



## **Cisco Intrusion Prevention System Command Reference for IPS 5.1**

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Customer Order Number:  
Text Part Number: OL-17104-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

*Cisco Intrusion Prevention System Command Reference for IPS 5.1*  
Copyright © 2005-2012 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** vii

Contents	vii
Audience	vii
Conventions	vii
Related Documents	viii
Obtaining Documentation and Submitting a Service Request	ix

---

## **CHAPTER 1**

### **Introducing the CLI** 1-1

User Roles	1-1
CLI Behavior	1-2
Command Line Editing	1-4
IPS Command Modes	1-5
Regular Expression Syntax	1-5
General CLI Commands	1-7
CLI Keywords	1-8

---

## **CHAPTER 2**

### **Available Commands** 2-1

banner login	2-3
clear denied-attackers	2-5
clear events	2-6
clear line	2-7
clock set	2-9
configure	2-10
copy	2-11
display serial	2-14
downgrade	2-15
end	2-16
erase	2-17
exit	2-18
iplog	2-19
iplog-status	2-21
more	2-23

more begin 2-25

more exclude 2-27

more include 2-29

packet 2-31

password 2-34

ping 2-36

privilege 2-38

recover 2-39

reset 2-41

service 2-42

setup 2-45

show begin 2-51

show clock 2-53

show configuration 2-55

show events 2-56

show exclude 2-58

show history 2-60

show include 2-61

show interfaces 2-63

show inventory 2-65

show privilege 2-66

show settings 2-67

show ssh authorized-keys 2-70

show ssh server-key 2-72

show ssh host-keys 2-73

show statistics 2-74

show tech-support 2-77

show tls fingerprint 2-79

show tls trusted-hosts 2-80

show users 2-81

show version 2-83

ssh authorized-key 2-85

ssh generate-key 2-87

ssh host-key 2-88

terminal 2-90

tls generate-key	2-91
tls trusted-host	2-92
trace	2-94
upgrade	2-95
username	2-97

---

**APPENDIX A****Deprecated Commands and Command Platform Dependencies** A-1

Deprecated Commands	A-1
Command/Platform Dependencies	A-2

---

**APPENDIX B****CLI Error Messages** B-1

---

**GLOSSARY**

---

**INDEX**





# Preface

---

Revised: September 9, 2012, OL-17104-01

## Contents

This guide provides reference information for the commands available in Cisco Intrusion Prevention System 5.1. This guide also includes a glossary, which contains expanded acronyms and pertinent IPS terms. This guide is part of the documentation set for Cisco Intrusion Prevention System 5.1. Use this guide in conjunction with the documents listed in [Related Documents](#), page viii.

This preface contains the following sections:

- [Audience](#), page vii
- [Conventions](#), page vii
- [Related Documents](#), page viii
- [Obtaining Documentation and Submitting a Service Request](#), page ix

## Audience

This guide is for experienced network security administrators who configure and maintain Cisco Intrusion Prevention System (IPS) sensors, including the supported IPS appliances and modules.

## Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	<b>boldface font</b>
Variables for which you supply values and new or important terminology	<i>italic font</i>
Displayed session and system information, paths and filenames	screen font
Information you enter	<b>boldface screen font</b>

Item	Convention
Variables you enter	<i>italic screen font</i>
Menu items and button names	<b>boldface font</b>
Indicates menu items to select, in the order you select them.	<b>Option &gt; Network Preferences</b>

**Note**

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Tip**

Identifies information to help you get the most benefit from your product

**Warning**

**Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

## Related Documents

The following documents support Cisco Intrusion Prevention System 5.1 and are found at the following URL:

[http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html)

- *Documentation Roadmap for Cisco Intrusion Prevention System 5.1*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*
- *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.





# CHAPTER 1

## Introducing the CLI

---

The IPS 5.1 CLI lets you access the sensor through Telnet, SSH, and serial interface connections.

This chapter contains the following topics:

- [User Roles, page 1-1](#)
- [CLI Behavior, page 1-2](#)
- [Command Line Editing, page 1-4](#)
- [IPS Command Modes, page 1-5](#)
- [Regular Expression Syntax, page 1-5](#)
- [General CLI Commands, page 1-7](#)
- [CLI Keywords, page 1-8](#)

## User Roles

The CLI for IPS 5.1 permits multiple users to log in at a time. You can create and remove users from the local sensor. You can only modify 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 will 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.

---

## CLI Behavior

Follow these tips when using the 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
```




---

**Note** 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**.




---

**Note** 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
```

### 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**.

# Command Line Editing

Table 1-1 describes the command line editing capabilities provided by the 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 redisplay the system prompt and command line
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.
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, <i>not</i> 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.

**Table 1-1** *Command Line Editing (continued)*

Keys	Description
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

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 typing `configure terminal`.  
The command prompt is `sensor(config)#`.
- **service mode configuration**—Entered from global configuration mode by typing `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 typing `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 signature definition and event action rules.

## Regular Expression Syntax

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.’

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 “alb” 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, then \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.

## General CLI Commands

The following CLI commands are generic to IPS 5.1.

- **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, authentication, event-action-rules, host, interface, logger, network-access, notification, signature-definition, ssh-known-hosts, trusted-certificates, and web-server.



**Note** The event-action-rules and signature-definition submodes are multiple instance services. Only one predefined instance is allowed for each. For event-action-rules, the only supported instance name is rules0. For signature-definition, the only supported instance name is sig0.

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

- **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 ipaddress** adds an entry to the known hosts table, the command **no ssh host-key ipaddress** 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. Typing **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.



## CHAPTER 2

# Available Commands

---

This chapter contains the IPS 5.1 commands listed in alphabetical order. It contains the following sections:.

- [banner login, page 2-3](#)
- [clear denied-attackers, page 2-5](#)
- [clear events, page 2-6](#)
- [clear line, page 2-7](#)
- [clock set, page 2-9](#)
- [configure, page 2-10](#)
- [copy, page 2-11](#)
- [display serial, page 2-14](#)
- [downgrade, page 2-15](#)
- [end, page 2-16](#)
- [erase, page 2-17](#)
- [exit, page 2-18](#)
- [iplog, page 2-19](#)
- [iplog-status, page 2-21](#)
- [more, page 2-23](#)
- [more begin, page 2-25](#)
- [more exclude, page 2-27](#)
- [more include, page 2-29](#)
- [packet, page 2-31](#)
- [password, page 2-34](#)
- [ping, page 2-36](#)
- [privilege, page 2-38](#)
- [recover, page 2-39](#)
- [reset, page 2-41](#)
- [service, page 2-42](#)
- [setup, page 2-45](#)

- [show begin, page 2-51](#)
- [show clock, page 2-53](#)
- [show configuration, page 2-55](#)
- [show events, page 2-56](#)
- [show exclude, page 2-58](#)
- [show history, page 2-60](#)
- [show include, page 2-61](#)
- [show interfaces, page 2-63](#)
- [show inventory, page 2-65](#)
- [show privilege, page 2-66](#)
- [show settings, page 2-67](#)
- [show ssh authorized-keys, page 2-70](#)
- [show ssh server-key, page 2-72](#)
- [show ssh host-keys, page 2-73](#)
- [show statistics, page 2-74](#)
- [show tech-support, page 2-77](#)
- [show tls fingerprint, page 2-79](#)
- [show tls trusted-hosts, page 2-80](#)
- [show users, page 2-81](#)
- [show version, page 2-83](#)
- [ssh authorized-key, page 2-85](#)
- [ssh generate-key, page 2-87](#)
- [ssh host-key, page 2-88](#)
- [terminal, page 2-90](#)
- [tls generate-key, page 2-91](#)
- [tls trusted-host, page 2-92](#)
- [trace, page 2-94](#)
- [upgrade, page 2-95](#)
- [username, page 2-97](#)

# banner login

To create a banner message to display on the terminal screen, use the **banner login** command in global configuration mode. To delete the login banner, use the **no** form of this command. The banner message appears when a user accesses the CLI and is displayed before the username and password prompts.

**banner login**

**no banner login**

## Syntax Description

<i>argument</i>	Text that appears before you log in to the CLI. Maximum message length is 2500 characters. A carriage return or question mark (?) must be preceded by the keystroke <b>Ctrl-V</b> .
-----------------	---

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## SupportedUserRoles

Administrator

## Command History

Release	Modification
5.0(1)	This command was introduced.

## Usage Guidelines

The **banner login** command lets you create a text message, up to 2500 characters, to display on the terminal screen. This message appears when you access the CLI. You can include a carriage return or question mark (?) in the message by first typing **Ctrl-V** followed by the carriage return or question mark. A carriage return is represented as **^M** in the text message you create, but appears as an actual carriage return when the message is displayed to the user.

Press **Ctrl-C** at the `Message` prompt to cancel the message request.



**Note** The format for this command is different from the Cisco IOS 12.0 implementation.

## Examples

The following example creates a message to display on the terminal screen at login:

```
sensor(config)# banner login
Banner[: This message will be displayed on login. ^M Thank you!
```

At login, the following message appears:

```
This message will be displayed on login.
```

```
Thank you!  
password:
```

# clear denied-attackers

To delete the current list of denied IP addresses, use the **clear denied-attackers** command in privileged EXEC mode.

## clear denied-attackers

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	5.0(1)	This command was introduced.

**Usage Guidelines** The **clear denied-attackers** command lets you restore communication with previously denied IP addresses by clearing the list of denied attackers. You cannot select and delete individual IP addresses on this list. If you clear the denied attackers list, all IP addresses are removed from the list.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example removes all IP addresses from the denied attackers list:

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the system.
Continue with clear? []: yes
sensor#
```

Related Commands	Command	Description
	show statistics denied-attackers	Displays the list of denied attackers.

# clear events

To clear the Event Store, use the **clear events** command in privileged EXEC mode.

**clear events**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** Use this command to clear all events from the Event Store.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example clears the Event Store:

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:yes
sensor#
```

# clear line

To terminate another CLI session, use the **clear line** command in privileged EXEC mode.

**clear line** *cli-id* [**message**]

Syntax Description		
<i>cli-id</i>		The CLI ID number associated with the login session. See the <b>show users</b> command.
<b>message</b>		(Optional) If you select <b>message</b> , you are prompted for a message to send to the receiving user.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	5.0(1)	This command was introduced.

**Supported User Roles** Administrator, Operator, Viewer



**Note** Operator and Viewer can only clear lines with the same username as the current login.

**Usage Guidelines** Use the **clear line** command to log out of a specific session running on another line. Use the **message** keyword if you want to include an optional message to display on the terminal of the login session you are terminating. **Ctrl-C** cancels the request and the carriage return sends the request with the specified message. The maximum message length is 2550 characters. Use **Ctrl-V** followed by a carriage return to put a carriage return in the message text.

You cannot use the **clear line** command to clear a Service account login.



**Note** The **message** keyword is not supported in the Cisco IOS 12.0 version of this command.

**Examples** The following example illustrates the output displayed when a user with Administrator privileges attempts to log in after the maximum sessions have been reached:

```
Error: The maximum allowed CLI sessions are currently open, would you like to terminate
one of the open sessions? [no] yes
CLI ID User Privilege
1253 admin1 administrator
1267 cisco administrator
1398 test operator
```

```
Enter the CLI ID to clear: 1253
Message:Sorry! I need access to the system, so I am terminating your session.
sensor#
```

The following example illustrates the message displayed on the terminal of admin1:

```
sensor#
***
***
Termination request from Admin0
***
Sorry! I need access to the system, so I am terminating your session.
```

The following example illustrates the output displayed when a user with Operator or Viewer privileges attempts to log in after the maximum sessions have been reached:

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

---

**Related Commands**

Command	Description
<b>show users</b>	Displays information about users logged in to the CLI.

# clock set

To manually set the system clock on the appliance, use the **clock set** command in privileged EXEC mode.

**clock set** *hh:mm[:ss] month day year*

Syntax Description		
	<i>hh:mm[:ss]</i>	Current time in hours (24-hour format), minutes, and seconds
	<i>month</i>	Current month (by name)
	<i>day</i>	Current day (by date) in the month
	<i>year</i>	Current year (no abbreviation)

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** You do not need to set the system clock under the following circumstances:

- When the system is synchronized by a valid outside timing mechanism, such as an NTP or VINES clock source.
- When you have a router with calendar capability.

Use the **clock set** command if no other time sources are available. The time specified in this command is relative to the configured time zone.

**Examples** The following example manually sets the system clock to 1:32 p.m. on July 29, 2002:

```
sensor# clock set 13:32 July 29 2002
sensor#
```

# configure

To enter global configuration mode, use the **configure terminal** command in privileged EXEC mode.

## **configure terminal**

<b>Syntax Description</b>	<b>terminal</b> Executes configuration commands from the terminal.
<b>Defaults</b>	No default behavior or values.
<b>Command Modes</b>	EXEC
<b>SupportedUserRoles</b>	Administrator, Operator, Viewer
<b>Usage Guidelines</b>	Executing the <b>configure terminal</b> command puts you in global configuration mode.
<b>Examples</b>	<p>The following example changes modes from privileged EXEC to global configuration:</p> <pre>sensor# <b>configure terminal</b> sensor(config)#</pre>

# copy

To copy iplogs and configuration files, use the **copy** command in privileged EXEC mode.

**copy** [/erase] *source-url destination-url*

**copy iplog** *log-id destination-url*

## Syntax Description

<b>/erase</b>	(Optional) Erases the destination file before copying. This keyword only applies to current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for destination current-config, the source configuration is merged with the current-config.
<i>source-url</i>	The location of the source file to be copied. Can be a URL or keyword.
<i>destination-url</i>	The location of the destination file to be copied. Can be a URL or keyword.
<i>log-id</i>	Log ID of the file to copy. Use the <b>iplog-status</b> command to retrieve the log-id.

## Defaults

No default behavior or values.

## Command Modes

EXEC

## SupportedUserRoles

Administrator, Operator (copy iplog or packet-file only), Viewer (copy iplog or packet-file only)

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The exact format of the source and destination URLs varies according to the file. The following valid types are supported:

Prefix	Source or Destination
ftp:	Source or destination URL for the FTP network server. The syntax for this prefix is: ftp://[username@] location/relativeDirectory/filename ftp://[username@]location//absoluteDirectory/filename
scp:	Source or destination URL for the SCP network server. The syntax for this prefix is: scp://[username@] location/relativeDirectory/filename scp://[username@] location//absoluteDirectory/filename

Prefix	Source or Destination
http:	Source URL for the web server. The syntax for this prefix is: http://[username@]location]/directory]/filename Can only be a source URL.
https:	Source URL for web server. The syntax for this prefix is: https://[username@]location]/directory]/filename Can only be a source URL.

Use keywords to designate the file location on the sensor. The following files are supported:

Keyword	Source or Destination
<b>current-config</b>	The current running configuration. This configuration, unlike that for Cisco IOS 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
<b>backup-config</b>	Storage location for configuration backup. The file format is CLI commands.
<b>iplog</b>	An iplog contained on the system. The IP logs are retrieved based on log-id. See the <b>iplog-status</b> command output. IP logs are stored in binary and are displayed with a log viewer.
<b>license-key</b>	The subscription license file.
<b>packet-file</b>	The locally stored libpcap file captured using the <b>packet capture</b> command.

If FTP or SCP is the selected protocol, you are prompted for a password. If no password is necessary for the FTP session, you can press Return without entering anything.

You can enter all necessary source and destination URL information and the username on the command line, or you can enter the **copy** command and have the sensor prompt you for any missing information.



#### Warning

**Copying a configuration file from another sensor can result in errors if the system sensing interfaces and virtual sensors are not configured the same.**



**Note** The Cisco IOS 12.0 **copy** command is more flexible and allows copying between different destinations.

#### Examples

The following example copies a file into the current configuration from the sensor with the IP address 10.1.1.1, directory/filename ~csidsuser/configuration/cfg, the directory and file are relative to the csidsuser's home account:

```
sensor# copy scp://csidsuser@10.1.1.1/configuration/cfg current-config
Password: *****
WARNING: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
csidsuser@10.1.1.1's password:
cfg                               100%
|*****| 36124          00:00
sensor#
```

The following example copies the iplog with ID 12345 to the sensor with the IP address 10.1.1.1, directory/filename ~csidsuser/iplog12345, the directory and file are relative to the csidsuser's home account:

```
sensor# copy iplog 12345 scp://csidsuser@10.1.1.1/iplog12345
Password: *****
iplog                               100%
|*****|
36124                               00:00
sensor#
```

### Related Commands

Command	Description
<b>iplog-status</b>	Displays a description of the available IP log contents.
<b>more</b>	Displays the contents of a logical file.
<b>packet</b>	Displays or captures live traffic on an interface.

# display serial

To direct all output to the serial connection, use the **display serial** command in global configuration mode. Use the **no display-serial** command to reset the output to the local terminal.

**display-serial**

**no display-serial**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** The default setting is no display-serial.

---

**Command Modes** EXEC

---

**SupportedUserRoles** Administrator, Operator

---

Release	Modification
4.0(1)	This command was introduced.

---



---

**Usage Guidelines** Using the **display-serial** command lets you view system messages on a remote console (using the serial port) during the boot process. The local console is not available as long as this option is enabled. Unless you set this option when you are connected to the serial port, you do not get any feedback until Linux has fully booted and enabled support for the serial connection.

---

**Examples** The following example redirects output to the serial port:

```
sensor(config)# display-serial
sensor(config)#
```

# downgrade

To remove the most recent upgrade, use the **downgrade** command in global configuration mode.

## downgrade

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Global configuration

**SupportedUserRoles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Examples** The following example removes the most recent upgrade from the system:

```

sensor(config)# downgrade
Warning: Executing this command will reboot the system and downgrade to
IDS-K9-sp-4.1-4-S91.rpm. Configuration changes made since the last upgrade will be lost
and the system may be rebooted.
Continue with downgrade?: yes
sensor#

```

If the **downgrade** command is not available, for example, if no upgrades have been applied, the following is displayed:

```

sensor# downgrade
Error: No downgrade available
sensor#

```

Related Commands	Command	Description
	<b>show version</b>	Displays the version information for all installed OS packages, signature packages, and IPS processes running on the system.

# end

To exit configuration mode, or any of the configuration submodes, use the **end** command in global configuration mode. This command exits to the top level EXEC menu.

