APPENDIX C

Troubleshooting

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

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve our customers' effectiveness in network risk management and device troubleshooting.

BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The service has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

Check out Bug Search Tools & Resources on Cisco.com. For more details on the tool overview and FAQs, check out the help page, located at this URL: http://www.cisco.com/web/applicat/cbsshelp/help.html.

Preventive Maintenance

This section describes how to perform preventive maintenance for your sensor, and contains the following topics:

- Understanding Preventive Maintenance, page C-2
- Creating and Using a Backup Configuration File, page C-2
- Backing Up and Restoring the Configuration File Using a Remote Server, page C-3
- Creating the Service Account, page C-5

Understanding 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.
- Save your backup configuration to a remote system.
- 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 special debug situations directed by TAC.

⚠ **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. Analyze your situation to decide if you want a service account existing on the system.

For More Information

- For the procedure for backing up a configuration file, see Creating and Using a Backup Configuration File, page C-2.
- For the procedure for using a remote server to copy and restore the a configuration file, see Backing Up and Restoring the Configuration File Using a Remote Server, page C-3.
- For more information about the service account, see Creating the Service Account, page C-5.

Creating and Using a Backup Configuration File

To protect your configuration, you can back up the current configuration and then display it to confirm that is the configuration you want to save. If you need to restore this configuration, you can merge the backup configuration file with the current configuration or overwrite the current configuration file with the backup configuration file.

To back up your current configuration, follow these steps:

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

Step 2 Save the current configuration. The current configuration is saved in a backup file.

```
sensor# copy current-config backup-config
```

Step 3 Display the backup configuration file. The backup configuration file is displayed.

```
sensor# more backup-config
```

Step 4 You can either merge the backup configuration with the current configuration, or you can overwrite the current configuration:

- Merge the backup configuration into the current configuration.

```
sensor# copy backup-config current-config
```

- Overwrite the current configuration with the backup configuration.

```
sensor# copy /erase backup-config current-config
```

Backing Up and Restoring the Configuration File Using a Remote Server

Note We recommend copying the current configuration file to a remote server before upgrading.

Use the **copy** [**/erase**] *source_url destination_url keyword* command to copy the configuration file to a remote server. You can then restore the current configuration from the remote server. You are prompted to back up the current configuration first.

The following options apply:

- **/erase**—Erases the destination file before copying.

  This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.
- *source_url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination_url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.
- **backup-config**—The storage location for the configuration backup.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

  - ftp:—Source or destination URL for an FTP network server. The syntax for this prefix is:

    ftp://[[username@]location][/relativeDirectory]/filename

    ftp://[[username@]location][//absoluteDirectory]/filename

Note You are prompted for a password.

- scp:—Source or destination URL for the SCP network server. The syntax for this prefix is:

  scp://[[username@]location][/relativeDirectory]/filename

  scp://[[username@]location][//absoluteDirectory]/filename

  Note You are prompted for a password. You must add the remote host to the SSH known hosts list.

- http:—Source URL for the web server. The syntax for this prefix is:

  http://[[username@]location][/directory]/filename

  Note The directory specification should be an absolute path to the desired file.

- https:—Source URL for the web server. The syntax for this prefix is:

  https://[[username@]location][/directory]/filename

  Note The directory specification should be an absolute path to the desired file. The remote host must be a TLS trusted host.

Caution Copying a configuration file from another sensor may result in errors if the sensing interfaces and virtual sensors are not configured the same.

Backing Up the Current Configuration to a Remote Server

To back up your current configuration to a remote server, follow these steps:

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

Step 2 Back up the current configuration to the remote server.

