



# CHAPTER 13

## 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:

- [Creating a Banner Login, page 13-1](#)
- [Terminating CLI Sessions, page 13-2](#)
- [Modifying Terminal Properties, page 13-3](#)
- [Events, page 13-4](#)
- [System Clock, page 13-7](#)
- [Clearing the Denied Attackers List, page 13-9](#)
- [Displaying Statistics, page 13-10](#)
- [Displaying Tech Support Information, page 13-18](#)
- [Displaying Version Information, page 13-19](#)
- [Directing Output to a Serial Connection, page 13-21](#)
- [Diagnosing Network Connectivity, page 13-22](#)
- [Resetting the Appliance, page 13-23](#)
- [Displaying Command History, page 13-24](#)
- [Displaying Hardware Inventory, page 13-24](#)
- [Tracing the Route of an IP Packet, page 13-25](#)
- [Displaying Submode Settings, page 13-26](#)

### 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** Type 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.

**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#
```

**Step 4** 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
```

---

## Events

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

- [Displaying Events, page 13-4](#)
- [Clearing Events from the Event Store, page 13-7](#)

## Displaying Events

Use the **show events** `[[alert [informational] [low] [medium] [high] [include-traits traits] [exclude-traits traits]] | error [warning] [error] [fatal] | NAC | status]] [hh:mm:ss [month day [year]] | past hh:mm:ss]` 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 until you cancel the request by pressing 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.  
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).
- **error**—Displays error events. Error events are generated by services when error conditions are encountered.
- **NAC**—Displays ARC (block) requests.



### Note

---

ARC is formerly known as Network Access Controller (NAC). This name change has not been completely implemented throughout the IDM and CLI for IPS 5.1.

---

- **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 waits until a specified event is available. It continues to wait and display events until you exit by pressing Ctrl-C.

To display events from the 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: 2003/01/07 04:41:45 2003/01/07 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: 2003/01/07 04:41:45 2003/01/07 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, 2005:

```
sensor# @ show events NAC 10:00:00 Feb 9 2005
evShunRqst: eventId=1106837332219222281 vendor=Cisco
originator:
  deviceName: Sensor1
  appName: NetworkAccessControllerApp
  appInstance: 654
time: 2005/02/09 10:33:31 2004/08/09 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. February 9 2005:

```
sensor# show events error warning 10:00:00 Feb 9 2005
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
originator:
  hostId: sensor
  appName: cidwebserver
  appInstanceId: 12160
```

```
time: 2003/01/07 04:49:25 2003/01/07 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: 2005/03/02 14:15:59 2005/03/02 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: 2003/01/08 02:41:00 2003/01/08 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: 2003/01/08 02:41:00 2003/01/08 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 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** Type **yes** to clear the events.

---

## System Clock

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

- [Displaying the System Clock, page 13-7](#)
- [Manually Setting the Clock, page 13-8](#)

## 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.

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
```

```
22:39:21 UTC Sat Jan 25 2003
```

**Step 3** Display the system clock with details:

```
sensor# show clock detail
```

```
22:39:21 CST Sat Jan 25 2003
```

```
Time source is NTP
```

```
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

This indicates that the sensor is getting its time from NTP and that is configured and synchronized.

```
sensor# show clock detail
*12:19:22 CST Sat Dec 04 2004
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2004
Summer time ends 02:00:00 CDT Sun Oct 27 2004
```

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.

For the procedure for configuring NTP, see [Configuring NTP, page 4-29](#). For an explanation of the importance of having a valid time source for the sensor, see [Time Sources and the Sensor, page 4-18](#). For an explanation of what to do if you set the clock incorrectly, see [Correcting Time on the Sensor, page 4-21](#).

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

- IDSM-2
- NM-CIDS
- AIP-SSM-10
- AIP-SSM-20

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 July 29 2004
```



### Note

The time format is 24-hour time.

# Clearing the Denied Attackers List

Use the **clear denied-attackers** command in service event action rules submode 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 will be 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.

To delete the list of denied attackers 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** Type **yes** to clear the list.

**Step 5** Verify that you have cleared the list:

```
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.
```

There is no longer any information under the Denied Attackers and hit count for each category.

**Step 6** To clear only the statistics:

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

**Step 7** 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 Statistics

Use the **show statistics virtual-sensor [clear]** command to display the statistics for the virtual sensor. Use the **show statistics [analysis-engine | authentication | denied-attackers | event-server | event-store | host | logger | network-access | notification | sdee-server | transaction-server | transaction-source | web-server] [clear]** command to generate statistics for each sensor application.



### Note

The **clear** option is not available for the analysis engine, host, or network access applications.

To display statistics for the sensor, follow these steps:

- Step 1** Log in to the CLI.
- Step 2** Display the statistics for the virtual 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 = fe0_1
  General Statistics for this Virtual Sensor
  Number of seconds since a reset of the statistics = 1675
  Measure of the level of resource utilization = 0
  Total packets processed since reset = 241
  Total IP packets processed since reset = 12
  Total packets that were not IP processed since reset = 229
  Total TCP packets processed since reset = 0
  Total UDP packets processed since reset = 0
  Total ICMP packets processed since reset = 12
  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 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 = 22513
  The rate of packets per second since reset = 0
  The rate of bytes per second since reset = 13
  The average bytes per packet since reset = 93
  Denied Address Information
  Number of Active Denied Attackers = 0