**end**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** All modes

---

**SupportedUserRoles** Administrator, Operator, Viewer

---

Command History	Release	Modification
	4.0(1)	This command was introduced.

---



---

**Examples** The following example shows how to exit configuration mode:

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

# erase

To delete a logical file, use the **erase** command in privileged EXEC mode.

**erase** { **backup-config** | **current-config** | **packet-file** }

Syntax Description	Option	Description
	<b>backup-config</b>	The current running configuration. This configuration, unlike that for Cisco IOS 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
	<b>current-config</b>	Storage location for configuration backup. The file format is CLI commands.
	<b>packet-file</b>	The locally stored libpcap file captured using the packet capture command.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Supported User Roles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** The Cisco IOS 12.0 version of this command lets you remove entire file systems. IPS does not support this concept.

**Examples** The following example erases the current configuration file and returns all settings back to default. You may need to reboot the sensor with this command.

```
sensor# erase current-config
Warning: Removing the current-config file will result in all configuration being reset to
default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no username"
command.
Continue? []: yes
sensor#
```

# exit

To exit a configuration mode or close an active terminal session and terminate privileged EXEC mode, use the **exit** command.

**exit**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** All modes

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** Use the **exit** command to return to the previous menu level. If you have made any changes in the contained submodes, you are asked if you want to apply them. If you select no, you are returned to the parent submode.

**Examples** The following example shows how to return to the previous menu level:

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

# iplog

To start IP logging on a virtual sensor, use the **iplog** command in privileged EXEC mode. Use the **no** form of this command to disable all logging sessions on a virtual sensor, a particular logging session based on log-id, or all logging sessions.

**iplog** *name ip-address* [**duration** *minutes*] [**packets** *numPackets*] [**bytes** *numBytes*]

**no iplog** [**log-id** *log-id* | **name** *name*]

## Syntax Description

<i>name</i>	Virtual sensor on which to begin and end logging.
<i>ip-address</i>	Logs only log packets containing the specified IP address. See the <b>setup</b> command for parameter details.
<i>minutes</i>	Duration the logging should be active, in minutes. Valid range is 1-60. Default is 10 minutes.
<i>numPackets</i>	Total number of packets to log. Valid range is 0-4294967295. Default is 1000 packets. A value of 0 indicates unlimited.
<i>numBytes</i>	Total number of bytes to log. Valid range is 0-4294967295. A value of 0 indicates unlimited.
<i>log-id</i>	Log ID of logging session to stop. The log-id can be retrieved using the <b>iplog-status</b> command.

## Defaults

See the Syntax Description table.

## Command Modes

EXEC

## Supported User Roles

Administrator, Operator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

If the **no** form of this command is specified without parameters, all logging is stopped.

If duration, packets, and bytes are entered, logging terminates whenever the first event occurs.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples**

The following example begins logging all packets containing 10.2.3.1 in the source or destination address on virtual sensor vs0:

```
sensor# iplog vs0 10.2.3.1
Logging started for virtual sensor vs0, IP address 10.2.3.1, Log ID 2342
WARNING: IP Logging will affect system performance.
sensor#
```

## Related Commands

Command	Description
<b>iplog-status</b>	Displays a description of the available IP log contents.
<b>packet</b>	Displays or captures live traffic on an interface.

# iplog-status

To display a description of the available IP log contents, use the **iplog-status** command in privileged EXEC mode.

## iplog-status

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	The Status field was added to this command.

**Usage Guidelines** When the log is created, the status is *added*. If and when the first entry is inserted in the log, the status changes to *started*. When the log is completed, because it has reached the packet count limit for example, the status changes to *completed*.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example displays the status of all IP logs:

```

sensor# iplog-status
Log ID:          2425
IP Address:      10.1.1.2
Virtual Sensor:  vs0
Status:          started
Start Time:      2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured: 1039438

Log ID:          2342
IP Address:      10.2.3.1
Virtual Sensor:  vs0
Status:          completed
Event ID:        209348
Start Time:      2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:        2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#

```

Related Commands	Command	Description
	<b>iplog</b>	Starts IP logging on a virtual sensor.

## more

To display the contents of a logical file, use the **more** command in privileged EXEC mode.

**more** *keyword*

Syntax Description	current-config	The current running configuration. This configuration, unlike that for Cisco IOS 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
	backup-config	Storage location for configuration backup. The file format is CLI commands.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator (current-config only), Viewer (current-config only)

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** IPS allows display of logical files only.  
Hidden fields, such as passwords, are displayed for Administrators only.



**Note** The Cisco IOS 12.0 version of this command lets you display the contents of files stored on various partitions in the device.

**Examples** The following example shows the output from the **more** command:

```
sensor# more current-config
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
```

```

service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
--MORE--

```

---

**Related Commands**

Command	Description
<b>more begin</b>	Searches the output of the <b>more</b> command and displays the output from the first instance of a specified string.
<b>more exclude</b>	Filters the <b>more</b> command output so that it excludes lines that contain a particular regular expression.
<b>more include</b>	Filters the <b>more</b> command output so that it displays only lines that contain a particular regular expression.

## more begin

To search the output of any **more** command, use the **more begin** command in privileged EXEC mode. This command begins unfiltered output of the **more** command with the first line that contains the regular expression specified.

```
more keyword | begin regular-expression
```

Syntax Description	<i>keyword</i>	<b>backup-config</b>	The current running configuration. This configuration, unlike that for Cisco IOS 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
		<b>current-config</b>	Storage location for configuration backup. The file format is CLI commands.
			A vertical bar indicates that an output processing specification follows.
	<i>regular expression</i>		Any regular expression found in more command output.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Supported User Roles** Administrator, Operator (current-config only), Viewer (current-config only)

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	The <b>begin</b> extension of the <b>more</b> command was introduced.

**Usage Guidelines** The *regular-expression* argument is case sensitive and allows for complex matching requirements.

**Examples** The following example shows how to search the **more** command output beginning with the regular expression “ip”:

```
sensor# more current-config | begin ip
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
```

```

exit
! -----
service interface
exit
! -----
service logger
exit
! -----
service network-access
user-profiles mona
enable-password foobar
exit
exit
! -----
service notification
--MORE--

```

### Related Commands

Command	Description
<b>more exclude</b>	Filters the <b>more</b> command output so that it excludes lines that contain a particular regular expression.
<b>more include</b>	Filters the <b>more</b> command output so that it displays only lines that contain a particular regular expression.
<b>show begin</b>	Searches the output of certain <b>show</b> commands and displays the output from the first instance of a specified string.
<b>show exclude</b>	Filters the <b>show</b> command output so that it excludes lines that contain a particular regular expression.
<b>show include</b>	Filters the <b>show</b> command output so that it displays only lines that contain a particular regular expression.

# more exclude

To filter the **more** command output so that it excludes lines that contain a particular regular expression, use the **more exclude** command in privileged EXEC mode.

**more** *keyword* | **exclude** *regular-expression*

Syntax Description	<i>keyword</i>	<b>backup-config</b>	The current running configuration. This configuration, unlike that for Cisco IOS 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
		<b>current-config</b>	Storage location for configuration backup. The file format is CLI commands.
			A vertical bar indicates that an output processing specification follows.
	<i>regular expression</i>		Any regular expression found in more command output.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Supported User Roles** Administrator, Operator (current-config only), Viewer (current-config only)

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	The <b>exclude</b> extension of the <b>more</b> command was added.

**Usage Guidelines** The *regular-expression* argument is case sensitive and allows for complex matching requirements.

**Examples** The following example shows how to search the **more** command output excluding the regular expression “ip”:

```
sensor# more current-config | exclude ip
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
```

## more exclude

```

exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
--MORE--

```

### Related Commands

Command	Description
<b>more begin</b>	Searches the output of the <b>more</b> command and displays the output from the first instance of a specified string.
<b>more include</b>	Filters the <b>more</b> command output so that it displays only lines that contain a particular regular expression.
<b>show begin</b>	Searches the output of certain <b>show</b> commands and displays the output from the first instance of a specified string.
<b>show exclude</b>	Filters the <b>show</b> command output so that it excludes lines that contain a particular regular expression.
<b>show include</b>	Filters the <b>show</b> command output so that it displays only lines that contain a particular regular expression.

# more include

To filter the **more** command output so that it displays only lines that contain a particular regular expression, use the **more include** command in privileged EXEC mode.

**more** *keyword* | **include** *regular-expression*

Syntax Description	<i>keyword</i>	<b>backup-config</b>	The current running configuration. This configuration, unlike that for Cisco IOS 12.0, becomes persistent as the commands are entered. The file format is CLI commands.
		<b>current-config</b>	Storage location for configuration backup. The file format is CLI commands.
			A vertical bar indicates that an output processing specification follows.
	<i>regular expression</i>		Any regular expression found in more command output.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**Supported User Roles** Administrator, Operator (current-config only), Viewer (current-config only)

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	The <b>include</b> extension of the <b>more</b> command was added.

**Usage Guidelines** The regular-expression argument is case sensitive and allows for complex matching requirements.

**Examples** The following example shows how to search the **more** command output to include only the regular expression "ip":

```
sensor# more current-config | include ip
host-ip 10.89.147.31/25,10.89.147.126
sensor#
```

Related Commands	Command	Description
	<b>more begin</b>	Searches the output of the <b>more</b> command and displays the output from the first instance of a specified string.
	<b>more exclude</b>	Filters the <b>more</b> command output so that it excludes lines that contain a particular regular expression.
	<b>show begin</b>	Searches the output of certain <b>show</b> commands and displays the output from the first instance of a specified string.
	<b>show exclude</b>	Filters the <b>show</b> command output so that it excludes lines that contain a particular regular expression.
	<b>show include</b>	Filters the <b>show</b> command output so that it displays only lines that contain a particular regular expression.

# packet

To display or capture live traffic on an interface, use the **packet** command in EXEC mode. Use the **display** option to dump live traffic or a previously captured file output directly to the screen. Use the **capture** option to capture the libpcap output into a local file. There is only one local file storage location, subsequent capture requests overwrite the existing file. You can copy the local file off the machine using the **copy** command with the **packet-file** keyword. You can view the local file using the **display packet-file** option. Use the **info** option to display information about the local file, if any. Use the **packet display iplog id [verbose] [expression expression]** to display iplogs.

**packet display interface-name [snaplen length] [count count] [verbose] [expression expression]**

**packet display packet-file [verbose] [expression expression]**

**packet display iplog id [verbose] [expression expression] vlan and**

**packet capture interface-name [snaplen length] [count count] [expression expression]**

**packet display file-info**

Syntax Description	display	Displays the packet on the screen.
<i>interface-name</i>		Interface name, interface type followed by slot/port. You are allowed to enter only a valid interface name existing in the system.
<b>snaplen</b>		(Optional) Specifies to use snapshot length.
<i>length</i>		(Optional) Snapshot length. The default is 0. A valid range is 0 to 1600.
<b>count</b>		(Optional) Specifies to capture packets.
<i>count</i>		(Optional) Number of packets to capture. If not specified, the capture terminates after the maximum file size has been captured. The valid range is 1 to 10000.
<b>verbose</b>		(Optional) Displays the protocol tree for each packet rather than a one-line summary.
<b>expression</b>		(Optional) Specifies to use an expression to filter the packet.
<i>expression</i>		(Optional) Packet capture filter expression. This expression is passed directly to tcpdump and must meet the tcpdump expression syntax.
<i>id</i>		Existing IP log ID to display.
<b>file-info</b>		Displays information about the stored packet file.
<b>vlan and</b>		Matches packets with VLAN headers.

**Defaults** See the Syntax Description table.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer (display only)

**Command History**

Release	Modification
5.0(1)	This command was introduced.

**Usage Guidelines**

Storage is available for one local file. The size of this file varies depending on the platform. If possible, a message is displayed if the maximum file size is reached before the requested packet count is captured. Only one user can use the **packet capture interface-name** command at a time. A second user request results in an error message containing information about the user executing the capture. A configuration change involving the interface can result in abnormal termination of any packet command running on that interface.

**Note**

The command does not exist in Cisco IOS 12.0 or earlier.

**Caution**

Executing this command causes significant performance degradation.

**Note**

If you use the **expression** option when monitoring packets with VLAN headers, the expression does not match properly unless **vlan and** is added to the beginning of the expression. For example, **packet display iplog 926299444 verbose expression icmp** Will NOT show ICMP packets; **packet display iplog 926299444 verbose expression vlan and icmp** WILL show ICMP packets. It is often necessary to use **expression vlan and** on the IDSM2 and IPS appliance interfaces connected to trunk ports.

Press **Ctrl-C** to terminate the live display or file capture.

The expression syntax is described in the `ethereal-filter` man page.

The file-info displays:

Captured by: *user:id*, Cmd: *cliCmd*

Start: *yyyy/mm/dd hh:mm:ss zone*, End: *yyyy/mm/dd hh:mm:ss zone* or *in-progress*

Where

*user* = Username of user initiating capture,

*id* = User's CLI ID,

*cliCmd* = Command entered to perform the capture.

**Examples**

The following example displays the live traffic occurring on fastethernet 0/0:

```
sensor# packet display fastethernet0/0
Warning This command will cause significant performance degradation.
Executing command: tethereal -i fastethernet0/0
0.000000 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=56
0.000262 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470 Ack=2972370007
Win=9184 Len=0
0.029148 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.029450 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470 Ack=2972370231
Win=9184 Len=0
0.030273 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.030575 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470 Ack=2972370455
Win=9184 Len=0
```

```
0.031361 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.031666 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470 Ack=2972370679
Win=9184 Len=0
0.032466 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.032761 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK]
```

The following example displays information about the stored capture file:

```
sensor# packet display file-info
Captured by: raboyd:5292, Cmd: packet capture fastethernet0/0
Start: 2004/01/07 11:16:21 CST, End: 2004/01/07 11:20:35 CST
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>iplog</b>	Starts IP logging on a virtual sensor.
<b>iplog-status</b>	Displays a description of the available IP log contents.

# password

To update your password on the local sensor, use the **password** command in global configuration mode. The administrator can also use the **password** command to change the password for an existing user. The administrator can use the **no** form of the command to disable a user account.

## password

Administrator syntax: **password** [*name* [*newPassword*]]

**no password** [*name*]

### Syntax Description

<i>name</i>	Specifies the users's name. A valid username is 1 to 64 characters in length. The username must begin with an alphanumeric character, otherwise all characters except spaces are accepted.
password	The password is requested when the user enters this command. Specifies the password for the user. A valid password is 6 to 32 characters in length. All characters except space and '?' are allowed.

### Defaults

The cisco account default password is cisco.

### Command Modes

Global configuration

### Supported User Roles

Administrator, Operator (current user's password only), Viewer (current user's password only)

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

Use the **password** command to update the current user's login password. The administrator can also use this command to modify the password for an existing user. The administrator is not prompted for the current password in this case.

You receive an error if you try to disable the last administrator account. Use the **password** command to reenable a disabled user account and reset the user password.

The password is protected in IPS.



**Note** The Cisco IOS 12.0 password command lets you enter the new password in the clear on the password line.

**Examples**

The following example shows how to modify the current user's password:

```
sensor(config)# password
Enter Old Login Password: *****
Enter New Login Password: *****
Re-enter New Login Password: *****
sensor(config)#
```

The following example modifies the password for the user `tester`. Only Administrators can execute this command:

```
sensor(config)# password tester
Enter New Login Password: *****
Re-enter New Login Password: *****
sensor(config)#
```

**Related Commands**

Command	Description
<code>username</code>	Creates users on the local sensor.

# ping

To diagnose basic network connectivity, use the **ping** command in privileged EXEC mode.

**ping** *address* [*count*]

Syntax Description	<i>address</i>	IP address of the system to ping.
	<i>count</i>	Number of echo requests to send. If no value is entered, four requests are sent. The valid range is 1 to 10000.

**Defaults** See the Syntax Description table.

**Command Modes** EXEC

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Supported User Roles** Administrator, Operator, Viewer

**Usage Guidelines** This command is implemented using the **ping** command provided by the operating system. The output from the command varies slightly between operating systems.

**Examples** The following example shows the output of the **ping** command for Solaris systems:

```
sensor# ping 10.1.1.1
PING 10.1.1.1: 32 data bytes
40 bytes from 10.1.1.1: icmp_seq=0. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=1. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=2. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=3. time=0. ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
sensor#
```

The following example shows the output of the **ping** command for Linux systems:

```
sensor# ping 10.1.1.1 2
PING 10.1.1.1 from 10.1.1.2 : 32(60) bytes of data.
40 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=0.2 ms
40 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.2 ms

--- 10.1.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
sensor#
```

The following example shows the output for an unreachable address:

```
sensor# ping 172.21.172.1
PING 172.21.172.1 (172.21.172.1) from 10.89.175.50 : 56(84) bytes of data.

--172.21.172.1 ping statistics--
5 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

# privilege

To modify the privilege level for an existing user, use the **privilege** command in global configuration mode. You can also specify the privilege while creating a user with the **username** command.

**privilege user** *name* [**administrator** | **operator** | **viewer**]

<b>Syntax Description</b>	<i>name</i>	Specifies the users's name. A valid username is 1 to 64 characters in length. The username must begin with an alphanumeric character, otherwise all characters except spaces are accepted.
---------------------------	-------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	Use the command to modify the privilege for a user.
-------------------------	---



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

<b>Examples</b>	The following example changes the privilege of the user “tester” to operator.
-----------------	---

```
sensor(config)# privilege user tester operator
Warning: The privilege change does not apply to current CLI sessions. It will be applied
to subsequent logins.
sensor(config)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>username</b>	Creates users on the local sensor.

# recover

To reimage the application partition with the application image stored on the recovery partition, use the **recover** command in privileged EXEC mode. The sensor is rebooted multiple times and most configuration—except for network, access list, and time parameters—is reset to the default settings.

More specifically, the following settings are maintained after a local recovery using the "recover application-partition" command: Network Settings (IP Address, Netmask, Default Gateway, Hostname, and Telnet (enabled/disabled)); Access List Entries/ACL0 Settings (IP Address and Netmask); and Time Settings (Offset and Standard Time Zone Name); the rest of the parameters are reset to the default settings.

## recover application-partition

<b>Syntax Description</b>	<b>application-partition</b> Reimages the application partition.
---------------------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>SupportedUserRoles</b>	Administrator
---------------------------	---------------

<b>Usage Guidelines</b>	<p>Valid answers to the continue with recover question are <b>yes</b> or <b>no</b>. <b>Y</b> or <b>N</b> are not valid responses.</p> <p>Shutdown begins immediately after the command is executed. Because shutdown may take a little time, you may continue to access CLI commands (access is not denied), but access is terminated without warning. If necessary, a period (.) will be displayed on the screen once a second to indicate progress while the applications are shutting down.</p>
-------------------------	--



<b>Note</b>	This command does not exist in Cisco IOS 12.0 or earlier.
-------------	---

<b>Examples</b>	The following example reimages the application partition using the version 4.0(1)S29 image stored on the recovery partition:
-----------------	--

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 5.0(1)Sx. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:yes
Request Succeeded
```

```
sensor (config) #
```

# reset

To shut down the applications running on the sensor and reboot the appliance, use the **reset** command in privileged EXEC mode. If the **powerdown** option is included, the appliance is powered off if possible or left in a state where the power can be turned off.