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg            100% |************************************************| 36124       00:00
```

Restoring the Current Configuration From a Backup File

To restore your current configuration from a backup file, follow these steps:

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

Step 2 Back up the current configuration to the remote server.

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg            100% |************************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

Step 4 Enter **no** to retain the currently configured hostname, IP address, subnet mask, management interface, and access list. We recommend you retain this information to preserve access to your sensor after the rest of the configuration has been restored.

For More Information

For a list of supported HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page 27-3.

Creating the Service Account

You can create a service account for TAC to use during troubleshooting. Although more than one user can have access to the sensor, only one user can have service privileges on a sensor. The service account is for support purposes only.

The root user password is synchronized to the service account password when the service account is created. To gain root access you must log in with the service account and switch to user root with the **su - root** command.

Caution Do not make modifications to the sensor through the service account except under the direction of TAC. If you use the service account to configure the sensor, your configuration is not supported by TAC. Adding services to the operating system through the service account affects proper performance and functioning of the other IPS services. TAC does not support a sensor on which additional services have been added.

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 password if the administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

Note For IPS 5.0 and later, you can no longer remove the **cisco** account. You can disable it using the **no password cisco** command, but you cannot remove it. To use the **no password cisco** command, there must be another administrator account on the sensor. Removing the **cisco** account through the service account is not supported. If you remove the **cisco** account through the service account, the sensor most likely will not boot up, so to recover the sensor you must reinstall the sensor system image.

To create the service account, follow these steps:

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

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Specify the parameters for the service account. The username follows the pattern ^[A-Za-z0-9()+:,_/-]+$, which means the username must start with a letter or number, and can include any letter A to Z (capital or small), any number 0 to 9, - and _, and can contain 1 to 64 characters.

```
sensor(config)# user username privilege service
```

Step 4 Specify a password when prompted. A valid password is 8 to 32 characters long. All characters except space are allowed. If a service account already exists for this sensor, the following error is displayed and no service account is created.

```
Error: Only one service account may exist
```

Step 5 Exit configuration mode.

```
sensor(config)# exit
sensor#
```

When you use the service account to log in to the CLI, you receive this warning.

```
************************ WARNING *******************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. This account is intended to be
used for support and troubleshooting purposes only. Unauthorized modifications are not
supported and will require this device to be reimaged to guarantee proper operation.
****************************************************************************************
```

Disaster Recovery

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

- If you are using the CLI, IDM, or IME for configuration, copy the current configuration from the sensor to an FTP or SCP server any time a change has been made.
- You should note the specific software version for that configuration. You can apply the copied configuration only to a sensor of the same version.
- 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.

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

1. Reimage the sensor.

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

Note You are prompted to change the **cisco** password.

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

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.
6. Update clients to use the new key and certificate of the sensor. Reimaging changes the sensor SSH keys and HTTPS certificate, so you must add the hosts back to the SSN known hosts list.
7. Create previous users.

For More Information

- For the procedure for backing up a configuration file, see Creating and Using a Backup Configuration File, page C-2.
- For the procedure for obtaining a list of the current users on the sensor, see Configuring Authentication, page 6-17.
- For the procedures for reimage a sensor, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for using the **setup** command to initialize the sensor, see Chapter 25, "Initializing the Sensor."
- For more information on obtaining IPS software and how to install it, see Obtaining Cisco IPS Software, page 26-1.
- For the procedure for using a remote server to copy and restore the a configuration file, see Backing Up and Restoring the Configuration File Using a Remote Server, page C-3.
- For the procedure for adding hosts to the SSH known hosts list, see Defining Known Host RSA1 Keys, page 15-9.
- For the procedure for adding users, see Configuring Authentication, page 6-17.

Password Recovery

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

- Verifying the State of Password Recovery, page C-14
- Troubleshooting Password Recovery, page C-15

Understanding Password Recovery

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

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

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

Table C-1 Password Recovery Methods According to Platform

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

Recovering the Appliance Password

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

- Using the GRUB Menu, page C-8
- Using ROMMON, page C-9

Using the GRUB Menu

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

For the IPS 4355, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance to see the GRUB menu.

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

```
-------------------------------------------

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

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

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

Using ROMMON

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

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

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

Step 1 Reboot the appliance.