```

```

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 = 0
Denied Attackers 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 = 28
    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 = 6
  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
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 = 491
  Number of Alerts Consumed by AlertInterval = 0
  Number of Alerts Consumed by Event Count = 0
  Number of FireOnce First Alerts = 6
  Number of FireOnce Intermediate Alerts = 480
  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 Alerts Output for further processing = 491
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-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
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
  Actions Filtered
    deny-attacker-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
SigEvent Action Handling Stage Statistics.
  Number of Alerts received to Action Handling Processor = 491
  Number of Alerts where produceAlert was forced = 0
  Number of Alerts where produceAlert was off = 0
  Actions Performed
    deny-attacker-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 = 11
    produce-verbose-alert = 0
    request-block-connection = 0

```

```

request-block-host = 5
request-snmp-trap = 0
reset-tcp-connection = 0
Deny Actions Requested in Promiscuous Mode
deny-packet not performed = 0
deny-connection not performed = 0
deny-attacker not performed = 0
modify-packet not performed = 0
Number of Alerts where deny-connection was forced for deny-packet action = 0
Number of Alerts where deny-packet was forced for non-TCP deny-connection action
= 0
Per-Signature SigEvent count since reset
Sig 2004 = 5
Sig 2156 = 486
sensor#

```

**Step 3** Display the statistics for AnalysisEngine:

```

sensor# show statistics analysis-engine
Analysis Engine Statistics
Number of seconds since service started = 1999
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 = 13
Receiver Statistics
Total number of packets processed since reset = 290
Total number of IP packets processed since reset = 12
Transmitter Statistics
Total number of packets transmitted = 290
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 = 491
Statistics for Actions executed on a SigEvent
Number of Alerts written to the IdsEventStore = 11
sensor#

```

**Step 4** Display the statistics for authentication:

```

sensor# show statistics authentication
General
totalAuthenticationAttempts = 2
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.

```

```
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 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 2005
  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 = N/A
  lastDownloadAttempt = N/A
  lastInstallAttempt = N/A
  nextAttempt = N/A
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 the transaction source:

```

sensor# show statistics transaction-source
General
  totalControlTransactions = 0
  failedControlTransactions = 0
sensor#

```

**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:

a. Type 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. Type 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
```

The following examples show sample version output for the appliance and the NM-CIDS.

Sample version output for the appliance:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.1(0.16)S185.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 5 days.
Using 722145280 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.3M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)

MainApp          2005_Feb_18_03.00  (Release)  2005-02-18T03:13:47-0600  Running
AnalysisEngine   2005_Feb_18_03.00  (Release)  2005-02-18T03:13:47-0600  Running
CLI              2005_Feb_18_03.00  (Release)  2005-02-18T03:13:47-0600
```

Upgrade History:

```
IDS-K9-min-5.1-0.16 03:00:00 UTC Mon Oct 31 2005
```

Recovery Partition Version 1.1 - 5.1(0.16)

sensor#

Sample version output for NM-CIDS:

```
nm-cids# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.1(0.16)S185.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: NM-CIDS
Serial Number: JAD06490681
No license present
Sensor up-time is 1 day.
Using 485675008 out of 509448192 bytes of available memory (95% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 31.1M out of 166.8M bytes of available disk space (20% usage)
boot is using 39.5M out of 68.6M bytes of available disk space (61% usage)
application-log is using 529.6M out of 2.8G bytes of available disk space (20% usage)

MainApp          2005_Feb_09_03.00  (Release)  2005-02-09T03:22:27-0600  Running
AnalysisEngine   2005_Feb_09_03.00  (Release)  2005-02-09T03:22:27-0600  Running
CLI              2005_Feb_09_03.00  (Release)  2005-02-09T03:22:27-0600
```

Upgrade History:

```
IDS-K9-min-5.1-0.16 03:00:00 UTC Mon Oct 31 2005
```

Recovery Partition Version 1.1 - 5.1(0.16)

nm-cids#



**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
! -----
! Version 5.1(0.16)
! Current configuration last modified Wed Oct 31 03:20:54 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on banner login.
exit
time-zone-settings
--MORE--
```

## Directing Output to a Serial Connection

Use the **display-serial** command to direct all output to a serial connection. This lets you view system messages on a remote console (using the serial port) during the boot process. The local console is not available as long as this option is enabled. Use the **no display-serial** command to reset the output to the local terminal.



### Caution

If you are connected to the serial port, you will not get any feedback until Linux has fully booted and enabled support for the serial connection.

The **display-serial** command does not apply to the following IPS platforms:

- IDSM-2
- NM-CIDS
- IDS-4215
- IPS-4240

- IPS-4255
- IPS-4260
- AIP-SSM 10
- AIP-SSM 20

To direct output to the serial port, follow these steps:

---

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

**Step 2** Direct the output to the serial port:

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

The default is not to direct the output to a serial connection.

**Step 3** Reset the output to the local console:

```
sensor(config)# no display-serial
```

---

## 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 gracefully 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.



### Note

To reset the modules, see the individual procedures: [Resetting IDSM-2, page 15-40](#), [Shutting Down, Reloading, and Resetting NM-CIDS, page 16-7](#), and [Reloading, Shutting Down, Resetting, and Recovering AIP-SSM, page 14-5](#).

Shut down (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 will be 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. Otherwise, to power down the appliance, go to Step 4.

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

**Step 3** Type **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** Type **yes** to continue with the reset and powerdown:

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

---

## 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.

The **show inventory** command does not apply to the following platforms:

- IDSM-2
- NM-CIDS
- IDS-4210
- IDS-4215

- IDS-4235
- IDS-4250

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: netrangr default:
-----
profile-name: insidePix
-----
enable-password: <hidden>
password: <hidden>
username: <defaulted>
-----
profile-name: gatest
-----
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: 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)#
```

---