Administrative Tasks for the Sensor

This chapter contains procedures that will help you with the administrative aspects of your sensor. It contains the following sections:

- Administrative Notes and Caveats, page 17-2
- Recovering the Password, page 17-2
- Clearing the Sensor Databases, page 17-10
- Displaying and Deleting SDEE Server Subscriptions, page 17-11
- Displaying the Inspection Load of the Sensor, page 17-12
- Configuring Health Status Information, page 17-14
- Showing Sensor Overall Health Status, page 17-19
- Creating a Banner Login, page 17-20
- Terminating CLI Sessions, page 17-20
- Modifying Terminal Properties, page 17-21
- Configuring Events, page 17-22
- Configuring the System Clock, page 17-25
- Clearing the Denied Attackers List, page 17-27
- Displaying Policy Lists, page 17-29
- Displaying Statistics, page 17-30
- Displaying Tech Support Information, page 17-42
- Displaying Version Information, page 17-43
- Diagnosing Network Connectivity, page 17-45
- Resetting the Appliance, page 17-46
- Displaying Command History, page 17-47
- Displaying Hardware Inventory, page 17-48
- Tracing the Route of an IP Packet, page 17-50
- Displaying Submode Settings, page 17-51

Administrative Notes and Caveats

The following notes and caveats apply to administrative tasks for the sensor:

- Administrators may need to disable the password recovery feature for security reasons.
- If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimage your sensor.
- We do not recommend that you use **clear database** command unless under the direction of TAC or in some testing conditions when you need to clear accumulated state information and start with a clean database.
- The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.
- When the sensor is first starting, it is normal for certain health metric statuses to be red until the sensor is fully up and running.
- You do not need to set the system clock if your sensor is synchronized by a valid outside timing mechanism such as an NTP clock source.
- The **show inventory** command does not apply to the ASA 5500-X IPS SSP and ASA 5585-X IPS SSP.

Recovering the Password

This section describes how to recover the password for the various IPS platforms. It contains the following topics:

- Understanding Password Recovery, page 17-2
- Recovering the Password for the Appliance, page 17-3
- Recovering the Password for the ASA 5500-X IPS SSP, page 17-4
- Recovering the Password for the ASA 5585-X IPS SSP, page 17-6
- Disabling Password Recovery, page 17-8
- Verifying the State of Password Recovery, page 17-9
- Troubleshooting Password Recovery, page 17-9

Understanding Password Recovery

Note Administrators may need to disable the password recovery feature for security reasons.

Password recovery implementations vary according to IPS platform requirements. Password recovery is implemented only for the cisco administrative account and is enabled by default. The IPS administrator can then recover user passwords for other accounts using the CLI. The cisco user password reverts to **cisco** and must be changed after the next login.

Table 17-1 lists the password recovery methods according to platform.

Table 17-1 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4300 series sensors 4500 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
ASA 5500-X IPS SSP ASA 5585-X IPS SSP	ASA 5500 series adaptive security appliance IPS modules	Adaptive security appliance CLI command

Recovering the Password for the Appliance

This section describes the two ways to recover the password for appliances. It contains the following topics:

- Using the GRUB Menu, page 17-3
- Using ROMMON, page 17-4

Using the GRUB Menu

Note You must have a terminal server or direct serial connection to the appliance to use the GRUB menu to recover the password.

For the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance to see the GRUB menu.

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
------------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
------------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **`2: Cisco IPS Clear Password (cisco)`**. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Using ROMMON

For the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL, you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

Note After recovering the password, you must reset the confreg to **0**, otherwise, when you try to upgrade the sensor, the upgrade fails because when the sensor reboots, it goes to password recovery (**confreg 0x7**) rather than to the upgrade option.

To recover the password using the ROMMON CLI, follow these steps:

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection). The boot code either pauses for 10 seconds or displays something similar to one of the following:

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

Step 3 Enter the following commands to reset the password:

```
confreg 0x7
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4360-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Step 4 Enter the following command to reset the confreg value to 0:

```
confreg 0
```

Recovering the Password for the ASA 5500-X IPS SSP

You can reset the password to the default (**cisco**) for the ASA 5500-X IPS SSP using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Note To reset the password, you must have ASA 8.6.1 or later.

Use the **sw-module module ips password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

To reset the password on the ASA 5500-X IPS SSP, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command:

```
asa# sw-module module ips password-reset
Reset the password on module ips? [confirm]
```

Step 2 Press **Enter** to confirm.

```
Password-Reset issued for module ips.
```

Step 3 Verify the status of the module. Once the status reads `Up`, you can session to the ASA 5500-X IPS SSP.

```
asa# show module ips
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
ips ASA 5555-X IPS Security Services Processor   ASA5555-IPS        FCH151070GR

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
ips 503d.e59c.7c4c to 503d.e59c.7c4c  N/A          N/A          7.2(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
ips IPS                            Up               7.2(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up

Mod License Name   License Status  Time Remaining
--- -------------- --------------- ---------------
ips IPS Module     Enabled         210 days
```

Step 4 Session to the ASA 5500-X IPS SSP.

```
asa# session ips
Opening command session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-^X'.
```

Step 5 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 6 Enter your new password twice.

```
New password: new password
Retype new password: new password
```

```
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.

asa-ssp#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Recovering the Password for the ASA 5585-X IPS SSP

Note To reset the password, you must have ASA 8.2.(4.4) or later or ASA 8.4.2 or later. The ASA 5585-X IPS SSP is not supported in ASA 8.3(*x*).

You can reset the password to the default (**cisco**) for the ASA 5585-X IPS SSP using the CLI or the ASDM. Resetting the password causes it to reboot. IPS services are not available during a reboot.

Use the **hw-module module** *slot_number* **password-reset** command to reset the password to the default **cisco**. If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

To reset the password on the ASA 5585-X IPS SSP, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command:

```
asa# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm]
```

Step 2 Press **Enter** to confirm.

```
Password-Reset issued for slot 1.
```

Step 3 Verify the status of the module. Once the status reads `Up`, you can session to the ASA 5585-X IPS SSP.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5585-X IPS Security Services Processor-4 ASA5585-SSP-IPS40  JAF1436ABSG

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 5475.d029.8c74 to 5475.d029.8c7f  0.1          2.0(12)3     7.2(1)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.2(1)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Step 4 Session to the ASA 5585-X IPS SSP.

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 5 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

You are required to change your password immediately (password aged)
Changing password for cisco.
(current) password: cisco
```

Step 6 Enter your new password twice.

```
New password: new password
Retype new password: new password

***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.
```

```
***LICENSE NOTICE***
There is no license key installed on this IPS platform. The system will continue to
operate with the currently installed signature set. A valid license must be obtained in
order to apply signature updates. Please go to http://www.cisco.com/go/license to obtain a
new license or install a license.
ips_ssp#
```

Using the ASDM

To reset the password in the ASDM, follow these steps:

Step 1 From the ASDM menu bar, choose **Tools > IPS Password Reset**.

Note This option does not appear in the menu if there is no IPS present.

Step 2 In the IPS Password Reset confirmation dialog box, click **OK** to reset the password to the default (**cisco**). A dialog box displays the success or failure of the password reset. If the reset fails, make sure you have the correct ASA and IPS software versions.

Step 3 Click **Close** to close the dialog box. The sensor reboots.

Disabling Password Recovery

Caution If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimage your sensor.

Password recovery is enabled by default. You can disable password recovery through the CLI, IDM, or IME.

Disabling Password Recovery Using the CLI

To disable password recovery in the CLI, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

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

Step 4 Disable password recovery.

```
sensor(config-hos)# password-recovery disallowed
```

Disabling Password Recovery Using the IDM or IME

To disable password recovery in the IDM or IME, follow these steps:

Step 1 Log in to the IDM or IME using an account with administrator privileges.

Step 2 Choose **Configuration > *sensor_name* > Sensor Setup > Network**.

Step 3 To disable password recovery, uncheck the **Allow Password Recovery** check box.

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled.

To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

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

Step 3 Verify the state of password recovery by using the **include** keyword to show settings in a filtered output.

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

Troubleshooting Password Recovery

When you troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If you attempt password recovery, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as ROMMON, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.

Clearing the Sensor Databases

Caution We do not recommend that you use **clear database** command unless under the direction of TAC or in some testing conditions when you need to clear accumulated state information and start with a clean database.

Use the **clear database** [*virtual-sensor*] **all | nodes | alerts | inspectors** command in privileged EXEC mode to clear specific parts of the sensor database. The **clear database** command is useful for troubleshooting and testing.

The following parameters apply:

- *virtual-sensor*—Specifies the name of a virtual sensor configured on the sensor.
- **all**— Clears all nodes, inspectors, and alerts databases.

Caution This command causes summary alerts to be discarded.

- **nodes**—Clears the overall packet database elements, including the packet nodes, TCP session information, and inspector lists.
- **alerts**—Clears the alert database including the alerts nodes, Meta inspector information, summary state, and event count structures.
- **inspectors**—Clears the inspector lists in the nodes. Inspector lists represent the packet work and observations collected during the time the sensor is running.

Clearing the Sensor Database

To clear the sensor database, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Clear the entire sensor database.