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

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

Step 3 Enter the following commands to reset the password:

```
confreg 0x7
boot
```

Sample ROMMON session:

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

```
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

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

```
confreg 0
```

Recovering the and ASA 5500-X IPS SSP Password

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

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

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

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

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

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

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

Step 2 Press **Enter** to confirm.

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

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

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

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

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

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

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

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

```
asa# session ips
```

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

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

```
login: cisco
Password: cisco

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

Step 6 Enter your new password twice.

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

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

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

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

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

asa-ssp#
```

Using the ASDM

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

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

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

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

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

Recovering the ASA 5585-X IPS SSP Password

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

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

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

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

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

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

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

Step 2 Press **Enter** to confirm.

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

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

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

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

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

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

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

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

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

```
login: cisco
Password: cisco

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

Step 6 Enter your new password twice.

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

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

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

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

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

Using the ASDM

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

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

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

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

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

Disabling Password Recovery

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

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

Disabling Password Recovery Using the CLI

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

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

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

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

Step 4 Disable password recovery.

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

Disabling Password Recovery Using the IME

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

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

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

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

Verifying the State of Password Recovery

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

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

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

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

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

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

Troubleshooting Password Recovery

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

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

Time Sources and the Sensor

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

- Time Sources and the Sensor, page C-15
- Synchronizing IPS Module Clocks with Parent Device Clocks, page C-16
- Verifying the Sensor is Synchronized with the NTP Server, page C-16
- Correcting Time on the Sensor, page C-17

Time Sources and the Sensor

Note We recommend that you use an NTP server to regulate time on your sensor. You can use authenticated or unauthenticated NTP. For authenticated NTP, you must obtain the NTP server IP address, NTP server key ID, and the key value from the NTP server. You can set up NTP during initialization or you can configure NTP through the CLI, IDM, IME, or ASDM.

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. This section provides a summary of the various ways to set the time on sensors.

The IPS Standalone Appliances

- Use the **clock set** command to set the time. This is the default.
- Configure the appliance to get its time from an NTP time synchronization source.

  Note The currently supported Cisco IPS appliances are the IPS 4345, IPS 4360, IPS 4510, IPS 4520, and IPS 4520-XL.

The ASA IPS Modules

- The ASA 5500-X IPS SSP and ASA 5585-X IPS SSP automatically synchronize their clocks with the clock in the adaptive security appliance in which they are installed. This is the default.
- Configure them to get their time from an NTP time synchronization source, such as a Cisco router other than the parent router.

For More Information

For the procedure for configuring NTP, see Configuring NTP, page 6-13.

Synchronizing IPS Module Clocks with Parent Device Clocks

The ASAIPS modules (ASA 5500-X IPS SSP ASA 5585-X IPS SSP) synchronize their clocks to the parent chassis clock (adaptive security appliance) each time the IPS boots up and any time the parent chassis clock is set. The IPS 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 IPS clock and the parent clock are synchronized to an external NTP server. If only the IPS clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In IPS, 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.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events, see Clearing Events, page C-100.

Advantages and Restrictions of Virtualization

To avoid configuration problems on your sensor, make sure you understand the advantages and restrictions of virtualization on your sensor.

Virtualization has the following advantages:

- You can apply different configurations to different sets of traffic.
- You can monitor two networks with overlapping IP spaces with one sensor.
- You can monitor both inside and outside of a firewall or NAT device.

Virtualization has the following restrictions:

- You must assign both sides of asymmetric traffic to the same virtual sensor.
- Using VACL capture or SPAN (promiscuous monitoring) is inconsistent with regard to VLAN tagging, which causes problems with VLAN groups.
  - When using Cisco IOS software, a VACL capture port or a SPAN target does not always receive tagged packets even if it is configured for trunking.
  - When using the MSFC, fast path switching of learned routes changes the behavior of VACL captures and SPAN.
- Persistent store is limited.

