APPENDIX C

Troubleshooting

Caution The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Obtaining Cisco IPS Software, page 18-1.

This appendix contains troubleshooting tips and procedures for sensors and software. It contains the following sections:

Bug Toolkit

For the most complete and up-to-date list of caveats, use the Bug Toolkit to refer to the caveat release note. You can use the Bug Toolkit to search for known bugs based on software version, feature set, and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable. It also lets you save the results of a search in Bug Groups, and also create persistent Alert Agents that can feed those groups with new defect alerts.

Note You must be logged in to Cisco.com to access the Bug Toolkit.

If you are a registered Cisco.com user, you can view the Bug Toolkit at this URL:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

To become a registered cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Preventive Maintenance

The following actions will help you maintain your sensor:

- Back up a good configuration. If your current configuration becomes unusable, you can replace it with the backup version.

  For the procedure, see Creating and Using a Backup Configuration File, page 12-18.

- Save your backup configuration to a remote system.

  For the procedure, see Copying and Restoring the Configuration File Using a Remote Server, page 12-16.

- Always back up your configuration before you do a manual upgrade. If you have auto upgrades configured, make sure you do periodic backups.

- Create a service account.

  A service account is needed for password recovery and other special debug situations directed by TAC.

  For the procedure, see Creating the Service Account, page 4-13.

Caution You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a new password if the Administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Note You cannot use the service account for password recovery on AIP-SSM, because you cannot get shell access to AIP-SSM. You must use ROMMON to get shell access to AIP-SSM.

Disaster Recovery

This section provides recommendations and steps to take if you need to recover your sensor after a disaster.

Follow these recommendations so that you are ready in case of a disaster:

- If you are using the CLI or IDM for configuration, copy the current configuration from the sensor to an FTP or SCP server any time a change has been made.

  For the procedure, see Creating and Using a Backup Configuration File, page 12-18.

  Note You should note the specific software version for that configuration. You can apply the copied configuration only to a sensor of the same version.

Note You also need the list of user IDs that have been used on that sensor. The list of user IDs and passwords are not saved in the configuration. For the procedure for obtaining a list of the current users on the sensor, see Viewing User Status, page 4-16.

- If you are using IDS MC, the current configuration is saved in the IDS MC database and a separate copy is not needed.

Note The list of user IDs is not saved in the IDS MC database. You must make a note of the user IDs.

Note You should note the specific software version for that configuration. You can push the copied configuration only to a sensor of the same version.

When a disaster happens and you need to recover the sensor, try the following:

1. Reimage the sensor.

   For the procedures for appliances and modules, see Chapter 17, "Upgrading, Downgrading, and Installing System Images."

2. Log in to the sensor with the default user ID and password—**cisco**.

Note You are prompted to change the cisco password.

3. Run the **setup** command.

   For the procedure, see Initializing the Sensor, page 3-2.

4. Upgrade the sensor to the IPS software version it had when the configuration was last saved and copied.

   For more information on obtaining IPS software versions and how to install them, see Obtaining Cisco IPS Software, page 18-1.

Warning **Trying to copy the saved configuration without getting the sensor back to the same IPS software version it had before the disaster can cause configuration errors.**

5. Copy the last saved configuration to the sensor.

   For the procedure, see Creating and Using a Backup Configuration File, page 12-18.

6. Update clients to use the new key and certificate of the sensor.

   Reimaging changes the sensor's SSH keys and HTTPS certificate. For the procedure, see Adding Hosts to the Known Hosts List, page 4-32.

7. Create previous users.

   For the procedure, see Configuring User Parameters, page 4-11.

Password Recovery

The following password recovery options exist:

- If another Administrator account exists, the other Administrator can change the password.
- If a Service account exists, you can log in to the service account and switch to user root using the command **su - root**. Use the **password** command to change the CLI Administrator account's password. For example, if the Administrator username is "adminu," the command is **password adminu**. You are prompted to enter the new password twice. For more information, see Creating the Service Account, page 4-13.

You can reimage the sensor using either the recovery partition or a system image file. For more information, see Chapter 17, "Upgrading, Downgrading, and Installing System Images."

PIX 7.1 Devices and Normalizer Inline Mode

For IPS 5.0 and 5.1, normalizer inline mode may deny packets and/or connections if a PIX 7.1 device is in the traffic flow and the PIX device has been configured for the MSS workaround.

Certain web applications on port 80 cause the PIX device to require the MSS workaround. If that workaround is active, the IPS must have a complimentary workaround.

Problem There is an incompatibility with PIX and IPS when the PIX MSS workaround has been applied. The **show stat vi** command shows many deny packet or deny connection actions along with many 13*xx* signature firings.

Solution Disable or remove all actions from the following normalizer signatures: 1306 and 1311.

Time and the Sensor

This section describes how to maintain accurate time on the sensor, and contains the following topics:

Time Sources and the Sensor

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings. For more information, see Initializing the Sensor, page 3-2.

Here is a summary of ways to set the time on sensors:

- For appliances
  - Use the **clock set** command to set the time. This is the default.

    For the procedure, see Manually Setting the Clock, page 13-8.

  - Use NTP

    You can configure the appliance to get its time from an NTP time synchronization source. For more information, see Configuring a Cisco Router to be an NTP Server, page 4-29. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can set up NTP on the appliance during initialization or you can configure NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For IDSM-2
  - The IDSM-2 can automatically synchronize its clock with the switch time. This is the default.

    Note The UTC time is synchronized between the switch and the IDSM-2. The time zone and summertime settings are not synchronized between the switch and the IDSM-2.

Caution Be sure to set the time zone and summertime settings on both the switch and IDSM-2 to ensure that the UTC time settings are correct. The local time of IDSM-2 could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch. For more information, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page C-6.

  - Use NTP

    You can configure IDSM-2 to get its time from an NTP time synchronization source. For more information, see Configuring a Cisco Router to be an NTP Server, page 4-29. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure IDSM-2 to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For NM-CIDS
  - NM-CIDS can automatically synchronize its clock with the clock in the router chassis in which it is installed (parent router). This is the default.

    Note The UTC time is synchronized between the parent router and NM-CIDS. The time zone and summertime settings are not synchronized between the parent router and NM-CIDS.

Caution Be sure to set the time zone and summertime settings on both the parent router and NM-CIDS to ensure that the UTC time settings are correct. The local time of NM-CIDS could be incorrect if the time zone and/or summertime settings do not match between NM-CIDS and the router. For more information, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page C-6.

  - Use NTP

    You can configure NM-CIDS to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. For more information, see Configuring a Cisco Router to be an NTP Server, page 4-29. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure NM-CIDS to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

- For AIP-SSM
  - AIP-SSM can automatically synchronize its clock with the clock in the adaptive security appliance in which it is installed. This is the default.

    Note The UTC time is synchronized between the adaptive security appliance and AIP-SSM. The time zone and summertime settings are not synchronized between the adaptive security appliance and AIP-SSM.

Caution Be sure to set the time zone and summertime settings on both the adaptive security appliance and AIP-SSM to ensure that the UTC time settings are correct. The local time of AIP-SSM could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and the adaptive security appliance. For more information, see Synchronizing IPS Module System Clocks with Parent Device System Clocks, page C-6.

