



CHAPTER 16

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:

- [Recovering the Password, page 16-2](#)
- [Clearing the Sensor Databases, page 16-8](#)
- [Configuring Health Status Information, page 16-9](#)
- [Showing Sensor Overall Health Status, page 16-13](#)
- [Creating a Banner Login, page 16-14](#)
- [Terminating CLI Sessions, page 16-14](#)
- [Modifying Terminal Properties, page 16-15](#)
- [Displaying and Clearing Events, page 16-16](#)
- [Setting the System Clock, page 16-19](#)
- [Clearing the Denied Attackers List, page 16-21](#)
- [Displaying Policy Lists, page 16-23](#)
- [Displaying Statistics, page 16-24](#)
- [Displaying Tech Support Information, page 16-33](#)
- [Displaying Version Information, page 16-34](#)
- [Diagnosing Network Connectivity, page 16-36](#)
- [Resetting the Appliance, page 16-37](#)
- [Displaying Command History, page 16-38](#)
- [Displaying Hardware Inventory, page 16-38](#)
- [Tracing the Route of an IP Packet, page 16-39](#)
- [Displaying Submode Settings, page 16-40](#)

Recovering the Password

For most IPS platforms, you can now recover the password on the sensor rather than using the service account or reimaging the sensor. This section describes how to recover the password for the various IPS platforms. It contains the following topics:

- [Understanding Password Recovery, page 16-2](#)
- [Password Recovery for Appliances, page 16-2](#)
- [Password Recovery for AIM-IPS, page 16-4](#)
- [Password Recovery for AIP-SSM, page 16-5](#)
- [Password Recovery for IDSM-2, page 16-5](#)
- [Password Recovery for NME-IPS, page 16-6](#)
- [Disabling Password Recovery, page 16-6](#)
- [Verifying the State of Password Recovery, page 16-7](#)
- [Troubleshooting Password Recovery, page 16-8](#)

Understanding Password Recovery

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.



Note

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

[Table 16-1](#) lists the password recovery methods according to platform.

Table 16-1 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4200 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
AIM-IPS NME-IPS	Router IPS modules	Bootloader command
AIP-SSM	ASA 5500 series adaptive security appliance modules	ASA CLI command
IDSM-2	Switch IPS module	Download image through maintenance partition

Password Recovery for Appliances

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

- [Using the GRUB Menu, page 16-3](#)
- [Using ROMMON, page 16-3](#)

Using the GRUB Menu

For 4200 series 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.



Note

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

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance.

The following menu appears:

```
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 Recovery**.

The password is reset to **cisco**. You can change the password the next time you log in to the CLI.

Using ROMMON

For IPS-4240 and IPS-4255 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.

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-4240-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

```

Password Recovery for AIM-IPS

To recover the password for AIM-IPS, use the **clear password** command. You must have console access to AIM-IPS and administrative access to the router.

To recover the password for AIM-IPS, follow these steps:

-
- Step 1** Log in to the router.
- Step 2** Enter privileged EXEC mode on the router:
- ```
router> enable
```
- Step 3** Confirm the module slot number in your router:
- ```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```
- Step 4** Session in to AIM-IPS:
- ```
router# service-module ids-sensor slot/port session
```
- Example:
- ```
router# service-module ids-sensor 0/0 session
```
- Step 5** Press **Control-shift-6** followed by **x** to navigate to the router CLI.
- Step 6** Reset AIM-IPS from the router console:
- ```
router# service-module ids-sensor 0/0 reset
```
- Step 7** Press **Enter** to return to the router console.
- Step 8** When prompted for boot options, enter **\*\*\*** quickly.
- You are now in the bootloader.

**Step 9** Clear the password:

```
ServicesEngine boot-loader# clear password
```

AIM-IPS reboots.

The password is reset to **cisco**. Log in to the CLI with username cisco and password cisco. You can then change the password.

---

## Password Recovery for AIP-SSM

**Note**

To recover the password on AIP-SSM, you must have ASA 7.2.3.

---

Use the **hw-module module slot\_number password-reset** command to reset the AIP-SSM password to the default **cisco**. The ASA 5500 series adaptive security appliance sets the ROMMON confreg bits to 0x7 and then reboots the sensor. The ROMMON bits cause the GRUB menu to default to option 2 (**reset password**).

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.
```