Virtualization has the following traffic capture requirements:

- The virtual sensor must receive traffic that has 802.1q headers (other than traffic on the native VLAN of the capture port).
- The sensor must see both directions of traffic in the same VLAN group in the same virtual sensor for any given sensor.

The following sensors support virtualization:

- ASA 5500-X IPS SSP
- ASA 5585-X IPS SSP
- IPS 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520

Supported MIBs

Note To receive sensor health information through SNMP traps, you must have the sensor health metrics enabled. Choose **Configuration >** ***sensor_name*** **> Sensor Management > Sensor Health** to enable sensor health metrics.

To avoid problems with configuring SNMP, be aware of the MIBs that are supported on the sensor.

The following private MIBs are supported on the sensor:

- CISCO-CIDS-MIB

  The CISCO-CIDS-MIB has been updated to include SNMP health data.
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

You can obtain these private Cisco MIBs under the heading SNMP v2 MIBs at this URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Note MIB II is available on the sensor, but we do not support it. We know that some elements are not correct (for example, the packet counts from the IF MIB on the sensing interfaces). While you can use elements from MIB II, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

Note CISCO-PROCESS-MIB is available on the sensor, but we do not support it. We know that some elements are not available. While you can use elements from CISCO-PROCESS-MIB, we do not guarantee that they all provide correct information. We fully support the other listed MIBs and their output is correct.

When to Disable Anomaly Detection

If you have anomaly detection enabled and you have your sensor configured to see only one direction of traffic, you should disable anomaly detection. Otherwise, you will receive many alerts, because anomaly detection sees asymmetric traffic as having incomplete connections, that is, like worm scanners, and fires alerts.

To disable anomaly detection, follow these steps:

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

Step 2 Enter analysis engine submode.

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

Step 3 Enter the virtual sensor name that contains the anomaly detection policy you want to disable.

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

Step 4 Disable anomaly detection operational mode.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

Step 5 Exit analysis engine submode.

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# exit
sensor(config-ana-)# exit
Apply Changes:?[yes]:
```

Step 6 Press **Enter** to apply your changes or enter `no` to discard them.

For More Information

For more information about Worms, see Worms, page 13-2.

The Analysis Engine is Not Responding

Error Message `Output from show statistics analysis-engine`

```
Error: getAnalysisEngineStatistics : ct-sensorApp.424 not responding, please
check system processes - The connect to the specified Io::ClientPipe failed.
```

Error Message `Output from show statistics anomaly-detection`

```
Error: getAnomalyDetectionStatistics : ct-sensorApp.424 not responding, please
check system processes - The connect to the specified Io::ClientPipe failed.
```

Error Message `Output from show statistics denied-attackers`

```
Error: getDeniedAttackersStatistics : ct-sensorApp.424 not responding, please
check system processes - The connect to the specified Io::ClientPipe failed.
```

Possible Cause These error messages appear when you run the **show tech support** command and the Analysis Engine is not running.

Recommended Action Verify the Analysis Engine is running and monitor it to see if the issue is resolved.

To verify the Analysis Engine is running and to monitor the issue, follow these steps:

Step 1 Log in to the sensor.

Step 2 Verify that the Analysis Engine is not running, Check to see if the Analysis Engine reads `Not Running`.