  - Use NTP

    You can configure AIP-SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router. For more information, see Configuring a Cisco Router to be an NTP Server, page 4-29. You need the NTP server IP address, the NTP key ID, and the NTP key value. You can configure AIP-SSM to use NTP during initialization or you can set up NTP through the CLI, IDM, or ASDM.

    Note We recommend that you use an NTP time synchronization source.

Synchronizing IPS Module System Clocks with Parent Device System Clocks

All IPS modules (IDSM-2, NM-CIDS, and AIP-SSM) synchronize their system clocks to the parent chassis clock (switch, router, or firewall) each time the module boots up and any time the parent chassis clock is set. The module clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the module clock and the parent clock are synchronized to an external NTP server. If only the module clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs. For more information on NTP, see Configuring NTP, page 4-29. For more information on verifying that the module and NTP server are synchronized, see Verifying the Sensor is Synchronized with the NTP Server, page C-7.

Verifying the Sensor is Synchronized with the NTP Server

In IPS 5.1, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics:

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

Step 3 Generate the hosts statistics again after a few minutes:

```
  sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

Step 4 If the status continues to read `Not Synchronized`, check with the NTP server administrator to make sure the NTP server is configured correctly.

Correcting Time on the Sensor

If you set the time incorrectly, your stored events will have the incorrect time because they are stamped with the time the event was created.

The Event Store time stamp is always based on UTC time. If during the original sensor setup, you set the time incorrectly by specifying 8:00 p.m. rather than 8:00 a.m., when you do correct the error, the corrected time will be set backwards. New events might have times older than old events.

For example, if during the initial setup, you configure the sensor as central time with daylight saving time enabled and the local time is 8:04 p.m., the time is displayed as 20:04:37 CDT and has an offset from UTC of -5 hours (01:04:37 UTC, the next day). A week later at 9:00 a.m., you discover the error: the clock shows 21:00:23 CDT. You then change the time to 9:00 a.m. and now the clock shows 09:01:33 CDT. Because the offset from UTC has not changed, it requires that the UTC time now be 14:01:33 UTC, which creates the time stamp problem.

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command. For more information on the **clear events** command, see Clearing Events from the Event Store, page 13-7.

Caution You cannot remove individual events.

Troubleshooting the 4200 Series Appliance

This section contains information to troubleshoot the 4200 series appliance.

Tip Before troubleshooting the appliance, check the Caveats section of the Readme for the software version you have installed on your sensor to see if you are dealing with a known issue.

This section contains the following topics:

Communication Problems

This section helps you troubleshoot communication problems with the 4200 series sensor. It contains the following topics:

Cannot Access the Sensor CLI Through Telnet or SSH

If you cannot access the sensor CLI through Telnet (if you already have it enabled) or SSH, follow these steps:

Note For the procedure for enabling and disabling Telnet on the sensor, see Enabling and Disabling Telnet, page 4-4.

Step 1 Log in to the sensor CLI through a console, terminal, or module session.

For the various ways to open a CLI session directly on the sensor, see Chapter 2, "Logging In to the Sensor."

Step 2 Make sure that the sensor management interface is enabled:

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

The management interface is the interface in the list with the status line `Media Type = TX`. If the Link Status is `Down`, go to Step 3. If the Link Status is `Up`, go to Step 5.

Step 3 Make sure the sensor's IP address is unique.

```
sensor# setup
--- System Configuration Dialog ---

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


Current Configuration:
```

```
service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

If the management interface detects that another device on the network has the same IP address, it will not come up.

For more information, see Changing the IP Address, Netmask, and Gateway, page 4-3.

Step 4 Make sure the management port is connected to an active network connection.

If the management port is not connected to an active network connection, the management interface will not come up.

Step 5 Make sure the IP address of the workstation that is trying to connect to the sensor is permitted in the sensor's access list:

```
sensor# setup
--- System Configuration Dialog ---

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


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

If the network address of the workstation is permitted in the sensor access list, go to Step 6.

Step 6 Add a permit entry for the workstation's network address, save the configuration, and try to connect again.

For more information, see Changing the Access List, page 4-5.

Step 7 Make sure the network configuration allows the workstation to connect to the sensor.

If the sensor is protected behind a firewall and the workstation is in front of the firewall, make sure the firewall is configured to allow the workstation to access the sensor. Or if the workstation is behind a firewall that is performing network address translation on the IP address of the workstation, and the sensor is in front of the firewall, make sure that the sensor's access list contains a permit entry for the workstation's translated address.

For more information, see Changing the Access List, page 4-5.

Misconfigured Access List

To correct a misconfigured access list, follow these steps:

Step 1 Log in to the CLI.

Step 2 View your configuration to see the access list:

```
sensor# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
sensor#
```

Step 3 Verify that the client IP address is listed in the allowed networks. If it is not, add it:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 171.69.70.0/24
```

Step 4 Verify the settings:

```
sensor(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.89.149.238/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
      host-name: qsensor-238 default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 3)
      -----------------------------------------------
         network-address: 10.0.0.0/8
         -----------------------------------------------
         network-address: 64.0.0.0/8
         -----------------------------------------------
         network-address: 171.69.70.0/24
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
sensor(config-hos-net)#
```

Duplicate IP Address Shuts Interface Down

If you have two newly imaged sensors with the same IP address that come up on the same network at the same time, the interface shuts down. Linux prevents the command and control interface from activating if it detects an address conflict with another host.

To verify that the sensor in question does not have an IP address conflict with another host on the network, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine whether the interface is up:

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
```

```
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

If the output says the command and control interface link status is down, there is a hardware issue or an IP address conflict.

Step 3 Make sure the cabling of the sensor is correct.

Refer to the chapter for your sensor in *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*.

Step 4 Run the **setup** command to make sure the IP address is correct.

For the procedure, see Initializing the Sensor, page 3-2.

SensorApp and Alerting

This section helps you troubleshoot issues with SensorApp and alerting. It contains the following topics:

SensorApp Not Running

The sensing process, SensorApp, should always be running. If it is not, you do not receive any alerts. SensorApp is part of Analysis Engine, so you must make sure the Analysis Engine is running.

To make sure Analysis Engine is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Determine the status of the Analysis Engine service:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: ASA-SSM-20
Serial Number: 021
No license present
Sensor up-time is 19 days.
Using 505495552 out of 1984704512 bytes of available memory (25% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 37.7M out of 166.6M bytes of available disk space (24% usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Running
AnalysisEngine   2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149

sensor#
```

Step 3 If Analysis Engine is not running, look for any errors connected to it:

```
sensor# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=1077219258696330005 severity=warning

originator:
hostId: sensor
appName: sensorApp
appInstanceId: 1045
time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC
errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.
```

Note The date and time of the last restart is listed. In this example, the last restart was on 2-19-2004 at 7:34.

Step 4 Make sure you have the latest software updates:

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

If you do not have the latest software updates, download them from Cisco.com. For the procedure, see Obtaining Cisco IPS Software, page 18-1.

Step 5 Read the Readme that accompanies the software upgrade for any known DDTS for SensorApp or Analysis Engine.

Physical Connectivity, SPAN, or VACL Port Issue

If the sensor is not connected properly, you do not receive any alerts.

To make sure the sensor is connected properly, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the interfaces are up and that the packet count is increasing:

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
```

```
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1830137
   Total Bytes Received = 131624465
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 220052
   Total Bytes Transmitted = 103796666
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 If the Link Status is down, make sure the sensing port is connected properly:

a. Make sure the sensing port is connected properly on the appliance.

Refer to the chapter on your appliance in *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*.

b. Make sure the sensing port is connected to the correct SPAN or VACL capture port on IDSM-2.

For more information, see Chapter 15, "Configuring IDSM-2."

Step 4 Verify the interface configuration:

a. Make sure you have the interfaces configured properly.

For the procedure, see Chapter 5, "Configuring Interfaces."

b. Verify the SPAN and VACL capture port configuration on the Cisco switch.

Refer to your switch documentation for the procedure.

Step 5 Verify again that the interfaces are up and that the packet count is increasing.