## Password Recovery for IDSM-2

To recover the password for IDSM-2, you must perform a system image upgrade, which installs a special password recovery image instead of a typical system image. This upgrade only resets the password, all other configuration remains intact. You must have administrative access to the Cisco 6500 series switch to recover the password. You boot to the maintenance partition and execute the **upgrade** command to install a new image. Use the following commands:

- For Catalyst software:

```
reset module_number cf:1
session module_number
```
- For Cisco IOS software:

```
hw-module module module_number reset cf:1
session slot slot_number processor 1
```

The only protocol for upgrades is FTP. Make sure you put the password recovery image file (WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz) on an FTP server.

**Note**

Reimaging the IDSM-2 only changes the **cisco** account password.

---

## Password Recovery for NME-IPS

To recover the password for NME-IPS, use the **clear password** command. You must have console access to NME-IPS and administrative access to the router.

To recover the password for NME-IPS, follow these steps:

---

**Step 1** Log in to the router.

**Step 2** Enter privileged EXEC mode on the router:

```
router> enable
```

**Step 3** Confirm the module slot number in your router:

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

**Step 4** Session in to NME-IPS:

```
router# service-module ids-sensor slot/port session
```

Example:

```
router# service-module ids-sensor 1/0 session
```

**Step 5** Press **Control-shift-6** followed by **x** to navigate to the router CLI.

**Step 6** Reset NME-IPS from the router console:

```
router# service-module ids-sensor 1/0 reset
```

**Step 7** Press **Enter** to return to the router console.

**Step 8** When prompted for boot options, enter **\*\*\*** quickly.

You are now in the bootloader.

**Step 9** Clear the password:

```
ServicesEngine boot-loader# clear password
```

NME-IPS reboots.

The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

---

## 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.

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
```

---

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

---

**Step 1** Log in to 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 the AIM-IPS and NME-IPS bootloader, ROMMON, and the maintenance partition for IDSM-2, 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.

- When performing password recovery on IDSM-2, you see the following message: `Upgrading will wipe out the contents on the storage media.` You can ignore this message. Only the password is reset when you use the specified password recovery image.

## Clearing the Sensor Databases

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.



### Caution

---

We do not recommend that you use this 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 following options apply:

- *virtual-sensor*—Name of a virtual sensor configured on the sensor.
- **all**— Clear all the 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.

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.
- 

## Configuring Health Status Information

Use the **health-monitor** command in service submode to configure the health statistics for the sensor. Use the **show health** command to see the results of the **health-monitor** command.

The following options 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.
- **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 IME. Disable event retrieval policy if you are not doing external event monitoring.

- **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.
- **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.
- **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

The health status categories are rated by red and green with red being critical.

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 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 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 sensor health and security monitoring:

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

**Step 6** Set the event retrieval thresholds:

```
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 heartbeat events to be emitted at the specified interval of seconds:

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

**Step 8** 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 9** 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 10** 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 11** 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 12** 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 13** 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 14** 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 15** 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 16** Exit health monitoring submode:

```

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

```

**Step 17** Press **Enter** to apply the changes or enter **no** to discard them.

## Showing Sensor Overall Health Status

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.



### 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.

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

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 of a completed banner login:

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

**Step 5** To remove the banner login:

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

The banner no longer appears at login.

---

## Terminating CLI Sessions

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 options apply:

- **cli\_id**—CLI ID number associated with the login session. Use the **show users** command to find the CLI ID number.
- **message**—Message to send to the receiving user.

**Caution**

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

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

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.