```
sensor# clear database all
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

Step 3 Enter **yes** to clear all the databases on the sensor.

Step 4 Clear the packet nodes.

```
sensor# clear database nodes
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

Step 5 Enter **yes** to clear the packet nodes database.

Step 6 Clear the alerts database on a specific virtual sensor.

```
sensor# clear database vs0 alerts
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

Step 7 Enter **yes** to clear the alerts database.

Step 8 Clear inspector lists on the sensor.

```
sensor# clear database inspectors
```

```
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

Step 9 Enter **yes** to clear the inspectors database.

Displaying and Deleting SDEE Server Subscriptions

Note Support for SDEE subscription is valid for IPS 7.2(2)E4 and later.

You can display the details of the SDEE client subscriptions on the sensor. You can view the SDEE subscription ID, the status (expired or valid) of the subscription, the IP address of each SDEE client for each listed subscription, and see the last time the subscription was read. The SDEE server automatically deletes SDEE subscriptions that appear to be idle or left open for 24 hours, although the timer checks for expired subscriptions every 12 hours.

To display and delete SDEE server subscriptions, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the SDEE server subscriptions.

```
sensor#  show statistics sdee-server
General
   Open Subscriptions = 3
   Blocked Subscriptions = 1
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
   sub-13-13979b85
      State = Read Pending
      IP Address = 10.142.52.151
      Last Read Time = 17:12:54 UTC Tue Jan 28 2014
      Last Read Time (nanoseconds) = 1390929174555130000
      Status = Valid
   sub-14-798ebed7
      State = Open
      IP Address = 10.142.52.127
      Last Read Time = 17:12:53 UTC Tue Jan 28 2014
      Last Read Time (nanoseconds) = 1390929173318336000
      Status = Valid
   sub-15-fb8e1c5e
      State = Open
      IP Address = 10.89.11.67
      Last Read Time = 17:12:51 UTC Tue Jan 28 2014
      Last Read Time (nanoseconds) = 1390929171920713000
      Status = Valid
sensor#
```

Step 3 Use the subscription ID to clear a specific SDEE subscription.

```
sensor# clear sdee-subscription sub-13-13979b85
Warning: Going to delete  sdee subscription id sub-13-13979b85

Continue? []:
```

Step 4 Enter **yes** to delete the subscription.

Step 5 Verify that the subscription was deleted. Subscription ID sub-13-13979b85 no longer appears in the list.

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 3
   Blocked Subscriptions = 2
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
   sub-14-798ebed7
      State = Read Pending
      IP Address = 10.142.52.127
      Last Read Time = 12:01:14 UTC Wed Jan 29 2014
      Last Read Time (nanoseconds) = 1390996874294610000
      Status = Valid
   sub-15-fb8e1c5e
      State = Open
      IP Address = 10.89.11.67
      Last Read Time = 12:01:11 UTC Wed Jan 29 2014
      Last Read Time (nanoseconds) = 1390996871880999000
      Status = Valid
   sub-16-d4220496
      State = Read Pending
      IP Address = 10.142.52.151
      Last Read Time = 12:01:14 UTC Wed Jan 29 2014
      Last Read Time (nanoseconds) = 1390996874311401000
      Status = Valid
sensor#
```

For More Information

For detailed information about the SDEE Server, see SDEE, page A-33.

Displaying the Inspection Load of the Sensor

Use the **show inspection-load** command in privileged EXEC mode to display a timestamp and the current inspection load of the sensor. Use the **history** option to display a histogram of the inspection load over the past 60 minutes and over the past 72 hours.

Use this command to determine the load on the sensor instead of the CPU Usage information from the **show statistics host** command. The inspection load is a more accurate representation of the processing level of the sensor. The calculation of the inspection load has also been enhanced to provide a more accurate calculation of the sensor load at lower traffic levels.

Note The Processing Load category in the **show statistics virtual-sensor** output has been renamed to Inspection Load and shows the same value seen in the **show inspection load** command.

Note The **show inspection-load** command is not currently supported for the IPS 4500 series sensors.

To display the inspection load of the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Show the current inspection load with a timestamp of the sensor.

```
sensor# show inspection-load

sensor 08:18:13 PM Friday Jan 15 2011 UTC

Inspection Load Percentage = 1
```

Step 3 Show the histogram of the inspection load:

```
sensor# show inspection-load history
sensor 15:36:42 UTC Mon Jan 30 2012

sensor 08:18:13 PM Friday Jan 15 2011 UTC

Inspection Load Percentage = 65


100

90

80

70 * *

60 * * *** * ****** ** * * * * * * ** ** *

50 * * *** * ****** ** * * * * * * ** ** *

40 * *** ******************** * * * * ** * * * * * ***********

30 ******************************** ************ *************

20 ************************************************************

10 ************************************************************

0.........1.........2.........3.........4.........5.........6


Inspection Load Percentage (last 6 minutes at 10 second intervals)


100

90

80

70

60 * * *** * ****** ** * * * * * * ** ** *

50 * * *** * ****** ** * * * * * * ** ** *

40 * *** *********####******** * * * * ** * * * * * ***********
```

```
30 ########*###*#######**#*****#*#* *********#*# #*##*****#####
20 ############################################################
10 ############################################################
0....5....1....1....2....2....3....3....4....4....5....5....6
          0    5    0    5    0    5    0    5    0    5    0

Inspection Load Percentage (last 60 minutes) *=maximum #=average

100
90
80
70
60 * * *** * ****** ** * * * * * * ** ** * * * *** *
50 * * *** * ****** ** * * * * * * ** ** * * * *** *
40 * *** ******************** * * * * ** * * * * * ********** * * ***
30 ********###**#######**#*****#*#* *********#*# #*#######**## #*#*###
20 ########################################################################
10 ########################################################################
0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.
          0    5    0    5    0    5    0    5    0    5    0    5    0

Inspection Load Percentage (last 72 hours) *=maximum #=average
sensor#
```

Configuring Health Status Information

Configure the health statistics for the sensor in service health monitor submode. Use the **show health** command to see the results. The health status categories are rated by red and green with red being critical.

The following parameters apply:

- **application-failure-policy {enable | disable} {true | false} status {green | yellow | red}**—Lets you choose to have an application failure applied to the overall sensor health rating.
- **bypass-policy {enable | disable} {true | false} status {green | yellow | red}**—Lets you choose to know if bypass mode is active and have that apply to the overall sensor health rating.

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

- **enable-monitoring** {**true | false**}—Lets you choose to monitor sensor health and security.
- **event-retrieval-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*—Lets you set a threshold for when the last event was retrieved and have that apply to the overall sensor health rating. The health status is degraded to red or yellow when that threshold is met. The range for the threshold is 0 to 4294967295 seconds.

Note The event retrieval metric keeps track of when the last event was retrieved by an external monitoring application such as the IME. Disable **event retrieval policy** if you are not doing external event monitoring.

- **global-correlation-policy {enable | disable} {true | false}**—Lets you apply this metric to the overall sensor health rating.
- **heartbeat-events {enable | disable}** *seconds*—Lets you enable heartbeat events to be emitted at the specified interval in seconds and have that apply to the overall sensor health rating. The range for the interval is 15 to 86400 seconds.
- **inspection-load-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*—Lets you set the threshold for inspection load. The health status is degraded to red or yellow when that threshold is met. The range is 0 to 100.
- **interface-down-policy {enable | disable} {true | false} status {green | yellow | red}**—Lets you choose to know if one or more enabled interfaces are down and have that apply to the overall sensor health rating.
- **license-expiration-policy {enable | disable} {true | false} red-threshold yellow-threshold**—Lets you set a threshold for when the license expires and whether this metric is applied to the overall sensor health rating. The range for the threshold is 0 to 4294967295 seconds.
- **memory-usage-policy {enable | disable} {true | false} red-threshold yellow-threshold**—Lets you set a threshold percentage for memory usage and whether this metric is applied to the overall sensor health rating. The range is 0 to 100. The default for red is 91% and the default for yellow is 80%.
- **missed-packet-policy {enable | disable} {true | false} red-threshold yellow-threshold**—Lets you set a threshold percentage for missed packets and whether this metric is applied to the overall sensor health rating.
- **network-participation-policy {enable | disable} {true | false}**—Lets you apply this metric to the overall sensor health rating.
- **persist-security-status**—Lets you set the number of minutes that a lower security persists following the occurrence of the latest event to lower the security status.
- **signature-update-policy {enable | disable} {true | false} red-threshold yellow-threshold**—Lets you set a threshold for the number of days elapsed since the last signature update and whether this metric is applied to the overall sensor health rating. The range for the threshold is 0 to 4294967295 seconds

ASA 5500-X IPS SSP and Memory Usage

For the ASA 5500-X IPS SSP, the memory usage is 93%. The default health thresholds for the sensor are 80% for yellow and 91% for red, so the sensor health will be shown as red on these platforms even for normal operating conditions. You can tune the threshold percentage for memory usage so that it reads more accurately for these platforms by configuring the **memory-usage-policy** option in the sensor health metrics.