```
sensor# show interfaces
```

Unable to See Alerts

If you are not seeing alerts, try the following:

- Make sure the signature is enabled.
- Make sure the signature is not retired.
- Make sure that you have Produce Alert configured as an action.

Note If you choose Produce Alert, but come back later and add another event action and do not add Produce Alert to the new configuration, alerts are not be sent to the Event Store. Every time you configure a signature, the new configuration overwrites the old one, so make sure you have configured all the event actions you want for each signature.

- Make sure the sensor is seeing packets.
- Make sure that alerts are being generated.

To make sure you can see alerts, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the signature is enabled:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# show settings
   status
   -----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   -----------------------------------------------
sensor(config-sig-sig-sta)#
```

Step 3 Make sure you have Produce Alert configured:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer     Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
sensor#
```

Step 4 Make sure the sensor is seeing packets:

```
sensor# show interfaces FastEthernet0/1
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 267581
   Total Bytes Received = 24886471
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 57301
   Total Bytes Transmitted = 3441000
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 1
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 5 Check for alerts:

```
sensor# show statistics virtual-sensor
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 Alerts Output for further processing = 0alertDetails: Traffic Source: int0;
```

Sensor Not Seeing Packets

If the sensor is not seeing any packets on the network, you could have the interfaces set up incorrectly.

If the sensor is not seeing packets, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the interfaces are up and receiving packets:

```
sensor# show interfaces GigabitEthernet0/1
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Down
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Step 3 If the interfaces are not up, do the following:

a. Check the cabling.

For information on installing the sensor properly, refer to the chapter that pertains to your sensor in *Installing Cisco Intrusion Prevention System Appliances and Modules 5.1.*

b. Enable the interface.

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/1
   -----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      -------------------------------------------------
         none
         -------------------------------------------------
         -------------------------------------------------
      -------------------------------------------------
   -----------------------------------------------
sensor(config-int-phy)#
```

Step 4 Check to see that the interface is up and receiving packets:

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 3
   Total Bytes Received = 900
   Total Multicast Packets Received = 3
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0 ...
```

Cleaning Up a Corrupted SensorApp Configuration

If the SensorApp configuration has become corrupted and SensorApp cannot run, you must delete it entirely and restart SensorApp.

To delete the SensorApp configuration, follow these steps:

Step 1 Log in to the service account.

Step 2 Su to root.

Step 3 Stop the IPS applications:

```
/etc/init.d/cids stop
```

Step 4 Replace the virtual sensor file:

```
cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml
/usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml
```

Step 5 Remove the cache files:

```
rm /usr/cids/idsRoot/var/virtualSensor/*.pmz
```

Step 6 Exit the service account.

Step 7 Log in to the sensor CLI.

Step 8 Start the IPS services:

```
sensor# cids start
```

Step 9 Log in to an account with administrator privileges.

Step 10 Reboot the sensor:

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

Bad Memory on IDS-4250-XL

Some IDS-4250-XLs were shipped with faulty DIMMs on the XL cards. The faulty DIMMs cause the sensor to hang or SensorApp to stop functioning and generate a core file.

For the procedure for checking IDS-4250-XL for faulty memory, see the Partner Field Notice 52563.

Blocking

This section provides troubleshooting help for blocking and the ARC service. It contains the following topics.

Troubleshooting Blocking

After you have configured ARC, you can verify if it is running properly by using the **show version** command. To verify that ARC is connecting to the network devices, use the **show statistics network-access** command.

Note ARC was formerly known as Network Access Controller. Although the name has been changed for IPS 5.1, it still appears in IDM and the CLI as Network Access Controller, **nac**, and **network-access**.

To troubleshoot ARC, follow these steps:

1. Verify that ARC is running.

   For the procedure, see Verifying ARC is Running, page C-20.
2. Verify that ARC is connecting to the network devices.

   For the procedure, see Verifying ARC Connections are Active, page C-21.
3. Verify that the Event Action is set to Block Host for specific signatures.

   For the procedure, see Blocking Not Occurring for a Signature, page C-25.
4. Verify that the master blocking sensor is properly configured.

   For the procedure, see Verifying the Master Blocking Sensor Configuration, page C-26.

Note For a discussion of ARC architecture, see Attack Response Controller, page A-11.

Verifying ARC is Running

To verify that ARC is running, use the **show version** command. If MainApp is not running, ARC cannot run. ARC is part of MainApp.

To verify ARC is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify that MainApp is running:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1.1)S152.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
```

```
Sensor up-time is 3 days.
Using 734863360 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 35.6M out of 166.8M bytes of available disk space (23% usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not Running
AnalysisEngine   2005_Mar_18_12.53   (Release)   2005-03-18T13:03:21-0600   Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-sp-5.0-1.1-   12:53:00 UTC Fri Mar 18 2005

Recovery Partition Version 1.1 - 5.0(1.1)

sensor#
```

Step 3 If MainApp displays `Not Running`, ARC has failed. Contact the TAC.

Verifying ARC Connections are Active

If the State is not `Active` in the ARC statistics, there is a problem.

To verify that the State is Active in the statistics, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify that ARC is connecting:

Check the State section of the output to verify that all devices are connecting.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.89.147.54
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.89.147.54
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
sensor#
```

Step 3 If ARC is not connecting, look for recurring errors:

```
sensor# show events error hh:mm:ss month day year | include : nac
```

Example:

```
sensor# show events error 00:00:00 Apr 01 2005 | include : nac
```

Step 4 Make sure you have the latest software updates:

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

If you do not have the latest software updates, download them from Cisco.com. For the procedure, see Obtaining Cisco IPS Software, page 18-1.

Step 5 Read the Readme that accompanies the software upgrade for any known DDTS for ARC.

Step 6 Make sure the configuration settings for each device are correct (the username, password, and IP address). For the procedure, see Device Access Issues, page C-22.

Step 7 Make sure the interface and directions for each network device are correct. For the procedure, see Verifying the Interfaces and Directions on the Network Device, page C-24.

Step 8 If the network device is using SSH-DES or SSH-3DES, make sure that you have enabled SSH connections to the device. For the procedure, see Enabling SSH Connections to the Network Device, page C-24.

Step 9 Verify that each interface and direction on each controlled device is correct. For the procedure, see Verifying the Interfaces and Directions on the Network Device, page C-24.

Device Access Issues

ARC may not be able to access the devices it is managing. Make sure the you have the correct IP address and username and password for the managed devices and the correct interface and direction configured.

Note SSH devices must support SSH 1.5. The sensor does not support SSH 2.0.

To troubleshoot device access issues, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify the IP address for the managed devices:

