



CHAPTER 1

Available Commands

This chapter contains the IPS 6.0 commands listed in alphabetical order. It contains the following sections:.

- [anomaly-detection load](#), page 1-4
- [anomaly-detection save](#), page 1-5
- [banner login](#), page 1-6
- [clear denied-attackers](#), page 1-8
- [clear events](#), page 1-10
- [clear line](#), page 1-11
- [clear os-identification](#), page 1-13
- [clock set](#), page 1-14
- [configure](#), page 1-15
- [copy](#), page 1-16
- [copy ad-knowledge-base](#), page 1-19
- [copy instance](#), page 1-21
- [display serial](#), page 1-22
- [downgrade](#), page 1-23
- [end](#), page 1-24
- [erase](#), page 1-25
- [erase ad-knowledge-base](#), page 1-26
- [exit](#), page 1-28
- [iplog](#), page 1-29
- [iplog-status](#), page 1-31
- [list component-configurations](#), page 1-33
- [more](#), page 1-34
- [more begin](#), page 1-36
- [more exclude](#), page 1-38
- [more include](#), page 1-40
- [packet](#), page 1-42

- password, page 1-45
- ping, page 1-47
- privilege, page 1-49
- recover, page 1-50
- rename ad-knowledge-base, page 1-52
- reset, page 1-53
- service, page 1-54
- setup, page 1-57
- show ad-knowledge-base diff, page 1-71
- show ad-knowledge-base files, page 1-73
- show ad-knowledge-base thresholds, page 1-74
- show begin, page 1-77
- show clock, page 1-79
- show configuration, page 1-81
- show events, page 1-82
- show exclude, page 1-84
- show history, page 1-86
- show include, page 1-87
- show interfaces, page 1-89
- show inventory, page 1-91
- show os-identification, page 1-92
- show privilege, page 1-94
- show settings, page 1-95
- show ssh authorized-keys, page 1-98
- show ssh server-key, page 1-100
- show ssh host-keys, page 1-101
- show statistics, page 1-102
- show tech-support, page 1-105
- show tls fingerprint, page 1-107
- show tls trusted-hosts, page 1-108
- show users, page 1-109
- show version, page 1-111
- ssh authorized-key, page 1-113
- ssh generate-key, page 1-115
- ssh host-key, page 1-116
- terminal, page 1-118
- tls generate-key, page 1-119
- tls trusted-host, page 1-120

- [trace](#), page 1-122
- [upgrade](#), page 1-123
- [username](#), page 1-125

anomaly-detection load

To set the KB file as the current KB for the specified virtual sensor, use the **anomaly-detection load** command in privileged EXEC mode.

anomaly-detection *virtual-sensor* **load** [**initial** | **file** *name*]

Syntax Description		
<i>virtual-sensor</i>	The virtual sensor. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”	
<i>name</i>	The KB filename. This is a case-sensitive character string containing 1 to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”	
initial	The initial KB.	
file	An existing KB file.	

Defaults No default behavior or values.

Command Modes EXEC

SupportedUserRoles Administrator

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples

The following example loads 2006-Mar-16-10_00_00 as the current KB file:

```
sensor# anomaly-detection vs0 load file 2006-Mar-16-10_00_00
sensor#
```

anomaly-detection save

To retrieve the current AD KB file and save it locally, use the **anomaly-detection save** command in privileged EXEC mode.

anomaly-detection *virtual-sensor* **save** [*new-name*]

Syntax Description

<i>virtual-sensor</i>	The virtual sensor. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
<i>new-name</i>	(Optional) The new KB filename. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”

Defaults

The default generated filename is *YYYY-Mon-dd-hh_mm_ss*. Where Mon is a three letter abbreviation of the current month.

Command Modes

EXEC

Supported User Roles

Administrator

Command History

Release	Modification
6.0(1)	This command was introduced.

Usage Guidelines

An error is generated if AD is not active when you execute this command. You cannot overwrite the initial KB file. If the KB file name already exists, whether you choose a new name or use the default, the old KB file is overwritten.

There is a limit on the size the KB file can occupy. If a new KB is generated, and this limit is reached, the oldest KB (assuming it is not current or initial) is deleted.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples

The following example saves the current KB and stores it as my-kb:

```
sensor# anomaly-detection vs0 save my-kb
sensor#
```

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 Ctrl-V .
-----------------	---

Defaults

No default behavior or values.

Command Modes

Global configuration

Supported User Roles

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.

Enter **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 [*virtual-sensor*] [**ip-address** *ip-address*]

Syntax Description		
<i>virtual-sensor</i>	(Optional) The name of the virtual sensor configured on the sensor. The clear operation is restricted to learned addresses associated with the identified virtual sensor. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.” If you do not provide the virtual sensor name, all denied attackers are cleared.	
<i>ip-address</i>	(Optional) The IP address to clear.	

Defaults No default behavior or values.

Command Modes EXEC

SupportedUserRoles Administrator

Command History	Release	Modification
	5.0(1)	This command was introduced.
	6.0(1)	Added optional <i>virtual-sensor</i> and <i>ip-address</i> parameters.

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.

The virtual sensor and IP address are optional. If you provide the virtual sensor name, the IP address is cleared on the requested virtual sensor only; otherwise, it is cleared on all virtual sensors.



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 is IPS-specific. There is no related IOS command in version 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 show users command.
message		(Optional) If you select message , 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
show users	Displays information about users logged in to the CLI.

clear os-identification

To delete OS ID associations with IP addresses that were learned by the sensor through passive analysis, use the **clear os-identification** command in privileged EXEC mode.

clear os-identification [*virtual-sensor*] **learned** [*ip-address*]

Syntax Description

<i>virtual-sensor</i>	(Optional) The name of the virtual sensor configured on the sensor. The clear operation is restricted to learned addresses associated with the identified virtual sensor. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
<i>ip-address</i>	(Optional) The IP address to clear. The sensor clears the OS ID mapped to the specified IP address.

Defaults

No default behavior or values.

Command Modes

EXEC

Supported User Roles

Administrator, Operator

Command History

Release	Modification
6.0(1)	This command was introduced.

Usage Guidelines

The virtual sensor and IP address are optional. When you specify an IP address, only the OS identification for the specified IP address is cleared; otherwise, all learned OS identifications are cleared. If you specify a virtual sensor, only the OS identification for the specified virtual sensor is cleared; otherwise, the learned OS identifications for all virtual sensors are cleared. If you specify an IP address without a virtual sensor, the IP address is cleared on all virtual sensors.

