verifying Initialization, page 3-27.
- For the procedure for obtaining and installing the license key, see Installing the License Key, page 4-49.
- For the procedures for setting up your sensor, see Chapter 4, “Setting Up the Sensor.”
- For the procedure for creating the service account, see Creating the Service Account, page 4-14.
- For the procedures for configuring interfaces on your sensor, see Chapter 5, “Configuring Interfaces.”
- For the procedures for configuring virtual sensors on your sensor, see Chapter 6, “Configuring Virtual Sensors.”

- For the procedures for configuring event action rules policies, see Chapter 7, "Configuring Event Action Rules."
- For the procedures for configuring signatures for intrusion prevention, see Chapter 8, "Defining Signatures."
- For the procedure for configuring anomaly detection policies, see Chapter 9, "Configuring Anomaly Detection."
- For the procedure for setting up external product interfaces, see Chapter 10, "Configuring External Product Interfaces."
- For the procedures for configuring IP logging, see Chapter 11, "Configuring IP Logging."
- For the procedures for configuring blocking on your sensor, see Chapter 13, "Configuring Attack Response Controller for Blocking and Rate Limiting."
- For the procedures for configuring SNMP on your sensor, see Chapter 14, "Configuring SNMP."
- For the administrative procedures, see Chapter 16, "Administrative Tasks for the Sensor."
- For more information on how to obtain Cisco IPS software, see Chapter 21, "Obtaining Software."
- For the procedures for working with images, see Chapter 22, "Upgrading, Downgrading, and Installing System Images."
- For procedures specific to the modules, see the following chapters:
  - Chapter 17, "Configuring the AIM IPS"
  - Chapter 18, "Configuring the AIP SSM"
  - Chapter 19, "Configuring the IDSM2"
  - Chapter 20, "Configuring the NME IPS"

User Roles

Note All IPS platforms allow ten concurrent log in sessions.

The CLI for Cisco IPS 6.1 permits multiple users to log in at the same time. You can create and remove users from the local sensor. You can modify only one user account at a time. Each user is associated with a role that controls what that user can and cannot modify.

The CLI supports four user roles: administrator, operator, viewer, and Service. The privilege levels for each role are different; therefore, the menus and available commands vary for each role.

- **Administrators**—This user role has the highest level of privileges. Administrators have unrestricted view access and can perform the following functions:
  - Add users and assign passwords
  - Enable and disable control of physical interfaces and virtual sensors
  - Assign physical sensing interfaces to a virtual sensor
  - Modify the list of hosts allowed to connect to the sensor as a configuring or viewing agent
  - Modify sensor address configuration
  - Tune signatures
  - Assign configuration to a virtual sensor

  - Manage routers

- **Operators**—This user role has the second highest level of privileges. Operators have unrestricted view access and can perform the following functions:
  - Modify their passwords
  - Tune signatures
  - Manage routers
  - Assign configuration to a virtual sensor
- **Viewers**—This user role has the lowest level of privileges. Viewers can view configuration and event data and can modify their passwords.

Tip Monitoring applications only require viewer access to the sensor. You can use the CLI to set up a user account with viewer privileges and then configure the event viewer to use this account to connect to the sensor.

- **Service**—This user role does not have direct access to the CLI. Service account users are logged directly into a bash shell. Use this account for support and troubleshooting purposes only. Unauthorized modifications are not supported and require the device to be reimaged to guarantee proper operation. You can create only one user with the service role.

  When you log in to the service account, you receive the following warning:

```
***************************** WARNING ************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
******************************************************************************
```

Note The service role is a special role that allows you to bypass the CLI if needed. Only a user with administrator privileges can edit the service account.

Note In the service account you can also switch to user root by executing **su-**. The root password is synchronized to the service account password. Some troubleshooting procedures may require you to execute commands as the root user.

CLI Behavior

The following tips help you use the Cisco IPS CLI.

Prompts

- You cannot change the prompt displayed for the CLI commands.
- User interactive prompts occur when the system displays a question and waits for user input. The default input is displayed inside brackets [ ]. To accept the default input, press **Enter**.

Help

- To display the help for a command, type **?** after the command.

  The following example demonstrates the ? function:

  ```
  sensor# configure ?
  terminal     Configure from the terminal
  sensor# configure
  ```

  When the prompt returns from displaying help, the command previously entered is displayed without the ?.

- You can type **?** after an incomplete token to view the valid tokens that complete the command. If there is a trailing space between the token and the ?, you receive an ambiguous command error:

  ```
  sensor# show c ?
  % Ambiguous command: "show c"
  ```

  If you enter the token without the space, a selection of available tokens for the completion (with no help description) appears:

  ```
  sensor# show c?
  clock configuration
  sensor# show c
  ```

- Only commands available in the current mode are displayed by help.

Tab Completion

- Only commands available in the current mode are displayed by tab complete and help.
- If you are unsure of the complete syntax for a command, you can type a portion of the command and press **Tab** to complete the command.
- If multiple commands match for tab completion, nothing is displayed.