Note Make sure you have the **memory-usage-policy** option in the sensor health metrics enabled.

Table 17-2 lists the yellow-threshold and red-threshold health values.

Table 17-2 ASA 5500-X IPS SSP Memory Usage Values

Platform	Yellow	Red	Memory Used
ASA 5512-X IPS SSP	85%	91%	28%
ASA 5515-X IPS SSP	88%	92%	14%
ASA 5525-X IPS SSP	88%	92%	14%
ASA 5545-X IPS SSP	93%	96%	13%
ASA 5555-X IPS SSP	95%	98%	17%

Configuring Health Statistics

To configure the health statistics for the sensor, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter service health monitor submode.

```
sensor# configure terminal
sensor(config)# service health-monitor
sensor(config-hea)#
```

Step 3 Enable the metrics for application failure status.

```
sensor(config-hea)# application-failure-policy
sensor(config-hea-app)# enable true
sensor(config-hea-app)# status red
sensor(config-hea-app)# exit
sensor(config-hea)#
```

Step 4 Enable the metrics for bypass policy.

```
sensor(config-hea)# bypass-policy
sensor(config-hea-byp)# enable true
sensor(config-hea-byp)# status yellow
sensor(config-hea-byp)# exit
sensor(config-hea)#
```

Step 5 Enable the metrics for sensor health and security monitoring.

```
sensor(config-hea)# enable-monitoring true
sensor(config-hea)#
```

Step 6 Set the event retrieval thresholds for event retrieval metrics.

```
sensor(config-hea)# event-retrieval-policy
sensor(config-hea-eve)# enable true
```

```
sensor(config-hea-eve)# red-threshold 100000
sensor(config-hea-eve)# yellow-threshold 100
sensor(config-hea-eve)# exit
sensor(config-hea)#
```

Step 7 Enable health metrics for global correlation.

```
sensor(config-hea)# global-correlation-policy
sensor(config-hea-glo)# enable true
sensor(config-hea-glo)# exit
sensor(config-hea)#
```

Step 8 Enable the metrics for heartbeat events to be emitted at the specified interval of seconds.

```
sensor(config-hea)# heartbeat-events enable 20000
sensor(config-hea)#
```

Step 9 Set the inspection load threshold.

```
sensor(config-hea)# inspection-load-policy
sensor(config-hea-ins)# enable true
sensor(config-hea-ins)# red-threshold 100
sensor(config-hea-ins)# yellow-threshold 50
sensor(config-hea-ins)# exit
sensor(config-hea)#
```

Step 10 Enable the interface down policy.

```
sensor(config-hea)# interface-down-policy
sensor(config-hea-int)# enable true
sensor(config-hea-int)# status yellow
sensor(config-hea-int)# exit
sensor(config-hea)#
```

Step 11 Set the number of days until the license expires.

```
sensor(config-hea)# license-expiration-policy
sensor(config-hea-lic)# enable true
sensor(config-hea-lic)# red-threshold 400000
sensor(config-hea-lic)# yellow-threshold 200000
sensor(config-hea-lic)# exit
sensor(config-hea)#
```

Step 12 Set the threshold for memory usage.

```
sensor(config-hea)# memory-usage-policy
sensor(config-hea-mem)# enable true
sensor(config-hea-mem)# red-threshold 100
sensor(config-hea-mem)# yellow-threshold 50
sensor(config-hea-mem)# exit
sensor(config-hea)#
```

Step 13 Set the missed packet threshold.

```
sensor(config-hea)# missed-packet-policy
sensor(config-hea-mis)# enable true
sensor(config-hea-mis)# red-threshold 50
sensor(config-hea-mis)# yellow-threshold 20
sensor(config-hea-mis)# exit
sensor(config-hea)#
```

Step 14 Set the number of minutes that a lower security persists following the occurrence of the latest event to lower the security status.

```
sensor(config-hea)# persist-security-status 10
sensor(config-hea)#
```

Step 15 Set the number of days since the last signature update.

```
sensor(config-hea)# signature-update-policy
sensor(config-hea-sig)# enable true
sensor(config-hea-sig)# red-threshold 30000
sensor(config-hea-sig)# yellow-threshold 10000
sensor(config-hea-sig)# exit
sensor(config-hea)#
```

Step 16 Verify your settings.

```
sensor(config-hea)# show settings
   enable-monitoring: true default: true
   persist-security-status: 10 minutes default: 5
   heartbeat-events
   -----------------------------------------------
      enable: 20000 seconds default: 300
   -----------------------------------------------
   application-failure-policy
   -----------------------------------------------
      enable: true default: true
      status: red default: red
   -----------------------------------------------
   bypass-policy
   -----------------------------------------------
      enable: true default: true
      status: yellow default: red
   -----------------------------------------------
   interface-down-policy
   -----------------------------------------------
      enable: true default: true
      status: yellow default: red
   -----------------------------------------------
   inspection-load-policy
   -----------------------------------------------
      enable: true default: true
      yellow-threshold: 50 percent default: 80
      red-threshold: 100 percent default: 91
   -----------------------------------------------
   missed-packet-policy
   -----------------------------------------------
      enable: true default: true
      yellow-threshold: 20 percent default: 1
      red-threshold: 50 percent default: 6
   -----------------------------------------------
   memory-usage-policy
   -----------------------------------------------
      enable: true default: false
      yellow-threshold: 50 percent default: 80
      red-threshold: 100 percent default: 91
   -----------------------------------------------
   signature-update-policy
   -----------------------------------------------
      enable: true default: true
      yellow-threshold: 10000 days default: 30
      red-threshold: 30000 days default: 60
   -----------------------------------------------
   license-expiration-policy
   -----------------------------------------------
      enable: true default: true
      yellow-threshold: 200000 days default: 30
      red-threshold: 400000 days default: 0
   -----------------------------------------------
```

```
   event-retrieval-policy
   -----------------------------------------------
      enable: true <defaulted>
      yellow-threshold: 100000 seconds default: 300
      red-threshold: 100 seconds default: 600
   -----------------------------------------------
sensor(config-hea)#
```

Step 17 Exit health monitoring submode.

```
sensor(config-hea)# exit
Apply Changes:?[yes]:
```

Step 18 Press **Enter** to apply the changes or enter **no** to discard them.

Showing Sensor Overall Health Status

Caution When the sensor is first starting, it is normal for certain health metric statuses to be red until the sensor is fully up and running.

Note The ASA 5500-X IPS SSP and the ASA 5585-X IPS SSP do not support bypass mode. The adaptive security appliance will either fail open, fail close, or fail over depending on the configuration of the adaptive security appliance and the type of activity being done on the IPS.

Use the **show health** command in privileged EXEC mode to display the overall health status information of the sensor. The health status categories are rated by red and green with red being critical.

To display the overall health status of the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Show the health and security status of the sensor.

```
sensor# show health
Overall Health Status                                 Red
Health Status for Failed Applications                 Green
Health Status for Signature Updates                   Green
Health Status for License Key Expiration              Red
Health Status for Running in Bypass Mode              Green
Health Status for Interfaces Being Down               Red
Health Status for the Inspection Load                 Green
Health Status for the Time Since Last Event Retrieval Green
Health Status for the Number of Missed Packets        Green
Health Status for the Memory Usage                    Not Enabled
Health Status for Global Correlation                  Red
Health Status for Network Participation               Not Enabled

Security Status for Virtual Sensor vs0   Green
sensor#
```

Creating a Banner Login

Use the **banner login** command to create a banner login that will be displayed before the user and password login prompts. The maximum message length is 2500 characters. Use the **no banner login** command to remove the banner.

To create a banner login, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Create the banner login.

```
sensor(config)# banner login
Banner[]:
```

Step 4 Enter your message.

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

Note To use a ? or a carriage return in the message, press **Ctrl-V-?** or **Ctrl-V-Enter**. They are represented by ^M.

Example

```
This message will be displayed on login.
Thank you
login: cisco
Password:****
```

Step 5 Remove the banner login. The banner no longer appears at login.

```
sensor(config)# no banner login
```

Terminating CLI Sessions

Caution You can only clear CLI login sessions with the **clear line** command. You cannot clear service logins with this command.

Use the **clear line** *cli_id* [**message**] command to terminate another CLI session. If you use the **message** keyword, you can send a message along with the termination request to the receiving user. The maximum message length is 2500 characters.

The following parameters apply:

- *cli_id*—Specifies the CLI ID number associated with the login session. Use the **show users** command to find the CLI ID number.
- **message**—Specifies the message to send to the receiving user.