**reset [powerdown]**

Syntax Description	powerdown	This option causes the sensor to power off after the applications are shutdown.
--------------------	-----------	---

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	4.0(1)	This command was introduced.

**SupportedUserRoles** Administrator

**Usage Guidelines** Valid answers to the continue with reset question are **yes** or **no**. **Y** or **N** are not valid responses.

Shutdown begins immediately after the command is executed. Access to the CLI commands is not denied during the shutdown, however, an open session is terminated without warning as soon as the shutdown is completed. If necessary, a period (.) will be displayed on the screen once a second to indicate progress while the applications are shutting down.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example reboots the sensor:

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:yes
sensor#
```

# service

To enter configuration menus for various sensor services, use the **service** command in global configuration mode. Use the **default** form of the command to reset the entire configuration for the application back to factory defaults.

```
service {authentication | analysis-engine | event-action-rules name | host | interface | logger |
network-access | notification | signature-definition name | ssh-known-hosts |
trusted-certificate | web-server}
```

```
default service {authentication | analysis-engine | host | interface | logger | network-access |
notification | ssh-known-hosts | trusted-certificate | web-server}
```

## Syntax Description

<b>authentication</b>	Configures the order of methods that should be used to authenticate users.
<b>analysis-engine</b>	Configures the global analysis engine parameters. This configuration lets you create virtual sensors and assign signature definitions, event action rules, and sensing interfaces to virtual sensors.
<b>event-action-rules</b>	Configures the parameters for an event action rules configuration. This configuration replaces the 4.X alarm channel configuration.
<b>host</b>	Configures the system clock settings, upgrades, and IP access list.
<b>interface-config</b>	Configures the physical interfaces and inline interface pairs.
<b>logger</b>	Configures debug levels.
<b>network-access</b>	Configures parameters relating to ARC.  <b>Note</b> Network Access Controller is now known as Attack Response Controller (ARC). Although the service has a new name, the change is not reflected in the IPS 5.1 CLI. You will still see <b>network-access</b> and <b>nac</b> throughout the CLI.
<b>notification</b>	Configures the notification application.
<b>signature-definition</b>	Configures the parameters for a signature definition configuration.
<b>ssh-known-hosts</b>	Configures the known hosts keys for the system.
<b>trusted-certificate</b>	Configures the list of X.509 certificates for trusted certificate authorities.
<b>web-server</b>	Configures parameters relating to the web server such as web server port.
<b>name</b>	Logical name of the event action rules or signature definition configuration.  <b>Note</b> There are only two valid names: rules0 for event action rules and sig0 for signature definition.

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Supported User Roles

Administrator, Operator, Viewer (display only)

**Command History**

Release	Modification
4.0(1)	This command was introduced.
5.0(1)	The <b>default</b> keyword was added. Notification application support was added.

**Usage Guidelines**

This command lets you configure service-specific parameters. The items and menus in this configuration are service dependent and are built dynamically based on the configuration retrieved from the service when the command is executed.

**Caution**

**The modifications made in this mode and any submodes contained within it are applied to the service when you exit the service mode.**

The command mode is indicated on the command prompt by the name of the service. For example, service authentication has the following prompt:

```
sensor(config-aut)#
```

This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

Within the service event-action-rules and service signature-definition modes, you can create variables and configure rules to filter events. If you use a variable in a filter, you must use a dollar sign (\$SIG1) in front of the variable to indicate that the string you have entered represents a variable.

To enter more than one IP address, use a comma (no space) between the addresses. An IP address range can be expressed in the form A.B.C.D/b, where A.B.C.D represents an IP address and b represents the number of low-order bits that are masked in the IP address to specify the range. For example, the value 10.1.0.0/8 indicates an IP address of 10.1.0.0 with the lower 8 bits masked off to form a range of 10.1.0.0-10.1.0.255. Partial IP addresses can be used as part of the v4 IP address range when the allowPartialInput attribute is set to true. Because the range values are inclusive, the range 10.2-10.3 is equivalent to 10.2.0.0-10.3.255.255. The data for a range type can also be a set of ranges. A set of ranges consists of two or more ranges separated by commas—for example, 10.1.9.20-10.1.9.30,10.1.10.40-10.1.10.50,10.2-10.3.

A configuration can only be deleted if it is not assigned to a virtual sensor.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples**

The following command enters the configuration mode for the authentication service:

```
sensor(config)# service authentication
sensor(config-aut)#
```

The following command enters the configuration mode for the analysis engine service:

```
sensor(config)# service analysis-engine
sensor(config-ana)#
```

The following command enters the configuration mode for the event action rules service:

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

The following command enters the configuration mode for the host service:

```
sensor(config)# service host  
sensor(config-hos)#
```

The following command enters the configuration mode for the interface service:

```
sensor(config)# service interface  
sensor(config-int)#
```

The following command enters the configuration mode for the logger service:

```
sensor(config)# service logger  
sensor(config-log)#
```

The following command enters the configuration mode for the ARC service:

```
sensor(config)# service network-access  
sensor(config-net)#
```

The following command enters the configuration mode for the SNMP notification service:

```
sensor(config)# service notification  
sensor(config-not)#
```

The following command enters the configuration mode for the signature definition service:

```
sensor(config)# service signature-definition sig0  
sensor(config-sig)#
```

The following command enters the configuration mode for the SSH known hosts service:

```
sensor(config)# service ssh-known-hosts  
sensor(config-ssh)#
```

The following command enters the configuration mode for the trusted certificate service:

```
sensor(config)# service trusted-certificate  
sensor(config-tru)#
```

The following command enters the configuration mode for the web server service:

```
sensor(config)# service web-server  
sensor(config-web)#
```

# setup

To configure basic sensor configuration, use the **setup** command in privileged EXEC mode.

## setup

**Syntax Description** This command has no arguments or keywords.

### Defaults

hostname sensor

IP interface 10.1.9.201/24,10.1.9.1

telnet-server disabled

web-server port 443

summer time disabled

If summer time is enabled by the user, the defaults are as follows:

- Summertime type Recurring
- Start Month april
- Start Week first
- Start Day sunday
- Start Time 02:00:00
- End Month october
- End Week last
- End Day sunday
- End Time 02:00:00
- Offset 60

System timezone defaults:

- Timezone UTC
- UTC Offset 0

**Command Modes** EXEC

**SupportedUserRoles** Administrator

### Command History

Release	Modification
4.0(2)	Added configuration of access lists and time settings.
5.1(1)	Added configuration of inline vlan pairs and virtual sensor settings.

**Usage Guidelines**

When you type the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process.

The values shown in brackets next to each prompt are the default values last set.

You must run through the entire System Configuration Dialog until you come to the item that you want to change. To accept default settings for items that you do not want to change, press **Enter**.

To return to the EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

The facility also provides help text for each prompt. To access help text, type the question mark (?) at a prompt.

When you complete your changes, the configuration that was created during the setup session appears. You are prompted to save this configuration. If you type **yes**, the configuration is saved to disk. If you type **no**, the configuration is not saved and the process begins again. There is no default for this prompt; you must type either **yes** or **no**.

Valid ranges for configurable parameters are as follows:

IP Address/Netmask/Gateway: *X.X.X.X/nn.Y.Y.Y.Y*, where

*X.X.X.X* specifies the sensor IP address as a 32-bit address written as four octets separated by periods where *X* = 0-255.

*nn* specifies the number of bits in the netmask.

*Y.Y.Y.Y* specifies the default gateway as a 32-bit address written as four octets separated by periods where *Y* = 0-255.

Host Name: Case sensitive character string, up to 256 characters. Numbers, “\_” and “-” are valid, spaces are not accepted.

Enter the clock settings in setup mode only if the system is NOT using NTP. NTP commands are provided separately.

You can configure daylight savings time either in recurring mode or date mode. If you select recurring mode, the start and end days are entered based on week, day, month, and time. If you select date mode, the start and end days are entered based on month, day, year, and time. Selecting disable turns off daylight savings time.

[Table 2-1](#) shows the clock setting parameters.

**Table 2-1 Clock Setting Parameters**

DST zone	Name of time zone to be displayed when summer time is in effect.
week	Week of the month (1 to 5 or last).
day	Day of the week (Sunday, Monday,...).
date	Date of the month (1 to 31).
month	Month (January, February,...).
year	Year, no abbreviation (2001 to 2035).
hh:mm	Start/end DST (24-hour format) in hours and minutes.
offset	(Optional) Number of minutes to add during summertime. The default is 60.
timezone	Name of the time zone to be displayed when standard time is in effect.

**Table 2-1 Clock Setting Parameters (continued)**

hours	Hours offset from UTC.
hh:mm:ss	Current time in hours (24-hour format), minutes, and seconds.

You can also edit the default virtual sensor, vs0. You can assign promiscuous, inline pairs, and/or inline VLAN pairs to the virtual sensor, which in turn enables the assigned interfaces. After setup is complete, the virtual sensor is configured to monitor traffic.

**Examples**

The following example shows the **setup** command and the System Configuration program:

```
sensor# setup
```

```
--- System Configuration Dialog ---
```

```
At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].
```

```
Current Configuration:
```

```
service host
network-settings
host-ip 172.21.172.25/8,172.21.172.1
host-name sensor
telnet-option disabled
access-list 10.0.0.0/24
access-list 172.0.0.0/24
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
service interface
physical-interfaces GigbitEthernet0/0
admin-state enabled
exit
exit
physical-interfaces GigbitEthernet1/0
```

```

admin-state enabled
subinterface-type inline-vlan-pair
subinterface 3
description Created via setup by user cisco
vlan1 5
vlan2 6
exit
exit
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0
physical-interface GigabitEthernet1/0 subinterface-number 3
exit
exit

```

Current time: Wed May 5 10:25:35 2004

Setup Configuration last modified: Mon May 3 15:34:30 2004

```

Continue with configuration dialog?[yes]:
Enter host name[sensor]:
Enter IP interface[172.21.172.25/8,172.21.172.1]:
Enter telnet-server status[enabled]:
Enter web-server port[8080]: 80
Modify current access list? [no]: yes
Current access list entries:
    [1] 10.0.0.0/24
    [2] 172.0.0.0/24
Delete: 1
Delete:
Permit: 173.0.0.0/24
Permit:

Modify system clock settings? [no]: yes
Use NTP? [yes] no
Modify summer time settings? [no]: yes
    Recurring, Date or Disable[recurring]:
    Start Month[apr]:
    Start Week[1]:
    Start Day[sun]:
    Start Time[02:00:00]:
    End Month[oct]:
    End Week[last]:
    End Day[sun]:
    End Time[02:00:00]:
    DST Zone[]: CDT
    Offset[60]:
Modify system timezone? [no]: yes
    Timezone[UTC]: CST
    GMT Offset[-360]
Modify virtual sensor "vs0" configuration?[no]: yes
Current interface configuration
Command control: GigabitEthernet0/1
Unused:
    GigabitEthernet1/1
    GigabitEthernet2/0
    GigabitEthernet2/1
Promiscuous:
    GigabitEthernet0/0

```

```

Inline:
  None
Inline Vlan Pair:
  GigabitEthernet1/0 : 3; Vlans: 5, 6
Delete Promiscuous interfaces?[no]:
Delete Inline Vlan Pairs? [no] yes
Inline Vlan Pair Interfaces:
  [1] GigabitEthernet1/0
Interface to modify: 1
Inline Vlan Pairs for GigabitEthernet1/0:
  [1] Subinterface: 3; Vlans: 5, 6
Delete: 1
Delete:
Delete Inline Vlan Pairs?[no]:
Add Promiscuous interfaces?[no]:
Add Inline pairs?[no]: yes
Pair name: test
Description[Created via setup by user cisco]:
Interface1[]: GigabitEthernet2/0
Interface2[]: GigabitEthernet2/1
Pair name:
Add Inline Vlan Pairs?[no]: yes
Available Interfaces:
  [1] GigabitEthernet1/0
  [2] GigabitEthernet1/1
Interface to modify: 2
Inline Vlan Pairs for GigabitEthernet1/1:
  None
Subinterface number: 1
Description[Created via setup by user cisco]:
Vlan1[]: 1
Vlan2[]: 2
Subinterface number:
Add Inline Vlan Pairs?[no]:

```

The following configuration was entered.

```

service host
network-settings
host-ip 172.21.172.25/8,172.21.172.1
host-name sensor
telnet-option enabled
access-list 172.0.0.0/24
access-list 173.0.0.0/24
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month april
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit

```

```

end-summertime
month october
week-of-month last
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option disabled
exit
service web-server
port 80
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet1/1
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user cisco
vlan1 1
vlan2 2
exit
exit
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
inline-interfaces test
description Created via setup by user cisco
interface1 GigabitEthernet2/0
interface2 GigabitEthernet2/1
exit
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0
physical-interface GigabitEthernet1/1 subinterface-number 1
logical-interface test
exit
exit

```

- [0] Go to the command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration and exit.

```

Enter your selection [2]:
Configuration Saved.
Modify system date and time? [no] yes
  Local Date[]: 2003-01-18
  Local Time[4:33:49]: 10:33:49
System Time Updated successfully
sensor#

```

# show begin

To search the output of certain **show** commands, use the **show begin** command in privileged EXEC mode. This command begins unfiltered output of the **show** command with the first line that contains the regular expression specified.

```
show [configuration | events | settings | tech-support] | begin regular-expression
```

Syntax Description	
	A vertical bar indicates that an output processing specification follows.
<i>regular-expression</i>	Any regular expression found in show command output.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator (current-config only), Viewer (current-config only)

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	The <b>begin</b> extension of the <b>show</b> command was added.
	5.1(1)	Added <b>tech-support</b> option.

**Usage Guidelines** The *regular-expression* argument is case sensitive and allows for complex matching requirements.

**Examples** The following example shows the output beginning with the regular expression “ip”:

```
sensor# show configuration | begin ip
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
exit
! -----
service interface
exit
! -----
service logger
exit
! -----
```

## show begin

```

service network-access
user-profiles mona
enable-password foobar
exit
exit
! -----
service notification
--MORE--

```

### Related Commands

Command	Description
<b>more begin</b>	Searches the output of the <b>more</b> command and displays the output from the first instance of a specified string.
<b>more exclude</b>	Filters the <b>more</b> command output so that it excludes lines that contain a particular regular expression.
<b>more include</b>	Filters the <b>more</b> command output so that it displays only lines that contain a particular regular expression.
<b>show exclude</b>	Filters the <b>show</b> command output so that it excludes lines that contain a particular regular expression.
<b>show include</b>	Filters the <b>show</b> command output so that it displays only lines that contain a particular regular expression.

# show clock

To display the system clock, use the **show clock** command in privileged EXEC mode.

**show clock [detail]**

<b>Syntax Description</b>	<b>detail</b>	(Optional) Indicates the clock source (NTP or system) and the current summertime setting (if any).
---------------------------	---------------	--

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines** The system clock keeps an “authoritative” flag that indicates whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. [Table 2-2](#) shows the authoritative flags.

**Table 2-2 Authoritative Flags**

<b>Symbol</b>	<b>Description</b>
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but NTP is not synchronized.

**Examples** The following example shows NTP configured and synchronized:

```
sensor# show clock detail
12:30:02 CST Tues Dec 19 2002
Time source is NTP
Summer time starts 03:00:00 CDT Sun Apr 7 2003
Summer time ends 01:00:00 CST Sun Oct 27 2003
sensor#
```

The following example shows no time source configured:

```
sensor# show clock
*12:30:02 EST Tues Dec 19 2002
sensor#
```

The following example shows no time source is configured:

```
sensor# show clock detail
*12:30:02 CST Tues Dec 19 2002
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2003
Summer time ends 02:00:00 CDT Sun Oct 27 2003
```

# show configuration

See the **more current-config** command under the **more** command.

Command History	Release	Modification
	4.0(2)	This command was added.

# show events

To display the local event log contents, use the **show events** command in privileged EXEC mode.

```
show events [{alert [informational] [low] [medium] [high] [include-traits traits] [exclude-traits
traits] | error [warning] [error] [fatal] | NAC | status}] [hh:mm:ss [month day [year]] | past
hh:mm:ss]
```

## Syntax Description

<b>alert</b>	Displays alerts. Provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis engine whenever an IPS signature is triggered by network activity. If no level is selected (informational, low, medium, high), all alert events are displayed.
<b>include-traits</b>	Displays alerts that have the specified <i>traits</i> .
<b>exclude-traits</b>	Does not display alerts that have the specified <i>traits</i> .
<i>traits</i>	Trait bit position in decimal (0-15).
<b>error</b>	Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
<b>NAC</b>	Displays ARC requests (block requests).  <b>Note</b> Network Access Controller is now known as Attack Response Controller (ARC). Although the service has a new name, the change is not reflected in the IPS 5.1 CLI. You will still see <b>network-access</b> and <b>nac</b> throughout the CLI.
<b>status</b>	Displays status events.
<i>hh:mm:ss</i>	Starts time in hours (24-hour format), minutes, and seconds.
<i>day</i>	Starts day (by date) in the month.
<i>month</i>	Starts month (by name).
<i>year</i>	Starts year (no abbreviation).
<b>past</b>	Displays events starting in the past. The <i>hh:mm:ss</i> specify a time in the past to begin the display.

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Supported User Roles

Administrator, Operator, Viewer

## Command History

Release	Modification
4.0(1)	This command was introduced.

Release	Modification
4.0(2)	Ability to select multiple error event levels simultaneously was added.
4.1(1)	<b>include-traits</b> , <b>exclude-traits</b> , and <b>past</b> options were added.

### Usage Guidelines

The **show events** command displays the requested event types beginning at the requested start time. If no start time is entered, the selected events are displayed beginning at the current time. If no event types are entered, all events are displayed. Events are displayed as a live feed. You can cancel the live feed by the pressing **Ctrl-C**.

Use the regular expression **| include shunInfo** with the **show events** command to view the blocking information, including source address, for the event.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

### Examples

The following example displays block requests beginning at 10:00 a.m. on December 25, 2004:

```
sensor# show events NAC 10:00:00 Dec 25 2004
```

The following example displays error and fatal error messages beginning at the current time:

```
sensor# show events error fatal error
```

The following example displays all events beginning at 10:00 a.m. on December 25, 2004:

```
sensor# show events 10:00:00 Dec 25 2004
```

The following example displays all events beginning 30 seconds in the past:

```
sensor# show events past 00:00:30
```

The following output is taken from the XML content:

```
evAlert: eventId=1025376040313262350 severity=high
  originator:
    deviceName: sensor1
    appName: sensorApp
    time: 2002/07/30 18:24:18 2002/07/30 12:24:18 CST
    signature: sigId=4500 subSigId=0 version=1.0 IOS Embedded SNMP Community Names
  participants:
    attack:
      attacker: proxy=false
      addr: 132.206.27.3
      port: 61476
    victim:
      addr: 132.202.9.254
      port: 161
  protocol: udp
```

# show exclude

To filter the **show** command output so that it excludes lines that contain a particular regular expression, use the **show exclude** command in privileged EXEC mode.