**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.

---

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
```

---

## Displaying and Clearing Events

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

- [Displaying Events, page 16-16](#)
- [Clearing Events from Event Store, page 16-19](#)

## Displaying Events

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.

**Note**


---

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

---

The following options 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 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**—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 ARC (block) requests.



**Note** ARC is formerly known as NAC. This name change has not been completely implemented throughout IDM, IME, and the CLI for Cisco IPS 6.1.

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

To display events from Event Store, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Display all events starting now:

```
sensor# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
originator:
 hostId: sensor2
 appName: cidwebserver
 appInstanceId: 12075
time: 2008/01/07 04:41:45 2008/01/07 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: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exception:
handshake incomplete.
```

The feed continues showing all events until you press **Ctrl-C**.

**Step 3** Display the block requests beginning at 10:00 a.m. on February 9, 2008:

```
sensor# show events NAC 10:00:00 Feb 9 2008
evShunRqst: eventId=1106837332219222281 vendor=Cisco
originator:
 deviceName: Sensor1
 appName: NetworkAccessControllerApp
 appInstance: 654
```

```

time: 2008/02/09 10:33:31 2008/08/09 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, 2008:

```

sensor# show events error warning 10:00:00 Feb 9 2008
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
originator:
 hostId: sensor
 appName: cidwebserver
 appInstanceId: 12160
time: 2008/01/07 04:49:25 2008/01/07 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: 2008/03/02 14:15:59 2008/03/02 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: 2008/01/08 02:41:00 2008/01/08 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: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
syslogMessage:
 description: session opened for user cisco by cisco(uid=0)
```

---

## Clearing Events from Event Store

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

To clear events from Event Store, follow these steps:

---

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

**Step 2** Clear 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.

---

## Setting 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 16-19](#)
- [Manually Setting the Clock, page 16-20](#)

## 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 16-2 lists the system clock flags.

**Table 16-2 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:

```
sensor# show clock detail
20:09:43 UTC Thu Apr 03 2008
Time source is NTP
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

This 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 2008
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

This indicates that no time source is configured.

## Manually Setting the Clock

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.



### 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.

The **clock set** command does not apply to the following platforms:

- AIM-IPS
- AIP-SSM
- IDSM-2
- NME-IPS

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 2008
```



**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 options apply:

- *virtual\_sensor*—(Optional) The virtual sensor whose denied attackers list should be cleared.
- *ip\_address*—(Optional) The IP address to clear.

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:

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

The statistics show that there are two IP addresses being denied at this time.

**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 10.1.1.1
Warning: Executing this command will delete ip address 10.1.1.1 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** To clear only the statistics:

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

**Step 11** Verify that you have cleared the statistics:

```
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

```

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.

## 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 | authentication | event-server | event-store | external-product-interface | host | logger | network-access | notification | sdee-server | transaction-server | 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] 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.

To display statistics for the sensor, follow these steps:

**Step 1** Log in to the CLI.

**Step 2** Display the statistics for Analysis Engine:

```

sensor# show statistics analysis-engine
Analysis Engine Statistics
 Number of seconds since service started = 1421127
 Measure of the level of current resource utilization = 0
 Measure of the level of maximum resource utilization = 0
 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 = 0
 Total number of packets denied = 0
 Total number of packets reset = 0
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
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-4240#

```

**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 Event Server:

```

sensor# show statistics event-server

```

```

General
 openSubscriptions = 0
 blockedSubscriptions = 0
Subscriptions
sensor#

```

**Step 7** Display the statistics for Event Store:

```

sensor# show statistics event-store
Event 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 queries issued = 0
 The number of times the event store circular buffer has wrapped = 0
 Number of events of each type currently stored
 Debug events = 0
 Status events = 9904
 Log transaction events = 0
 Shun request events = 61
 Error events, warning = 67
 Error events, error = 83
 Error events, fatal = 0
 Alert events, informational = 60
 Alert events, low = 1
 Alert events, medium = 60
 Alert events, high = 0
sensor#

```

**Step 8** Display the statistics for the host:

```

sensor# show statistics host
General Statistics
 Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2008
 Command Control Port Device = FastEthernet0/0
Network Statistics
 fe0_0 Link encap:Ethernet HWaddr 00:0B:46:53:06:AA
 inet addr:10.89.149.185 Bcast:10.89.149.255 Mask:255.255.255.128
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
 TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:57547021 (54.8 Mib) TX bytes:63832557 (60.8 MiB)
 Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
 status = Not applicable
Memory Usage
 usedBytes = 500592640
 freeBytes = 8855552
 totalBytes = 509448192
Swap Usage
 Used Bytes = 77824
 Free Bytes = 600649728

 Total Bytes = 600727552
CPU Statistics
 Usage over last 5 seconds = 0
 Usage over last minute = 1
 Usage over last 5 minutes = 1
Memory Statistics
 Memory usage (bytes) = 500498432
 Memory free (bytes) = 894976032
Auto Update Statistics
 lastDirectoryReadAttempt = 15:26:33 CDT Tue Jun 17 2008