If an administrator tries to log in when the maximum sessions have been reached, the following message appears:

```
Error: The maximum allowed CLI sessions are currently open, would you like to terminate
one of the open sessions? [no]
```

If an operator or viewer tries to log in when the maximum sessions are open, the following message appears:

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

To terminate a CLI session, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

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

Step 2 Find the CLI ID number associated with the login session.

```
sensor# show users
    CLI ID   User    Privilege
*   13533    jtaylor administrator
    15689    jsmith  operator
    20098    viewer  viewer
```

Step 3 Terminate the CLI session of jsmith.

```
sensor# clear line cli_id message
Message[]:
```

Example

```
sensor# clear line 15689 message
Message{}: Sorry! I need to terminate your session.
sensor#
```

The user jsmith receives the following message from the administrator jtaylor.

```
sensor#
***
***
*** Termination request from jtaylor
***
Sorry! I need to terminate your session.
```

Modifying Terminal Properties

Note You are not required to specify the screen length for some types of terminal sessions because the specified screen length can be learned by some remote hosts.

Use the **terminal [length]** *screen _length* command to modify terminal properties for a login session. The *screen_ length* option lets you set the number of lines that appear on the screen before the `--more--` prompt is displayed. A value of zero results in no pause in the output. The default value is 24 lines.

To modify the terminal properties, follow these steps:

Step 1 Log in to the CLI.

Step 2 To have no pause between multi-screen outputs, use 0 for the screen length value.

```
sensor# terminal length 0
```

Note The screen length values are not saved between login sessions.

Step 3 To have the CLI pause and display the `--more--` prompt every 10 lines, use 10 for the *screen length* value.

```
sensor# terminal length 10
```

Configuring Events

This section describes how to display and clear events from the Event Store, and contains the following topics:

- Displaying Events, page 17-22
- Clearing Events from the Event Store, page 17-25

Displaying Events

Note The Event Store has a fixed size of 30 MB for all platforms.

Note Events are displayed as a live feed. To cancel the request, press **Ctrl-C.**

Use the **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*] command to display events from Event Store. Events are displayed beginning at the start time. If you do not specify a start time, events are displayed beginning at the current time. If you do not specify an event type, all events are displayed.

The following parameters apply:

- **alert**—Displays alerts. Provides notification of some suspicious activity that may indicate an attack is in process or has been attempted. Alert events are generated by the Analysis Engine whenever a signature is triggered by network activity. If no level is selected (informational, low, medium, or high), all alert events are displayed.
- **include-traits**—Displays alerts that have the specified traits.
- **exclude-traits**—Does not display alerts that have the specified traits.
- **traits**—Specifies the trait bit position in decimal (0 to 15).

- **min-threat-rating**—Displays events with a threat rating above or equal to this value. The default is 0. The valid range is 0 to 100.
- **max-threat-rating**—Displays events with a threat rating below or equal to this value. The default is 100. The valid range is 0 to 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 the ARC (block) requests.

  Note The ARC is formerly known as NAC. This name change has not been completely implemented throughout the IDM, the IME, and the CLI.

- **status**—Displays status events.
- **past**—Displays events starting in the past for the specified hours, minutes, and seconds.
- *hh:mm:ss*—Specifies the hours, minutes, and seconds in the past to begin the display.

Note The **show events** command continues to display events until a specified event is available. To exit, press **Ctrl-C**.

Displaying Events

To display events from the Event Store, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display all events starting now. The feed continues showing all events until you press **Ctrl-C**.

```
sensor# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

Step 3 Display the block requests beginning at 10:00 a.m. on February 9, 2011.

```
sensor# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
```

```
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

Step 4 Display errors with the warning level starting at 10:00 a.m. on February 9, 2011.

```
sensor# show events error warning 10:00:00 Feb 9 2011
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2011/01/07 04:49:25 2011/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

Step 5 Display alerts from the past 45 seconds.

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2011/03/02 14:15:59 2011/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

Step 6 Display events that began 30 seconds in the past.

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
```

```
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

Clearing Events from the Event Store

Use the **clear events** command to clear the Event Store.

To clear events from the Event Store, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Clear the Event Store.

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

Step 3 Enter **yes** to clear the events.

Configuring the System Clock

This section explains how to display and manually set the system clock. It contains the following topics:

- Displaying the System Clock, page 17-25
- Manually Setting the System Clock, page 17-26

Displaying the System Clock

Use the **show clock** [**detail**] command to display the system clock. You can use the **detail** option to indicate the clock source (NTP or system) and the current summertime setting (if any). 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 17-3 lists the system clock flags.

Table 17-3 System Clock Flags

Symbol	Description
*	Time is not authoritative.
(blank)	Time is authoritative.
.	Time is authoritative, but NTP is not synchronized.

To display the system clock, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the system clock.

```
sensor# show clock
*19:04:52 UTC Thu Apr 03 2008
```

Step 3 Display the system clock with details. The following example indicates that the sensor is getting its time from NTP and that is configured and synchronized.

```
sensor# show clock detail
20:09:43 UTC Thu Apr 03 2011
Time source is NTP
Summer time starts 03:00:00 UTC Sun Mar 09 2011
Summer time stops 01:00:00 UTC Sun Nov 02 2011
```

Step 4 Display the system clock with details. The following example indicates that no time source is configured.

```
sensor# show clock detail
*20:09:43 UTC Thu Apr 03 2011
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2011
Summer time stops 01:00:00 UTC Sun Nov 02 2011
```

Manually Setting the System Clock

Note You do not need to set the system clock if your sensor is synchronized by a valid outside timing mechanism such as an NTP clock source.

Use the **clock set** *hh:mm [:ss] month day year* command to manually set the clock on the appliance. Use this command if no other time sources are available. The **clock set** command does not apply to the following platforms, because they get their time from the adaptive security appliance in which they are installed:

- ASA 5500-X IPS SSP
- ASA 5585-X IPS SSP

To manually set the clock on the appliance, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Set the clock manually.

```
sensor# clock set 13:21 Mar 29 2011
```

Note The time format is 24-hour time.

Clearing the Denied Attackers List

Use the **show statistics denied-attackers** command to display the list of denied attackers. Use the **clear denied-attackers** [*virtual_sensor*] [**ip-address** *ip_address*] command to delete the denied attackers list and clear the virtual sensor statistics.

If your sensor is configured to operate in inline mode, the traffic is passing through the sensor. You can configure signatures to deny packets, connections, and attackers while in inline mode, which means that single packets, connections, and specific attackers are denied, that is, not transmitted, when the sensor encounters them. When the signature fires, the attacker is denied and placed in a list. As part of sensor administration, you may want to delete the list or clear the statistics in the list.

The following parameters apply:

- *virtual_sensor*—(Optional) Specifies the virtual sensor whose denied attackers list should be cleared.
- *ip_address*—(Optional) Specifies the IP address to clear.

Displaying and Deleting Denied Attackers

To display the list of denied attackers and delete the list and clear the statistics, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 Display the list of denied IP addresses. The statistics show that there are two IP addresses being denied at this time.

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

Step 3 Delete 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 sensor.
Continue with clear? [yes]:
```

Step 4 Enter **yes** to clear the list.

Step 5 Delete the denied attackers list for a specific virtual sensor.

```
sensor# clear denied-attackers vs0
```

```
Warning: Executing this command will delete all addresses from the list of attackers being
denied by virtual sensor vs0.
Continue with clear? [yes]:
```

Step 6 Enter **yes** to clear the list.

Step 7 Remove a specific IP address from the denied attackers list for a specific virtual sensor.

```
sensor# clear denied-attackers vs0 ip-address 192.0.2.0
Warning: Executing this command will delete ip address 192.0.2.0 from the list of
attackers being denied by virtual sensor vs0.
Continue with clear? [yes]:
```

Step 8 Enter **yes** to clear the list.

Step 9 Verify that you have cleared the list. You can use the **show statistics denied-attackers** or **show statistics virtual-sensor** command.

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.
sensor#

sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

Step 10 Clear only the statistics.

```
sensor# show statistics virtual-sensor clear
```

Step 11 Verify that you have cleared the statistics. The statistics have all been cleared except for the `Number of Active Denied Attackers` and `Number of exec Clear commands during uptime` categories. It is important to know if the list has been cleared.

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
```

```
      Number of Denied Attackers Inserted = 0
      Number of Denied Attackers Total Hits = 0
      Number of times max-denied-attackers limited creation of new entry = 0
      Number of exec Clear commands during uptime = 1
   Denied Attackers and hit count for each.
      10.20.2.5 = 0
      10.20.5.2 = 0
```

Displaying Policy Lists

Use the **list** {**anomaly-detection-configurations** | **event-action-rules-configurations** | **signature-definition-configurations**} in EXEC mode to display the list of policies for these components. The file size is in bytes. A virtual sensor with N/A indicates that the policy is not assigned to a virtual sensor.

To display a list of policies on the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the list of policies for anomaly detection.