Examples

The following example clears the learned OS identification for IP address 10.1.1.12 on all virtual sensors:

```
sensor# clear os-identification learned 10.1.1.12
sensor#
```

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

Syntax Description	terminal	Executes configuration commands from the terminal.
---------------------------	-----------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	EXEC
----------------------	------

SupportedUserRoles	Administrator, Operator, Viewer
---------------------------	---------------------------------

Usage Guidelines	Executing the configure terminal command puts you in global configuration mode.
-------------------------	--

Examples	The following example changes modes from privileged EXEC to global configuration:
-----------------	---

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

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	
/erase	(Optional) Erases the destination file before copying. Note 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 iplog-status 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
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.
iplog	An iplog contained on the system. The IP logs are retrieved based on log-id. See the iplog-status command output. IP logs are stored in binary and are displayed with a log viewer.
license-key	The subscription license file.
packet-file	The locally stored libpcap file captured using the packet capture 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
iplog-status	Displays a description of the available IP log contents.
more	Displays the contents of a logical file.
packet	Displays or captures live traffic on an interface.

copy ad-knowledge-base

To copy a KB file, use the **copy ad-knowledge-base** command in privileged EXEC mode.

copy ad-knowledge-base *virtual-sensor* [**current** | **initial** | **file name**] *destination-url*

copy ad-knowledge-base *virtual-sensor source-url new-name*

Syntax Description

<i>virtual-sensor</i>	The virtual sensor containing the KB file. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
<i>name</i>	The KB filename. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
current	The currently loaded KB.
file	An existing KB file.
initial	The initial KB.
<i>new-name</i>	The new KB filename. This is a case-sensitive character string containing 1 to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
<i>source-url</i>	The source URL can be FTP, SCP, HTTP, or HTTPS. For syntax details, see copy, page 1-16 .
<i>destination-url</i>	The destination URL can be FTP, SCP, HTTP, or HTTPS. For syntax details, see copy, page 1-16 .

Defaults

No default behavior or values.

Command Modes

EXEC

Supported User Roles

Administrator

Command History

Release	Modification
6.0(1)	This command was introduced.

Usage Guidelines

Copying a file to a name that already exists overwrites that file. You cannot use the **current** keyword as a *new-name*. The new current KB is created by the **load** command.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples

The following example copies 2006-Mar-16-10_00_00 to ~cidsuser/AD/my-kb on the computer with the IP address 10.1.1.1:

```
sensor# copy ad-knowledge-base vs0 file 2006-Mar-16-10_00_00
scp://cidsuser@10.1.1.1/AD/my-kb
Password: *****
2006-Mar-16-10_00_00          100%   14920   0.0KB/s
00:00
sensor#
```

copy instance

To copy a configuration instance, use the **copy instance** command in privileged EXEC mode.

copy [**anomaly-detection** | **event-action-rules** | **signature-definition**] *source destination*

Syntax Description		
	<i>source</i>	The name of the existing component instance to copy.
	<i>destination</i>	The name of the new or existing component instance.

Defaults No default behavior or values.

Command Modes EXEC

SupportedUserRoles Administrator

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines Use this command to copy configuration instances. An error is generated if the instance already exists or if there is not enough space available for the new instance.

Examples The following example copies the signature definition named “sig0” to a new definition named “mySig”:

```
sensor# copy signature-definition sig0 mySig
sensor#
```

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

Supported User Roles Administrator, Operator

Command History	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 last applied signature update or service pack, 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 recently applied signature update from the sensor:

```

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
	show version	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
	backup-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.
	current-config	Storage location for configuration backup. The file format is CLI commands.
	packet-file	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 Erasing the current configuration resets the configuration values back to default. It does not remove configuration instances created by the **service** command.

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#
```

erase ad-knowledge-base

To remove a KB from the sensor, use the **erase ad-knowledge-base** command in privileged EXEC mode.

erase ad-knowledge-base [*virtual-sensor* [*name*]]

Syntax Description		
<i>virtual-sensor</i>	(Optional) The virtual sensor containing the KB file. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”	
<i>name</i>	(Optional) The KB filename. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”	

Defaults No default behavior or values.

Command Modes EXEC

SupportedUserRoles Administrator

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines You cannot remove the KB file that is loaded as the current KB file. You cannot remove the initial KB file.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples

The following example removes 2006-Mar-16-10_00_00 from virtual sensor vs0:

```
sensor# erase ad-knowledge-base vs0 2006-Mar-16-10_00_00
sensor#
```

The following example removes all KBs except the file loaded as current and the initial KB from virtual sensor vs0.

```
sensor# erase ad-knowledge-base vs0
Warning: Executing this command will delete all virtual sensor 'vs0' knowledge bases
except the file loaded as current and the initial knowledge base.
Continue with erase? : yes
sensor#
```

The following example removes all KBs except the file loaded as current and the initial KB from all virtual sensors.

```
sensor# erase ad-knowledge-base
Warning: Executing this command will delete all virtual sensor knowledge bases except the
file loaded as current and the initial knowledge base.
Continue with erase? : 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 submenu.

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. For parameter details, see setup, page 1-57 .
<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 iplog-status 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 is IPS-specific. There is no related IOS command in version 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
iplog-status	Displays a description of the available IP log contents.
packet	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 [**log-id** *log-id*] [**brief**] [**reverse**] [{**begin** *regular-expression* | **exclude** *regular-expression* | **include** *regular-expression* | **redirect** *destination-url*}]

Syntax Description		
<i>log-id</i>	(Optional)	Log ID of the file to status.
brief	(Optional)	Displays a summary of iplog status information for each log.
reverse	(Optional)	Displays the list in reverse chronological order (newest log first).
	(Optional)	A vertical bar indicates that an output processing specification follows.
<i>regular-expression</i>		Any regular expression found in the iplog status output.
begin		Searches the output of the more command and displays the output from the first instance of a specified string.
exclude		Filters the iplog-status command output so that it excludes lines that contain a particular regular expression.
include		Filters the iplog-status command output so that it includes lines that contain a particular regular expression.
redirect		Redirects the iplog-status command output to a destination URL.
<i>destination-url</i>		The location of the destination file to be copied. May be a URL or a keyword.

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.
	6.0(1)	Added log-id , brief , reverse , begin , exclude , include , and redirect options.

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 is IPS-specific. There is no related IOS command in version 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#

```

The following example displays a brief list of all IP logs:

```

sensor# iplog-status brief
Log ID  VS   IP Address1  Status   Event ID  Start Date
2425    vs0   10.1.1.2    started  N/A       2003/07/30
2342    vs0   10.2.3.1    completed 209348    2003/07/30

```

Related Commands

Command	Description
iplog	Starts IP logging on a virtual sensor.

list *component-configurations*

To display the existing configuration instances for a component, use the **list *component-configurations*** command in privileged EXEC mode.

```
list [anomaly-detection-configurations | event-action-rules-configurations |
signature-definition-configurations]
```

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
	6.0(1)	This command was introduced.