```

```

= Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
= Success
lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2008
= Download: http://bmarquardt@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/IPS-
sig-S338-req-E1.pkg
= Error: httpResponse status returned: Unauthorized
lastInstallAttempt = N/A
nextAttempt = 16:26:30 CDT Tue Jun 17 2008

sensor#

```

**Step 9** 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 10** Display the statistics for 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 = 10.89.150.219
 NATAddr = 0.0.0.0
 Communications = ssh-des
NetDevice
 Type = PIX
 IP = 10.89.150.250
 NATAddr = 0.0.0.0
 Communications = telnet
NetDevice
 Type = Cisco
 IP = 10.89.150.158
 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 = 10.89.150.138
 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 = 10.89.150.171
 AclSupport = Does not use ACLs
 Version = 6.3
 State = Active
 Firewall-type = PIX
 NetDevice
 IP = 10.89.150.219
 AclSupport = Does not use ACLs
 Version = 7.0
 State = Active
 Firewall-type = ASA
 NetDevice
 IP = 10.89.150.250
 AclSupport = Does not use ACLs
 Version = 2.2
 State = Active
 Firewall-type = FWSM
 NetDevice
 IP = 10.89.150.158
 AclSupport = uses Named ACLs
 Version = 12.2
 State = Active
 NetDevice
 IP = 10.89.150.138
 AclSupport = Uses VACLs
 Version = 8.4
 State = Active
 BlockedAddr
 Host
 IP = 22.33.4.5
 Vlan =
 ActualIp =
 BlockMinutes =
 Host
 IP = 21.21.12.12
 Vlan =
 ActualIp =
 BlockMinutes =
 Host
 IP = 122.122.33.4
 Vlan =
 ActualIp =
 BlockMinutes = 60
 MinutesRemaining = 24

```

```

Network
 IP = 111.22.0.0
 Mask = 255.255.0.0
 BlockMinutes =
sensor#

```

**Step 11** 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 12** Display the statistics for the SDEE server:

```

sensor# show statistics sdee-server
General
 Open Subscriptions = 0
 Blocked Subscriptions = 0
 Maximum Available Subscriptions = 5
 Maximum Events Per Retrieval = 500
Subscriptions
sensor#

```

**Step 13** Display the statistics for the transaction server:

```

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

```

**Step 14** Display the statistics for a virtual sensor:

```

sensor# show statistics virtual-sensor vs0
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 =
 General Statistics for this Virtual Sensor
 Number of seconds since a reset of the statistics = 1421711
 Measure of the level of resource utilization = 0
 Total packets processed since reset = 0
 Total IP 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 =
 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 packets with bad IP checksums processed since reset = 0
 Total packets with bad layer 4 checksums processed 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 (can not be reset
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 constraint
TCP nodes keyed on both IP addresses and both ports = 0
Packets dropped because they would exceed Database insertion rate limit
s = 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 Initial 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
Current Streams = 0
Current Streams Closed = 0
Current Streams Closing = 0
Current Streams Embryonic = 0
Current Streams Established = 0
Current Streams Denied = 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
SigEvent Action Override Stage Statistics
Number of Alerts received to Action Override Processor = 0
Number of Alerts where an override was applied = 0
Actions Added
deny-attacker-inline = 0
deny-attacker-victim-pair-inline = 0
deny-attacker-service-pair-inline = 0
deny-connection-inline = 0
deny-packet-inline = 0
modify-packet-inline = 0
log-attacker-packets = 0
log-pair-packets = 0
log-victim-packets = 0
produce-alert = 0
produce-verbose-alert = 0
request-block-connection = 0
request-block-host = 0
request-snmp-trap = 0
reset-tcp-connection = 0
request-rate-limit = 0
SigEvent Action Filter Stage Statistics
Number of Alerts received to Action Filter Processor = 0
Number of Alerts where an action was filtered = 0
Number of Filter Line matches = 0
Number of Filter Line matches causing decreased DenyPercentage = 0
Actions Filtered
deny-attacker-inline = 0
deny-attacker-victim-pair-inline = 0
deny-attacker-service-pair-inline = 0
deny-connection-inline = 0
deny-packet-inline = 0
modify-packet-inline = 0
log-attacker-packets = 0
log-pair-packets = 0
log-victim-packets = 0
produce-alert = 0
produce-verbose-alert = 0
request-block-connection = 0
request-block-host = 0
request-snmp-trap = 0
reset-tcp-connection = 0
request-rate-limit = 0
SigEvent Action Handling Stage Statistics.
Number of Alerts received to Action Handling Processor = 0

```