```
sensor# list anomaly-detection-configurations
Anomaly Detection
   Instance   Size   Virtual Sensor
   ad0        255    vs0
   temp       707    N/A
   MyAD       255    N/A
   ad1        141    vs1
sensor#
```

Step 3 Display the list of policies for event action rules.

```
sensor# list event-action-rules-configurations
Event Action Rules
   Instance   Size   Virtual Sensor
   rules0     112    vs0
   rules1     141    vs1
sensor#
```

Step 4 Display the list of policies for signature definition.

```
sensor# list signature-definition-configurations
Signature Definition
   Instance   Size   Virtual Sensor
   sig0       336    vs0
   sig1       141    vs1
   sig2       141    N/A
sensor#
```

Displaying Statistics

Use the **show statistics [analysis-engine | anomaly-detection | authentication | denied-attackers | event-server | event-store | external-product-interface | global-correlation | host | logger | network-access | notification | os-identification | sdee-server | transaction-server | virtual-sensor | web-server**] [**clear**] command to display statistics for each sensor application.

Use the **show statistics** {**anomaly-detection | denied-attackers | os-identification | virtual-sensor**} [***name*** **| clear**] command to display statistics for these components for all virtual sensors. If you provide the virtual sensor name, the statistics for that virtual sensor only are displayed.

Note The **clear** option is not available for the analysis engine, anomaly detection, host, network access, or OS identification applications.

For the IPS 4500 series, at the end of the command output, there are extra details for the Ethernet controller statistics, such as the total number of packets received at the Ethernet controller, the total number of packets dropped at the Ethernet controller under high load conditions, and the total packets transmitted including the customer traffic packets and the internal keepalive packet count.

Note The Ethernet controller statistics are polled at an interval of 5 seconds from the hardware side. The keepalives are sent or updated at an interval of 10 ms. Because of this, there may be a disparity in the actual count reflected in the total packets transmitted. At times, it is even possible that the total packets transmitted may be less that the keepalive packets transmitted.

To display statistics for the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the statistics for the Analysis Engine.

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 431157
   Processing Load Percentage
         Thread    5 sec   1 min   5 min
         0         1       1       1
         1         1       1       1
         2         1       1       1
         3         1       1       1
         4         1       1       1
         5         1       1       1
         6         1       1       1
         Average   1       1       1

   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 133698
      Total number of packets denied = 203
      Total number of packets reset = 3
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
```

```
   Number of datagrams currently in FRU = 0
TCP Stream Reassembly Unit Statistics
   TCP streams currently in the embryonic state = 0
   TCP streams currently in the established state = 0
   TCP streams currently in the closing state = 0
   TCP streams currently in the system = 0
   TCP Packets currently queued for reassembly = 0
The Signature Database Statistics.
   Total nodes active = 0
   TCP nodes keyed on both IP addresses and both ports = 0
   UDP nodes keyed on both IP addresses and both ports = 0
   IP nodes keyed on both IP addresses = 0
Statistics for Signature Events
   Number of SigEvents since reset = 0
Statistics for Actions executed on a SigEvent
   Number of Alerts written to the IdsEventStore = 0
Inspection Stats
      Inspector            active   call   create   delete   loadPct
      AtomicAdvanced       0        2312   4        4        33
      Fixed                0        1659   1606     1606     1
      MSRPC_TCP            0        20     4        4        0
      MSRPC_UDP            0        1808   1575     1575     0
      MultiString          0        145    10       10       2
      ServiceDnsUdp        0        1841   3        3        0
      ServiceGeneric       0        2016   14       14       1
      ServiceHttp          0        2      2        2        51
      ServiceNtp           0        3682   3176     3176     0
      ServiceP2PTCP        0        21     9        9        0
      ServiceRpcUDP        0        1841   3        3        0
      ServiceRpcTCP        0        130    9        9        0
      ServiceSMBAdvanced   0        139    3        3        0
      ServiceSnmp          0        1841   3        3        0
      ServiceTNS           0        18     14       14       0
      String               0        225    16       16       0
      SweepUDP             0        1808   1555     1555     6
      SweepTCP             0        576    17       17       0
      SweepOtherTcp        0        288    6        6        0
      TrojanBO2K           0        261    11       11       0
      TrojanUdp            0        1808   1555     1555     0

GlobalCorrelationStats
   SwVersion = 7.2(1)E4
   SigVersion = 645.0
   DatabaseRecordCount = 0
   DatabaseVersion = 0
   RuleVersion = 0
   ReputationFilterVersion = 0
   AlertsWithHit = 0
   AlertsWithMiss = 0
   AlertsWithModifiedRiskRating = 0
   AlertsWithGlobalCorrelationDenyAttacker = 0
   AlertsWithGlobalCorrelationDenyPacket = 0
   AlertsWithGlobalCorrelationOtherAction = 0
   AlertsWithAuditRepDenies = 0
   ReputationForcedAlerts = 0
   EventStoreInsertTotal = 0
   EventStoreInsertWithHit = 0
   EventStoreInsertWithMiss = 0
   EventStoreDenyFromGlobalCorrelation = 0
   EventStoreDenyFromOverride = 0
   EventStoreDenyFromOverlap = 0
   EventStoreDenyFromOther = 0
   ReputationFilterDataSize = 0
   ReputationFilterPacketsInput = 0
```

```
      ReputationFilterRuleMatch = 0
      DenyFilterHitsNormal = 0
      DenyFilterHitsGlobalCorrelation = 0
      SimulatedReputationFilterPacketsInput = 0
      SimulatedReputationFilterRuleMatch = 0
      SimulatedDenyFilterInsert = 0
      SimulatedDenyFilterPacketsInput = 0
      SimulatedDenyFilterRuleMatch = 0
      TcpDeniesDueToGlobalCorrelation = 0
      TcpDeniesDueToOverride = 0
      TcpDeniesDueToOverlap = 0
      TcpDeniesDueToOther = 0
      SimulatedTcpDeniesDueToGlobalCorrelation = 0
      SimulatedTcpDeniesDueToOverride = 0
      SimulatedTcpDeniesDueToOverlap = 0
      SimulatedTcpDeniesDueToOther = 0
      LateStageDenyDueToGlobalCorrelation = 0
      LateStageDenyDueToOverride = 0
      LateStageDenyDueToOverlap = 0
      LateStageDenyDueToOther = 0
      SimulatedLateStageDenyDueToGlobalCorrelation = 0
      SimulatedLateStageDenyDueToOverride = 0
      SimulatedLateStageDenyDueToOverlap = 0
      SimulatedLateStageDenyDueToOther = 0
      AlertHistogram
      RiskHistogramEarlyStage
      RiskHistogramLateStage
      ConfigAggressiveMode = 0
      ConfigAuditMode = 0
   RegexAccelerationStats
      Status = Enabled
      DriverVersion = 6.2.1
      Devices = 1
      Agents = 12
      Flows = 7
      Channels = 0
      SubmittedJobs = 4968
      CompletedJobs = 4968
      SubmittedBytes = 72258005
      CompletedBytes = 168
      TCPFlowsWithoutLCB = 0
      UDPFlowsWithoutLCB = 0
      TCPMissedPacketsDueToUpdate = 0
      UDPMissedPacketsDueToUpdate = 0
      MemorySize = 1073741824
      HostDirectMemSize = 0
   MaliciousSiteDenyHitCounts
   MaliciousSiteDenyHitCountsAUDIT
Ethernet Controller Statistics
   Total Packets Received = 0
   Total Received Packets Dropped = 0
   Total Packets Transmitted = 13643"
sensor#
```

Step 3 Display the statistics for anomaly detection.

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
```

```
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor#
```

Step 4 Display the statistics for authentication.

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
sensor#
```

Step 5 Display the statistics for the denied attackers in the system.

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


sensor#
```

Step 6 Display the statistics for the Event Server.

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
```

```
sensor#
```

Step 7 Display the statistics for the Event Store.

```
sensor# show statistics event-store
EEvent store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of filtered events not written to the event store = 850763
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Status events = 4257
      Shun request events = 0
      Error events, warning = 669
      Error events, error = 8
      Error events, fatal = 0
      Alert events, informational = 0
      Alert events, low = 0
      Alert events, medium = 0
      Alert events, high = 0
      Alert events, threat rating 0-20 = 0
      Alert events, threat rating 21-40 = 0
      Alert events, threat rating 41-60 = 0
      Alert events, threat rating 61-80 = 0
      Alert events, threat rating 81-100 = 0
   Cumulative number of each type of event
      Status events = 4257
      Shun request events = 0
      Error events, warning = 669
      Error events, error = 8
      Error events, fatal = 0
      Alert events, informational = 0
      Alert events, low = 0
      Alert events, medium = 0
      Alert events, high = 0
      Alert events, threat rating 0-20 = 0
      Alert events, threat rating 21-40 = 0
      Alert events, threat rating 41-60 = 0
      Alert events, threat rating 61-80 = 0
      Alert events, threat rating 81-100 = 0
sensor#
```

Step 8 Display the statistics for global correlation.

```
sensor# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
```

```
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
sensor#
```

Step 9 Display the statistics for the host.