Usage Guidelines The file size is in bytes. A virtual sensor of N/A means the instance is not currently assigned to a virtual sensor.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples The following example displays the existing configuration for signature definition:

```
sensor# list signature-definition-configurations
Signature Definition
  Instance   Size   Virtual Sensor
  sig0       2293   vs0
  mySig      3422   N/A
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
! -----
! Current configuration last modified Tue Jan 24 08:24:44 2006
! -----
! Version 6.0(0.9)
! Host:
!   Realm Keys          key1.0
! Signature Definition:
!   Signature Update    S212.0   2006-01-12
! -----
service interface
physical-interfaces FastEthernet0/1
admin-state enabled
```

```

exit
physical-interfaces FastEthernet1/0
admin-state enabled
exit
physical-interfaces FastEthernet1/1
admin-state enabled
exit
physical-interfaces FastEthernet1/2
admin-state enabled
exit
physical-interfaces FastEthernet1/3
admin-state enabled
exit
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.149.118/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! -----
service logger
exit
! -----
service network-access
exit

```

Related Commands

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

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
```

```

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
more begin	Searches the output of the more command and displays the output from the first instance of a specified string.
more include	Filters the more command output so that it displays only lines that contain a particular regular expression.
show begin	Searches the output of certain show commands and displays the output from the first instance of a specified string.
show exclude	Filters the show command output so that it excludes lines that contain a particular regular expression.
show include	Filters the show 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>	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.
			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)	Added the include extension to the more command.

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
more begin	Searches the output of the more command and displays the output from the first instance of a specified string.
more exclude	Filters the more command output so that it excludes lines that contain a particular regular expression.
show begin	Searches the output of certain show commands and displays the output from the first instance of a specified string.
show exclude	Filters the show command output so that it excludes lines that contain a particular regular expression.
show include	Filters the show 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. You can 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.
snaplen	(Optional) Specifies to use snapshot length.
<i>length</i>	(Optional) Snapshot length. The default is 0. A valid range is 0 to 1600.
count	(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.
verbose	(Optional) Displays the protocol tree for each packet rather than a one-line summary.
expression	(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.
file-info	Displays information about the stored packet file.
vlan and	Matches packets with VLAN headers.

Defaults

See the Syntax Description table.

Command Modes

EXEC

Supported User Roles

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**

This command is IPS-specific. There is no related IOS command in version 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

Command	Description
iplog	Starts IP logging on a virtual sensor.
iplog-status	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 8 to 32 characters in length. All characters except space are allowed.

Defaults

The cisco account default password is cisco.

Command Modes

Global configuration

SupportedUserRoles

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 reenble 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	address	IP address of the system to ping.
	count	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.

SupportedUserRoles 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**]

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.
-------------	--

Defaults

No default behavior or values.

Command Modes

Global configuration

Supported User Roles

Administrator

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the command to modify the privilege for a user.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples

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)#
```

Related Commands

Command	Description
username	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 of the 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

Syntax Description	application-partition Reimages the application partition.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

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

SupportedUserRoles	Administrator
---------------------------	---------------

Usage Guidelines	<p>Valid answers to the continue with recover question are yes or no. Y or N 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>
-------------------------	--



Note	This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.
-------------	---

Examples	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)#
```

rename ad-knowledge-base

To rename an existing KB file, use the **rename ad-knowledge-base** command in privileged EXEC mode.

```
rename ad-knowledge-base virtual-sensor [current | file name] new-name
```

Syntax Description		
<i>virtual-sensor</i>		The virtual sensor containing the KB file. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
<i>name</i>		The KB filename. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
current		The currently loaded KB.
file		An existing KB file.
<i>new-name</i>		The new KB filename. This is a case-sensitive character string containing 1 to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”

Defaults No default behavior or values.

Command Modes EXEC

SupportedUserRoles Administrator

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines If you use the **current** keyword, you are renaming the KB that is currently being used. You cannot rename the initial KB file.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples The following example renames 2006-Mar-16-10_00_00 to my-kb:

```
sensor# rename ad-knowledge-base vs0 file 2006-Mar-16-10_00_00 my-kb
sensor#
```

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 is IPS-specific. There is no related IOS command in version 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 | external-product-interface | host | interface | logger
| network-access | notification | ssh-known-hosts | trusted-certificate | web-server}
```

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

To enter configuration mode for a logically named event action rules configuration, use the **service event-action-rules** *name* command in global configuration mode. The **default** keyword resets the configuration to factory settings. The **no** keyword removes the event action rules configuration from the sensor. This command only succeeds if the configuration is not assigned to a virtual sensor.

```
service event-action-rules name
```

```
default service event-action-rules name
```

```
no service event-action-rules name
```

To enter configuration mode for a logically named signature definition configuration, use the **service signature-definition** *name* command in global configuration mode. The **default** keyword resets the configuration to factory settings. The **no** keyword removes the signature definition configuration from the sensor. This command only succeeds if the configuration is not assigned to a virtual sensor.

```
service signature-definition name
```

```
default service signature-definition name
```

```
no service signature-definition name
```

To enter configuration mode for a logically named anomaly-detection configuration, use the **service anomaly-detection** *name* command in global configuration mode. The **default** keyword resets the configuration to factory settings. The **no** keyword removes the anomaly detection configuration from the sensor. This command only succeeds if the configuration is not assigned to a virtual sensor.

```
service anomaly-detection name
```

```
default anomaly-detection name
```

```
no service anomaly-detection name
```

Syntax Description

authentication	Configures the order of methods that should be used to authenticate users.
analysis-engine	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.
anomaly-detection	Configures the parameters for anomaly-detection.
event-action-rules	Configures the parameters for an event action rules configuration.

external-product-interface	Configures the parameters for the external product interface.
host	Configures the system clock settings, upgrades, and IP access list.
logger	Configures debug levels.
network-access	Configures parameters relating to ARC. 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 6.0 CLI. You will still see network-access and nac throughout the CLI.
notification	Configures the notification application.
signature-definition	Configures the parameters for a signature definition configuration.
ssh-known-hosts	Configures the known hosts keys for the system.
trusted-certificate	Configures the list of X.509 certificates for trusted certificate authorities.
web-server	Configures parameters relating to the web server such as web server port.
name	Logical name of the event action rules or signature definition configuration. If the logical name does not already exist, a new configuration file is created.

Defaults

No default behavior or values.

Command Modes

Global configuration

Supported User Roles

Administrator, Operator (except host and interface), Viewer (display only)

Command History

Release	Modification
4.0(1)	This command was introduced.
5.0(1)	Added the default keyword and notification application support.
6.0(1)	Added the anomaly-detection , external-product-interface , and os-identification commands.

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)#
```



Note This command is IPS-specific. There is no related IOS command in version 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.
5.0(1)	Added configuration of virtual sensor settings.