```

Number of Alerts where produceAlert was forced = 0
Number of Alerts where produceAlert was off = 0
Actions Performed
 deny-attacker-inline = 0
 deny-attacker-victim-pair-inline = 0
 deny-attacker-service-pair-inline = 0
 deny-connection-inline = 0
 deny-packet-inline = 0
 modify-packet-inline = 0
 log-attacker-packets = 0
 log-pair-packets = 0
 log-victim-packets = 0
 produce-alert = 0
 produce-verbose-alert = 0
--MORE--

```

**Step 15** Display the statistics for Web Server:

```

sensor# show statistics web-server
listener-443
 number of server session requests handled = 61
 number of server session requests rejected = 0
 total HTTP requests handled = 35
 maximum number of session objects allowed = 40
 number of idle allocated session objects = 10
 number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#

```

**Step 16** To clear the statistics for an application, for example, the logging application:

```

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

```

The statistics were retrieved and cleared.

**Step 17** Verify that the statistics have been cleared:

```

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#

```

The statistics all begin from 0.

## Displaying Tech Support Information

Use the **show tech-support [page] [password] [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.
- **password**—Leaves passwords and other security information in the output.
- **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.

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:

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

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.

**Step 3** To send the output (in HTML format) to a file, follow these steps:

- Enter the following command, followed by a valid destination:

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

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.

For 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
```

The `password:` prompt appears.

- 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.

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 6.1(1)E1

Host:
 Realm Keys key1.0
Signature Definition:
 Signature Update S323.0 2008-03-24
 Virus Update V1.2 2005-11-24
OS Version: 2.4.30-IDS-smp-bigphys
Platform: IPS-4240-K9
Serial Number: P30000000652
No license present
Sensor up-time is 4 days.
Using 1421475840 out of 1984548864 bytes of available memory (71% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 41.0M out of 166.8M bytes of available disk space (26%
usage)
boot is using 40.4M out of 68.6M bytes of available disk space (62% usage)

MainApp M-2008_APR_16_21_44 (Release) 2008-04-16T22:25:36-0500 Running
AnalysisEngine M-2008_APR_16_21_44 (Release) 2008-04-16T22:25:36-0500 Running
CLI M-2008_APR_16_21_44 (Release) 2008-04-16T22:25:36-0500

Upgrade History:

 IPS-K9-6.1-1-E1 21:44:00 UTC Wed Apr 16 2008

Recovery Partition Version 1.1 - 6.1(1)E1

Host Certificate Valid from: 23-Apr-2008 to 24-Apr-2010

sensor#
```



**Note** If the `--MO RE--` 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 Thu Apr 24 16:21:25 2008
! -----
! Version 6.1(1)
! Host:
! Realm Keys key1.0
! Signature Definition:
! Signature Update S323.0 2008-03-24
! Virus Update V1.2 2005-11-24
! -----
service interface
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.147.45/25,10.89.147.126
telnet-option enabled
access-list 0.0.0.0/0
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
exit
! -----
service anomaly-detection ad0
exit
! -----

```

```
service external-product-interface
exit
! -----
service health-monitor
exit
! -----
service analysis-engine
exit
sensor#
```

---

## Diagnosing Network Connectivity

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



### Caution

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

---

To diagnose basic network connectivity, follow these steps:

---

**Step 1** Log in to the CLI.

**Step 2** Ping the address you are interested in:

```
sensor# ping ip_address count
```

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.