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 25-Jan-2012 02:59:18
   Command Control Port Device = Management0/0
Network Statistics
    = ma0_0     Link encap:Ethernet  HWaddr 00:04:23:D5:A1:8D
    =           inet addr:10.89.130.98  Bcast:10.89.131.255  Mask:255.255.254.0
    =           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    =           RX packets:1688325 errors:0 dropped:0 overruns:0 frame:0
    =           TX packets:38546 errors:0 dropped:0 overruns:0 carrier:0
    =           collisions:0 txqueuelen:1000
    =           RX bytes:133194316 (127.0 MiB)  TX bytes:5515034 (5.2 MiB)
    =           Base address:0xcc80 Memory:fcee0000-fcf00000
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 1889357824
   freeBytes = 2210988032
   totalBytes = 4100345856
CPU Statistics
   Note: CPU Usage statistics are not a good indication of the sensor processin load. The
Inspection Load Percentage in the output of 'show inspection-load' should be used instead.
   Usage over last 5 seconds = 0
   Usage over last minute = 2
   Usage over last 5 minutes = 2
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 1889357824
   Memory free (bytes) = 2210988032
Auto Update Statistics
   lastDirectoryReadAttempt = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
Auxilliary Processors Installed
sensor#
```

Step 10 Display the statistics for the logging application.

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
```

```
   TOTAL = 31928
sensor#
```

Step 11 Display the statistics for the ARC.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.4
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.5
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 192.0.2.6
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 192.0.2.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 192.0.2.3
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 192.0.2.7
      AclSupport = Does not use ACLs
```

```
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 102.0.2.8
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 192.0.2.9
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 192.0.2.10
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 203.0.113.1
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.2
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 203.0.113.9
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

Step 12 Display the statistics for the notification application.

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

Step 13 Display the statistics for OS identification.

```
sensor# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
sensor#
```

Step 14 Display the statistics for the SDEE server.

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 4
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
   sub-1-9ce8d1dc
      State = Open
      IP Address = 10.89.11.67
      Last Read Time = 18:32:19 UTC Fri Jan 31 2014
      Last Read Time (nanoseconds) = 1391193139172303000
      Status = Valid
   sub-2-8701fb19
      State = Open
      IP Address = 10.142.52.127
      Last Read Time = 18:32:17 UTC Fri Jan 31 2014
      Last Read Time (nanoseconds) = 1391193137284703000
      Status = Valid
   sub-3-5aae57d4
      State = Open
      IP Address = 10.142.52.151
      Last Read Time = 18:32:17 UTC Fri Jan 31 2014
      Last Read Time (nanoseconds) = 1391193137250568000
      Status = Valid
   sub-4-c4685a12
      State = Open
      IP Address = 10.142.52.110
      Last Read Time = 18:32:19 UTC Fri Jan 31 2014
      Last Read Time (nanoseconds) = 1391193139400954000
      Status = Valid
sensor#
```

Step 15 Display the statistics for the transaction server.

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

Step 16 Display the statistics for a virtual sensor.

```
sensor# show statistics virtual-sensor vs0
Statistics for Virtual Sensor vs0
      Name of current Signature-Defintion instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1151770
         MemoryAlloPercent = 23
         MemoryUsedPercent = 22
         MemoryMaxCapacity = 3500000
         MemoryMaxHighUsed = 4193330
         MemoryCurrentAllo = 805452
         MemoryCurrentUsed = 789047
         Processing Load Percentage = 1
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total IPv4 packets processed since reset = 0
         Total IPv6 packets processed since reset = 0
         Total IPv6 AH packets processed since reset = 0
         Total IPv6 ESP packets processed since reset = 0
```

```
   Total IPv6 Fragment packets processed since reset = 0
   Total IPv6 Routing Header packets processed since reset = 0
   Total IPv6 ICMP packets processed since reset = 0
   Total packets that were not IP processed since reset = 0
   Total TCP packets processed since reset = 0
   Total UDP packets processed since reset = 0
   Total ICMP packets processed since reset = 0
   Total packets that were not TCP, UDP, or ICMP processed since reset = 0
   Total ARP packets processed since reset = 0
   Total ISL encapsulated packets processed since reset = 0
   Total 802.1q encapsulated packets processed since reset = 0
   Total GRE Packets processed since reset = 0
   Total GRE Fragment Packets processed since reset = 0
   Total GRE Packets skipped since reset = 0
   Total GRE Packets with Bad Header skipped since reset = 0
   Total IpIp Packets with Bad Header skipped since reset = 0
   Total Encapsulated Tunnel Packets with Bad Header skipped since reset = 0
   Total packets with bad IP checksums processed since reset = 0
   Total packets with bad layer 4 checksums processed since reset = 0
   Total cross queue TCP packets processed since reset = 0
   Total cross queue UDP packets processed since reset = 0
   Packets dropped due to regex resources unavailable since reset = 0
   Total number of bytes processed since reset = 0
   The rate of packets per second since reset = 0
   The rate of bytes per second since reset = 0
   The average bytes per packet since reset = 0
Denied Address Information
   Number of Active Denied Attackers = 0
   Number of Denied Attackers Inserted = 0
   Number of Denied Attacker Victim Pairs Inserted = 0
   Number of Denied Attacker Service Pairs Inserted = 0
   Number of Denied Attackers Total Hits = 0
   Number of times max-denied-attackers limited creation of new entry = 0
   Number of exec Clear commands during uptime = 0
Denied Attackers and hit count for each.
Denied Attackers with percent denied and hit count for each.


The Signature Database Statistics.
   The Number of each type of node active in the system
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The number of each type of node inserted since reset
      Total nodes inserted = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The rate of nodes per second for each time since reset
      Nodes per second = 0
      TCP nodes keyed on both IP addresses and both ports per second = 0
      UDP nodes keyed on both IP addresses and both ports per second = 0
      IP nodes keyed on both IP addresses per second = 0
   The number of root nodes forced to expire because of memory constraints
      TCP nodes keyed on both IP addresses and both ports = 0
   Packets dropped because they would exceed Database insertion rate limits = 0
Fragment Reassembly Unit Statistics for this Virtual Sensor
   Number of fragments currently in FRU = 0
   Number of datagrams currently in FRU = 0
   Number of fragments received since reset = 0
   Number of fragments forwarded since reset = 0
   Number of fragments dropped since last reset = 0
   Number of fragments modified since last reset = 0
```

```
            Number of complete datagrams reassembled since last reset = 0
            Fragments hitting too many fragments condition since last reset = 0
            Number of overlapping fragments since last reset = 0
            Number of Datagrams too big since last reset = 0
            Number of overwriting fragments since last reset = 0
            Number of Inital fragment missing since last reset = 0
            Fragments hitting the max partial dgrams limit since last reset = 0
            Fragments too small since last reset = 0
            Too many fragments per dgram limit since last reset = 0
            Number of datagram reassembly timeout since last reset = 0
            Too many fragments claiming to be the last since last reset = 0
            Fragments with bad fragment flags since last reset = 0
         TCP Normalizer stage statistics
            Packets Input = 0
            Packets Modified = 0
            Dropped packets from queue = 0
            Dropped packets due to deny-connection = 0
            Duplicate Packets = 0
            Current Streams = 0
            Current Streams Closed = 0
            Current Streams Closing = 0
            Current Streams Embryonic = 0
            Current Streams Established = 0
            Current Streams Denied = 0
            Total SendAck Limited Packets = 0
            Total SendAck Limited Streams = 0
            Total SendAck Packets Sent = 0
         Statistics for the TCP Stream Reassembly Unit
            Current Statistics for the TCP Stream Reassembly Unit
               TCP streams currently in the embryonic state = 0
               TCP streams currently in the established state = 0
               TCP streams currently in the closing state = 0
               TCP streams currently in the system = 0
               TCP Packets currently queued for reassembly = 0
            Cumulative Statistics for the TCP Stream Reassembly Unit since reset
               TCP streams that have been tracked since last reset = 0
               TCP streams that had a gap in the sequence jumped = 0
               TCP streams that was abandoned due to a gap in the sequence = 0
               TCP packets that arrived out of sequence order for their stream = 0
               TCP packets that arrived out of state order for their stream = 0
               The rate of TCP connections tracked per second since reset = 0
         SigEvent Preliminary Stage Statistics
            Number of Alerts received = 0
            Number of Alerts Consumed by AlertInterval = 0
            Number of Alerts Consumed by Event Count = 0
            Number of FireOnce First Alerts = 0
            Number of FireOnce Intermediate Alerts = 0
            Number of Summary First Alerts  = 0
            Number of Summary Intermediate Alerts  = 0
            Number of Regular Summary Final Alerts  = 0
            Number of Global Summary Final Alerts  = 0
            Number of Active SigEventDataNodes  = 0
            Number of Alerts Output for further processing = 0
--MORE--
```

Step 17 Display the statistics for the web server.