Release	Modification
5.1(1)	Added configuration of inline VLAN pairs.
6.0(1)	Added configuration of multiple virtual sensors and VLAN groups. Added prompting to automatically deny threats by default.

Usage Guidelines

When you enter 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, enter 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 enter **yes**, the configuration is saved to disk. If you enter **no**, the configuration is not saved and the process begins again. There is no default for this prompt; you must enter either **yes** or **no**.

Valid ranges for configurable parameters are as follows:

IP Address/Netmask/Gateway: *X.X.X.X/mn, 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.

mn 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 1-1](#) shows the clock setting parameters.

Table 1-1 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,...).

Table 1-1 Clock Setting Parameters (continued)

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.
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.

While in setup, you can enable/disable the overrides rule associated with the **deny-packet-inline** action. You can modify all instances of event action rules configuration that are assigned to a virtual sensor. Event action rules configuration instances that are not assigned to a virtual sensor are not changed.

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 8080
exit
service event-action-rules rules0
```

```

overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 75-100
exit
exit
service event-action-rules myEvr
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
exit
physical-interfaces GigabitEthernet1/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user cisco
vlan1 2
vlan2 3
exit
subinterface 2
description Created via setup by user cisco
vlan1 344
vlan2 23
exit
subinterface 10
description Created via setup by user cisco
vlan1 20
vlan2 10
exit
exit
exit
physical-interfaces GigabitEthernet1/1
admin-state enabled
subinterface-type vlan-group
subinterface 3
description Created via setup by user cisco
vlans 5-7,9
exit
exit
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
exit
inline-interface foo
description Create via setup by user cisco
interface1 GigabitEthernet3/0
interface2 GigabitEthernet3/1
subinterface-type vlan-group
subinterface 3
vlans 200-299
exit
subinterface 8
vlans 300-399
exit
exit
exit
exit
service analysis-engine

```

```

virtual-sensor vs0
anomaly-detection ad0
event-action-rules rules0
signature-definition sig0
physical-interface GigabitEthernet0/0
physical-interface GigabitEthernet1/0 subinterface-number 1
physical-interface GigabitEthernet1/0 subinterface-number 2
exit
virtual-sensor myVs
anomaly-detection myAd
event-action-rules myEvr
signature-definition mySigs
physical-interface GigabitEthernet2/0
physical-interface GigabitEthernet1/1 subinterface-number 3
logical-interface foo subinterface 3
logical-interface foo subinterface 8
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 interface/virtual sensor configuration?[no]: yes
Current interface configuration
Command control GigabitEthernet0/1
Unassigned:
Promiscuous:
    GigabitEthernet2/1

```

```

    GigabitEthernet4/0
    GigabitEthernet4/1
  Inline Vlan Pairs:
    GigabitEthernet1/0:10 (Vlans: 20, 10)

Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Promiscuous:
    GigabitEthernet0/0
  Inline Vlan Pairs:
    GigabitEthernet1/0:1 (Vlans: 2, 3)
    GigabitEthernet1/0:2 (Vlans: 344, 23)

Virtual Sensor: myVs
  Anomaly Detection: myAd
  Event Action Rules: myEvr
  Signature Definition: mySigs
  Promiscuous:
    GigabitEthernet2/0
  Promiscuous Vlan Groups:
    GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pair Vlan Groups:
    foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
    foo:8 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 300-399)

[1] Edit Interface Configuration
[2] Edit Virtual Sensor Configuration
[3] Display configuration
Option: 1

```

The following prompts let you create/delete interfaces. You can assign the interfaces to virtual sensors in the edit virtual sensor configuration section. If interfaces are monitored promiscuously and not subdivided by VLAN, no additional configuration is necessary. Proceed to virtual sensor configuration to assign interfaces to the virtual sensor.

```

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 1
Inline Vlan Pairs:
  [1] GigabitEthernet1/0:1 (Vlans: 2, 3)
  [2] GigabitEthernet1/0:2 (Vlans: 344, 23)
  [3] GigabitEthernet1/0:10 (Vlans: 20, 10)
Promiscuous Vlan Groups:
  [4] GigabitEthernet1/1:3 (Vlans: 5-7,9)
Inline Interface Pair Vlan Groups:
  [5] foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
  [6] foo:8 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 300-399)
Remove Interface: 6
Remove Interface:

```

```

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.

```

```
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 2
```

```
Available Interfaces
  [1] GigabitEthernet1/0
  [2] GigabitEthernet2/1
  [3] GigabitEthernet4/0
  [4] GigabitEthernet4/1
Interface to modify: 2
Inline Vlan Pairs for GigabitEthernet2/1:
  None
Subinterface number: 1
Description[Created via setup by user cisco]:
Vlan1: 5
Vlan2: 6
Subinterface number:
Available Interfaces
  [1] GigabitEthernet1/0
  [2] GigabitEthernet2/1
  [3] GigabitEthernet4/0
  [4] GigabitEthernet4/1
Interface to modify:
```

```
[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 3
```

```
Available Interfaces
  [1] GigabitEthernet1/1
  [2] GigabitEthernet4/0
  [3] GigabitEthernet4/1
Interface to modify: 1
Promiscuous Vlan Groups for GigabitEthernet1/1:
  GigabitEthernet1/1:3 (Vlans: 5-7,9)
Subinterface number: 1
Description[Created via setup by user cisco]:
Vlans: 3,8,34-69
Subinterface number:
Available Interfaces
  [1] GigabitEthernet1/1
  [2] GigabitEthernet4/0
  [3] GigabitEthernet4/1
Interface to modify:
```

```
[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 4
```

```
Available Interfaces
  GigabitEthernet4/0
  GigabitEthernet4/1
```

```

Pair Name: test
Description[Created via setup by user cisco]:
Interface1: GigabitEthernet4/0
Interface2: GigabitEthernet4/1

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 5

Available inline interface pairs:
  [1] foo (GigabitEthernet3/0, GigabitEthernet3/1)
  [2] test (GigabitEthernet4/0, GigabitEthernet4/1)
Interface to modify: 1
Inline Interface Pair Vlan Groups for foo:
  Subinterface: 3; Vlans: 200-299
Subinterface number: 1
Description[Created via setup by user cisco]:
Vlans: 100-199
Subinterface number:
Available inline interface pairs:
  [1] foo (GigabitEthernet3/0, GigabitEthernet3/1)
  [2] test (GigabitEthernet4/0, GigabitEthernet4/1)
Interface to modify:

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 6

GigabitEthernet0/0 default-vlan[0]:
GigabitEthernet1/0 default-vlan[0]:
GigabitEthernet1/1 default-vlan[0]:
GigabitEthernet2/0 default-vlan[0]:
GigabitEthernet2/1 default-vlan[0]:
GigabitEthernet3/0 default-vlan[0]: 100
GigabitEthernet3/1 default-vlan[0]: 100
GigabitEthernet4/0 default-vlan[0]:
GigabitEthernet4/1 default-vlan[0]:

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option:

[1] Edit Interface Configuration
[2] Edit Virtual Sensor Configuration
[3] Display configuration
Option: 3

Current interface configuration
Command control GigabitEthernet0/1
Unassigned:
Promiscuous:
  GigabitEthernet2/1

```



```

Inline Vlan Pairs:
  GigabitEthernet1/0:10 (Vlans: 20, 10)
Promiscuous Vlan Groups:
GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
Inline Interface Pairs:
  test (GigabitEthernet4/0, GigabitEthernet4/1)
Inline Interface Pair Vlan Groups:
  foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
Promiscuous:
  GigabitEthernet0/0
Inline Vlan Pairs:
  GigabitEthernet1/0:1 (Vlans: 2, 3)
  GigabitEthernet1/0:2 (Vlans: 344, 23)

Virtual Sensor: myVs
  Anomaly Detection: myAd
  Event Action Rules: myEvr
  Signature Definition: mySigs
Promiscuous:
  GigabitEthernet2/0
Promiscuous Vlan Groups:
  GigabitEthernet1/1:3 (Vlans: 5-7,9)
Inline Interface Pair Vlan Groups:
  foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)

[1] Edit Interface Configuration
[2] Edit Virtual Sensor Configuration
[3] Display configuration
Option: 2

[1] Remove virtual sensor.
[2] Modify "vs0" virtual sensor configuration.
[3] Modify "myVs" virtual sensor configuration.
[4] Create new virtual sensor.
Option: 1

Virtual sensors
  [1] vs0
  [2] myVs
Remove: 2
Remove:

[1] Remove virtual sensor.
[2] Modify "vs0" virtual sensor configuration.
[3] Create new virtual sensor.
Option: 2

Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
Promiscuous:
  GigabitEthernet0/0
Inline Vlan Pairs:
  [1] GigabitEthernet1/0:1 (Vlans: 2, 3)
  [2] GigabitEthernet1/0:2 (Vlans: 344, 23)
Remove Interface: 2
Remove Interface:

Unassigned:

```

```

Promiscuous:
  [1] GigabitEthernet2/1
  [2] GigabitEthernet2/0
Inline Vlan Pairs:
  [3] GigabitEthernet1/0:2 (Vlans: 344, 23)
  [4] GigabitEthernet1/0:10 (Vlans: 20, 10)
Promiscuous Vlan Groups:
  [5] GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
  [6] GigabitEthernet1/1:3 (Vlans: 5-7,9)
Inline Interface Pairs:
  [7] test (GigabitEthernet4/0, GigabitEthernet4/1)
Inline Interface Pair Vlan Groups:
  [8] foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
  [9] foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
Add Interface: 4
Add Interface:

```

Current interface configuration

```

Command control GigabitEthernet0/1
Unassigned:
Promiscuous:
  GigabitEthernet2/0
  GigabitEthernet2/1
Inline Vlan Pairs:
  GigabitEthernet1/0:2 (Vlans: 344, 23)
Promiscuous Vlan Groups:
  GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
  GigabitEthernet1/1:3 (Vlans: 5-7,9)
Inline Interface Pairs:
  test (GigabitEthernet4/0, GigabitEthernet4/1)
Inline Interface Pair Vlan Groups:
  foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
  foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)

```

Virtual Sensor: vs0

```

Anomaly Detection: ad0
Event Action Rules: rules0
Signature Definitions: sig0
Promiscuous:
  GigabitEthernet0/0
Inline Vlan Pairs:
  GigabitEthernet1/0:1 (Vlans: 2, 3)
  GigabitEthernet1/0:10 (Vlans: 20, 10)

```

```

[1] Remove virtual sensor.
[2] Modify "myVs" virtual sensor configuration.
[3] Create new virtual sensor.
Option: 3
Name: newVs
Description[Created via setup by user cisco]:
Anomaly Detection Configuration:
  [1] ad0
  [2] myAd
  [3] Create a new anomaly detection configuration
Option[3]: 2
Signature Definition Configuration:
  [1] sig0
  [2] mySigs
  [3] Create new signature definition configuration
Option[3]: 2
Event Action Rules Configuration:
  [1] rules0
  [2] myEvr

```

```

[3] newRules
[4] Create new event action rules configuration
Option[4]: 2
Unassigned:
  Promiscuous:
    [1] GigabitEthernet2/0
    [2] GigabitEthernet2/1
  Inline Vlan Pairs:
    [3] GigabitEthernet1/0:1 (Vlans: 2, 3)
  Promiscuous Vlan Groups:
    [4] GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
    [5] GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pairs:
    [6] test (GigabitEthernet4/0, GigabitEthernet4/1)
  Inline Interface Pair Vlan Groups:
    [7] foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
    [8] foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
Add Interface: 1
Add Interface: 2
Add Interface:

```

```

Current interface configuration
Command control GigabitEthernet0/1
Unassigned:
  Inline Vlan Pairs:
    GigabitEthernet1/0:1 (Vlans: 2, 3)
  Promiscuous Vlan Groups:
    GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
    GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pairs:
    test (GigabitEthernet4/0, GigabitEthernet4/1)
  Inline Interface Pair Vlan Groups:
    foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
    foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)

```

```

Virtual Sensor: vs0
Anomaly Detection: ad0
Event Action Rules: rules0
Signature Definitions: sig0
Promiscuous:
  GigabitEthernet0/0
  Inline Vlan Pairs:
    GigabitEthernet1/0:1 (Vlans: 2, 3)
    GigabitEthernet1/0:2 (Vlans: 344, 23)
    GigabitEthernet1/0:10 (Vlans: 20, 10)

```

```

Virtual Sensor: newVs
Anomaly Detection: myAd
Event Action Rules: newRules
Signature Definition: mySigs
Promiscuous:
  GigabitEthernet2/0
  GigabitEthernet2/1

```

```

[1] Remove virtual sensor.
[2] Modify "vs0" virtual sensor configuration.
[3] Modify "newVs" virtual sensor configuration.
[4] Create new virtual sensor.
Option:

```

```

[1] Edit Interface Configuration
[2] Edit Virtual Sensor Configuration
[3] Display configuration
Option:

```

```

Modify default threat prevention settings? [no] yes
  Virtual sensor vs0 is NOT configured to prevent a modified range of threats in inline
  mode. (Risk Rating 75-100)
  Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
  Rating 90-100)

```

```

Do you want to enable automatic threat prevention on all virtual sensors? [no]

```



Note If you answer yes to the above question, the next question is not displayed.



Note If all virtual sensors are enabled, only the disable question is displayed.



Note If all virtual sensors are disabled, only the enable question is displayed.