```
show [configuration | events | settings | tech-support] | exclude regular-expression
```

## Syntax Description

	A vertical bar indicates that an output processing specification follows.
<i>regular-expression</i>	Any regular expression found in <b>show</b> command output.

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Supported User Roles

Administrator, Operator (current-config only), Viewer (current-config only)

## Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(2)	The <b>exclude</b> extension of the <b>show</b> command was added.
5.1(1)	Added <b>tech-support</b> option.

## Usage Guidelines

The *regular-expression* argument is case sensitive and allows for complex matching requirements.

## Examples

The following example shows the regular expression “ip” being excluded from the output:

```
sensor# show configuration | exclude ip
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-name sensor
```

```

access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
--MORE-

```

**Related Commands**

Command	Description
<b>more begin</b>	Searches the output of the <b>more</b> command and displays the output from the first instance of a specified string.
<b>more exclude</b>	Filters the <b>more</b> command output so that it excludes lines that contain a particular regular expression.
<b>more include</b>	Filters the <b>more</b> command output so that it displays only lines that contain a particular regular expression.
<b>show begin</b>	Searches the output of certain <b>show</b> commands and displays the output from the first instance of a specified string.
<b>show include</b>	Filters the <b>show</b> command output so that it displays only lines that contain a particular regular expression.

# show history

To list the commands you have entered in the current menu, use the **show history** command in all modes.

**show history**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** All modes

---

**SupportedUserRoles** Administrator, Operator, Viewer

---

Command History	Release	Modification
	4.0(1)	This command was introduced.

---



---

**Usage Guidelines** The **show history** command provides a record of the commands you have entered in the current menu. The number of commands that the history buffer records is 50.

---

**Examples** The following example shows the command record for the show history command:

```
sensor# show history
show users
show events
sensor#
```

# show include

To filter the **show** command output so that it displays only lines that contain a particular regular expression, use the **show include** command in privileged EXEC mode.

```
show [ configuration | events | settings | tech-support ] | include regular-expression
```

Syntax Description	
	A vertical bar indicates that an output processing specification follows.
regular-expression	Any regular expression found in show command output.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator (current-config only), Viewer (current-config only)

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	The <b>include</b> extension of the <b>show</b> command was added.
	5.1(1)	Added <b>tech-support</b> option.

**Usage Guidelines** The *regular-expression* argument is case sensitive and allows for complex matching requirements. The **show settings** command output also displays header information for the matching request so that the context of the match can be determined.

**Examples** The following example shows only the regular expression “ip” being included in the output:

```
sensor# show configuration | include ip
host-ip 10.89.147.31/25,10.89.147.126
sensor#
```

Related Commands	Command	Description
	<b>more begin</b>	Searches the output of the <b>more</b> command and displays the output from the first instance of a specified string.
	<b>more exclude</b>	Filters the <b>more</b> command output so that it excludes lines that contain a particular regular expression.
	<b>more include</b>	Filters the <b>more</b> command output so that it displays only lines that contain a particular regular expression.

Command	Description
<b>show begin</b>	Searches the output of certain <b>show</b> commands and displays the output from the first instance of a specified string.
<b>show exclude</b>	Filters the <b>show</b> command output so that it excludes lines that contain a particular regular expression.

# show interfaces

To display statistics for all system interfaces, use the `show interfaces` command in privileged EXEC mode. This command displays **show interfaces management**, **show interfaces fastethernet**, and **show interface gigabitethernet**.

**show interfaces** [**clear**]

**show interfaces** {**FastEthernet** | **GigabitEthernet** | **Management**} [*slot/port*]

Syntax Description		
<b>clear</b>		Clears the diagnostics.
<b>FastEthernet</b>		Displays the statistics for FastEthernet interfaces.
<b>GigabitEthernet</b>		Displays the statistics for GigabitEthernet interfaces.
<b>Management</b>		Displays the statistics for the Management interface.
	<b>Note</b>	Only platforms with external ports marked as Management support this keyword. The management interface for the remaining platforms is displayed in the <b>show interfaces</b> output based on the interface type, normally FastEthernet.
	<i>slot/port</i>	Refer to the appropriate hardware manual for slot and port information.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	5.0(1)	<b>show interfaces group</b> , <b>show interfaces sensing</b> , and <b>show interfaces command-control</b> were removed.

**Usage Guidelines** This command displays statistics for the command control and sensing interfaces. The clear option also clears statistics that can be reset.

**Examples** The following example shows the interface statistics:

```
sensor# show interfaces
Interface Statistics
  Total Packets Received = 0
  Total Bytes Received = 0
  Missed Packet Percentage = 0
  Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
```

```
Media Type = TX
Missed Packet Percentage = 0
Inline Mode = Unpaired
Pair Status = N/A
Link Status = Down
Link Speed = N/A
Link Duplex = N/A
Total Packets Received = 0
Total Bytes Received = 0
Total Multicast Packets Received = 0
Total Broadcast Packets Received = 0
Total Jumbo Packets Received = 0
Total Undersize Packets Received = 0
Total Receive Errors = 0
Total Receive FIFO Overruns = 0
Total Packets Transmitted = 0
Total Bytes Transmitted = 0
Total Multicast Packets Transmitted = 0
--MORE--
```

# show inventory

To display PEP information, use the **show inventory** command in privileged EXEC mode. This command displays the UDI information that consists of PID, VID and SN of the sensor.

## show inventory

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	5.0(1)	This command was introduced.

**Usage Guidelines** This is same as the **show inventory** Cisco IOS command required by Cisco PEP policy. The output of **show inventory** is different depending on the hardware.

**Examples** The following example shows a sample **show inventory** command output:

```
sensor# show inventory
NAME: "Chassis", DESCR: "Chasis-4240"
PID: 4240-515E , VID: V04, SN: 639156

NAME: "slot 0", DESCR: "4 port I/O card"
PID: 4240-4IOE , VID: V04, SN: 4356785466
sensor#
```

# show privilege

To display your current level of privilege, use the **show privilege** command in privileged EXEC mode.

**show privilege**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** EXEC

---

**SupportedUserRoles** Administrator, Operator, Viewer

---

Command History	Release	Modification
	4.0(1)	This command was introduced.

---



---

**Usage Guidelines** Use this command to display your current level of privilege. A privilege level can only be modified by the administrator. See the **username** command for more information.

---

**Examples** The following example shows the privilege of the user:

```
sensor# show privilege
Current privilege level is viewer
sensor#
```

---

Related Commands	Command	Description
	<b>username</b>	Creates users on the local sensor.

---

# show settings

To display the contents of the configuration contained in the current submode, use the **show settings** command in any **service** command mode.

## show settings [terse]

<b>Syntax Description</b>	<b>terse</b>	Displays a terse version of the output.
---------------------------	--------------	---

**Defaults** No default behavior or values.

**Command Modes** All **service** command modes.

**SupportedUserRoles** Administrator, Operator, Viewer (only presented with the top-level command tree)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	
4.0(2)		The <b>terse</b> keyword was added.

**Usage Guidelines** This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example shows the output for the **show settings** command in ARC configuration mode.



**Note** Network Access Controller is now known as Attack Response Controller (ARC). Although the service has a new name, the change is not reflected in the IPS 5.1 CLI. You will still see **network-access** and **nac** throughout the CLI.

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings
  general
  -----
  log-all-block-events-and-errors: true <defaulted>
  enable-nvram-write: false <defaulted>
  enable-acl-logging: false <defaulted>
  allow-sensor-block: true default: false
  block-enable: true <defaulted>
  block-max-entries: 250 <defaulted>
  max-interfaces: 250 <defaulted>
```

```

master-blocking-sensors (min: 0, max: 100, current: 0)
-----
never-block-hosts (min: 0, max: 250, current: 0)
-----
never-block-networks (min: 0, max: 250, current: 0)
-----
block-hosts (min: 0, max: 250, current: 0)
-----
block-networks (min: 0, max: 250, current: 0)
-----
-----
user-profiles (min: 0, max: 250, current: 0)
-----
cat6k-devices (min: 0, max: 250, current: 0)
-----
router-devices (min: 0, max: 250, current: 0)
-----
firewall-devices (min: 0, max: 250, current: 0)
-----
-----
sensor(config-net)#

```

The following example shows the **show settings** terse output for the signature definition submode.

```

sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings terse
  variables (min: 0, max: 256, current: 2)
  -----
  <protected entry>
  variable-name: WEBPORTS
  variable-name: user2
  -----
  application-policy
  -----
  http-policy
  -----
  http-enable: false <defaulted>
  max-outstanding-http-requests-per-connection: 10 <defaulted>
  aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,
24326-24326 <defaulted>
  -----
  ftp-enable: true default: false
  -----
  fragment-reassembly
  -----
  ip-reassemble-mode: nt <defaulted>
  -----
  stream-reassembly
  -----
  tcp-3-way-handshake-required: true <defaulted>
  tcp-reassembly-mode: strict <defaulted>
--MORE--

```

The following example shows the **show settings** filtered output. The command indicates the output should only include lines containing HTTP.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings | include HTTP
Searching:
sig-string-info: Bagle.Q HTTP propagation (jpeg) <defaulted>
sig-string-info: Bagle.Q HTTP propagation (php) <defaulted>
sig-string-info: GET ftp://@@:@@/pub HTTP/1.0 <defaulted>
sig-name: IMail HTTP Get Buffer Overflow <defaulted>
sig-string-info: GET shellcode HTTP/1.0 <defaulted>
sig-string-info: ..%c0%af..*HTTP <defaulted>
sig-string-info: ..%c1%9c..*HTTP <defaulted>
sig-name: IOS HTTP Unauth Command Execution <defaulted>
sig-name: Null Byte In HTTP Request <defaulted>
sig-name: HTTP tunneling <defaulted>
sig-name: HTTP tunneling <defaulted>
sig-name: HTTP tunneling <defaulted>
sig-name: HTTP tunneling <defaulted>
sig-name: HTTP CONNECT Tunnel <defaulted>
sig-string-info: CONNECT.*HTTP/ <defaulted>
sig-name: HTTP 1.1 Chunked Encoding Transfer <defaulted>
sig-string-info: INDEX / HTTP <defaulted>
sig-name: Long HTTP Request <defaulted>
sig-string-info: GET \x3c400+ chars? HTTP/1.0 <defaulted>
sig-name: Long HTTP Request <defaulted>
sig-string-info: GET .....?\x3c400+ chars HTTP/1.0 <defaulted>
sig-string-info: /mod_ssl:error:HTTP-request <defaulted>
sig-name: Dot Dot Slash in HTTP Arguments <defaulted>
sig-name: HTTPBench Information Disclosure <defaulted>

--MORE--
```

# show ssh authorized-keys

To display the public RSA keys for the current user, use the **show ssh authorized-keys** command in privileged EXEC mode.

```
show ssh authorized-keys [id]
```

<b>Syntax Description</b>	<i>id</i>	1 to 256-character string uniquely identifying the authorized key. Numbers, “_” and “-” are valid; spaces and “?” are not accepted.
---------------------------	-----------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>SupportedUserRoles</b>	Administrator, Operator, Viewer
---------------------------	---------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

<b>Usage Guidelines</b>	Running this command without the optional ID displays a list of the configured IDs in the system. Running the command with a specific ID displays the key associated with the ID. This command is IPS-specific.
-------------------------	---



<b>Note</b>	This command does not exist in Cisco IOS 12.0 or earlier.
-------------	---

<b>Examples</b>	The following example shows the list of SSH authorized keys:
-----------------	--

```
sensor# show ssh authorized-keys
system1
system2
system3
system4
```

The following example shows the SSH key for system1:

```
sensor# show ssh authorized-keys system1

1023 37
660222729556609833380897067163729433570828686860008172017802434921804214207813035920829509
101701358480525039993932112503147452768378620911189986653716089813147922086044739911341369
642870682319361928148521864094557416306138786468335115835910404940213136954353396163449793
49705016792583146548622146467421997057
sensor#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ssh authorized-key</b>	Adds a public key to the current user for a client allowed to use RSA authentication to log in to the local SSH server.

# show ssh server-key

To display the SSH server's host key and host key's fingerprint, use the **show ssh server-key** command in privileged EXEC mode.

**show ssh server-key**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier

**Examples** The following example shows the output from the **show ssh server-key** command:

```
sensor# show ssh server-key
1024 35 144719237233791547030730646600884648599022074867561982783071499320643934
48734496072779375489584407249259840037709354850629125941930828428605183115777190
69953460097510388011424663818234783053872210554889384417232132153750963283322778
52374794118697053304026570851868326130246348580479834689461788376232451955011
MD5: F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble: xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
sensor#
```

Related Commands	Command	Description
	ssh generate-key	Changes the server host key used by the SSH server on the sensor.

# show ssh host-keys

To display the known hosts table containing the public keys of remote SSH servers with which the sensor can connect, use the **show ssh host-keys** in privileged EXEC mode.

```
show ssh host-keys [ipaddress]
```

<b>Syntax Description</b>	<i>ipaddress</i>	32-bit address written as 4 octets separated by periods. X.X.X.X where X=0-255
---------------------------	------------------	--

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.1(1)	Bubble Babble and MD5 output to the command were added.

**Usage Guidelines** Running this command without the optional IP address ID displays a list of the IP addresses configured with public keys. Running the command with a specific IP address displays the key associated with the IP address. This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example shows the output of the **show ssh host-keys** command:

```
sensor# show ssh host-keys 10.1.2.3
1024 35 144719237233791547030730646600884648599022074867561982783071499320643934
48734496072779375489584407249259840037709354850629125941930828428605183115777190
69953460097510388011424663818234783053872210554889384417232132153750963283322778
52374794118697053304026570851868326130246348580479834689461788376232451955011
MD5: F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble: xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
sensor#
```

Related Commands	Command	Description
	ssh host-key	Adds an entry to the known hosts table.

# show statistics

To display the requested statistics, use the **show statistics** command in privileged EXEC mode.

```
show statistics {analysis-engine | authentication | denied-attackers | event-server | event-store
| host | logger | network-access | notification | sdee-server | transaction server |
transaction-source | virtual-sensor | web-server } [clear]
```

Syntax	Description
<b>clear</b>	Clears the statistics after they are retrieved. <b>Note</b> This option is not available for analysis engine, host, or network access statistics.
<b>analysis-engine</b>	Displays analysis engine statistics.
<b>authentication</b>	Displays authorization authentication statistics.
<b>denied-attackers</b>	Displays the list of denied IP addresses and the number of packets from each attacker.
<b>event-server</b>	Displays event server statistics.
<b>event-store</b>	Displays event store statistics.
<b>host</b>	Displays host (main) statistics.
<b>logger</b>	Displays logger statistics.
<b>network-access</b>	Displays ARC statistics. <b>Note</b> Network Access Controller is now known as Attack Response Controller (ARC). Although the service has a new name, the change is not reflected in the IPS 5.1 CLI. You will still see <b>network-access</b> and <b>nac</b> throughout the CLI.
<b>notification</b>	Displays notification statistics.
<b>sdee-server</b>	Displays SDEE server statistics.
<b>transaction server</b>	Displays transaction server statistics.
<b>transaction-source</b>	Displays transaction source statistics.
<b>web-server</b>	Displays web server statistics.
<b>virtual-sensor</b>	Displays virtual sensor statistics.
<i>name</i>	Logical name for the virtual sensor.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

**Command History**

Release	Modification
4.0(1)	This command was introduced.
5.0(1)	<b>analysis-engine</b> , <b>virtual-sensor</b> , and <b>denied-attackers</b> were added.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples**

The following example shows the authentication statistics:

```
sensor# show statistics authentication
General
  totalAuthenticationAttempts = 9
  failedAuthenticationAttempts = 0
sensor#
```

The following example shows the statistics for the Event Store:

```
sensor# show statistics event-store
Event store statistics
  General information about the event store
    The current number of open subscriptions = 1
    The number of events lost by subscriptions and queries = 0
    The number of queries issued = 1
    The number of times the event store circular buffer has wrapped = 0
  Number of events of each type currently stored
    Debug events = 0
    Status events = 129
    Log transaction events = 0
    Shun request events = 0
    Error events, warning = 8
    Error events, error = 13
    Error events, fatal = 0
    Alert events, informational = 0
    Alert events, low = 0
    Alert events, medium = 0
    Alert events, high = 0
sensor#
```

The following example shows the logger statistics:

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 27
The number of <evError> events written to the event store by severity
  Fatal Severity = 0
  Error Severity = 13
  Warning Severity = 35
  TOTAL = 48
The number of log messages written to the message log by severity
  Fatal Severity = 0
  Error Severity = 13
  Warning Severity = 8
  Timing Severity = 0
  Debug Severity = 0
  Unknown Severity = 26
  TOTAL = 47
sensor#
```

The following example shows the ARC statistics:

```
sensor# show statistics network-access
Current Configuration
  LogAllBlockEventsAndSensors = true
  EnableNvramWrite = false
  EnableAclLogging = false
  AllowSensorBlock = false
  BlockMaxEntries = 250
  MaxDeviceInterfaces = 250
State
  BlockEnable = true
sensor#
```

# show tech-support

To display the current system status, use the **show tech-support** command in privileged EXEC mode.