```
sensor# show statistics web-server
listener-443
   session-11
      remote host = 64.101.182.167
      session is persistent = no
      number of requests serviced on current connection = 1
      last status code = 200
```

```
      last request method = GET
      last request URI = cgi-bin/sdee-server
      last protocol version = HTTP/1.1
      session state = processingGetServlet
   number of server session requests handled = 957134
   number of server session requests rejected = 0
   total HTTP requests handled = 365871
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 12
   number of busy allocated session objects = 1
summarized log messages
   number of TCP socket failure messages logged = 0
   number of TLS socket failure messages logged = 0
   number of TLS protocol failure messages logged = 0
   number of TLS connection failure messages logged = 595015
   number of TLS crypto warning messages logged = 0
   number of TLS expired certificate warning messages logged = 0
   number of receipt of TLS fatal alert message messages logged = 594969
crypto library version = 6.2.1.0
sensor#
```

Step 18 Clear the statistics for an application, for example, the logging application. The statistics are retrieved and cleared.

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

Step 19 Verify that the statistics have been cleared. The statistics now all begin from 0.

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

Displaying Tech Support Information

Note The **show tech-support** command now displays historical interface data for each interface for the past 72 hours.

Use the **show tech-support** [**page**] [**destination-url** *destination_url*] command to display system information on the screen or have it sent to a specific URL. You can use the information as a troubleshooting tool with TAC.

The following parameters are optional:

- **page**—Displays the output, 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.
- **destination-url**—Indicates the information should be formatted as HTML and sent to the destination that follows this command. If you use this keyword, the output is not displayed on the screen.
- *destination_url*—Indicates the information should be formatted as HTML.The URL specifies where the information should be sent. If you do not use this keyword, the information is displayed on the screen.
- You can specify the following destination types:
  - **ftp:**—Destination URL for FTP network server. The syntax for this prefix is:
    `ftp://[[username@location]/relativeDirectory]/filename` or
    `ftp://[[username@location]//absoluteDirectory]/filename`
  - **scp:**—Destination URL for the SCP network server. The syntax for this prefix is:
    `scp://[[username@]location]/relativeDirectory]/filename` or
    `scp://[[username@]location]//absoluteDirectory]/filename`

Varlog Files

The /var/log/messages file has the latest logs. A new softlink called varlog has been created under the /usr/cids/idsRoot/log folder that points to the /var/log/messages file. Old logs are stored in varlog.1 and varlog.2 files. The maximum size of these varlog files is 200 KB. Once they cross the size limit the content is rotated. The content of varlog, varlog.1, and varlog.2 is displayed in the output of the **show tech-support** command. The log messages (/usr/cids/idsRoot/varlog files) persist only across sensor reboots. The old logs are lost during software upgrades.

Displaying Tech Support Information

To display tech support information, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 View the output on the screen. The system information appears on the screen, one page at a time. Press the spacebar to view the next page or press **Ctrl-C** to return to the prompt

```
sensor# show tech-support page
```

Step 3 To send the output (in HTML format) to a file:

a. Enter the following command, followed by a valid destination. The `password:` prompt appears.

```
sensor# show tech-support destination-url destination_url
```

Example

To send the tech support output to the file `/absolute/reports/sensor1Report.html`:

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

b. Enter the password for this user account. The `Generating report:` message is displayed.

Displaying Version Information

Use the **show version** command to display version information for all installed operating system packages, signature packages, and IPS processes running on the system. To view the configuration for the entire system, use the **more current-config** command.

Note The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

Note For the IPS 4500 series sensors, the **show version** command output contains an extra application called the SwitchApp.

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View version information.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0        2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
No license present
Sensor up-time is 3 days.
Using 14470M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.1M out of 376.1M bytes of available disk space (24%
 usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
```

```
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500

Upgrade History:

  IPS-K9-7.2-1-E4   11:17:07 UTC Thu Jan 10 2013

Recovery Partition Version 1.1 - 7.2(1)E4

Host Certificate Valid from: 17-Apr-2013 to 18-Apr-2015

sensor#
```

Note If the --MORE-- prompt is displayed, press the spacebar to see more information or **Ctrl-C** to cancel the output and get back to the CLI prompt.

Step 3 View configuration information.

Note You can use the **more current-config** or **show configuration** commands.

```
sensor# more current-config
! ------------------------------
! Current configuration last modified Fri Apr 19 19:01:05 2013
! ------------------------------
! Version 7.2(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S697.0   2013-02-15
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
inline-interfaces pair0
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
bypass-mode auto
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.106.133.159/23,10.106.132.1
host-name q4360-159
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
```

```
dns-tertiary-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
websession-inactivity-timeout 3600
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
logical-interface pair0
exit
exit
sensor#
```

Diagnosing Network Connectivity

Caution No command interrupt is available for this command. It must run to completion.

Use the **ping** *ip_address* [**count**] command to diagnose basic network connectivity.

To diagnose basic network connectivity, follow these steps:

Step 1 Log in to the CLI.

Step 2 Ping the address you are interested in. The count is the number of echo requests to send. If you do not specify a number, 4 requests are sent. The range is 1 to 10,000.

```
sensor# ping ip_address count
```

The following example shows a successful ping:

```
sensor# ping 192.0.2.1 6
PING 192.0.2.1 (192.0.2.1): 56 data bytes
64 bytes from 192.0.2.1: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 192.0.2.1: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 192.0.2.1: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 192.0.2.1: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 192.0.2.1: icmp_seq=5 ttl=61 time=0.2 ms

--- 192.0.2.1 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
```

The following example shows an unsuccessful ping:

```
sensor# ping 172.16.0.0 3
PING 172.16.0.0 (172.16.0.0): 56 data bytes

--- 172.16.0.0 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

Resetting the Appliance

Use the **reset** [**powerdown**] command to shut down the applications running on the appliance and to reboot the appliance. You can include the **powerdown** option to power off the appliance, if possible, or to have the appliance left in a state where the power can be turned off.

Shutdown (stopping the applications) begins immediately after you execute the command. Shutdown can take a while, and you can still access CLI commands while it is taking place, but the session is terminated without warning.

To reset the appliance, follow these steps:

Step 1 Log in to the CLI using an account with administrator privileges.

Step 2 To stop all applications and reboot the appliance, follow these Steps 2 and 3. Otherwise, to power down the appliance, go to Steps 4 and 5.

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

Step 3 Enter **yes** to continue the reset.

```
sensor# yes
Request Succeeded.
```

```
sensor#
```

Step 4 Stop all applications and power down the appliance.

```
sensor# reset powerdown
Warning: Executing this command will stop all applications and power off the node if
possible. If the node can not be powered off it will be left in a state that is safe to
manually power down.
Continue with reset? []:
```

Step 5 Enter **yes** to continue with the reset and power down.

```
sensor# yes
Request Succeeded.
sensor#
```

For More Information

To reset the ASA IPS modules, see the following individual procedures:

- Reloading, Shutting Down, Resetting, and Recovering the ASA 5500-X IPS SSP, page 18-12
- Reloading, Shutting Down, Resetting, and Recovering the ASA 5585-X IPS SSP, page 19-12

Displaying Command History

Use the **show history** command to obtain a list of the commands you have entered in the current menu. The maximum number of commands in the list is 50.

To obtain a list of the commands you have used recently, follow these steps:

Step 1 Log in to the CLI.

Step 2 Show the history of the commands you have used in EXEC mode, for example.

```
sensor# show history
clear line
configure terminal
show history
```

Step 3 Show the history of the commands you have used in network access mode, for example.

```
sensor# configure terminal
sensor (config)# service network-access
sensor (config-net)# show history
show settings
show settings terse
show settings | include profile-name|ip-address
exit
show history
sensor (config-net)#
```

Displaying Hardware Inventory

Use the **show inventory** command to display PEP information. This command displays the UDI information that consists of the PID, the VID, and the SN of your sensor. If your sensor supports SFP/SFP+ modules and Regex accelerator cards, they are also displayed. PEP information provides an easy way to obtain the hardware version and serial number through the CLI.

Note The show inventory command now displays the FRUable components of the 4300 series sensors.

To display PEP information, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the PEP information. You can use this information when dealing with TAC.