Recall

- To recall the commands entered in a mode, use the Up Arrow or Down Arrow keys or press **Ctrl-P** or **Ctrl-N**.

  Help and tab complete requests are not reported in the recall list.

- A blank prompt indicates the end of the recall list.

Case Sensitivity

- The CLI is not case sensitive, but it does echo back the text in the same case you typed it. For example, if you type:

  ```
  sensor# CONF
  ```

  and press **Tab**, the sensor displays:

  ```
  sensor# CONFigure
  ```

  CLI commands are not case sensitive, but values are case sensitive. Remember this when you are creating regular expressions in signatures. A regular expression of "STRING" will not match "string" seen in a packet.

Display Options

- –More– is an interactive prompt that indicates that the terminal output exceeds the allotted display space. To display the remaining output, press the **spacebar** to display the next page of output or press **Enter** to display the output one line at a time.
- To clear the current line contents and return to a blank command line, press **Ctrl-C**.

For More Information

For more information on CLI command regular expression syntax, see Regular Expression Syntax, page 1-7.

Command Line Editing

Table 1-1 describes the command line editing capabilities provided by the Cisco IPS CLI.

Table 1-1 Command Line Editing

Keys	Description
Tab	Completes a partial command name entry. When you type a unique set of characters and press Tab, the system completes the command name. If you type a set of characters that could indicate more than one command, the system beeps to indicate an error. Type a question mark (?) immediately following the partial command (no space). The system provides a list of commands that begin with that string.
Backspace	Erases the character to the left of the cursor.
Enter	At the command line, pressing Enter processes a command. At the ---More--- prompt on a terminal screen, pressing Enter scrolls down a line.
Spacebar	Enables you to see more output on the terminal screen. Press the Spacebar when you see the line ---More--- on the screen to display the next screen.
Left arrow	Moves the cursor one character to the left. When you type a command that extends beyond a single line, you can press the Left Arrow key repeatedly to scroll back toward the system prompt and verify the beginning of the command entry.
Right arrow	Moves the cursor one character to the right.
Up Arrow or Ctrl-P	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Down Arrow or Ctrl-N	Returns to more recent commands in the history buffer after recalling commands with the Up Arrow or Ctrl-P. Repeat the key sequence to recall successively more recent commands.
Ctrl-A	Moves the cursor to the beginning of the line.
Ctrl-B	Moves the cursor back one character.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Moves the cursor to the end of the command line.
Ctrl-F	Moves the cursor forward one character.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-L	Clears the screen and redisplays the system prompt and command line
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

Table 1-1 Command Line Editing (continued)

Keys	Description
Ctrl-U	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-V	Inserts a code to indicate to the system that the keystroke immediately following should be treated as a command entry, *not* as an editing key.
Ctrl-W	Deletes the word to the left of the cursor.
Ctrl-Y	Recalls the most recent entry in the delete buffer. The delete buffer contains the last ten items you deleted or cut.
Ctrl-Z	Ends configuration mode and returns you to the EXEC prompt.
Esc-B	Moves the cursor back one word.
Esc-C	Capitalizes the word at the cursor.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Esc-L	Changes the word at the cursor to lowercase.
Esc-U	Capitalizes from the cursor to the end of the word.

IPS Command Modes

Cisco IPS CLI has the following command modes:

- privileged EXEC—Entered when you log in to the CLI interface.
- global configuration—Entered from privileged EXEC mode by entering **`configure terminal`**.

  The command prompt is `sensor(config)#`.
- service mode configuration—Entered from global configuration mode by entering **`service`** *service-name*.

  The command prompt is `sensor(config-ser)#`, where `ser` is the first three characters of the service name.
- multi-instance service mode—Entered from global configuration mode by entering **`service`** *service-name log-instance-name*.

  The command prompt is `sensor(config-log)#` where `log` is the first three characters of the log instance name. The only multi-instance services in the system are anomaly detection, signature definition, and event action rules.

Regular Expression Syntax

Note The syntax in this section applies only to regular expressions used as part of a CLI command. It does not apply to regular expressions used by signatures.

Regular expressions are text patterns that are used for string matching. Regular expressions contain a mix of plain text and special characters to indicate what kind of matching to do. For example, if you are looking for a numeric digit, the regular expression to search for is "[0-9]". The brackets indicate that the

character being compared should match any one of the characters enclosed within the bracket. The dash (-) between 0 and 9 indicates that it is a range from 0 to 9. Therefore, this regular expression will match any character from 0 to 9, that is, any digit.

To search for a specific special character, you must use a backslash before the special character. For example, the single character regular expression "*" matches a single asterisk.

The regular expressions defined in this section are similar to a subset of the POSIX Extended Regular Expression definitions. In particular, "[..]", "[==]", and "[::]" expressions are not supported. Also, escaped expressions representing single characters are supported. A character can be represented as its hexadecimal value, for example, \x61 equals 'a,' so \x61 is an escaped expression representing the character 'a.'

The regular expressions are case sensitive. To match "STRING" or "string" use the following regular expression: "[Ss][Tt][Rr][Ii][Nn][Gg]."