```

Do you want to disable automatic threat prevention on all virtual sensors? [no] yes
  The Event Action "overrides" rule for action "deny-packet-inline" has been Disabled on
  all virtual sensors.

```

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 event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 75-100
exit
exit
service event-action-rules myEvr
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit
service event-action-rules newRules
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit
service interface
service event-action-rules rules0
overrides deny-packet-inline
risk-rating-range 85-100
exit
exit
service event-action-rules newRules
overrides deny-packet-inline
risk-rating-range 85-100
exit
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet1/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user cisco
vlan1 2
vlan2 3
exit
subinterface 2
description Created via setup by user cisco
vlan1 344
vlan2 23
exit
subinterface 10
description Created via setup by user cisco
vlan1 20
vlan2 10
exit
exit
exit
physical-interfaces GigabitEthernet1/1
subinterface-type vlan-group
subinterface 3
description Created via setup by user cisco
vlans 5-7,9
exit
subinterface 1
description Created via setup by user cisco
vlans 3,8,34-39
```

```

exit
exit
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
physical-interfaces GigabitEthernet3/0
default-vlan 100
exit
physical-interfaces GigabitEthernet3/1
default-vlan 100
exit
inline-interface foo
description Create via setup by user cisco
interface1 GigabitEthernet3/0
interface2 GigabitEthernet3/1
subinterface-type vlan-group
subinterface 3
vlans 200-299
exit
subinterface 1
vlans 100-199
exit
exit
exit
inline-interface test
description Created via setup by user cisco
interface1 GigabitEthernet4/0
interface2 GigabitEthernet4/1
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet1/0 subinterface-number 2
physical-interface GigabitEthernet1/0 subinterface-number 10
exit
virtual-sensor newVs
anomaly-detection myAd
event-action-rulse newRules
signature-definition mySigs
physical-interface GigabitEthernet2/0
physical-interface GigabitEthernet2/1
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 ad-knowledge-base diff

To display the difference between two KBs, use the **show ad-knowledge-base diff** command in privileged EXEC mode.

```
show ad-knowledge-base virtual-sensor diff [current | initial | file name1][current | initial | file
name2] diff-percentage
```

Syntax Description		
<i>virtual-sensor</i>		The virtual sensor containing the KB files to compare. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, "-", and "_".
<i>name1</i>		The name of the first existing KB file to compare. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, "-", and "_".
<i>name2</i>		The name of the second existing KB file to compare. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, "-", and "_".
current		The currently loaded KB.
initial		The initial KB.
file		An existing KB file.
<i>diff-percentage</i>		(Optional) Displays services where the thresholds differ more than the specified percentage. The valid values are 1 to 100. The default is 10%.

Defaults See Syntax Description table.

Command Modes EXEC

Supported User Roles Administrator, Operator, Viewer

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples The following example compares 2006-Mar-16-10_00_00 with the currently loaded KB for virtual sensor vs0:

```
sensor# show ad-knowledge-base vs0 diff current file 2006-Mar-16-10_00_00
2006-Mar-17-10_00_00 Only Services/Protocols
  External Zone
    TCP Services
      Service = 30
      Service = 20
    UDP Services
      None
    Other Protocols
      Protocol = 1
  Illegal Zone
    None
  Internal Zone
    None
2006-Mar-16-10_00_00 Only Services/Protocols
  External Zone
    None
  Illegal Zone
    None
  Internal Zone
    None
Thresholds differ more than 10%
  External Zone
    None
  Illegal Zone
    TCP Services
      Service = 31
      Service = 22
    UDP Services
      None
    Other Protocols
      Protocol = 3
  Internal Zone
    None
sensor#
```


show ad-knowledge-base files

To display the anomaly detection KB files available for a virtual sensor, use the **show ad-knowledge-base files** command in privileged EXEC mode.

show ad-knowledge-base *virtual-sensor* **files**

Syntax Description	<i>virtual-sensor</i>	(Optional) The virtual sensor containing the KB file. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, "-", and "_."
---------------------------	-----------------------	--

Defaults No default behavior or values.

Command Modes EXEC

SupportedUserRoles Administrator, Operator, Viewer

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines The * before the filename indicates the KB file that is currently loaded. The current KB always exists (it is the initial KB after installation). It shows the currently loaded KB in the AD, or the one that is loaded if the AD is currently not active.

If you do not provide the virtual sensor, all KB files are retrieved for all virtual sensors.

The initial KB is a KB with factory-configured thresholds.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples The following example displays the KB files available for all virtual sensors. The file 2006-Mar-16-10_00_00 is the current KB file loaded for virtual sensor vs0.

```

sensor# show ad-knowledge-base files
Virtual Sensor vs0
  Filename           Size   Created
  initial            84    04:27:07 CDT Wed Jan 28 2006
* 2006-Jan-29-10_00_01 84    04:27:07 CDT Wed Jan 29 2006
  2006-Mar-17-10_00_00 84    10:00:00 CDT Fri Mar 17 2006
  2006-Mar-18-10_00_00 84    10:00:00 CDT Sat Mar 18 2006
sensor#

```

show ad-knowledge-base thresholds

To display the thresholds for a KB, use the **show ad-knowledge-base thresholds** command in privileged EXEC mode.

```
show ad-knowledge-base virtual-sensor thresholds { current | initial | file name } [zone { external | illegal | internal }] { [protocol { tcp | udp }] [dst-port port] | [protocol other] [number protocol-number] }
```

Syntax Description

<i>virtual-sensor</i>	The virtual sensor containing the KB files to compare. This is a case-sensitive character string containing 1 to 64 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
current	The currently loaded KB.
initial	The initial KB.
file	An existing KB file.
<i>name</i>	The KB filename. This is a case-sensitive character string containing up to 32 characters. Valid characters are A-Z, a-z, 0-9, “-” and “_.”
zone	(Optional) Only displays thresholds for the specified zone. The default displays information about all zones.
external	Displays the external zone.
illegal	Displays the illegal zone.
internal	Displays the internal zone.
protocol	(Optional) Only displays thresholds for the specified protocol. The default displays information about all protocols.
tcp	Displays the TCP protocol.
udp	Displays the UDP protocol.
dst-port	(Optional) Only displays thresholds for the specified port. The default displays information about all TCP and/or UDP ports.
<i>port</i>	(Optional) Only displays thresholds for the specified port. The default displays information about all TCP and/or UDP ports. The valid values are 0 to 65535.
number	(Optional) Only displays thresholds for the specific other protocol number. The default displays information about all other protocols.
other	Display other protocols besides TCP or UDP.
<i>protocol-number</i>	The protocol number. The valid values are 0 to 255.

Defaults

See the Syntax Description table for default values.

Command Modes

EXEC

Supported User Roles

Administrator, Operator, Viewer

Command History

Release	Modification
6.0(1)	This command was introduced.

Examples

The displayed thresholds are the thresholds contained in the KB. For thresholds where overriding user configuration exists, both knowledge-based thresholds and user configuration are displayed.



Note This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.

Examples

The following example displays thresholds contained in the KB 2006-Mar-16-10_00_00 illegal zone:

```

sensor# show ad-knowledge-base vs0 thresholds file 2006-Mar-16-10_00_00 zone illegal
2006-Mar-16-10_00_00
  Illegal Zone
    TCP Port 20
      Scanner Threshold
        >> User Configuration = 100
        >> Knowledge Base = 20
      Threshold Histogram
        Destination IP           5   10   100
        >> User Configuration: source IP 100 1   0
        >> Knowledge Base: source IP   10 1   0
    TCP Port 30
      Scanner Threshold
        Knowledge Base = 110
      Threshold Histogram
        Destination IP           5   10   100
        Knowledge Base: source IP 10 1   0
    TCP Port any
      Scanner Threshold
        Knowledge Base = 9
      Threshold Histogram
        Destination IP           5   10   100
        Knowledge Base: source IP 2 1   0
    UDP Port any
      Scanner Threshold
        Knowledge Base = 19
      Threshold Histogram
        Destination IP           5   10   100
        Knowledge Base: source IP 12 10  0
    Other Protocol any
      Scanner Threshold
        Knowledge Base = 1
      Threshold Histogram
        Destination IP           5   10   100
        Knowledge Base: source IP 1 1   0
    Other Protocol 1
      Scanner Threshold
        Knowledge Base = 10
      Threshold Histogram
        Destination IP           5   10   100
        Knowledge Base: source IP 10 10  0
sensor#

```

The following example displays thresholds contained in the current KB illegal zone, protocol TCP, and destination port 20:

```

sensor# show ad-knowledge-base vs0 thresholds current zone illegal protocol tcp dst-port
20
2006-Mar-16-10_00_00
  Illegal Zone
    TCP Port 20
      Scanner Threshold
        >> User Configuration = 100
        >> Knowledge Base = 50
      Threshold Histogram
        Destination IP           5    10    100
        >> User Configuration: source IP 100 1    0
        >> Knowledge Base: source IP    10 1    0
sensor#

```

The following example displays thresholds contained in the current KB illegal zone, protocol other, and protocol number 1.

```

sensor# show ad-knowledge-base vs0 thresholds current zone illegal protocol other number 1
2006-Mar-16-10_00_00
  Illegal Zone
    Other Protocol 1
      Scanner Threshold
        >> User Configuration = 79
        >> Knowledge Base = 50
      Threshold Histogram
        Destination IP           5    10    100
        >> User Configuration: source IP 100 5    0
        >> Knowledge Base: source IP    12 1    0
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

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 begin extension of the show command was added.
5.1(1)	Added tech-support 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
more begin	Searches the output of the more command and displays the output from the first instance of a specified string.
more exclude	Filters the more command output so that it excludes lines that contain a particular regular expression.
more include	Filters the more command output so that it displays only lines that contain a particular regular expression.
show exclude	Filters the show command output so that it excludes lines that contain a particular regular expression.
show include	Filters the show 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]

Syntax Description	detail	(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

Command History	Release	Modification
	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 1-2](#) shows the authoritative flags.

Table 1-2 Authoritative Flags

Symbol	Description
*	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] [min-threat-rating min-rr] [max-threat-rating max-rr] | error [warning] [error] [fatal]
| NAC | status}] [hh:mm:ss [month day [year]]] | past hh:mm:ss
```

Syntax Description

alert	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.
include-traits	Displays alerts that have the specified <i>traits</i> .
exclude-traits	Does not display alerts that have the specified <i>traits</i> .
<i>traits</i>	Trait bit position in decimal (0-15).
min-threat-rating	Displays events with a threat rating above or equal to this value. The valid range is 0 to 100. The default is 0.
max-threat-rating	Displays events with a threat rating below or equal to this value. The valid range is 0 to 100. The default is 100.
error	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.
NAC	Displays ARC requests (block requests). 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 6.0 CLI. You will still see network-access and nac throughout the CLI.
status	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).
past	Displays events starting in the past. The <i>hh:mm:ss</i> specify a time in the past to begin the display.

Defaults

See the Syntax Description table for the default values.

Command Modes

EXEC

Supported User Roles

Administrator, Operator, Viewer

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(2)	Ability to select multiple error event levels simultaneously was added.
4.1(1)	Added include-traits , exclude-traits , and past options.
6.0(1)	Added min-threat-rating and max-threat-rating options.

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 is IPS-specific. There is no related IOS command in version 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 show 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 exclude extension of the show command was added.
5.1(1)	Added tech-support 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
more begin	Searches the output of the more command and displays the output from the first instance of a specified string.
more exclude	Filters the more command output so that it excludes lines that contain a particular regular expression.
more include	Filters the more command output so that it displays only lines that contain a particular regular expression.
show begin	Searches the output of certain show commands and displays the output from the first instance of a specified string.
show include	Filters the show 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.
<i>regular-expression</i>	Any regular expression found in show 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 include extension of the show command was added.
5.1(1)	Added tech-support 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
more begin	Searches the output of the more command and displays the output from the first instance of a specified string.
more exclude	Filters the more command output so that it excludes lines that contain a particular regular expression.
more include	Filters the more command output so that it displays only lines that contain a particular regular expression.

Command	Description
show begin	Searches the output of certain show commands and displays the output from the first instance of a specified string.
show exclude	Filters the show 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] [brief]
```

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

Syntax Description

clear	(Optional) Clears the diagnostics.
brief	(Optional) Displays a summary of the usability status information for each interface.
FastEthernet	Displays the statistics for FastEthernet interfaces.
GigabitEthernet	Displays the statistics for GigabitEthernet interfaces.
Management	Displays the statistics for the Management interface. Note Only platforms with external ports marked as Management support this keyword. The management interface for the remaining platforms is displayed in the show interfaces 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

Supported User Roles

Administrator, Operator, Viewer

Command History

Release	Modification
5.0(1)	The show interfaces group , show interfaces sensing , and show interfaces command-control commands were removed. The show interfaces FastEthernet , show interfaces GigabitEthernet , and show interfaces Management commands were added.
6.0(1)	The brief keyword was added.

Usage Guidelines

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

Using this command with an interface type displays statistics for all interfaces of that type. Adding the slot and/or port number displays the statistics for that particular interface.

An * next to an entry indicates the interface is the command and control interface.

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--

```

The following example shows the brief output for interface statistics:

```

sensor# show interfaces brief
CC  Interface          Sensing State  Link  Inline Mode  Pair Status
   GigabitEthernet0/0  Enabled       Up    Unpaired    N/A
*   GigabitEthernet0/1  Enabled       Up    Unpaired    N/A
   GigabitEthernet2/1  Disabled     Up    Subdivided  N/A
sensor#
#

```

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 os-identification

To display OS IDs associated with IP addresses learned by the sensor through passive analysis, use the **show os-identification** command in privileged EXEC mode.