```
show tech-support [page] [password] [destination-url destination url]
```

Syntax Description		
<b>page</b>	(Optional) Causes the output to display one page of information at a time. Press <b>Enter</b> to display the next line of output or use the spacebar to display the next page of information. If <b>page</b> is not used, the output is displayed without page breaks.	
<b>password</b>	(Optional) Leaves passwords and other security information in the output. If <b>password</b> is not used, passwords and other security sensitive information in the output are replaced with the label <i>&lt;removed&gt;</i> by default.	
<b>destination-url</b>	(Optional) Tag indicating the information should be formatted as HTML and sent to the destination following this tag. If this option is selected, the output is not displayed on the screen.	
<i>destination url</i>	(Optional) The destination for the report file. If a URL is provided, the output is formatted into an HTML file and sent to the specified destination; otherwise the output is displayed on the screen.	

**Defaults** See Syntax Description table.

**Command Modes** EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.



**Usage Guidelines** **Note** Cisco IOS version 12.0 does not support the destination portion of this command.

The exact format of the destination URL varies according to the file. You can select a filename, but it must be terminated by .html.

You can specify the following destination types:

- **ftp:**—Destination URL for FTP network server. The syntax for this prefix is:  
ftp:[[/username@location]/relativeDirectory]/filename or  
ftp:[[/username@location]//absoluteDirectory]/filename
- **scp:**—Destination URL for the SCP network server. The syntax for this prefix is:  
scp:[[/username@]location]/relativeDirectory]/filename or  
scp:[[/username@]location]//absoluteDirectory]/filename

The report contains HTML-linked output from the following commands:

- **show interfaces**
- **show statistics network-access**
- **cidDump**

---

## Examples

The following example places the tech support output into the file

~csidsuser/reports/sensor1Report.html. The path is relative to csidsuser's home account:

```
sensor# show tech support destination-url  
ftp://csidsuser@10.2.1.2/reports/sensor1Report.html password:*****
```

The following example places the tech support output into the file

/absolute/reports/sensor1Report.html:

```
sensor# show tech support destination-url  
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html password:*****
```

# show tls fingerprint

To display the server's TLS certificate fingerprint, use the **show tls fingerprint** in privileged EXEC mode.

## show tls fingerprint

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example shows the output of the **show tls fingerprint** command:

```
sensor# show tls fingerprint
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

Related Commands	Command	Description
	tls generate-key	Regenerates the server's self-signed X.509 certificate.

# show tls trusted-hosts

To display the sensor's trusted hosts, use the **show tls trusted-hosts** command in privileged EXEC mode.

```
show tls trusted-hosts [id]
```

<b>Syntax Description</b>	<i>id</i>	1 to 32 character string uniquely identifying the authorized key. Numbers, “_” and “-” are valid; spaces and “?” are not accepted.
---------------------------	-----------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>SupportedUserRoles</b>	Administrator, Operator, Viewer
---------------------------	---------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines**

Running this command without the optional ID displays a list of the configured IDs in the system. Running the command with a specific ID displays the fingerprint of the certificate associated with the ID. This command is IPS-specific.



<b>Note</b>	This command does not exist in Cisco IOS 12.0 or earlier
-------------	--

**Examples**

The following example shows the output from the **show tls trusted-hosts** command:

```
sensor# show tls trusted-hosts 172.21.172.1
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>tls trusted-host</b>	Adds a trusted host to the system.

# show users

To display information about users currently logged in to the CLI, use the **show users** command in privileged EXEC mode:

```
show users [all]
```

## Syntax Description

<b>all</b>	(Optional) List all user accounts configured on the system regardless of current login status.
------------	--

## Defaults

No default behavior or values.

## Command Modes

EXEC

## Supported User Roles

Administrator, Operator, Viewer (can only view their own logins)

## Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(1)	Updated this command to display locked accounts. Limited viewer display for <b>show users all</b> .

## Usage Guidelines

For the CLI, this command displays an ID, username, and privilege. An '\*' next to the description indicates the current user. A username surrounded by parenthesis "(" indicates that the account is locked. An account is locked if the user fails to enter the correct password in *X* subsequent attempts. Resetting the locked user's password with the **password** command unlocks an account.

The maximum number of concurrent CLI users allowed is based on platform.



**Note** The output for this command is different from the Cisco IOS 12.0 command.

## Examples

The following example shows the output of the **show users** command:

```
sensor# show users
```

```

      CLI ID      User           Privilege
-----
      1234        notheruser     viewer
*      9802        curuser        operator
      5824        tester         administrator

```

The following example shows user tester2's account is locked:

```
sensor# show users all

      CLI ID      User           Privilege
      1234        notheruser     viewer
*     9802        curuser        operator
      5824        tester         administrator
                        (tester2)      viewer
                        foobar         operator
```

The following example shows the **show users all** output for a viewer:

```
sensor# show users all

      CLI ID      User           Privilege
*     9802        tester         viewer
      5824        tester         viewer
```

---

**Related Commands**

Command	Description
<b>clear line</b>	Terminates another CLI session.

---

# show version

To display the version information for all installed OS packages, signature packages, and IPS processes running on the system, use the **show version** command in privileged EXEC mode.

## show version

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** The output for the **show version** command is IPS-specific and differs from the output for the Cisco IOS command.

The license information follows the serial number and can be one of the following:

No license present

Expired license: <expiration-date>

Valid license, expires: <expiration-date>

Valid demo license, expires: <expiration-date>

where <expiration-date> is the form *dd-mon-yyyy*, for example, 04-dec-2004.



### Note

The \* before the upgrade history package name indicates the remaining version after a downgrade is performed. If no package is marked by \*, no downgrade is available.

**Examples** The following example shows the output for the **show version** command:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(0.1)S91(0.1)

OS Version 2.4.26-IDS-smp-bigphys
Platform: IDS-4235
No license present
```

```
Sensor up-time is 6 days.
Using 701513728 out of 922509312 bytes of available memory (76% usage)
Using 527.6M out of 15.9G bytes of available disk space (3% usage)
Using 192.0k out of 31.0M bytes of available disk space (1% usage)

MainApp          2004_Aug_16_03.00  (Release)  2004-08-16T03:19:41-0500  Running
AnalysisEngine   2004_Aug_16_03.00  (Release)  2004-08-16T03:19:41-0500  Running
CLI              2004_Aug_16_03.00  (Release)  2004-08-16T03:19:41-0500
```

Upgrade History:

No upgrades installed

Recovery Partition Version 5.0.1.S91.0.1

sensor#

# ssh authorized-key

To add a public key to the current user for a client allowed to use RSA authentication to log in to the local SSH server, use the **ssh authorized-key** command in global configuration mode. Use the **no** form of this command to remove an authorized key from the system.

```
ssh authorized-key id key-modulus-length public-exponent public-modulus
```

```
no ssh authorized-key id
```

## Syntax Description

<i>id</i>	1 to 256 character string uniquely identifying the authorized key. Numbers, “_” and “-” are valid; spaces and “?” are not accepted.
<i>key-modulus-length</i>	ASCII decimal integer in the range [511, 2048].
<i>public-exponent</i>	ASCII decimal integer in the range [3, 2 <sup>32</sup> ].
<i>public-modulus</i>	ASCII decimal integer, x, such that $(2^{(key-modulus-length-1)}) < x < (2^{(key-modulus-length)})$ .

## Defaults

No default behavior or values.

## Command Modes

Global configuration

## Supported User Roles

Administrator, Operator, Viewer

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

This command adds an entry to the known hosts table for the current user. To modify a key the entry must be removed and recreated.

This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

## Examples

The following example shows how to add an entry to the known hosts table:

```
sensor(config)# ssh authorized-key system1 1023 37
660222729556609833380897067163729433570828686860008172017802434921804214207813035920829509
101701358480525039993932112503147452768378620911189986653716089813147922086044739911341369
642870682319361928148521864094557416306138786468335115835910404940213136954353396163449793
49705016792583146548622146467421997057
sensor(config)#
```

■ ssh authorized-key

**Related Commands**

<b>Command</b>	<b>Description</b>
ssh authorized-keys	Displays the public RSA keys for the current user.

# ssh generate-key

To change the server host key used by the SSH server on the sensor, use the **ssh generate-key** command in privileged EXEC mode.

**ssh generate-key**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** The displayed key fingerprint matches that displayed in the remote SSH client in future connections with this sensor if the remote client is using SSH protocol version 1.5.

This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example shows how to generate a new ssh server host key:

```
sensor# ssh generate-key
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble: xebiz-vykyk-fekuh-rukuk-cabaz-paret-gosym-serum-korus-fypop-huxyx
sensor#
```

Related Commands	Command	Description
	show ssh server-key	Displays the SSH server's host key and host key's fingerprint.

## ssh host-key

To add an entry to the known hosts table, use the **ssh host-key** command in global configuration mode. If the modulus, exponent, and length are not provided, the system displays the MD5 fingerprint and bubble babble for the requested IP address and allows you to add the key to the table. Use the **no** form of this command to remove an entry from the known hosts table.

```
ssh host-key ipaddress [key-modulus-length public-exponent public-modulus]
```

```
no ssh host-key ipaddress
```

### Syntax Description

<i>ipaddress</i>	32-bit address written as 4 octets separated by periods. X.X.X.X where X=0-255.
<i>key-modulus-length</i>	ASCII decimal integer in the range [511, 2048].
<i>public-exponent</i>	ASCII decimal integer in the range [3, 2 <sup>32</sup> ].
<i>public-modulus</i>	ASCII decimal integer, x, such that $(2^{(key-modulus-length-1)}) < x < (2^{(key-modulus-length)})$ .

### Defaults

No default behavior or values.

### Command Modes

Global configuration

### Supported User Roles

Administrator, Operator

### Command History

Release	Modification
4.0(1)	This command was introduced.

### Usage Guidelines

The **ssh host-key** command adds an entry to the known hosts table. To modify a key for an IP address, the entry must be removed and recreated.

If the modulus, exponent, and length are not provided, the SSH server at the specified IP address is contacted to obtain the required key over the network. The specified host must be accessible at the moment the command is issued.

This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples**

The following example shows how to add an entry to the known hosts table for 10.1.2.3:

```
sensor(config)# ssh host-key 10.1.2.3
1024 35
139306213541835240385332922253968814685684523520064131997839905113640120217816869696708721
704631322844292073851730565044879082670677554157937058485203995572114631296604552161309712
601068614812749969593513740598331393154884988302302182922353335152653860589163651944997842
874583627883277460138506084043415861927
sensor(config)#
```

The following example shows how to add an entry to the known hosts table for 10.1.2.3:

```
sensor(config)# ssh host-key 10.1.2.3
MD5 fingerprint is 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble is xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
Would you like to add this to the known hosts table for this host? [yes]
sensor(config)#
```

**Related Commands**

Command	Description
<code>show ssh host-key</code>	Displays the known hosts table containing the public keys of remote SSH servers with which the sensor can connect.

# terminal

To modify terminal properties for a login session, use the **terminal** command in privileged EXEC mode.

**terminal** [**length** *screen-length*]

## Syntax Description

<i>screen-length</i>	Sets the number of lines on the screen. This value is used to determine when to pause during multiple-screen output. A value of zero results in no pause when the output exceeds the screen length. The default is 24 lines. This value is not saved between login sessions.
----------------------	--

## Defaults

See Syntax Description table.

## Command Modes

EXEC

## Supported User Roles

Administrator, Operator, Viewer

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The **terminal length** command sets the number of lines that are displayed before the `--more--` prompt is displayed.

## Examples

The following example sets the CLI to not pause between screens for multiple-screen displays:

```
sensor# terminal length 0
sensor#
```

The following example sets the CLI to display 10 lines per screen for multiple-screen displays:

```
sensor# terminal length 10
sensor#
```

# tls generate-key

To regenerate the server's self-signed X.509 certificate, use the **tls generate-key** in privileged EXEC mode. An error is returned if the host is not using a self-signed certificate.

## tls generate-key

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

**SupportedUserRoles** Administrator

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** This command is IPS-specific.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following example shows how to generate the server's self-signed certificate:

```
sensor(config)# tls generate-key
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor(config)#
```

Related Commands	Command	Description
	<b>show tls fingerprint</b>	Displays the server's TLS certificate fingerprint.

# tls trusted-host

To add a trusted host to the system, use the **tls trusted-host** command in global configuration mode. Use the **no** form of the command to remove a trusted host certificate.

**tls trusted-host ip-address** *ip-address* [**port** *port*]

**no tls trusted-host ip-address** *ip-address* [**port** *port*]

**no tls trusted-host id** *id*

Syntax Description		
	<i>ip-address</i>	IP address of host to add or remove.
	<i>port</i>	(Optional) Port number of host to contact. The default is port 443.

**Defaults** See Syntax Description table.

**Command Modes** Global configuration

**SupportedUserRoles** Administrator, Operator

Command History	Release	Modification
	4.0(1)	This command was introduced.
	4.0(2)	Added optional port. Added <b>no</b> command to support removal based on ID.

**Usage Guidelines** This command retrieves the current fingerprint for the requested host/port and displays the result. You can choose to accept or reject the fingerprint based on information retrieved directly from the host being requested to add.

Each certificate is stored with an identifier field. For IP address and default port, the identifier field is *ipaddress*, for IP address and specified port, the identifier field is *ipaddress:port*.



**Note** This command does not exist in Cisco IOS 12.0 or earlier.

**Examples** The following command adds an entry to the trusted host table for IP address 172.21.172.1, port 443:

```
sensor(config)# tls trusted-host ip-address 172.21.172.1
Certificate MD5 fingerprint is D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
Certificate SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this host? [yes]
Certificate ID: 172.21.172.1 successfully added to the TLS trusted host table.
sensor(config)#
```



**Note** The Certificate ID stored for the requested certificate is displayed when the command is successfully completed.

The following command removes the trusted host entry for IP address 172.21.172.1, port 443:

```
sensor(config)# no tls trusted-host ip-address 172.21.172.1
sensor(config)#
```

Or you can use the following command to remove the trusted host entry for IP address 172.21.172.1, port 443:

```
sensor(config)# no tls trusted-host id 172.21.172.1
sensor(config)#
```

The following command adds an entry to the trusted host table for IP address 10.1.1.1, port 8000:

```
sensor(config)# tls trusted-host ip-address 10.1.1.1 port 8000
Certificate MD5 fingerprint is D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
Certificate SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this host? [yes]
Certificate ID: 10.1.1.1:8000 successfully added to the TLS trusted host table.
sensor(config)#
```



**Note** The Certificate ID stored for the requested certificate is displayed when the command is successfully completed.

The following command removes the trusted host entry for IP address 10.1.1.1, port 8000:

```
sensor(config)# no tls trusted-host ip-address 10.1.1.1 port 8000
sensor(config)#
```

Or you can use the following command to remove the trusted host entry for IP address 10.1.1.1, port 8000:

```
sensor(config)# no tls trusted-host id 10.1.1.1:8000
sensor(config)#
```

#### Related Commands

Command	Description
<code>show tls trusted-hosts</code>	Displays the sensor's trusted hosts.

# trace

To display the route an IP packet takes to a destination, use the **trace** command in privileged EXEC mode.

```
trace address [count]
```

Syntax Description	<i>address</i>	Address of system to trace route to.
	<i>count</i>	Number of hops to take. Default is 4. Valid values are 1–256.

**Defaults** See Syntax Description table.

**Command Modes** EXEC

**Command Types** Administrator, Operator, Viewer

Command History	Release	Modification
	4.0(1)	This command was introduced.

**Usage Guidelines** There is no command interrupt for the **trace** command. The command must run to completion.

**Examples** The following example shows the output for the **trace** command:

```
sensor# trace 10.1.1.1
traceroute to 172.21.172.24 (172.21.172.24), 30 hops max, 40 byte packets
 1 171.69.162.2 (171.69.162.2) 1.25 ms 1.37 ms 1.58 ms
 2 172.21.172.24 (172.21.172.24) 0.77 ms 0.66 ms
 0.68 ms
sensor#
```

# upgrade

To apply a service pack, signature update, or image upgrade, use the **upgrade** command in global configuration mode.

**upgrade** *source-url*

<b>Syntax Description</b>	<i>source-url</i>	The location of the upgrade to retrieve.
---------------------------	-------------------	--

**Defaults** No default behavior or values.

**Command Modes** Global configuration

**SupportedUserRoles** Administrator

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	4.0(1)	This command was introduced.

**Usage Guidelines** From the command line, you can type all necessary source and destination URL information and the username. If you type only the command (**upgrade**) followed by a prefix (ftp: or scp:), you are prompted for any missing information, including a password where applicable.

The directory specification should be an absolute path to the desired file. For recurring upgrades, do not specify a filename. You can configure the sensor for recurring upgrades that occur on specific days at specific times, or you can configure a recurring upgrade to occur after a specific number of hours have elapsed from the initial upgrade.

Use the following guidelines when designating the source:

- **ftp:**—Source URL for FTP network server. The syntax for this prefix is:  
ftp:[[/username@]location]/relativeDirectory/filename or  
ftp:[[/username@]location]//absoluteDirectory/filename
- **http:**—Source URL for web server. The syntax for this prefix is:  
http:[[/username@]location]/directory/filename
- **https:**—Source URL for web server. The syntax for this prefix is:  
https:[[/username@]location]/directory/filename



**Note** You need to set up a TLS trusted host before using the HTTPS protocol. Refer to the command for more information.

- **scp:**—Source URL for the SCP network server. The syntax for this prefix is:  
scp:[[/username@]location]/relativeDirectory/filename or  
scp:[[/username@]location]//absoluteDirectory/filename

**Note**

---

This command does not exist in Cisco IOS 12.0 or earlier.