```
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 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -------------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   -------------------------------------------------
      profile-name: r7200
      -----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      -----------------------------------------------
   -------------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   -------------------------------------------------
   -------------------------------------------------
   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: 0)
   -------------------------------------------------
   -------------------------------------------------
sensor(config-net)#
```

Step 3 Manually connect to the device to make sure you have used the correct username, password, and enable password, and to ensure that the device is reachable from the sensor.

- **a.** Log in to the service account.
- **b.** Telnet or SSH to the network device to verify the configuration.
- **c.** Make sure you can reach the device.
- **d.** Verify the username and password.

Step 4 Verify that each interface/direction on each network device is correct. For the procedure, see Verifying the Interfaces and Directions on the Network Device, page C-24.

Verifying the Interfaces and Directions on the Network Device

To verify that each interface and direction on each controlled device is correct, you can send a manual block to a bogus host and then check to see if deny entries exist for the blocked addresses in the ACL of the router.

Note Click **Monitoring > Active Host Blocks** to perform a manual block from IDM.

To initiate a manual block to a bogus host, follow these steps:

Step 1 Enter ARC general submode:

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
```

Step 2 Start the manual block of the bogus host IP address:

```
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 3 Exit general submode:

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

Step 4 Press **Enter** to apply the changes or type **no** to discard them.

Step 5 Telnet to the router and verify that a deny entry for the blocked address exists in the ACL of the router.

Refer to the router documentation for the procedure.

Step 6 Remove the manual block by repeating Steps 1 through 4 except in Step 2 place **no** in front of the command:

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

Enabling SSH Connections to the Network Device

If you are using SSH-DES or SSH-3DES as the communication protocol for the network device, you must make sure you have enabled it on the device.

To enable SSH connections to the network device, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter configuration mode:

```
sensor# configure terminal
```

Step 3 Enable SSH:

```
sensor(config)# ssh host blocking_device_ip_ address
```

Step 4 Type **yes** when prompted to accept the device.

Blocking Not Occurring for a Signature

If blocking is not occurring for a specific signature, check that the event action is set to block the host.

To make sure blocking is occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter signature definition submode:

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

Step 3 Make sure the event action is set to block the host:

Note If you want to receive alerts, you must always add **produce-alert** any time you configure the event actions.

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
         default-signatures-only
         -----------------------------------------------
            specify-service-ports
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-tcp-max-mss
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-tcp-min-mss
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
--MORE--
```

Step 4 Exit signature definition submode:

```
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Step 5 Press **Enter** to apply the changes or type **no** to discard them.

Verifying the Master Blocking Sensor Configuration

To verify that a master blocking sensor is set up properly or to troubleshoot a master blocking sensor that is not set up properly, you can use the **show statistics network-access** command. Make sure that the forwarding sensor is set up as TLS trusted host if the remote master blocking sensor is using TLS for web access.

To verify the master blocking sensor configuration of a sensor, follow these steps:

Step 1 View the ARC statistics and verify that the master blocking sensor entries are in the statistics:

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 122.122.122.44
         ShunMinutes = 60
         MinutesRemaining = 59
```

Step 2 If the master blocking sensor does not show up in the statistics, you need to add it. For the procedure, see Configuring the Sensor to be a Master Blocking Sensor, page 10-28.

Step 3 Initiate a manual block to a bogus host IP address to make sure the master blocking sensor is initialing blocks:

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

Step 4 Exit network access general submode:

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

Step 5 Press **Enter** to apply the changes or type **no** to discard them.

Step 6 Verify that the block shows up in the ARC's statistics:

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
```

```
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

Step 7 Log in to the master blocking sensor host CLI and, using the **show statistics network-access** command, verify that the block also shows up in the master blocking sensor ARC statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes = 60
         MinutesRemaining = 59
```

Step 8 If the remote master blocking sensor is using TLS for web access, make sure the forwarding sensor is configured as a TLS host:

```
sensor# configure terminal
sensor(config)# tls trust ip master_blocking_sensor_ip_address
```

Logging

TAC may suggest that you turn on debug logging for troubleshooting purposes. LogApp controls what log messages are generated by each application by controlling the logging severity for different logging zones. By default, debug logging is not turned on.

If you enable individual zone control, each zone uses the level of logging that it is configured for. Otherwise, the same logging level is used for all zones.

This section contains the following topics:

Enabling Debug Logging

Caution Enabling debug logging seriously affects performance and should only be done when instructed by TAC.

To enable debug logging, follow these steps:

Step 1 Log in to the service account.

Step 2 Edit the log.conf file to increase the size of the log to accommodate the additional log statements:

```
vi /usr/cids/idsRoot/etc/log.conf
```

Step 3 Change `fileMaxSizeInK=500` to `fileMaxSizeInK=5000`.

Step 4 Locate the zone and CID section of the file and set the severity to debug:

```
severity=debug
```

Step 5 Save the file, exit the vi editor, and exit the service account.

Step 6 Log in to the CLI as administrator.

Step 7 Enter master control submode:

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```

Step 8 To enable debug logging for all zones:

```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   -----------------------------------------------
sensor(config-log-mas)#
```

Step 9 To turn on individual zone control:

```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
sensor(config-log-mas)#
```

Step 10 Exit master zone control:

```
sensor(config-log-mas)# exit
```

Step 11 View the zone names:

```
sensor(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: true default: false
   -----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   -----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
```

```
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   -----------------------------------------------
sensor(config-log)#
```

For a list of what each zone name refers to, see Zone Names, page C-31.

Step 12 Change the severity level (debug, timing, warning, or error) for a particular zone:

```
sensor(config-log)# zone-control IdsEventStore severity error
sensor(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   -----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
```

```
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   -----------------------------------------------
sensor(config-log)#
```

Step 13 Turn on debugging for a particular zone:

```
sensor(config-log)# zone-control nac severity debug
sensor(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   -----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
```

```
        severity: warning <defaulted>
        <protected entry>
        zone-name: cplane
        severity: warning <defaulted>
        <protected entry>
        zone-name: csi
        severity: warning <defaulted>
        <protected entry>
        zone-name: ctlTransSource
        severity: warning <defaulted>
        <protected entry>
        zone-name: intfc
        severity: warning <defaulted>
        <protected entry>
        zone-name: nac
        severity: debug default: warning
        <protected entry>
        zone-name: sensorApp
        severity: warning <defaulted>
        <protected entry>
        zone-name: tls
        severity: warning <defaulted>
    -----------------------------------------------
sensor(config-log)#
```

Step 14 Exit the logger submode:

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

Step 15 Press **Enter** to apply changes or type **no** to discard them:

Zone Names

Table C-1 lists the debug logger zone names:

Table C-1 Debug Logger Zone Names

Zone Name	Description
AuthenticationApp	Authentication zone
Cid	General logging zone
Cli	CLI zone
IdapiCtlTrans	All control transactions zone
IdsEventStore	Event Store zone
MpInstaller	IDSM-2 master partition installer zone
cmgr	Card Manager service zone[1]
cplane	Control Plane zone[2]
csi	CIDS Servlet Interface[3]
ctlTransSource	Outbound control transactions zone
intfc	Interface zone
nac	ARC zone

Table C-1 Debug Logger Zone Names (continued)

Zone Name	Description
sensorApp	AnalysisEngine zone
tls	SSL and TLS zone

1. The Card Manager service is used on AIP-SSM to exchange control and state information between modules in the chassis.
2. The Control Plane is the transport communications layer used by Card Manager on AIP-SSM.
3. The CIDS servlet interface is the interface layer between the CIDS web server and the servlets.

Directing cidLog Messages to SysLog

It might be useful to direct cidLog messages to syslog.

To direct cidLog messages to syslog, follow these steps:

Step 1 Go to the idsRoot/etc/log.conf file.

Step 2 Make the following changes:

a. Set [logApp] `enabled=false`

Comment out the `enabled=true` because `enabled=false` is the default.

b. Set [drain/main] `type=syslog`

The following example shows the logging configuration file:

```
timemode=local
;timemode=utc

[logApp]
;enabled=true
;-------- FIFO parameters --------
fifoName=logAppFifo
fifoSizeInK=240
;-------- logApp zone and drain parameters --------
zoneAndDrainName=logApp
fileName=main.log
fileMaxSizeInK=500

[zone/Cid]
severity=warning
drain=main

[zone/IdsEventStore]
severity=debug
drain=main

[drain/main]
type=syslog
```

The syslog output is sent to the syslog facility local6 with the following correspondence to syslog message priorities:

```
LOG_DEBUG,         //   debug
LOG_INFO,               //    timing
LOG_WARNING,    //    warning
```

```
    LOG_ERR,              //    error
    LOG_CRIT              //     fatal
```

Note Make sure that your /etc/syslog.conf has that facility enabled at the proper priority.

Caution The syslog is much slower than logApp (about 50 messages per second as opposed to 1000 or so). We recommend that you enable debug severity on one zone at a time.

TCP Reset Not Occurring for a Signature

If you do not have the event action set to reset, the TCP reset does not occur for a specific signature.

To troubleshoot a reset not occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Make sure the event action is set to TCP reset:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
   atomic-ip
   -----------------------------------------------
      event-action: produce-alert|reset-tcp-connection default: produce-alert
      fragment-status: any <defaulted>
      specify-l4-protocol
      -----------------------------------------------
         no
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      specify-ip-payload-length
      -----------------------------------------------
         no
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      specify-ip-header-length
      -----------------------------------------------
         no
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
      specify-ip-tos
      -----------------------------------------------
--MORE--
```

Step 3 Exit signature definition submode:

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

Step 4 Press **Enter** to apply the changes or type **no** to discard them.

Step 5 Make sure the correct alerts are being generated:

```
sensor# show events alert
evAlert: eventId=1047575239898467370 severity=medium
originator:
hostId: sj_4250_40
appName: sensorApp
appInstanceId: 1004
signature: sigId=20000 sigName=STRING.TCP subSigId=0 version=Unknown
addr: locality=OUT 172.16.171.19
port: 32771
victim:
addr: locality=OUT 172.16.171.13 port: 23
actions:
tcpResetSent: true
```

Step 6 Make sure the switch is allowing incoming TCP reset packet from the sensor.

Refer to your switch documentation for the procedure.

Step 7 Make sure the resets are being sent:

```
root# ./tcpdump -i eth0 src host 172.16.171.19
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0
13:58:03.823929 172.16.171.19.32770 > 172.16.171.13.telnet: R 79:79(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
```

Software Upgrades

This section helps in troubleshooting software upgrades. It contains the following topics:

IDS-4235 and IDS-4250 Hang During A Software Upgrade

If the BIOS of IDS-4235 and IDS-4250 is at A03, you must upgrade it to A04 before applying the most recent IPS software, otherwise, the appliances hang during the software upgrade process. For the procedure for upgrading the BIOS, refer to Upgrading the BIOS. For the procedure for applying the latest IPS software, see Obtaining Cisco IPS Software, page 18-1.

Which Updates to Apply and Their Prerequisites

You must have the correct service pack and minor and major version of the software. If you are having trouble with applying new software, make sure that you are applying the proper updates with the proper prerequisites. For more information on software file versioning, see IPS Software Versioning, page 18-3.

Issues With Automatic Update

The following list provides suggestions for troubleshooting automatic update:

- Run tcpDump
  - Create a service account. Su to root and run tcpDump on the command and control interface to capture packets between the sensor and the FTP server.

    For the procedure, see Creating the Service Account, page 4-13.
  - Use the **upgrade** command to manually upgrade the sensor.

    For the procedure, see Chapter 17, "Upgrading, Downgrading, and Installing System Images."
  - Look at the tcpDump output for errors coming back from the FTP server.
- Make sure the sensor is in the correct directory.

  The directory must be specified correctly. This has caused issues with Windows FTP servers. Sometimes an extra "/" or even two "/" are needed in front of the directory name.

  To verify this, use the same FTP commands you see in the tcpDump output through your own FTP connection.
- Make sure you have not modified the FTP server to use custom prompts.

  If you modify the FTP prompts to give security warnings, for example, this causes a problem, because the sensor is expecting a hard-coded list of responses.

  Note Not modifying the prompt only applies to versions before 4.1(4).
- You must use the Windows FTP server setup option to emulate UNIX file structure and not MS-DOS file structure.
- If you are using SCP, make sure you have added the SSH host key to the known hosts list.

  For the procedure, see Adding Hosts to the Known Hosts List, page 4-32.

Try the manual **upgrade** command before attempting the automatic update. If it works with the **upgrade** command and does not work with the automatic update, try the following:

- Determine which IPS software version your sensor has (for the procedure, see Displaying Version Information, page 13-19.

  Version 4.0(1) has a known problem with automatic update. Upgrade manually to 4.1(1) before trying to configure and use automatic update.
- Make sure the passwords configured for automatic update. Make sure they match the same passwords used for manual update.
- Make sure that the filenames in the FTP server are exactly what you see on Downloads on Cisco.com. This includes capitalization.

  Some Windows FTP servers allow access to the file with the incorrect capitalization but the sensor ultimately rejects the file because the name has changed.

If necessary, run tcpDump on automatic update. You can compare the successful manual update with the unsuccessful automatic update and troubleshoot from there.

Updating a Sensor with the Update Stored on the Sensor

You can store the update package in the /var directory on the sensor and update the sensor from there if you need to.

To update the sensor with an update stored on the sensor, follow these steps:

Step 1 Log in to the service account.

Step 2 Obtain the update package file from Cisco.com.

For the procedure, see Obtaining Cisco IPS Software, page 18-1.

Step 3 FTP or SCP the update file to the sensor's /usr/cids/idsRoot/var directory.

Step 4 Set the file permissions:

```
chmod 644 ips_package_file_name
```

Step 5 Exit the service account.

Step 6 Log in to the sensor using an account with administrator privileges.