Example of a successful ping:

```
sensor# ping 10.89.146.110 6
PING 10.89.146.110 (10.89.146.110): 56 data bytes
64 bytes from 10.89.146.110: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 10.89.146.110: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=5 ttl=61 time=0.2 ms

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

Example of an unsuccessful ping:

```
sensor# ping 172.21.172.1 3
PING 172.21.172.1 (172.21.172.1): 56 data bytes

--- 172.21.172.1 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, follow 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** To 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 modules, see the following individual procedures:

- [Rebooting, Resetting, and Shutting Down AIM-IPS, page 17-17](#)
- [Reloading, Shutting Down, Resetting, and Recovering AIP-SSM, page 18-13](#)
- [Resetting IDSM-2, page 19-41](#)
- [Rebooting, Resetting, and Shutting Down NME-IPS, page 20-11](#)

## 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:

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

**Step 3** Show the history of the commands you have used in network access mode:

```
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.

PEP information provides an easy way to obtain the hardware version and serial number through the CLI.



### Note

---

The **show inventory** command does not apply to IPS modules, such as AIM-IPS, AIP-SSM, IDSM-2, or NME-IPS.

---

To display PEP information, follow these steps:

---

**Step 1** Log in to the CLI.

**Step 2** Display the PEP information:

```
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-4240# show inventory
```

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

You can use this information when dealing with the TAC.

## Tracing the Route of an IP Packet

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.



### Caution

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

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 10.1.1.1
traceroute to 10.1.1.1 (10.1.1.1), 4 hops max, 40 byte packets
 1 10.89.130.1 (10.89.130.1) 0.267 ms 0.262 ms 0.236 ms
 2 10.89.128.17 (10.89.128.17) 0.24 ms * 0.399 ms
 3 * 10.89.128.17 (10.89.128.17) 0.424 ms *
 4 10.89.128.17 (10.89.128.17) 0.408 ms * 0.406 ms
sensor#
```

**Step 3** To have the route take more hops than the default of 4, use the `count` option:

```
sensor# trace 10.1.1.1 8
traceroute to 10.1.1.1 (10.1.1.1), 8 hops max, 40 byte packets
 1 10.89.130.1 (10.89.130.1) 0.35 ms 0.261 ms 0.238 ms
 2 10.89.128.17 (10.89.128.17) 0.36 ms * 0.344 ms
 3 * 10.89.128.17 (10.89.128.17) 0.465 ms *
 4 10.89.128.17 (10.89.128.17) 0.319 ms * 0.442 ms
 5 * 10.89.128.17 (10.89.128.17) 0.304 ms *
 6 10.89.128.17 (10.89.128.17) 0.527 ms * 0.402 ms
 7 * 10.89.128.17 (10.89.128.17) 0.39 ms *
 8 10.89.128.17 (10.89.128.17) 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: netranger default:

 profile-name: insidePix

 enable-password: <hidden>
 password: <hidden>
 username: <defaulted>

 profile-name: qatest

 enable-password: <hidden>

```

```

password: <hidden>
username: <defaulted>

profile-name: fwsn

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: 10.89.147.61

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: 10.89.147.54

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: 10.89.147.10

communication: telnet default: ssh-3des
nat-address: 0.0.0.0 <defaulted>
profile-name: insidePix

ip-address: 10.89.147.82

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: gatest
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: 10.89.147.61

router-devices (min: 0, max: 250, current: 1)

ip-address: 10.89.147.54

firewall-devices (min: 0, max: 250, current: 2)

ip-address: 10.89.147.10
ip-address: 10.89.147.82

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: gatest
profile-name: fwsm
profile-name: outsidePix
profile-name: cat
profile-name: rcat
profile-name: nopass
profile-name: test
profile-name: sshswitch
ip-address: 10.89.147.61
profile-name: cat
ip-address: 10.89.147.54
profile-name: r7200
ip-address: 10.89.147.10
profile-name: insidePix
ip-address: 10.89.147.82
profile-name: test
sensor(config-net)#

```