Table 1-2 lists the special characters.

Table 1-2 Regular Expression Syntax

Character	Description
^	Beginning of the string. The expression "^A" will match an "A" only at the beginning of the string.
^	Immediately following the left-bracket ([). Excludes the remaining characters within brackets from matching the target string. The expression "[^0-9]" indicates that the target character should not be a digit.
$	Matches the end of the string. The expression "abc$" matches the sub-string "abc" only if it is at the end of the string.
|	Allows the expression on either side to match the target string. The expression "a|b" matches "a" as well as "b."
.	Matches any character.
*	Indicates that the character to the left of the asterisk in the expression should match 0 or more times.
+	Similar to * but there should be at least one match of the character to the left of the + sign in the expression.
?	Matches the character to its left 0 or 1 times.
()	Affects the order of pattern evaluation and also serves as a tagged expression that can be used when replacing the matched sub-string with another expression.
[]	Enclosing a set of characters indicates that any of the enclosed characters may match the target character.
\	Allows specifying a character that would otherwise be interpreted as special. \xHH represents the character whose value is the same as the value represented by (HH) hexadecimal digits [0-9A-Fa-f]. The value must be non-zero. BEL is the same as \x07, BS is \x08, FF is \x0C, LF is \x0A, CR is \x0D, TAB is \x09, and VT is \x0B. For any other character 'c', '\c' is the same as 'c' except that it is never interpreted as special

The following examples demonstrate the special characters:

- **a*** matches any number of occurrences of the letter a, including none.
- **a+** requires that at least one letter a be in the string to be matched.
- **ba?b** matches the string bb or bab.
- ***** matches any number of asterisks (*).

To use multipliers with multiple-character patterns, you enclose the pattern in parentheses.

- **(ab)*** matches any number of the multiple-character string ab.
- **([A-Za-z][0-9])+** matches one or more instances of alphanumeric pairs, but not none (that is, an empty string is not a match).

The order for matches using multipliers (*, +, or ?) is to put the longest construct first. Nested constructs are matched from outside to inside. Concatenated constructs are matched beginning at the left side of the construct. Thus, the regular expression matches A9b3, but not 9Ab3 because the letters are specified before the numbers.

You can also use parentheses around a single- or multiple-character pattern to instruct the software to remember a pattern for use elsewhere in the regular expression.

To create a regular expression that recalls a previous pattern, you use parentheses to indicate memory of a specific pattern and a backslash (\) followed by a digit to reuse the remembered pattern. The digit specifies the occurrence of a parentheses in the regular expression pattern. If you have more than one remembered pattern in your regular expression, \1 indicates the first remembered pattern, and \2 indicates the second remembered pattern, and so on.

The following regular expression uses parentheses for recall:

- **a(.)bc(.)\1\2** matches an *a* followed by any character, followed by *bc* followed by any character, followed by the first *any* character again, followed by the second *any* character again.

  For example, the regular expression can match aZbcTZT. The software remembers that the first character is Z and the second character is T and then uses Z and T again later in the regular expression.

Generic CLI Commands

The following CLI commands are generic to Cisco IPS 6.1.

- **configure terminal**—Enters global configuration mode.

  Global configuration commands apply to features that affect the system as a whole rather than just one protocol or interface.

  ```
  sensor# configure terminal
  sensor(config)#
  ```

- **service**—Takes you to the following configuration submodes: analysis-engine, anomaly-detection, authentication, event-action-rules, host, interface, logger, network-access, notification, signature-definition, ssh-known-hosts, trusted-certificates, and web-server.

  ```
  sensor# configure terminal
  sensor(config)# service event-action-rules rules0
  sensor(config-rul)#
  ```

The anomaly-detection, event-action-rules, and signature-definition submodes are multiple instance services. One predefined instance is allowed for each. For anomaly-detection, the predefined instance name is ad0. For event-action-rules, the predefined instance name is rules0. For signature-definition, the predefined instance name is sig0. The AIM IPS and NME IPS support only the predefined instances. All other sensors support the creation of additional instances.

- **end**—Exits configuration mode or any configuration submodes. It takes you back to the top-level EXEC menu.

```
sensor# configure terminal
sensor(config)# end
sensor#
```

- **exit**—Exits any configuration mode or closes an active terminal session and terminates the EXEC mode. It takes you to the previous menu session.

```
sensor# configure terminal
sensor(config)# service event-action-rules rules0
sensor(config-rul)# exit
sensor(config)# exit
sensor#
```

CLI Keywords

In general, use the **no** form of a command to disable a feature or function. Use the command without the keyword **no** to enable a disabled feature or function. For example, the command **ssh host-key** *ip_address* adds an entry to the known hosts table, the command **no ssh host-key** *ip_address* removes the entry from the known hosts table. Refer to the individual commands for a complete description of what the **no** form of that command does.

Service configuration commands can also have a default form. Use the **default** form of the command to return the command setting to its default. This keyword applies to the **service** submenu commands used for application configuration. Entering **default** with the command resets the parameter to the default value. You can only use the **default** keyword with commands that specify a default value in the configuration files.