---

**Examples**

The following example prompts the sensor to immediately check for the specified upgrade. The directory and path are relative to the tester's user account.

```
sensor(config)# upgrade scp://tester@10.1.1.1/upgrade/sp.rpm  
Enter password: *****  
Re-enter password: ****
```

# username

To create users on the local sensor, use the **username** command in global configuration mode. You must be Administrator to create users. Use the **no** form of the command to remove a user from the sensor. This removes the users from both CLI and web access.

```
username name [password password] [privilege privilege]
```

```
no username name
```

## Syntax Description

<b><i>name</i></b>	Specifies the username. A valid username is 1 to 64 characters in length. The username must begin with an alphanumeric otherwise all characters are accepted.
<b><i>password</i></b>	Specifies the password for the user. A valid password is 6 to 32 characters in length. All characters except space and '?' are allowed.
<b><i>privilege</i></b>	Sets the privilege level for the user. Allowed levels are Service, Administrator, Operator, Viewer. The default is Viewer.

## Defaults

See Syntax Description table.

## Command Modes

Global configuration

## SupportedUserRoles

Administrator

## Command History

Release	Modification
4.0(1)	This command was introduced.

## Usage Guidelines

The **username** command provides username and/or password authentication for login purposes only. The user executing the command cannot remove himself or herself.

If the password is not provided on the command line, the user is prompted. Use the **password** command to change the password for the current user or for a user already existing in the system. Use the **privilege** command to change the privilege for a user already existing in the system.

## Examples

The following example adds a user called tester with a privilege of viewer and the password testerpassword.

```
sensor(config)# username tester password testerpassword
```

The following example shows the password being entered as protected:

```
sensor(config)# username tester  
Enter Login Password: *****  
Re-enter Login Password: *****
```