```
show os-identification [name] learned [ip-address]
```

Syntax Description	
<i>name</i>	(Optional) The name of the virtual sensor configured on the sensor. The show operation is restricted to learned IP addresses associated with the identified virtual sensor.
<i>ip-address</i>	(Optional) The IP address to query. The sensor reports the OS ID mapped to the specified IP address.

Defaults No defaults or values.

Command Modes EXEC

SupportedUserRoles Administrator, Operator, Viewer

Command History	Release	Modification
	6.0(1)	This command was introduced.

Usage Guidelines The IP address and virtual sensor are optional. If you specify an IP address, only the OS identification for the specified IP address is reported. Otherwise, all learned OS identifications are reported.

If you specify a virtual sensor, only the OS identification for the specified virtual sensor is displayed; otherwise, the learned OS identifications for all virtual sensors are displayed. If you specify an IP address without a virtual sensor, the output displays all virtual sensors containing the requested IP address.

Examples The following example displays the OS identification for a specific IP address:

```
sensor# show os-identification learned 10.1.1.12
Virtual Sensor vs0:
  10.1.1.12 windows
```

The following example displays the OS identification for all virtual sensors:

```
sensor# show os-identification learned
Virtual Sensor vs0:
  10.1.1.12 windows
Virtual Sensor vs1:
  10.1.0.1  unix
  10.1.0.2  windows
  10.1.0.3  windows
```

```
sensor#
```

Related Commands

Command	Description
show statistics os-identification	Displays the statistics for OS IDs.
clear os-identification	Delete OS ID associations with IP addresses that were learned by the sensor through passive analysis.

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
	username	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]


Syntax Description	terse	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)

Command History	Release	Modification
	4.0(1)	
	4.0(2)	Added the terse keyword.

Usage Guidelines  **Note** This command is IPS-specific. There is no related IOS command in version 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 6.0 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]
```

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

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	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.
-------------------------	---



Note	This command is IPS-specific. There is no related IOS command in version 12.0 or earlier.
-------------	---

Examples

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

Command	Description
ssh authorized-key	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 **Note** This command is IPS-specific. There is no related IOS command in version 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]
```

Syntax Description	<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.



Note This command is IPS-specific. There is no related IOS command in version 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 | event-server | event-store |
external-product-interface | host | logger | network-access | notification | sdee-server |
transaction-server | web-server} [clear]
```

The **show statistics anomaly-detection**, **denied-attackers**, **virtual-sensor**, and **os-identification** commands display statistics for all the virtual sensors contained in the sensor. If you provide the optional name, the statistics for that virtual sensor are displayed.

```
show statistics {anomaly-detection | denied-attackers | os-identification | virtual-sensor}
[name] [clear]
```

Syntax Description		
clear	Clears the statistics after they are retrieved.	Note This option is not available for analysis engine, anomaly detection, host, OS identification, or network access statistics.
analysis-engine	Displays analysis engine statistics.	
anomaly-detection	Displays anomaly detection statistics.	
authentication	Displays authorization authentication statistics.	
denied-attackers	Displays the list of denied IP addresses and the number of packets from each attacker.	
event-server	Displays event server statistics.	
event-store	Displays event store statistics.	
external-product-interface	Displays external product interface statistics.	
host	Displays host (main) statistics.	
logger	Displays logger statistics.	
network-access	Displays ARC statistics.	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 6.0 CLI. You will still see network-access and nac throughout the CLI.
notification	Displays notification statistics.	
os-identification	Displays the OS identification statistics.	
sdee-server	Displays SDEE server statistics.	
transaction-server	Displays transaction server statistics.	
web-server	Displays web server statistics.	
virtual-sensor	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)	Added analysis-engine , virtual-sensor , and denied-attackers .
	6.0(1)	Added anomaly-detection , external-product-interface , and os-identification .



Usage Guidelines **Note** This command is IPS-specific. There is no related IOS command in version 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**] [**destination-url** *destination url*]

Syntax Description		
page	(Optional) Causes the output to display one page of information at a time. Press Enter to display the next line of output or use the spacebar to display the next page of information. If page is not used, the output is displayed without page breaks.	
destination-url	(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.
	6.0(1)	Removed the password option. Passwords are displayed encrypted.



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. The following valid types are supported:

Prefix	Source or Destination
ftp:	Destination URL for the FTP network server. The syntax for this prefix is: ftp://[username@] location[/relativeDirectory]/filename ftp://[username@]location//absoluteDirectory]/filename
scp:	Destination URL for the SCP network server. The syntax for this prefix is: scp://[username@] location[/relativeDirectory]/filename 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 **Note** This command is IPS-specific. There is no related IOS command in version 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]
```

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

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	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.
-------------------------	--



Note	This command is IPS-specific. There is no related IOS command in version 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#
```

Related Commands	Command	Description
	tls trusted-host	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	all	(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 show users all .

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
clear line	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 6.0(0.2)S184.0

Host:
  Realm Keys          key1.0
Signature Definition:
```

show version

```
Signature Update      S184.0                2005-11-09
OS Version:           2.4.30-IDS-smp-bigphys
Platform:              ASA-SSM-20
Serial Number:         021
No license present
```

```
Using 546975744 out of 2115760128 bytes of available memory (25% usage)
```

```
MainApp      2005_Nov_16_05.00  (Release)  2005-11-16T05:54:13-0600  Running
AnalysisEngine  2005_Nov_16_05.00  (Release)  2005-11-16T05:54:13-0600  Running
CLI          2005_Nov_16_05.00  (Release)  2005-11-16T05:54:13-0600
```

Upgrade History:

```
IPS-K9-maj-6.0-0.2  05:00:00 UTC Wed Nov 16 2005
```

```
Recovery Partition Version /var/idstmp
```

```
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 ³²].
<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)#
```

Related Commands

Command	Description
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.



Note This command is IPS-specific. There is no related IOS command in version 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-rukuh-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 ³²].
<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.



Note This command is IPS-specific. There is no related IOS command in version 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

SupportedUserRoles 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 **Note** This command is IPS-specific. There is no related IOS command in version 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
	show tls fingerprint	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 no 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 is IPS-specific. There is no related IOS command in version 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*

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

Defaults No default behavior or values.

Command Modes Global configuration

SupportedUserRoles Administrator

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

Usage Guidelines From the command line, you can enter all necessary source and destination URL information and the username. If you enter 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.

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

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

<i>name</i>	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.
<i>password</i>	Specifies the password for the user. A valid password is 8 to 32 characters in length. All characters except space are allowed.
<i>privilege</i>	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

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