Step 7 Store the sensor's host key:

```
sensor# configure terminal
sensor(config)# service ssh
sensor(config-ssh)# rsa1-keys sensor_ip_address
```

Step 8 Upgrade the sensor:

```
sensor(config)# upgrade scp://service@sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

UNIX-Style Directory Listings

To configure Auto Update using an FTP server, the FTP server must provide directory listing responses in UNIX style. MS-DOS style directory listing is not supported by the sensor Auto Update feature.

Note If the server supplies MS-DOS style directory listings, the sensor cannot parse the directory listing and does not know that there is a new update available.

To change Microsoft IIS to use UNIX-style directory listings, follow these steps:

Step 1 **Choose Start > Program Files > Administrative Tools**.

Step 2 Click the **Home Directory** tab.

Step 3 Click the **UNIX directory listings style** radio button.

Troubleshooting IDM

Note These procedures also apply to the IPS section of ASDM.

Note After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

This section contains troubleshooting procedures for IDM. This section contains the following topics:

Increasing the Memory Size of the Java Plug-In

To correctly run IDM, your browser must have Java Plug-in 1.4.2 or 1.5 installed. By default the Java Plug-in allocates 64 MB of memory to IDM. IDM can run out of memory while in use, which can cause IDM to freeze or display blank screens. Running out of memory can also occur when you click **Refresh**. An `OutofMemoryError` message appears in the Java console whenever this occurs.

Note We recommend that you use Sun Microsystems Java. Using any other version of Java could cause problems with IDM.

You must change the memory settings of Java Plug-in before using IDM. The mandatory minimum memory size is 256 MB.

This section contains the following topics:

Java Plug-In on Windows

To change the settings of Java Plug-in on Windows for Java Plug-in 1.4.2 and 1.5, follow these steps:

Step 1 Close all instances of Internet Explorer or Netscape.

Step 2 Click **Start > Settings > Control Panel**.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click Java Plug-in.

The Java Plug-in Control Panel appears.

b. Click the **Advanced** tab.

c. Type **-Xms256m** in the **Java RunTime Parameters** field.

d. Click **Apply** and exit the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click Java.

The Java Control Panel appears.

b. Click the **Java** tab.

c. Click **View** under Java Applet Runtime Settings.

The Java Runtime Settings Panel appears.

d. Type **-Xms256m** in the **Java Runtime Parameters** field and then click **OK**.

e. Click **OK** and exit the Java Control Panel.

Java Plug-In on Linux and Solaris

To change the settings of Java Plug-in 1.4.2 or 1.5 on Linux and Solaris, follow these steps:

Step 1 Close all instances of Netscape or Mozilla.

Step 2 Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.

Note In the Java 2 SDK, this file is located at <SDK installation directory>/jre/bin/ControlPanel. For example if your Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel.

Note In a Java 2 Runtime Environment installation, the file is located at <JRE installation directory>/bin/ControlPanel.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click the **Advanced** tab.

b. Type **-Xms256m** in the **Java RunTime Parameters** field.

c. Click **Apply** and close the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click the **Java** tab.

b. Click **View** under Java Applet Runtime Settings.

c. Type **-Xms256m** in the Java Runtime Parameters field and then click **OK**.

d. Click **OK** and exit the Java Control Panel.

Cannot Launch IDM - Loading Java Applet Failed

Symptom The browser displays `Loading Cisco IDM. Please wait ...` At the bottom left corner of the window, `Loading Java Applet Failed` is displayed.

Possible Cause This condition can occur if multiple Java Plug-ins (1.4.*x* and/or 1.3.*x*) are installed on the machine on which you are launching the IDM.

Recommended Action Clear the Java cache and remove temp files and clear history in the browser you are using. The result is that neither of these plug-ins will be used by default and each applet should use the correct plug-in.

To clear the cache, follow these steps:

Step 1 Close all browser windows.

Step 2 If you have Java Plug-in 1.3.*x* installed:

a. Click **Start > Settings > Control Panel > Java Plug-in 1.3.x**.

b. Click the **Advanced** tab.

c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.

d. Click the **Cache** tab.

e. Click **Clear**.

Step 3 If you have Java Plug-in 1.4.*x* installed:

a. Click **Start > Settings > Control Panel > Java Plug-in 1.4.x**.

b. Click the **Advanced** tab.

c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.

d. Click the **Cache** tab.

e. Click the **Browser** tab.

f. Deselect all browser check boxes.

g. Click **Clear Cache**.

Step 4 Delete the temp files and clear the history in the browser.

Cannot Launch IDM -Analysis Engine Busy

Error Message `Error connecting to sensor. Failed to load sensor-errNotAvailable-Analysis Engine is busy. Exiting IDM.`

Possible Cause This condition can occur if the Analysis Engine in the sensor is busy getting ready to perform a task and so does not respond to IDM.

Recommended Action Wait for a while and try again to connect.

IDM, Remote Manager, or Sensing Interfaces Cannot Access the Sensor

If IDM, a remote manager, or sensing interfaces cannot access the sensor, but you can access the sensor's CLI using SSH or Telnet (if enabled), follow these steps:

Note For the procedure for enabling and disabling Telnet on the sensor, see Enabling and Disabling Telnet, page 4-4.

Step 1 Make sure the network configuration allows access to the web server port that is configured on the sensor:

```
sensor# setup


    --- System Configuration Dialog ---

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


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
```

For more information, see Changing Web Server Settings, page 4-9.

Step 2 If network devices, such as routers, switches, or firewalls, are between the sensor and the workstation, make sure these devices are configured to allow the workstation to access the sensor's web server port.

All remote management communication is performed by the sensor's web server.

For more information, see Changing Web Server Settings, page 4-9.

Signatures Not Producing Alerts

If you are not seeing any alerts when signatures are firing, make sure that you have configured Produce Alert as an event action.

Caution You cannot add other actions each time you configure the event actions. You are actually replacing the list of event actions every time you configure it, so make sure you choose Produce Alert every time you configure event actions.

For example, if you choose Produce Alert, but later add another event action and do not add Produce Alert to the new configuration, alerts will not be sent to the Event Store. To make sure you are getting alerts, use statistics for the virtual sensor and event store.

Troubleshooting IDSM-2

IDSM-2 has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the 4200 Series Appliance, page C-8.

This section pertains specifically to troubleshooting IDSM-2.

This section contains the following topics:

Diagnosing IDSM-2 Problems

Use the following list to diagnose IDSM-2 problems:

- The ribbon cable between IDSM-2 and the motherboard is loose.

  During physical handling of the module, the connector can come loose from the base card, and cause the daughter card and the base card to lose contact with each other. A loose ribbon cable connector causes an on-line diagnostic error on ports 7 and 8. The module cannot operate when this condition exists. For more information, see Partner Field Notice 52816.

- Some IDSM-2s were shipped with faulty DIMMs. For the procedure for checking IDSM-2 for faulty memory see the Partner Field 52563.

- The hard-disk drive fails to read or write. When the hard-disk drive has been in constant use for extended periods of time (for more than 2 weeks), multiple symptoms, such as the following, can occur:

  – An inability to log in

  – I/O errors to the console when doing read/write operations (the **ls** command)

  - Commands do not execute properly (cannot find the path to the executable)

  The switch reports that the module is ok, but if you log in to the Service account and try to execute commands, you see that the problem exists. The 4.1(4) service pack alleviates this problem, but if you reimage IDSM-2 with the 4.1(4) application partition image, you must apply the 4.1(4b) patch. For more information see CSCef12198.

- SensorApp either crashes or takes 99% of the CPU when IP logging is enabled for stream-based signatures (1300 series). For the workaround, see CSCed32093.
- IDSM-2 appears to lock up and remote access is prohibited (SSH, Telnet, IDM, Event Server, Control Transaction Server, and IP log Server). This defect is related to using SWAP. IDSM-2 responds to pings. Apply the 4.1(4) service pack to resolve this issue. For more information, see CSCed54146.
- Shortly after you upgrade IDSM-2 or you tune a signature with VMS, IDSM-2 becomes unresponsive and often produces a SensorApp core file. Apply the 4.1(4b) patch to fix this issue.
- Confirm that IDSM-2 has the supported configurations. For more information, see Minimum Supported IDSM-2 Configurations, page 15-4.

If you have confirmed that IDSM-2 does not suffer from any of the problems listed above and yet it appears unresponsive, for example, you cannot log in through SSH or Telnet, nor can you session to the switch, determine if IDSM-2 responds to pings and if you can log in through the service account. If you can log in, obtain a cidDump and any core files and contact TAC.

Switch Commands for Troubleshooting

The following switch commands help you troubleshoot IDSM-2:

- **show module** (Cisco Catalyst Software and Cisco IOS Software)
- **show version** (Cisco Catalyst Software and Cisco IOS Software)
- **show port** (Cisco Catalyst Software)
- **show trunk** (Cisco Catalyst Software)
- **show span** (Cisco Catalyst Software)
- **show security acl** (Cisco Catalyst Software)
- **show intrusion-detection module** (Cisco IOS Software)
- **show monitor** (Cisco IOS Software)
- **show vlan access-map** (Cisco IOS Software)
- **show vlan filter** (Cisco IOS Software)

Status LED Off

If the status indicator is off on IDSM-2, you need to turn power on to IDSM-2.

To determine status of IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Verify that IDSM-2 is online:

For Catalyst Software:

```
cat6k> enable

Enter password:
cat6k> (enable) show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- -----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1       8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
cat6k> (enable)
```

For Cisco IOS software:

```
switch#show module
Mod Ports Card Type                                 Model              Serial No.
--- ----- ----------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet         WS-X6248-RJ-45     SAD04401012S
  2   48  48 port 10/100 mb RJ45                   WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5    8  Intrusion Detection System              WS-SVC-IDSM-2      SAD0751059U
  6   16  SFM-capable 16 port 1000mb GBIC          WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)           WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module        WS-X6502-10GE      SAD071903BT
```

```
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  5  0003.fead.651a to 0003.fead.6521   4.0   7.2(1)       5.0(1.1)     Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1.1)     Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model              Serial       Hw     Status
--- --------------------------- ------------------ ------------ ------ -------
  5 IDS 2 accelerator board     WS-SVC-IDSUPG      07E91E508A   2.0    Ok
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1  1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX  2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .            2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976   2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
switch#
```

Note It is normal for the status to read `other` when IDSM-2 is first installed. After IDSM-2 completes the diagnostics routines and comes online, the status reads `ok`. Allow up to 5 minutes for IDSM-2 to come online.

Step 3 If the status does not read `ok`, turn the module on:

```
switch# set module power up module_number
```

Status LED On But IDSM-2 Does Not Come Online

If the status indicator is on, but IDSM-2 does not come online, try the following troubleshooting tips:

- Reset IDSM-2.
- Make sure IDSM-2 is installed properly in the switch.
- If the hard-disk drive status has failed, reimage the application partition.

To enable IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure IDSM-2 is enabled:

```
router# show module
```

Step 3 If the status does not read `ok`, enable IDSM-2:

```
router# set module enable module_number
```

Step 4 If IDSM-2 still does not come online, reset it:

```
router# reset module_number
```

Wait for about 5 minutes for IDSM-2 to come online.

Step 5 If IDSM-2 still does not come online, make sure the hardware and operating system are ok:

```
router# show test module_number
```

Step 6 If the `port` status reads `fail`, make sure IDSM-2 is firmly connected in the switch.

Step 7 If the `hdd` status reads `fail`, you must reimage the application partition.

For the procedure, see Chapter 17, "Upgrading, Downgrading, and Installing System Images."

Cannot Communicate With IDSM-2 Command and Control Port

If you cannot communicate with the IDSM-2 command and control port, the command and control port may not be in the correct VLAN.

To communicate with the command and control port of IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure you can ping the command port from any other system.

Step 3 Make sure the IP address, mask, and gateway settings are correct:

```
router# show configuration
```

Step 4 Make sure the command and control port is in the correct VLAN:

For Catalyst software:

```
cat6k> (enable) show port 6/8
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 6/8                       connected  trunk        full        1000 IDS


Port  Status      ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  ----------  -------------------  ----------------------  -----------------
 6/8  connected                     -  Enable                  No Change
```

```
Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 6/8           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 6/8           0          0          0          0         0         0         -

Port  Last-Time-Cleared
----- --------------------------
 6/8  Wed Mar 2 2005, 15:29:49

Idle Detection
--------------
   --
cat6k> (enable)
```

For Cisco IOS software:

```
cat6k#show intrusion-detection module 5 management-port state
Intrusion-detection module 5 management-port:

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1
Vlans allowed and active in management domain: 1
Vlans in spanning tree forwarding state and not pruned:
   1
Access Vlan = 1


cat6k#
```

Step 5 If the command and control port is not in the correct VLAN, put it in the correct VLAN.

For the procedure, see Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2, page 15-5.

Using the TCP Reset Interface

IDSM-2 has a TCP reset interface—port 1. IDSM-2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have TCP reset problems with IDSM-2, try the following:

- If the sensing ports are access ports (a single VLAN), you must configure the TCP reset port to be in the same VLAN.
- If the sensing ports are dot1q trunk ports (multi-VLAN), the sensing ports and TCP reset port all must have the same native VLAN, and the TCP reset port must trunk all the VLANs being trunked by both the sensing ports.

Connecting a Serial Cable to IDSM-2

You can connect a serial cable directly to the serial console port on IDSM-2. This lets you bypass the switch and module network interfaces.

To connect a serial cable to IDSM-2, follow these steps:

Step 1 Locate the two RJ-45 ports on IDSM-2.

You can find them approximately in the center of the mother board. If you are facing the module faceplate, the RJ-45 port on the right is the serial console port.

Step 2 Connect a straight-through cable to the right port on IDSM-2, and then connect the other end of the cable to a terminal server port.

Step 3 Configure the terminal server port to be 19200 baud, 8 bits, no parity.

You can now log directly in to IDSM-2.

Note Connecting a serial cable to IDSM-2 works only if there is no module located above IDSM-2 in the switch chassis, because the cable has to come out through the front of the chassis.

Troubleshooting AIP-SSM

AIP-SSM has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the 4200 Series Appliance, page C-8.

The following section contains commands that are specific to troubleshooting AIP-SSM.

To see the general health of AIP-SSM, use the **show module 1 details** command:

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.1)S153.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

The output shows that AIP-SSM is up. If the status reads `Down`, you can reset AIP-SSM using the **hw-module module 1 reset** command:

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa(config)# show module

Mod Card Type                                    Model              Serial No.
```

```
--- ---------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Shutting Down
**************************************************
asa(config)# show module

Mod Card Type                                     Model              Serial No.
--- ---------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa(config)#
```

If you have problems with recovering AIP-SSM, use the **debug module-boot** command to see the output as AIP-SSM boots. Make sure you have the correct IP address for the TFTP server and you have the correct file on the TFTP server. Then use the **hw-module module 1 recover** command again to recover AIP-SSM:

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
asa(config)# debug module-boot
debug module-boot  enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2005
Slot-1 141> Platform ASA-SSM-10
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 152>   CONFIG=
```

```
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2005
Slot-1 161> Platform ASA-SSM-10
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

Gathering Information

You can use the following CLI commands and scripts to gather information and diagnose the state of the sensor when problems occur. You can use the **show tech-support** command to gather all the sensor's information, or you can use the other individual commands listed in this section for specific information.