The following command changes the privilege of user “tester” to operator:

```
sensor(config)# username tester privilege operator
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>password</b>	Updates your password on the local sensor.
<b>privilege</b>	Modifies the privilege level for an existing user.



# APPENDIX **A**

## Deprecated Commands and Command Platform Dependencies

This appendix lists commands that have been deprecated and commands that do not apply to certain platforms. It contains the following sections:

- [Deprecated Commands, page A-1](#)
- [Command/Platform Dependencies, page A-2](#)

### Deprecated Commands

[Table A-1](#) lists the commands that were deprecated for IPS 5.1.

**Table A-1** *Deprecated Commands*

Command	Replaced By
hostname	service host – network-settings – host-name
ip address	service host – network-settings – host-ip
ip default-gateway	service host – network-settings – host-ip
interface command-control	service host
telnet-sensor	service host – network-settings – telnet-option
interface group	service analysis-engine – virtual-sensor
interface sensing	service interface-config – physical-interfaces
interface sensing shutdown	service interface-config – physical-interfaces – state
sensing-interface	service analysis-engine – virtual-sensor – sensing-interface
service virtual-sensor-configuration	service signature-definition
service-alarm-channel-configuration	service event-action-rules
reset-signatures	No replacement. You can reset an individual signature or all signatures by using the <b>default</b> keyword.
show interfaces command-control	show statistics host

**Table A-1** *Deprecated Commands (continued)*

Command	Replaced By
<b>show interface group</b>	<b>show statistics virtual-sensor</b> . This command only displays the virtual sensor statistics. You can view the configuration by using <b>more current-config</b> or <b>show configuration</b> .
<b>show interface sensing</b>	<b>show interface fastethernet</b> and <b>show interface gigabitethernet</b>
<b>tune-micro-engines</b>	No replacement. The <b>service signature-definition</b> command directly enters signature editing.
<b>tune-alarm-channel</b>	No replacement. The <b>service event-action-rules</b> command directly enters rule editing.

## Command/Platform Dependencies

[Table A-2](#) lists the commands that are not valid on the specified platforms.

**Table A-2** *Command/Platform Dependencies*

Command	Platforms
<b>display-serial</b>	IDSM-2, NM-CIDS, IDS-4215, AIP-SSM-10, AIP-SSM-20, IPS-4240, IPS-4255
<b>clock set</b>	IDSM-2, NM-CIDS, AIP-SSM-10, AIP-SSM-20
<b>show inventory</b>	IDSM-2, NM-CIDS, IDS-4210, IDS-4235, IDS-4250, AIP-SSM-10, AIP-SSM-20
<b>show interfaces management</b>	IDSM-2, NM-CIDS, IDS-4210,IDS-4215, IDS-4235, IDS-4250, AIP-SSM-10, AIP-SSM-20



# APPENDIX **B**

## CLI Error Messages

This appendix contains the CLI error messages. [Table B-1](#) describes CLI error messages.

**Table B-1** CLI Error Messages

Error Message	Reason	Command
Invalid command received.	The .conf file and code are out of synchronization, which should never occur in the field.	All commands
Invalid port number was entered.	An out-of-range port number was entered in URI.	<b>copy, upgrade show tech-support</b>
Invalid scheme was entered.	Internal tables are out of synchronization, which should never occur in the field.	<b>copy, upgrade show tech-support</b>
Unknown scheme was entered.	An invalid scheme was entered in URI.	<b>copy, upgrade show tech-support</b>
The filename <file> is not a valid upgrade file type.	Attempt to install the wrong file for your platform and version.	<b>upgrade</b>
idsPackageMgr: digital signature of the update was not valid	The signature update or service pack is corrupt. Contact TAC.	<b>upgrade</b>
Invalid instance name. "rules0" is currently the only instance name allowed.	An invalid logical instance name was entered for service event action rules.	<b>service event-action-rules</b>
Invalid instance name. "sig0" is currently the only instance name allowed.	An invalid logical instance name was entered for service signature definition.	<b>service signature-definition</b>
User does not exist.	The Administrator is attempting to change the password for a username that does not exist in the system.	<b>password</b>
Incorrect password for user account.	The user entered an invalid password while attempting to change the password.	<b>password</b>
Empty user list.	The curUserAccountList.xml file does not contain any entries, which should never occur in the field.	<b>username</b>

**Table B-1** CLI Error Messages (continued)

<b>Error Message</b>	<b>Reason</b>	<b>Command</b>
User already exists.	An attempt to create a user that already exists in the system was made.	<b>username</b>
Cannot communicate with system processes. Please contact your system administrator.	One or more required applications is not responding to control transactions.	All commands
Source and Destination are the same.	—	<b>copy</b>
Backup config was missing.	The user attempted to copy or erase the backup config file but no backup config file has been generated.	<b>copy</b> <b>erase</b>
Could not load CLI configuration files, can not complete request.	The .conf files could not be located, which should never occur in the field.	<b>copy</b>
Error writing to <URL>.	The URL specified in the destination could not be written.	<b>copy</b>
Error reading from <URL>.	The URL specified in the source could not be read.	<b>copy</b>
Packet-file does not exist.	The user attempted to copy or erase the packet-file but no packet-file has been captured.	<b>copy</b> <b>erase</b>
No downgrade available.	The user attempted to downgrade a system that has not been upgraded.	<b>downgrade</b>
No packet-file available.	The user attempted to display the file-info or the packet-file but no packet-file exists.	<b>packet</b>
Log file exists but an error occurred during read.	The user was displaying or copying an iplog file that was overwritten. The partial file contents should still be viewable.	<b>packet</b>
Another user is currently capturing into the packet-file. Please try again later.	—	<b>packet capture</b>
Another CLI client is currently displaying packets from the interface.	The user must wait for the other CLI session to terminate display before this will be available. Multiple users may display the command control interface simultaneously.	<b>packet display</b>
Log does not exist.	The user attempted to copy or display an iplog that does not exist.	<b>copy iplog</b> <b>packet display iplog</b>
The requested IPLOG is not complete. Please try again after the IPLOG status is 'completed.'	The user attempted to copy or display an iplog that is not complete.	<b>copy iplog</b>

Table B-1 CLI Error Messages (continued)

Error Message	Reason	Command
Could not create pipe /usr/cids/idsRoot/tmp/ pipe_cliPacket.<pid>.tmp	Could not open pipe for sending iplog file. This indicates a space or resource limitation, which should not occur in the field.	<b>copy iplog</b>
The log file was overwritten while the copy was in progress. The copied log file may be viewable but is incomplete.	The iplog was overwritten while it was being copied off the sensor.	<b>copy iplog</b>
Could not read license file.	The license file was copied but cannot be opened.	<b>copy license-key</b>
Could not write the temporary license file location used to copy the file off the box.	Could not open the temporary storage location /usr/cids/idsRoot/tmp/ips.lic. This indicates a space issue, which should not occur in the field.	<b>copy license-key</b>
Can not create an IP log. \"vs0\" is currently the only virtual sensor allowed.	The user attempted to create an iplog on an invalid virtual sensor.	<b>iplog</b>
Can not stop an IP log. \"vs0\" is currently the only virtual sensor allowed.	The user attempted to stop an iplog on an invalid virtual sensor.	<b>iplog</b>
You do not have permission to terminate the requested CLI session.	An operator or viewer user attempted to terminate a CLI session belonging to another user.	<b>clear line</b>
Invalid CLI ID specified, use the 'show users all' command to view the valid CLI session IDs.	The user attempted to cancel a CLI session that does not exist.	<b>clear line</b>
The maximum allowed CLI sessions are currently open, please try again later.	Operator or viewer user attempted to log in when the maximum number of CLI sessions were already open.	initial login
The maximum allowed CLI sessions are currently open, would you like to terminate one of the open sessions?	Administrator user attempted to log in when the maximum number of CLI sessions were already open.	initial login
Can not communicate with system processes. Please contact your system administrator.	The CLI cannot contact the applications on the sensor to retrieve start-up information. This is a fatal error that should never happen. The user has to log in to the service account and manually reboot the sensor.	initial login





## GLOSSARY

---

### Numerals

**3DES** Triple Data Encryption Standard. A stronger version of DES, which is the default encryption method for SSH version 1.5. Used when establishing an SSH session with the sensor. It can be used when the sensor is managing a device.

---

### A

- aaa** authentication, authorization, and accounting. The primary and recommended method for access control in Cisco devices.
- AAA** authentication, authorization, and accounting. Pronounced “triple a.”
- ACE** Access Control Entry. An entry in the ACL that describes what action should be taken for a specified address or protocol. The sensor adds/removes ACE to block hosts.
- ACK** acknowledgement. Notification sent from one network device to another to acknowledge that some event occurred (for example, the receipt of a message).
- ACL** Access Control List. A list of ACEs that control the flow of data through a router. There are two ACLs per router interface for inbound data and outbound data. Only one ACL per direction can be active at a time. ACLs are identified by number or by name. ACLs can be standard, enhanced, or extended. You can configure the sensor to manage ACLs.
- action** The sensor’s response to an event. An action only happens if the event is not filtered. Examples include TCP reset, block host, block connection, IP logging, and capturing the alert trigger packet.
- active ACL** The ACL created and maintained by ARC and applied to the router block interfaces.
- AIC engine** Application Inspection and Control engine. Provides deep analysis of web traffic. It provides granular control over HTTP sessions to prevent abuse of the HTTP protocol. It allows administrative control over applications that try to tunnel over specified ports, such as instant messaging, and tunneling applications, such as gotomypc. It can also inspect FTP traffic and control the commands being issued.
- AIP-SSM** Advanced Inspection and Prevention Security Services Module. The IPS plug-in module in the Cisco ASA 5500 series adaptive security appliance. See ASA.
- Alarm Channel** The IPS software module that processes all signature events generated by the inspectors. Its primary function is to generate alerts for each event it receives.
- alert** Specifically, an IPS event type; it is written to the Event Store as an evidsAlert. In general, an alert is an IPS message that indicates a network exploit in progress or a potential security problem occurrence. Also known as an alarm.

<b>Analysis Engine</b>	The IPS software module that handles sensor configuration. It maps the interfaces and also the signature and alarm channel policy to the configured interfaces. It performs packet analysis and alert detection.
<b>API</b>	Application Programming Interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. Computer application programs run a set of standard software interrupts, calls, and data formats to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create links that an application needs to communicate with the operating system or with the network.
<b>application</b>	Any program (process) designed to run in the Cisco IPS environment.
<b>application instance</b>	A specific application running on a specific piece of hardware in the IPS environment. An application instance is addressable by its name and the IP address of its host computer.
<b>ARC</b>	Attack Response Controller. Formerly known as Network Access Controller (NAC). A component of the IPS. A software module that provides block and unblock functionality where applicable.
<b>architecture</b>	The overall structure of a computer or communication system. The architecture influences the capabilities and limitations of the system.
<b>ARP</b>	Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.
<b>ASA</b>	Adaptive Security Appliance. The ASA combines firewall, VPN concentrator, and intrusion prevention software functionality into one software image. You can configure ASA in single mode or multi-mode.
<b>ASDM</b>	Adaptive Security Device Manager. A web-based application that lets you configure and manage your ASA.
<b>atomic attack</b>	Represents exploits contained within a single packet. For example, the “ping of death” attack is a single, abnormally large ICMP packet.
<b>Atomic engine</b>	There are two Atomic engines: Atomic IP inspects IP protocol packets and associated Layer-4 transport protocols, and Atomic ARP inspects Layer-2 ARP protocol.
<b>attack</b>	An assault on system security that derives from an intelligent threat, that is, an intelligent act that is a deliberate attempt (especially in the sense of method or technique) to evade security services and violate the security policy of a system.
<b>authentication</b>	Process of verifying that a user has permission to use the system, usually by means of a password key or certificate.
<b>AuthenticationApp</b>	A component of the IPS. It verifies that users have the correct permissions to perform CLI, IDM, or RDEP actions.

---

## B

<b>backplane</b>	The physical connection between an interface processor or card and the data buses and the power distribution buses inside a chassis.
------------------	--

<b>base version</b>	A software release that must be installed before a follow-up release such as a service pack or signature update can be installed. Major and minor version upgrades are base version releases.
<b>benign trigger</b>	A situation in which a signature is fired correctly, but the source of the traffic is nonmalicious.
<b>BIOS</b>	Basic Input/Output System. The program that starts the sensor and communicates between the devices in the sensor and the system.
<b>block</b>	The ability of the sensor to direct a network device to deny entry to all packets from a specified network host or network.
<b>block interface</b>	The interface on the network device that the sensor manages.
<b>BO2K</b>	BackOrifice 2000. A windows back door Trojan that runs over TCP and UDP.
<b>Bpdu</b>	Bridge Protocol Data Unit. Spanning-Tree Protocol hello packet that is sent out at configurable intervals to exchange information among bridges in the network.
<b>bypass mode</b>	Mode that lets packets continue to flow through the sensor even if the sensor fails. Bypass mode is only applicable to inline-paired interfaces.

---

## C

<b>CA</b>	certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. Sensors use self-signed certificates.
<b>CA certificate</b>	Certificate for one CA issued by another CA.
<b>certificate</b>	Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.
<b>cidDump</b>	A script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.
<b>CIDEE</b>	Cisco Intrusion Detection Event Exchange. Specifies the extensions to SDEE that are used by Cisco IPS systems. The CIDEE standard specifies all possible extensions that may be supported by Cisco IPS systems.
<b>CIDS header</b>	The header that is attached to each packet in the IPS system. It contains packet classification, packet length, checksum results, timestamp, and the receive interface.
<b>cipher key</b>	The secret binary data used to convert between clear text and cipher text. When the same cipher key is used for both encryption and decryption, it is called symmetric. When it is used for either encryption or decryption (but not both), it is called asymmetric.
<b>Cisco IOS</b>	Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS allows centralized, integrated, and automated installation and management of internetworks while supporting a wide variety of protocols, media, services, and platforms.
<b>CLI</b>	command-line interface. A shell provided with the sensor used for configuring and controlling the sensor applications.

<b>command and control interface</b>	The interface on the sensor that communicates with the IPS manager and other network devices. This interface has an assigned IP address.
<b>community</b>	In SNMP, a logical group of managed devices and NMSs in the same administrative domain.
<b>composite attack</b>	Spans multiple packets in a single session. Examples include most conversation attacks such as FTP, Telnet, and most Regex-based attacks.
<b>connection block</b>	ARC blocks traffic from a given source IP address to a given destination IP address and destination port.
<b>console</b>	A terminal or laptop computer used to monitor and control the sensor.
<b>console port</b>	An RJ45 or DB9 serial port on the sensor that is used to connect to a console device.
<b>control interface</b>	When ARC opens a Telnet or SSH session with a network device, it uses one of the device's routing interfaces as the remote IP address. This is the control interface.
<b>control transaction</b>	An IPS message containing a command addressed to a specific application instance. Example control transactions include <i>start</i> , <i>stop</i> , <i>getConfig</i> .
<b>cookie</b>	A piece of information sent by a web server to a web browser that the browser is expected to save and send back to the web server whenever the browser makes additional requests of the web server.

---

## D

<b>Database Processor</b>	See DBP.
<b>datagram</b>	Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.
<b>DBP</b>	Database Processor. Maintains the signature state and flow databases.
<b>DCE</b>	data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.
<b>DDoS</b>	Distributed Denial of Service. An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.
<b>Deny Filters Processor</b>	See DFP.
<b>DES</b>	Data Encryption Standard. A strong encryption method where the strength lies in a 56-bit key rather than an algorithm.
<b>destination address</b>	Address of a network device that is receiving data.

<b>DFP</b>	Deny Filters Processor. Handles the deny attacker functions. It maintains a list of denied source IP addresses.
<b>DIMM</b>	Dual In-line Memory Modules.
<b>DMZ</b>	demilitarized zone. A separate network located in the neutral zone between a private (inside) network and a public (outside) network.
<b>DNS</b>	Domain Name System. An Internet-wide hostname to IP address mapping. DNS enables you to convert human-readable names into the IP addresses needed for network packets.
<b>DoS</b>	Denial of Service. An attack whose goal is just to disrupt the operation of a specific system or network.
<b>DRAM</b>	dynamic random-access memory. RAM that stores information in capacitors that must be refreshed periodically. Delays can occur because DRAMs are inaccessible to the processor when refreshing their contents. However, DRAMs are less complex and have greater capacity than SRAMs.
<b>DTE</b>	Data Terminal Equipment. Refers to the role of a device on an RS-232C connection. A DTE writes data to the transmit line and reads data from the receive line.

---

**E**

<b>egress</b>	Traffic leaving the network.
<b>encryption</b>	Application of a specific algorithm to data to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information.
<b>engine</b>	A component of the sensor designed to support many signatures in a certain category. Each engine has parameters that can be used to create signatures or tune existing signatures.
<b>enterprise network</b>	Large and diverse network connecting most major points in a company or other organization. Differs from a WAN in that it is privately owned and maintained.
<b>escaped expression</b>	Used in regular expression. A character can be represented as its hexadecimal value, for example, \x61 equals 'a,' so \x61 is an escaped expression representing the character 'a.'
<b>ESD</b>	electrostatic discharge. Electrostatic discharge is the rapid movement of a charge from one object to another object, which produces several thousand volts of electrical charge that can cause severe damage to electronic components or entire circuit card assemblies.
<b>event</b>	An IPS message that contains an alert, a block request, a status message, or an error message.
<b>Event Server</b>	One of the components of the IPS.
<b>Event Store</b>	One of the components of the IPS. A fixed-size, indexed store used to store IPS events.
<b>evldsAlert</b>	The XML entity written to the Event Store that represents an alert.

---

**F**

<b>fail closed</b>	Blocks traffic on the device after a hardware failure.
--------------------	--

<b>fail open</b>	Lets traffic pass through the device after a hardware failure.
<b>false negative</b>	A signature is not fired when offending traffic is detected.
<b>false positive</b>	Normal traffic or a benign action causes a signature to fire.
<b>Fast Ethernet</b>	Any of a number of 100-Mbps Ethernet specifications. Fast Ethernet offers a speed increase 10 times that of the 10BaseT Ethernet specification while preserving such qualities as frame format, MAC mechanisms, and MTU. Such similarities allow the use of existing 10BaseT applications and network management tools on Fast Ethernet networks. Based on an extension to the IEEE 802.3 specification.
<b>firewall</b>	Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network.
<b>Flood engine</b>	Detects ICMP and UDP floods directed at hosts and networks.
<b>flooding</b>	Traffic passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.
<b>fragment</b>	Piece of a larger packet that has been broken down to smaller units.
<b>fragmentation</b>	Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.
<b>Fragment Reassembly Processor</b>	See FRP.
<b>FRP</b>	Fragment Reassembly Processor. Reassembles fragmented IP datagrams. It is also responsible for normalization of IP fragments when the sensor is in inline mode.
<b>FTP</b>	File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.
<b>FTP server</b>	File Transfer Protocol server. A server that uses the FTP protocol for transferring files between network nodes.
<b>full duplex</b>	Capability for simultaneous data transmission between a sending station and a receiving station.
<b>FWSM</b>	Firewall Security Module. A module that can be installed in a Catalyst 6500 series switch. It uses the <b>shun</b> command to block. You can configure the FWSM in either single mode or multi-mode.

---

## G

<b>Gigabit Ethernet</b>	Standard for a high-speed Ethernet, approved by the IEEE (Institute of Electrical and Electronics Engineers) 802.3z standards committee in 1996.
<b>GMT</b>	Greenwich Mean Time. Time zone at zero degrees longitude. Now called Coordinated Universal Time (UTC).

---

**H**

<b>H.225.0</b>	An ITU standard that governs H.225.0 session establishment and packetization. H.225.0 actually describes several different protocols: RAS, use of Q.931, and use of RTP.
<b>H.245</b>	An ITU standard that governs H.245 endpoint control.
<b>H.323</b>	Allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.
<b>half duplex</b>	Capability for data transmission in only one direction at a time between a sending station and a receiving station. BSC is an example of a half-duplex protocol.
<b>handshake</b>	Sequence of messages exchanged between two or more network devices to ensure transmission synchronization.
<b>hardware bypass</b>	Passes traffic at the network interface, does not pass it to the IPS system.
<b>host block</b>	ARC blocks all traffic from a given IP address.
<b>HTTP</b>	Hypertext Transfer Protocol. The stateless request/response media transfer protocol used in the IPS architecture for remote data exchange.
<b>HTTPS</b>	An extension to the standard HTTP protocol that provides confidentiality by encrypting the traffic from the website. By default this protocol uses TCP port 443.

---

**I**

<b>ICMP</b>	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.
<b>ICMP flood</b>	Denial of Service attack that sends a host more ICMP echo request (“ping”) packets than the protocol implementation can handle.
<b>IDAPI</b>	Intrusion Detection Application Programming Interface. Provides a simple interface between IPS architecture applications. IDAPI reads and writes event data and provides a mechanism for control transactions.
<b>IDCONF</b>	Intrusion Detection Configuration. A data format standard that defines operational messages that are used to configure intrusion detection and prevention systems.
<b>IDIOM</b>	Intrusion Detection Interchange and Operations Messages. A data format standard that defines the event messages that are reported by intrusion detection systems and the operational messages that are used to configure and control intrusion detection systems.
<b>IDM</b>	IPS Device Manager. A web-based application that lets you configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through Netscape or Internet Explorer web browsers.
<b>IDMEF</b>	Intrusion Detection Message Exchange Format. The IETF Intrusion Detection Working Group draft standard.

<b>IDS M-2</b>	Intrusion Detection System Module. A switching module that performs intrusion detection in the Catalyst 6500 series switch.
<b>IDS MC</b>	Management Center for IDS Sensors. A web-based IDS manager that can manage configurations for up to 300 sensors.
<b>inline mode</b>	All packets entering or leaving the network must pass through the sensor.
<b>interface group</b>	Refers to the logical grouping of sensing interfaces. Multiple sensing interfaces can be assigned to a logical interface group. Signature parameters are tuned on a per-logical interface group basis.
<b>intrusion detection system</b>	A security service that monitors and analyzes system events to find and provide real-time or near real-time warning of attempts to access system resources in an unauthorized manner.
<b>IP address</b>	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.
<b>IPS</b>	Intrusion Prevention System. A system that alerts the user to the presence of an intrusion on the network through network traffic analysis techniques.
<b>IPS data or message</b>	Describes the messages transferred over the command and control interface between IPS applications.
<b>iplog</b>	A log of the binary packets to and from a designated address. Iplogs are created when the log Event Action is selected for a signature. Iplogs are stored in a libpcap format, which can be read by Wireshark and TCPDUMP.
<b>IP spoofing</b>	IP spoofing attack occurs when an attacker outside your network pretends to be a trusted user either by using an IP address that is within the range of IP addresses for your network or by using an authorized external IP address that you trust and to which you want to provide access to specified resources on your network. Should an attacker get access to your IPSec security parameters, that attacker can masquerade as the remote user authorized to connect to the corporate network.
<b>IPv6</b>	IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

---

**L**

<b>L2P</b>	Layer 2 Processor. Processes layer 2-related events. It also identifies malformed packets and removes them from the processing path.
<b>LAN</b>	Local Area Network. Refers to the Layer 2 network domain local to a given host. Packets exchanged between two hosts on the same LAN do not require Layer 3 routing.
<b>Layer 2 Processor</b>	See L2P.
<b>Logger</b>	A component of the IPS.

<b>logging</b>	Gathers actions that have occurred in a log file. Logging of security information is performed on two levels: logging of events (such as IPS commands, errors, and alerts), and logging of individual IP session information.
<b>LOKI</b>	Remote access, back door Trojan, ICMP tunneling software. When the computer is infected, the malicious code creates an ICMP tunnel that can be used to send small payload ICMP replies
<hr/>	
<b>M</b>	
<b>MainApp</b>	The main application in the IPS. The first application to start on the sensor after the operating system has booted.
<b>maintenance partition image</b>	A full IPS image used to reimage the maintenance partition of the IDSM-2.
<b>major update</b>	A base version that contains major new functionality or a major architectural change in the product.
<b>manufacturing image</b>	Full IPS system image used by manufacturing to image sensors.
<b>master blocking sensor</b>	A remote sensor that controls one or more devices. Blocking forwarding sensors send blocking requests to the master blocking sensor and the master blocking sensor executes the blocking requests.
<b>MD5</b>	Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. Also used for message authentication in SNMP v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.
<b>MEG</b>	Mega Event Generator. Signature based on the Meta engine. The Meta engine takes alerts as input rather than packets.
<b>Meta engine</b>	Defines events that occur in a related manner within a sliding time interval. This engine processes events rather than packets.
<b>MIB</b>	Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
<b>MIME</b>	Multipurpose Internet Mail Extension. Standard for transmitting nontext data (or data that cannot be represented in plain ASCII code) in Internet mail, such as binary, foreign language text (such as Russian or Chinese), audio, or video data. MIME is defined in RFC 2045.
<b>minor update</b>	A minor version that contains minor enhancements to the product line. Minor updates are incremental to the major version, and are also base versions for service packs.
<b>module</b>	A removable card in a switch, router, or security appliance chassis. AIP SSM, IDSM-2, and NM-CIDS are IPS modules.

<b>monitoring interface</b>	See sensing interface.
<b>MSFC, MSFC2</b>	Multilayer Switch Feature Card. An optional card on a Catalyst 6000 supervisor engine that performs L3 routing for the switch.