```
sensor# show inventory

Name: "Chassis", DESCR: "IPS 4360 with SW, 8 GE data + 1 GE mgmt"
PID: IPS-4360          , VID: V00, SN: FCH1504V04T

Name: "RegexAccelerator/0", DESCR: "LCPX8640 (humphrey)"
PID: PREAKNESS 2G      , VID: 335, SN: LXXXXXYYYY
sensor#

sensor# show inventory

Name: "Chassis", DESCR: "IPS 4255 Intrusion Prevention Sensor"
PID: IPS-4255-K9, VID: V01 , SN: JAB0815R017

Name: "Power Supply", DESCR: ""
PID: ASA-180W-PWR-AC, VID: V01 , SN: 123456789AB
sensor#

sensor# show inventory

Name: "Module", DESCR: "ASA 5500 Series Security Services Module-20"
PID: ASA-SSM-20, VID: V01 , SN: JAB0815R036
sensor#

sensor# show inventory

Name: "Chassis", DESCR: "IPS 4240 Appliance Sensor"
PID: IPS-4240-K9, VID: V01 , SN: P3000000653
sensor#

sensor# show inventory

Name: "Chassis", DESCR: "IPS 4345 Intrusion Protection System"
PID: IPS4345           , VID: V00, SN: FCH1445V00N

Name: "RegexAccelerator/0", DESCR: "LCPX8640 (humphrey)"
PID: FCH1442705J       , VID: 335, SN: LXXXXXYYYY
sensor#

sensor# show inventory

Name: "Module", DESCR: "IPS 4520- 6 Gig E, 4 10 Gig E SFP+"
PID: IPS-4520-INC-K9   , VID: V01, SN: JAF1547BJTJ
```

```
Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V02, SN: JMX15527050

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V03, SN: POG153700UC

Name: "power supply 1", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V03, SN: POG153700SY

Name: "RegexAccelerator/0", DESCR: "LCPX5110 (LCPX5110)"
PID: LCPX5110          , VID: 335, SN: SL14200225

Name: "RegexAccelerator/1", DESCR: "LCPX5110 (LCPX5110)"
PID: LCPX5110          , VID: 335, SN: SL14200242

Name: "TenGigabitEthernet0/0", DESCR: "10G Based-SR"
PID: SFP-10G-SR        , VID: V03, SN: AGD152740NV

Name: "TenGigabitEthernet0/1", DESCR: "10G Based-SR"
PID: SFP-10G-SR        , VID: V03, SN: AGD152741JT

Name: "TenGigabitEthernet0/2", DESCR: "10G Based-CX-1-5 Passive"
PID: SFP-H10GB-CU5M    , VID: V02, SN: MOC15210458

Name: "TenGigabitEthernet0/3", DESCR: "10G Based-CX-1-5 Passive"
PID: SFP-H10GB-CU5M    , VID: V02, SN: MOC15210458

sensor# show inventory

Name: "Module", DESCR: "IPS 4510- 6 Gig E, 4 10 Gig E SFP+"
PID: IPS-4510-INC-K9   , VID: V01, SN: JAF1546CECE

Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V02, SN: JMX1552705F

Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V03, SN: POG1540001Z

Name: "power supply 1", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V03, SN: POG1540000B

Name: "RegexAccelerator/0", DESCR: "LCPX5110 (LCPX5110)"
PID: LCPX5110          , VID: 335, SN: SL14200223

Name: "TenGigabitEthernet0/0", DESCR: "10G Based-SR"
PID: SFP-10G-SR        , VID: V03, SN: AGD152740KZ

Name: "TenGigabitEthernet0/1", DESCR: "10G Based-SR"
PID: SFP-10G-SR        , VID: V03, SN: AGD15264272

Name: "TenGigabitEthernet0/2", DESCR: "1000Based-SX"
PID: FTLF8519P2BCL-CS  , VID: 000, SN: FNS110210C1

sensor# show inventory

Name: "Chassis", DESCR: "IPS 4360 with SW, 8 GE Data + 1 GE Mgmt"
PID: IPS-4360          , VID: V01 , SN: FGL162740J6

Name: "RegexAccelerator/0", DESCR: "LCPX8640 (humphrey)"
PID: FCH162077NK       , VID: 33554537, SN: LXXXXXYYYY

Name: "power supply 1", DESCR: "IPS4360 AC Power Supply "
PID: IPS-4360-PWR-AC   , VID: 0700A, SN: 25Y1Y8
```

```
Name: "power supply 2", DESCR: "IPS4360 AC Power Supply "
PID: IPS-4360-PWR-AC   , VID: 0700A, SN: 25Y1Y9

sensor# show inventory

Name: "power supply 1", DESCR: "IPS-4345-K9 AC Power Supply "
PID: IPS-4345-PWR-AC   , VID: A1, SN: 000783
```

Tracing the Route of an IP Packet

Caution There is no command interrupt available for this command. It must run to completion.

Use the **trace** *ip_address count* command to display the route an IP packet takes to a destination. The *ip_address* option is the address of the system to trace the route to. The *count* option lets you define how many hops you want to take. The default is 4. The valid values are 1 to 256.

To trace the route of an IP packet, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the route of IP packet you are interested in.

```
sensor# trace 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 4 hops max, 40 byte packets
 1  192.0.2.2 (192.0.2.2)  0.267 ms  0.262 ms  0.236 ms
 2  192.0.2.12 (192.0.2.12)  0.24 ms *  0.399 ms
 3  * 192.0.2.12 (192.0.2.12)  0.424 ms *
 4  192.0.2.12 (192.0.2.12)  0.408 ms *  0.406 ms
sensor#
```

Step 3 To configure the route to take more hops than the default of 4, use the *count* option.

```
sensor# trace 10.0.0.1 8
traceroute to 10.0.0.1 (10.0.0.1), 8 hops max, 40 byte packets
 1  192.0.2.2 (192.0.2.2)  0.35 ms  0.261 ms  0.238 ms
 2  192.0.2.12 (192.0.2.12)  0.36 ms *  0.344 ms
 3  * 192.0.2.12 (192.0.2.12)  0.465 ms *
 4  192.0.2.12 (192.0.2.12)  0.319 ms *  0.442 ms
 5  * 192.0.2.12 (192.0.2.12)  0.304 ms *
 6  192.0.2.12 (192.0.2.12)  0.527 ms *  0.402 ms
 7  * 192.0.2.12 (192.0.2.12)  0.39 ms *
 8  192.0.2.12 (192.0.2.12)  0.37 ms *  0.486 ms
sensor#
```

Displaying Submode Settings

Use the **show settings** [**terse**] command in any submode to view the contents of the current configuration.

To display the current configuration settings for a submode, follow these steps:

Step 1 Log in to the CLI.

Step 2 Show the current configuration for ARC submode.

```
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: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      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: 11)
   ------------------------------------------------
      profile-name: 2admin
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      ------------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
      profile-name: insidePix
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: <defaulted>
      ------------------------------------------------
      profile-name: qatest
      ------------------------------------------------
         enable-password: <hidden>
```

```
      password: <hidden>
      username: <defaulted>
   ------------------------------------------------
   profile-name: fwsm
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: outsidePix
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: cat
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: <defaulted>
   ------------------------------------------------
   profile-name: rcat
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ------------------------------------------------
   profile-name: nopass
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: <defaulted>
   ------------------------------------------------
   profile-name: test
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: sshswitch
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ------------------------------------------------
------------------------------------------------
cat6k-devices (min: 0, max: 250, current: 1)
------------------------------------------------
   ip-address: 192.0.2.12
   ------------------------------------------------
      communication: telnet default: ssh-3des
      nat-address: 0.0.0.0 <defaulted>
      profile-name: cat
      block-vlans (min: 0, max: 100, current: 1)
      ---------------------------------------------
         vlan: 1
         ------------------------------------------------
            pre-vacl-name: <defaulted>
            post-vacl-name: <defaulted>
         ------------------------------------------------
      ---------------------------------------------
   ------------------------------------------------
------------------------------------------------
router-devices (min: 0, max: 250, current: 1)
```

```
   ------------------------------------------------
      ip-address: 192.0.2.25
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ------------------------------------------------
            interface-name: fa0/0
            direction: in
            ------------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ------------------------------------------------
      ip-address: 192.0.2.30
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: insidePix
      ------------------------------------------------
      ip-address: 192.0.2.3
      ------------------------------------------------
         communication: ssh-3des <defaulted>
         nat-address: 0.0.0.0 <defaulted>
         profile-name: f1
      ------------------------------------------------
   ------------------------------------------------
sensor (config-net)#
```

Step 3 Show the ARC settings in terse mode.

```
sensor(config-net)# show settings terse
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      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: 11)
   ------------------------------------------------
```

```
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
   ----------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 1)
   ----------------------------------------------
      ip-address: 192.0.2.12
   ----------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ----------------------------------------------
      ip-address: 192.0.2.25
   ----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ----------------------------------------------
      ip-address: 192.0.2.30
      ip-address: 192.0.2.3
   ----------------------------------------------
sensor(config-net)#
```

Step 4 You can use the **include** keyword to show settings in a filtered output, for example, to show only profile names and IP addresses in the ARC configuration.

```
sensor(config-net)# show settings | include profile-name|ip-address
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
      ip-address: 192.0.2.12
         profile-name: cat
      ip-address: 192.0.2.25
         profile-name: r7200
      ip-address: 192.0.2.30
         profile-name: insidePix
      ip-address: 192.0.2.3
         profile-name: test
sensor(config-net)#
```