This section contains the following topics:

Tech Support Information

The **show tech-support** command is useful for capturing all the status and configuration information of the sensor.

This section describes the **show tech-support** command, and contains the following topics:

Overview

The **show tech-support** command captures all status and configuration information on the sensor and includes the current configuration, version information, and cidDump information. The output can be large, over 1 MB. You can transfer the output to a remote system. for the procedure for copying the output to a remote system, see Displaying Tech Support Information, page C-51.

Note You can get the same information from IDM by clicking Monitoring > Support Information > System Information.

Note Always run the **show tech-support** command before contacting TAC.

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.

Tech Support Command Output

The following is an example of the **show tech-support** command output:

Note This output example shows the first part of the command and lists the information for the Interfaces, Network Access Controller, and cidDump services.

```
sensor# show tech-support page

System Status Report
This Report was generated on Fri Feb 21 03:33:52 2003.
Output from show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
```

```
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2208534
   Total Bytes Received = 157390286
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239437
   Total Bytes Transmitted = 107163351
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0

Output from show statistics networkAccess
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = true
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
State
   BlockEnable = true

Output from cidDump

cidDiag
CID Diagnostics Report Fri Feb 21 03:33:54 UTC 2003
5.0(1)
<defaultVersions>
<defaultVersion aspect="S">
<version>149.0</version>
<date>2005-03-04</date>
</defaultVersion>
</defaultVersions>
1.1 - 5.0(1)S149
Linux version 2.4.26-IDS-smp-bigphys (csailer@mcq) (gcc version 2.96 20000731 (R
ed Hat Linux 7.3 2.96-112)) #2 SMP Fri Mar 4 04:11:31 CST 2005
 03:33:54 up 21 days, 23:15,  3 users,  load average: 0.96, 0.86, 0.78
--MORE--
```

Version Information

The **show version** command is useful for establishing the general health of the sensor.

This section describes the **show version** command, and contains the following topics:

Overview

The **show version** command shows the general health of the sensor and can indicate where a failure is occurring. It gives the following information:

- Which applications are running
- Versions of the applications
- Disk and memory usage
- Upgrade history of the applications

Note Choose **Monitoring > Support Information > Diagnostics Report** to get the same information from IDM or ASDM.

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 5.0(0.29)S135.0

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-maj-5.0-0.29-S91-0.29-.pkg   03:00:00 UTC Mon Feb 16 2004

Recovery Partition Version 1.1 - 5.0(0.29)S91(0.29)
```

```
sensor#
```

Sample version output for NM-CIDS:

```
nm-cids# show version
Application Partition:
Cisco Intrusion Prevention System, Version 5.0(0.27)S129.0

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-maj-5.0-0.27-S91-0.27-.pkg   03:00:00 UTC Thu Feb 05 2004

Recovery Partition Version 1.1 - 5.0(0.27)S91(0.27)

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 5.0(0.26)
! Current configuration last modified Wed Feb 16 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--
```

Statistics Information

The **show statistics** command is useful for examining the state of the sensor services. This section describes the **show statistics** command, and contains the following topics:

Overview

The **show statistics** command provides a snapshot of the state of the sensor's services. The following services provide statistics:

- AnalysisEngine
- Authentication
- Denied Attackers
- Event Server
- Event Store
- Host
- Logger
- Attack Response (formerly known as Network Access)
- Notification
- SDEE Server
- Transaction Server
- Transaction Source
- Virtual Sensor
- Web Server

Note Click **Monitoring > Support Information > Statistics** to get the same information from IDM.

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.

Interfaces Information

The **show interfaces** command is useful for gathering information on the sensing and command and control interfaces.

This section describes the **show interfaces** command, and contains the following topics:

Overview

You can learn the following information from the **show interfaces** command:

- Whether the interface is up or down
- Whether or not packets are being seen, and on which interfaces
- Whether or not packets are being dropped by SensorApp
- Whether or not there are errors being reported by the interfaces that can result in packet drops

The **show interfaces** command displays statistics for all system interfaces. Or you can use the individual commands to display statistics for the command and control interface (**show interfaces** *command_control_interface_name*), the sensing interface (**show interfaces** *interface_name*).

Interfaces Command Output

The following example shows the output from the **show interfaces** command:

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
```

```
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

Events Information

You can use the **show events** command to view the alerts generated by SensorApp and errors generated by an application.

This section describes the **show events** command, and contains the following topics:

Sensor Events

There are five types of events:

- evAlert—Intrusion detection alerts
- evError—Application errors
- evStatus—Status changes, such as an IP log being created
- evLogTransaction—Record of control transactions processed by each sensor application
- evShunRqst—Block requests

Events remain in the Event Store until they are overwritten by newer events.

Overview

The **show events** command is useful for troubleshooting event capture issues in which you are not seeing events in Event Viewer or Security Monitor. You can use the **show events** command to determine which events are being generated on the sensor to make sure events are being generated and that the fault lies with the monitoring side.

You can clear all events from Event Store by using the **clear events** command.

Here are the parameters for the **show events** command:

```
sensor# show events
<cr>
alert          Display local system alerts.
error          Display error events.
hh:mm[:ss]     Display start time.
log            Display log events.
nac            Display NAC shun events.
past           Display events starting in the past specified time.
status         Display status events.
|              Output modifiers.
```

Displaying Events

Use the **show events** [{[**alert** [informational] [low] [medium] [high] [**include-traits** *traits*] [**exclude-traits** *traits*]] | **error** [warning] [error] [fatal] | **log** | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] command to display events from the 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.
- **log**—Displays log events. Log events are generated when a transaction is received and responded to by an application. Contains information about the request, response, and success or failure of the transaction.
- **NAC**—Displays Attack Response Controller (ARC) 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 exce
ption: 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

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.

cidDump Script

If you do not have access to IDM or the CLI, you can run the underlying script cidDump from the Service account by logging in as root and running /usr/cids/idsRoot/bin/cidDump. The cidDump file path is /usr/cids/idsRoot/htdocs/private/cidDump.html.

cidDump is a script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

To run the cidDump script, follow these steps:

Step 1 Log in to the sensor Service account.

Step 2 **Su** to **root** using the Service account password.

Step 3 Enter the following command:

```
/usr/cids/idsRoot/bin/cidDump
```

Step 4 Enter the following command to compress the resulting /usr/cids/idsRoot/log/cidDump.html file:

```
gzip /usr/cids/idsRoot/log/cidDump.html
```

Step 5 Send the resulting HTML file to TAC or the IPS developers in case of a problem.

For the procedure, see Uploading and Accessing Files on the Cisco FTP Site, page C-71.

Uploading and Accessing Files on the Cisco FTP Site

You can upload large files, for example, cidDump.html, the show tech-support command output, and cores, to the ftp-sj server.

To upload and access files on the Cisco FTP site, follow these steps:

Step 1 Log in to ftp-sj.cisco.com as anonymous.

Step 2 Change to the /incoming directory.

Step 3 Use the **put** command to upload the files.

Make sure to use the binary transfer type.

Step 4 To access uploaded files, log in to an ECS-supported host.

Step 5 Change to the /auto/ftp/incoming directory.