<b>MSRPC</b>	Microsoft Remote Procedure Call.

---

## N

<b>NAC</b>	Network Access Controller. See ARC.
<b>NAT</b>	Native Address Translation. A network device can present an IP address to the outside networks that is different from the actual IP address of a host.
<b>NBD</b>	Next Business Day. The arrival of replacement hardware according to Cisco service contracts.
<b>network device</b>	A device that controls IP traffic on a network and can block an attacking host. An example of a network device is a Cisco router or PIX Firewall.
<b>never block address</b>	Hosts and networks you have identified that should never be blocked.
<b>never shun address</b>	See never block address.
<b>NIC</b>	Network Interface Card. Board that provides network communication capabilities to and from a computer system.
<b>NM-CIDS</b>	A network module that integrates IPS functionality into the branch office router.
<b>NMS</b>	network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
<b>node</b>	A physical communicating element on the command and control network. For example, an appliance, an IDSM-2, or a router.
<b>Normalizer engine</b>	Configures how the IP and TCP normalizer functions and provides configuration for signature events related to the IP and TCP normalizer.
<b>NTP</b>	Network Timing Protocol. Protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
<b>NTP server</b>	Network Timing Protocol server. A server that uses NTP. NTP is a protocol built on top of TCP that ensures accurate local time-keeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
<b>NVRAM</b>	Non-Volatile Read/Write Memory. RAM that retains its contents when a unit is powered off.

---

**O**

**OIR** online insertion and removal. Feature that permits you to add, replace, or remove cards without interrupting the system power, entering console commands, or causing other software or interfaces to shutdown.

---

**P**

**packet** Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

**PASC Port Spoof** An attempt to open connections through a firewall to a protected FTP server to a non-FTP port. This happens when the firewall incorrectly interprets an FTP 227 (Entering Passive Mode) command by opening an unauthorized connection.

**passive fingerprinting** Act of determining the OS or services available on a system from passive observation of network interactions.

**PAT** Port Address Translation. A more restricted translation scheme than NAT in which a single IP address and different ports are used to represent the hosts of a network.

**PCI** Peripheral Component Interface. The most common peripheral expansion bus used on Intel-based computers.

**PDU** protocol data unit. OSI term for packet. See also BPDU and packet.

**PEP** Cisco Product Evolution Program. PEP is the UDI information that consists of the PID, the VID, and the SN of your sensor. PEP provides hardware version and serial number visibility through electronic query, product labels, and shipping items.

**PER** packed encoding rules. Instead of using a generic style of encoding that encodes all types in a uniform way, PER specializes the encoding based on the date type to generate much more compact representations.

**PFC** Policy Feature Card. An optional card on a Catalyst 6000 supervisor engine that supports VACL packet filtering.

**PID** Product Identifier. The orderable product identifier that is one of the three parts of the UDI. The UDI is part of the PEP policy.

**ping** packet internet groper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

**PIX Firewall** Private Internet Exchange Firewall. A Cisco network security device that can be programmed to block/enable addresses and ports between networks.

**PKI** Public Key Infrastructure. Authentication of HTTP clients using the clients' X.509 certificates.

**POST** Power-On Self Test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

<b>Post-ACL</b>	Designates an ACL from which ARC should read the ACL entries, and where it places entries after all deny entries for the addresses being blocked.
<b>Pre-ACL</b>	Designates an ACL from which ARC should read the ACL entries, and where it places entries before any deny entries for the addresses being blocked.
<b>promiscuous mode</b>	A passive interface for monitoring packets of the network segment. The sensing interface does not have an IP address assigned to it and is therefore invisible to attackers.

---

## Q

<b>Q.931</b>	ITU-T specification for signaling to establish, maintain, and clear ISDN network connections.
--------------	---

---

## R

<b>rack mounting</b>	Refers to mounting a sensor in an equipment rack.
<b>RAM</b>	random-access memory. Volatile memory that can be read and written by a microprocessor.
<b>RAS</b>	Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
<b>RDEP2</b>	Remote Data Exchange Protocol version 2. The published specification for remote data exchange over the command and control network using HTTP and TLS.
<b>reassembly</b>	The putting back together of an IP datagram at the destination after it has been fragmented either at the source or at an intermediate node.
<b>recovery partition image</b>	An IPS image file that includes the full application image and installer used for recovery on sensors.
<b>regex</b>	See regular expression.
<b>regular expression</b>	A mechanism by which you can define how to search for a specified sequence of characters in a data stream or file. Regular expressions are a powerful and flexible notation almost like a mini-programming language that allow you to describe text. In the context of pattern matching, regular expressions allow a succinct description of any arbitrary pattern.
<b>ROMMON</b>	Read-Only-Memory Monitor. ROMMON lets you TFTP system images onto the sensor for recovery purposes.
<b>round-trip time</b>	See RTT.
<b>RPC</b>	remote-procedure call. Technological foundation of client/server computing. RPCs are procedure calls that are built or specified by clients and are executed on servers, with the results returned over the network to the clients.

<b>RR</b>	Risk Rating. An RR is a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
<b>RSM</b>	Router Switch Module. A router module that is installed in a Catalyst 5000 switch. It functions exactly like a standalone router.
<b>RTP</b>	Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.
<b>RTT</b>	round-trip time. A measure of the time delay imposed by a network on a host from the sending of a packet until acknowledgement of the receipt.
<b>RU</b>	rack unit. A rack is measured in rack units. An RU is equal to 44 mm or 1.75 inches.

---

**S**

<b>SAP</b>	Signature Analysis Processor. Dispatches packets to the inspectors that are not stream-based and that are configured for interest in the packet in process.
<b>SCEP</b>	Simple Certificate Enrollment Protocol. The Cisco Systems PKI communication protocol that leverages existing technology by using PKCS#7 and PKCS#10. SCEP is the evolution of the enrollment protocol.
<b>SDEE</b>	Security Device Event Exchange. A product-independent standard for communicating security device events. It is an enhancement to RDEP. It adds extensibility features that are needed for communicating events generated by various types of security devices.
<b>SDP</b>	Slave Dispatch Processor.
<b>SEAF</b>	signature event action filter. Subtracts actions based on the signature event's signature ID, addresses, and RR. The input to the SEAF is the signature event with actions possibly added by the SEAO.
<b>SEAH</b>	signature event action handler. Performs the requested actions. The output from SEAH is the actions being performed and possibly an <evIdsAlert> written to the Event Store.
<b>SEAO</b>	signature event action override. Adds actions based on the RR value. SEAO applies to all signatures that fall into the range of the configured RR threshold. Each SEAO is independent and has a separate configuration value for each action type.
<b>SEAP</b>	Signature Event Action Processor. Processes event actions. Event actions can be associated with an event risk rating (RR) threshold that must be surpassed for the actions to take place.
<b>Secure Shell Protocol</b>	Protocol that provides a secure remote connection to a router through a Transmission Control Protocol (TCP) application.
<b>Security Monitor</b>	Monitoring Center for Security. Provides event collection, viewing, and reporting capability for network devices. Used with the IDS MC.

<b>sensing interface</b>	The interface on the sensor that monitors the desired network segment. The sensing interface is in promiscuous mode; it has no IP address and is not visible on the monitored segment.
<b>sensor</b>	The sensor is the intrusion detection engine. It analyzes network traffic searching for signs of unauthorized activity.
<b>SensorApp</b>	A component of the IPS. Performs packet capture and analysis. SensorApp analyzes network traffic for malicious content. Packets flow through a pipeline of processors fed by a producer designed to collect packets from the network interfaces on the sensor. Sensorapp is the standalone executable that runs Analysis Engine.
<b>Service engine</b>	Deals with specific protocols, such as DNS, FTP, H255, HTTP, IDENT, MS RPC, MS SL, NTP, RPC, SMB, SNMP, and SSH.
<b>service pack</b>	Used for the release of bug fixes with no new enhancements. Service packs are cumulative following a base version release (minor or major).
<b>session command</b>	Command used on routers and switches to provide either Telnet or console access to a module in the router or switch.
<b>shun command</b>	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection. It is used by ARC when blocking with a PIX Firewall.
<b>Signature Analysis Processor</b>	See SAP.
<b>signature</b>	A signature distills network information and compares it against a rule set that indicates typical intrusion activity.
<b>signature engine</b>	A component of the sensor that supports many signatures in a certain category. An engine is composed of a parser and an inspector. Each engine has a set of legal parameters that have allowable ranges or sets of values.
<b>signature event action filter</b>	See SEAF.
<b>signature event action handler</b>	See SEAH.
<b>signature event action override</b>	See SEAO.
<b>signature event action processor</b>	See SEAP.
<b>signature update</b>	Executable image that updates the IPS signature analysis engine (SensorApp) and the NSDB. Applying an IPS signature update is like updating virus definitions on a virus scanning program. Signature updates are released independently and have their own versioning scheme.
<b>Slave Dispatch Processor</b>	See SDP.
<b>SMB</b>	Server Message Block. File-system protocol used in LAN manager and similar NOSs to package data and exchange information with other systems.

<b>SMTP</b>	Simple Mail Transfer Protocol. Internet protocol providing e-mail services.
<b>SN</b>	Serial Number. Part of the UDI. The SN is the serial number of your Cisco product.
<b>sniffing interface</b>	See sensing interface.
<b>SNMP</b>	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
<b>SNMP2</b>	SNMP Version 2. Version 2 of the network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the SMI, protocol operations, management architecture, and security.
<b>software bypass</b>	Passes traffic through the IPS system without inspection.
<b>source address</b>	Address of a network device that is sending data.
<b>SP</b>	Statistics Processor. Keeps track of system statistics such as packet counts and packet arrival rates.
<b>SPAN</b>	Switched Port Analyzer. Feature of the Catalyst 5000 switch that extends the monitoring abilities of existing network analyzers into a switched Ethernet environment. SPAN mirrors the traffic at one switched segment onto a predefined SPAN port. A network analyzer attached to the SPAN port can monitor traffic from any other Catalyst switched port.
<b>spanning tree</b>	Loop-free subset of a network topology.
<b>SQL</b>	Structured Query Language. International standard language for defining and accessing relational databases.
<b>SRAM</b>	Type of RAM that retains its contents for as long as power is supplied. SRAM does not require constant refreshing, like DRAM
<b>SRP</b>	Stream Reassembly Processor. Reorders TCP streams to ensure the arrival order of the packets at the various stream-based inspectors. It is also responsible for normalization of the TCP stream. The normalizer engine lets you enable or disable alert and deny actions.
<b>SSH</b>	Secure Shell. A utility that uses strong authentication and secure communications to log in to another computer over a network.
<b>SSL</b>	Secure Socket Layer. Encryption technology for the Internet used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
<b>Stacheldraht</b>	A DDoS tool that relies on the ICMP protocol.
<b>State engine</b>	Stateful searches of HTTP strings.
<b>Statistics Processor</b>	See SP.
<b>Stream Reassembly Processor</b>	See SRP.
<b>String engine</b>	A signature engine that provides regular expression-based pattern inspection and alert functionality for multiple transport protocols, including TCP, UDP, and ICMP.

<b>subsignature</b>	A more granular representation of a general signature. It typically further defines a broad scope signature.
<b>surface mounting</b>	Refers to attaching rubber feet to the bottom of a sensor when it is installed on a flat surface. The rubber feet allow proper airflow around the sensor and they also absorb vibration so that the hard-disk drive is less impacted.
<b>switch</b>	Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model.
<b>SYN flood</b>	Denial of Service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.
<b>system image</b>	The full IPS application and recovery image used for reimaging an entire sensor.

---

**T**

<b>TAC</b>	A Cisco Technical Assistance Center. There are four TACs worldwide.
<b>TACACS+</b>	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.
<b>TCP</b>	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
<b>TCPDUMP</b>	The TCPDUMP utility is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can use different options for viewing summary and detail information for each packet. For more information, go to <a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a> .
<b>TCP reset interface</b>	The interface on the IDS-4250-XL and IDSM-2 that can send TCP resets. On most sensors the TCP resets are sent out on the same sensing interface on which the packets are monitored, but on the IDS-4250-XL and IDSM-2 the sensing interfaces cannot be used for sending TCP resets. On the IDS-4250-XL the TCP reset interface is the onboard 10/100/100 TX interface, which is normally used on the IDS-4250-TX appliance when the XL card is not present. On the IDSM-2 the TCP reset interface is designated as port 1 with Catalyst software, and is not visible to the user in Cisco IOS software. The TCP reset action is only appropriate as an action selection on those signatures that are associated with a TCP-based service.
<b>Telnet</b>	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
<b>terminal server</b>	A router with multiple, low speed, asynchronous ports that are connected to other serial devices. Terminal servers can be used to remotely manage network equipment, including sensors.
<b>TFN2K</b>	Tribe Flood Network 2000. A common type of Denial of Service (DoS) attack that can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks.

<b>TFTP</b>	Trivial File Transfer Protocol. Simplified version of FTP that lets files be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
<b>three-way handshake</b>	Process whereby two protocol entities synchronize during connection establishment.
<b>threshold</b>	A value, either upper- or lower-bound that defines the maximum/minimum allowable condition before an alarm is sent.
<b>Time Processor</b>	See TP.
<b>TLS</b>	Transport Layer Security. The protocol used over stream transports to negotiate the identity of peers and establish encrypted communications.
<b>topology</b>	Physical arrangement of network nodes and media within an enterprise networking structure.
<b>TP</b>	Time Processor. Processes events stored in a time-slice calendar. Its primary task is to make stale database entries expire and to calculate time-dependent statistics.
<b>TPKT</b>	RFC 1006-defined method of demarking messages in a packet.
<b>traceroute</b>	Program available on many systems that traces the path a packet takes to a destination. It is used mostly to debug routing problems between hosts. A traceroute protocol is also defined in RFC 1393.
<b>traffic analysis</b>	Inference of information from observable characteristics of data flow(s), even when the data is encrypted or otherwise not directly available. Such characteristics include the identities and locations of the source(s) and destination(s), and the presence, amount, frequency, and duration of occurrence.
<b>Traffic ICMP engine</b>	Analyzes traffic from nonstandard protocols, such as TFN2K, LOKI, and DDOS.
<b>Transaction Server</b>	A component of the IPS.
<b>Transaction Source</b>	A component of the IPS.
<b>trap</b>	Message sent by an SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.
<b>Trojan engine</b>	Analyzes traffic from nonstandard protocols, such as BO2K and TFN2K.
<b>trunk</b>	Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.
<b>trusted certificate</b>	Certificate upon which a certificate user relies as being valid without the need for validation testing; especially a public-key certificate that is used to provide the first public key in a certification path.
<b>trusted key</b>	Public key upon which a user relies; especially a public key that can be used as the first public key in a certification path.
<b>tune</b>	Adjusting signature parameters to modify an existing signature.

---

**U**

- UDI** Unique Device Identifier. Provides a unique identity for every Cisco product. The UDI is composed of the PID, VID, and SN. The UDI is stored in the Cisco IPS ID PROM.
- UDP** User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
- unblock** To direct a router to remove a previously applied block.
- UPS** Uninterruptible Power Source.
- UTC** Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

---

**V**

- VACL** VLAN ACL. An ACL that filters all packets (both within a VLAN and between VLANs) that pass through a switch. Also known as security ACLs.
- VID** Version identifier. Part of the UDI.
- VIP** Versatile Interface Processor. Interface card used in Cisco 7000 and Cisco 7500 series routers. The VIP provides multilayer switching and runs Cisco IOS. The most recent version of the VIP is VIP2.
- virtual sensor** A logical grouping of sensing interfaces and the configuration policy for the signature engines and alarm filters to apply to them. In other words, multiple virtual sensors running on the same appliance, each configured with different signature behavior and traffic feeds. IPS 5.x supports only one virtual sensor.
- virus** Hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting—that is, inserting a copy of itself into and becoming part of—another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.
- virus update** A signature update specifically addressing viruses.
- VLAN** Virtual Local Area Network. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
- VMS** CiscoWorks VPN/Security Management Solution. A suite of network security applications that combines web-based tools for configuring, monitoring, and troubleshooting enterprise VPN, firewalls, network intrusion detection systems and host-based intrusion prevention systems.

<b>VoIP</b>	Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.
<b>VPN</b>	Virtual Private Network(ing). Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.
<b>vulnerability</b>	One or more attributes of a computer or a network that permit a subject to initiate patterns of misuse on that computer or network.

---

## W

<b>WAN</b>	wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.
<b>Web Server</b>	A component of the IPS.
<b>Wireshark</b>	Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, go to <a href="http://www.wireshark.org">http://www.wireshark.org</a> .
<b>worm</b>	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and can consume computer resources destructively.

---

## X

<b>X.509</b>	Standard that defines information contained in a certificate.
<b>XML</b>	eXtensible Markup Language. Textual file format used for data interchange between heterogeneous hosts.





## INDEX

---

### A

- adding
  - an entry to the known hosts table [2-88](#)
  - a public key [2-85](#)
  - a trusted host [2-92](#)
- Administrators
  - privileges [1-1](#)
- alerts
  - viewing [2-56](#)
- application partition
  - reimaging [2-39](#)
- applying
  - service packs [2-95](#)
  - signature updates [2-95](#)
- attacker IP address
  - removing from list of denied IP addresses [2-5](#)

---

### B

- banner login
  - describing [2-3](#)
  - examples [2-3](#)
  - syntax [2-3](#)
  - using [2-3](#)
- banner message
  - creating [2-3](#)
- block requests
  - viewing [2-56](#)

---

### C

- capturing
  - live traffic [2-31](#)
- changing the password [2-34](#)
- clear denied-attackers
  - describing [2-5](#)
  - examples [2-5](#)
  - using [2-5](#)
- clear events
  - describing [2-6](#)
  - examples [2-6](#)
  - using [2-6](#)
- clear line
  - describing [2-7](#)
  - examples [2-7](#)
  - syntax [2-7](#)
  - using [2-7](#)
- CLI
  - command line editing [1-4](#)
  - command modes [1-5](#)
  - default keywords [1-8](#)
  - error messages [B-1](#)
  - generic commands [1-7](#)
  - regular expression syntax [1-5](#)
- CLI behavior [1-2](#)
  - case sensitivity [1-3](#)
  - display options [1-3](#)
  - help [1-2](#)
  - prompts [1-2](#)
  - recall [1-3](#)
  - tab completion [1-3](#)

clock set

- describing [2-9](#)
- examples [2-9](#)
- syntax [2-9](#)
- using [2-9](#)

closing an active terminal session [2-18](#)

command line editing (table) [1-4](#)

command modes [1-5](#)

- event action rules configuration [1-5](#)
- EXEC [1-5](#)
- global configuration [1-5](#)
- privileged EXEC [1-5](#)
- service mode configuration [1-5](#)
- signature definition configuration [1-5](#)

command platform dependencies [A-2](#)

commands

- deprecated [A-1](#)
- platform dependencies [A-2](#)
- viewing list of most recently used [2-60](#)

configure

- describing [2-10](#)
- examples [2-10](#)
- syntax [2-10](#)
- using [2-10](#)

conventions [i-vii](#)

copy

- describing [2-11](#)
- examples [2-12](#)
- syntax [2-11](#)
- using [2-11](#)

copying

- configuration files [2-11](#)
- iplogs [2-11](#)

creating

- banner message [2-3](#)
- users [2-97](#)

Ctrl-N [1-3](#)

Ctrl-P [1-3](#)

---

## D

default keywords

- using [1-8](#)

deleting a logical file [2-17](#)

denied attackers

- removing [2-5](#)

deprecated commands [A-1](#)

directing output to the serial connection [2-14](#)

display

- specifying number of lines on screen [2-90](#)

displaying

- current level of privilege [2-66](#)
- current system status [2-77](#)
- interface statistics [2-63](#)
- IP log contents [2-21](#)
- IP packet route [2-94](#)
- known hosts table [2-73](#)
- live traffic [2-31](#)
- local event log contents [2-56](#)
- PEP information [2-65](#)
- public RSA keys [2-70](#)
- sensor trusted hosts [2-80](#)
- server TLS certificate fingerprint [2-79](#)
- SSH server's host key [2-72](#)
- statistics [2-74](#)
- system clock [2-53](#)
- user information [2-81](#)
- version information [2-83](#)

display-serial

- describing [2-14](#)
- examples [2-14](#)
- using [2-14](#)

downgrade

- describing [2-15](#)
- examples [2-15](#)

---

**E**

end

describing [2-16](#)examples [2-16](#)

entering

global configuration [2-10](#)service configuration mode [2-42](#)

erase

describing [2-17](#)examples [2-17](#)syntax [2-17](#)using [2-17](#)

error events

viewing [2-56](#)error messages [B-1](#)

event log

viewing contents of [2-56](#)

events

clearing [2-6](#)deleting [2-6](#)

Event Store

clearing events [2-6](#)

exit

describing [2-18](#)examples [2-18](#)using [2-18](#)

exiting

configuration mode [2-16, 2-18](#)submodes [2-16](#)

---

**G**

generating

server host key [2-87](#)X.509 certificate [2-91](#)generic commands [1-7](#)

---

**H**

help

question mark [1-2](#)using [1-2](#)

---

**I**initializing the sensor [2-45](#)

iplog

describing [2-19](#)examples [2-20](#)syntax [2-19](#)using [2-19](#)

iplog-status

describing [2-21](#)examples [2-21](#)using [2-21](#)

IP packet

display route [2-94](#)

---

**K**

keywords

default [1-8](#)no [1-8](#)

---

**M**

modifying

privilege level [2-38](#)terminal properties for a login session [2-90](#)

monitoring

Viewer privileges [1-2](#)

more exclude

describing [2-27](#)examples [2-27](#)syntax [2-27](#)

using [2-27](#)

more include

describing [2-29](#)

---

## N

network connectivity

testing for [2-36](#)

---

## O

Operators

privileges [1-2](#)

output

clearing current line [1-3](#)

displaying [1-3](#)

setting number of lines to display [2-90](#)

---

## P

packet

describing [2-31](#)

examples [2-32](#)

syntax [2-31](#)

using [2-32](#)

password

changing [2-34](#)

describing [2-34](#)

examples [2-35](#)

syntax [2-34](#)

updating [2-34](#)

using [2-34](#)

ping

describing [2-36](#)

examples [2-36](#)

syntax [2-36](#)

using [2-36](#)

privilege

describing [2-38](#)

examples [2-38](#)

modifying [2-38](#)

syntax [2-38](#)

prompts

default input [1-2](#)

---

## R

recall

help and tab completion [1-3](#)

using [1-3](#)

recover

describing [2-39](#)

examples [2-39](#)

syntax [2-39](#)

using [2-39](#)

regular expression syntax [1-5](#)

regular expression syntax (table) [1-6](#)

removing the most recent upgrade [2-15](#)

reset

describing [2-41](#)

examples [2-41](#)

syntax [2-41](#)

using [2-41](#)

route

displaying for IP packet [2-94](#)

---

## S

Service

privileges [1-2](#)

service

analysis-engine [2-42](#)

authentication [2-42](#)

certificate-authority [2-42](#)

describing [2-42](#)

- event-action-rules [2-42](#)
- examples [2-43](#)
- host [2-42](#)
- interface [2-42](#)
- logger [2-42](#)
- network-access [2-42](#)
- notification [2-42](#)
- signature-definition [2-42](#)
- ssh-known-hosts [2-42](#)
- syntax [2-42](#)
- trusted-certificate [2-42](#)
- using [2-43](#)
- web-server [2-42](#)
- service account
  - privileges [1-2](#)
- service event-action-rules
  - using [2-43](#)
- service role [1-2](#)
- setting the system clock [2-9](#)
- setup
  - clock setting parameters (table) [2-46](#)
  - describing [2-45](#)
  - examples [2-47](#)
  - using [2-46](#)
- show begin
  - describing [2-51](#)
  - examples [2-51](#)
  - syntax [2-51](#)
  - using [2-51](#)
- show clock
  - authoritative flags [2-53](#)
  - describing [2-53](#)
  - examples [2-53](#)
  - syntax [2-53](#)
  - using [2-53](#)
- show events
  - describing [2-56](#)
  - examples [2-57](#)
  - syntax [2-56](#)
- using [2-57](#)
- show exclude
  - describing [2-58](#)
  - examples [2-58](#)
  - syntax [2-58](#)
  - using [2-58](#)
- show history
  - describing [2-60](#)
  - examples [2-60](#)
  - using [2-60](#)
- show include
  - describing [2-61](#)
  - examples [2-61](#)
  - using [2-61](#)
- show interfaces
  - describing [2-63](#)
  - examples [2-63](#)
  - syntax [2-63](#)
  - using [2-63](#)
- show inventory
  - describing [2-65](#)
  - examples [2-65](#)
  - using [2-65](#)
- show privilege
  - describing [2-66](#)
  - examples [2-66](#)
  - using [2-66](#)
- show settings
  - describing [2-67](#)
  - examples [2-67](#)
  - syntax [2-67](#)
- show ssh authorized-keys
  - describing [2-70](#)
  - examples [2-70](#)
  - syntax [2-70](#)
  - using [2-70](#)
- show ssh host-keys
  - describing [2-73](#)
  - examples [2-73](#)

- syntax [2-73](#)
    - using [2-73](#)
  - show ssh server-key
    - describing [2-72](#)
    - examples [2-72](#)
  - show statistics
    - describing [2-74](#)
    - syntax [2-74](#)
  - show tech-support
    - describing [2-77](#)
    - examples [2-78](#)
    - using [2-77](#)
  - show tls-fingerprint
    - describing [2-79](#)
    - examples [2-79](#)
  - show tls trusted-hosts
    - describing [2-80](#)
    - examples [2-80](#)
    - syntax [2-80](#)
    - using [2-80](#)
  - show users
    - describing [2-81](#)
    - examples [2-81](#)
    - syntax [2-81](#)
    - using [2-81](#)
  - show version
    - describing [2-83](#)
    - examples [2-83](#)
    - using [2-83](#)
  - ssh authorized-key
    - describing [2-85](#)
    - examples [2-85](#)
    - syntax [2-85](#)
    - using [2-85](#)
  - ssh generate-key
    - describing [2-87](#)
    - examples [2-87](#)
    - using [2-87](#)
  - ssh host-key
    - describing [2-88](#)
    - examples [2-89](#)
    - syntax [2-88](#)
    - using [2-88](#)
  - starting IP logging [2-19](#)
  - statistics
    - clearing [2-74](#)
    - viewing [2-74](#)
  - status events
    - viewing [2-56](#)
  - syntax
    - case sensitivity [1-3](#)
  - system
    - viewing status [2-77](#)
  - System Configuration Dialog [2-46](#)
  - system information
    - exporting to FTP or SCP server [2-77](#)
- 
- T**
- tab completion
    - using [1-3](#)
  - tech support
    - viewing
      - control transaction responses [2-77](#)
      - current configuration information [2-77](#)
      - debug logs [2-77](#)
      - version [2-77](#)
  - terminal
    - describing [2-90](#)
    - examples [2-90](#)
    - syntax [2-90](#)
    - using [2-90](#)
  - terminating a CLI session [2-7](#)
  - tls generate-key
    - describing [2-91](#)
    - examples [2-91](#)
  - tls trusted-host
    - describing [2-92](#)

examples [2-92](#)

syntax [2-92](#)

using [2-92](#)

trace

describing [2-94](#)

examples [2-94](#)

using [2-94](#)

signature packages [2-83](#)

status events [2-56s](#)

---

## U

updating the password [2-34](#)

upgrade

describing [2-95](#)

examples [2-96](#)

syntax [2-95](#)

using [2-95](#)

upgrading the system [2-95](#)

username

describing [2-97](#)

examples [2-97](#)

syntax [2-97](#)

using [2-97](#)

user roles

Administrator [1-1, 1-2](#)

Operator [1-1, 1-2](#)

Service [1-1, 1-2](#)

Viewer [1-1, 1-2](#)

---

## V

Viewers

privileges [1-2](#)

viewing

alerts [2-56](#)

block requests [2-56](#)

error events [2-56](#)

IPS processes [2-83](#)

operating system [2-83](#)