```
sensor# show version

-----
MainApp            V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
AnalysisEngine     V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500 Not
Running
CollaborationApp   V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
Running
CLI                V-2013_04_10_11_00_7_2_0_14   (Release)   2013-04-10T11:05:55-0500
```

Step 3 Enter **`show tech-support`** and save the output.

Step 4 Reboot the sensor.

Step 5 Enter **`show version`** after the sensor has stabilized to see if the issue is resolved.

Step 6 If the Analysis Engine still reads `Not Running`, contact TAC with the original **show tech support** command output.

Troubleshooting RADIUS Authentication

Symptom Attempt limit configured on the IPS sensor may not be enforced for a RADIUS user.

Conditions Applicable for RADIUS users only. The RADIUS user must have logged in to the sensor at least once after RADIUS authentication is enabled or after the sensor is reset or rebooted.

Workaround Log in to the sensor with the correct credentials and from that time on the attempt limit is enforced for that RADIUS user.

For More Information

For detailed information about RADIUS authentication, see Configuring Authentication, page 6-17.

Troubleshooting Global Correlation

Make sure you observe the following when configuring global correlation:

- Because global correlation updates occur through the sensor management interface, firewalls must allow port 443/80 traffic.
- You must have an HTTP proxy server or a DNS server configured to allow global correlation features to function.
- If you have an HTTP proxy server configured, the proxy must allow port 443/80 traffic from IPS systems.
- You must have a valid IPS license to allow global correlation features to function.
- Global correlation features only contain external IP addresses, so if you position a sensor in an internal lab, you may never receive global correlation information.
- Make sure your sensor supports the global correlation features.
- Make sure your IPS version supports the global correlation features.

For More Information

For more information on global correlation features and how to configure them, see Chapter 14, "Configuring Global Correlation."

Troubleshooting External Product Interfaces

This section lists issues that can occur with external product interfaces and provides troubleshooting tips. It contains the following topics:

- External Product Interfaces Issues, page C-22
- External Product Interfaces Troubleshooting Tips, page C-22

External Product Interfaces Issues

When the external product interface receives host posture and quarantine events, the following issues can arise:

- The sensor can store only a certain number of host records:
  - If the number of records exceeds 10,000, subsequent records are dropped.
  - If the 10,000 limit is reached and then it drops to below 9900, new records are no longer dropped.
- Hosts can change an IP address or appear to use another host IP address, for example, because of DHCP lease expiration or movement in a wireless network. In the case of an IP address conflict, the sensor presumes the most recent host posture event to be the most accurate.
- A network can include overlapping IP address ranges in different VLANs, but host postures do not include VLAN ID information. You can configure the sensor to ignore specified address ranges.
- A host can be unreachable from the CSA MC because it is behind a firewall. You can exclude unreachable hosts.
- The CSA MC event server allows up to ten open subscriptions by default. You can change this value. You must have an administrative account and password to open subscriptions.
- CSA data is not virtualized; it is treated globally by the sensor.
- Host posture OS and IP addresses are integrated into passive OS fingerprinting storage. You can view them as imported OS profiles.
- You cannot see the quarantined hosts.
- The sensor must recognize each CSA MC host X.509 certificate. You must add them as a trusted host.
- You can configure a maximum of two external product devices.

For More Information

- For more information on external product interfaces, see Chapter 19, "Configuring External Product Interfaces."
- For more information on working with OS maps and identifications, see Adding, Editing, Deleting, and Moving Configured OS Maps, page 12-27 and Configuring OS Identifications, page 21-17.
- For the procedure for adding trusted hosts, see Adding Trusted Hosts, page 15-13.

External Product Interfaces Troubleshooting Tips

To troubleshoot external product interfaces, check the following:

- Make sure the interface is active by checking the output from the **show statistics external-product-interface** command in the CLI, or choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information > Statistics** in the IME and check the Interface state line in the response.
- Make sure you have added the CSA MC IP address to the trusted hosts. If you forgot to add it, add it, wait a few minutes and then check again.
- Confirm subscription login information by opening and closing a subscription on the CSA MC using the browser.

- Check the Event Store for the CSA MC subscription errors.

For More Information

- For the procedure for adding trusted hosts, see Adding Trusted Hosts, page 15-13.
- For the procedure for displaying events, see Displaying Events, page C-97.

Troubleshooting the 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 information to troubleshoot the appliance. It contains the following topics:

Troubleshooting Loose Connections

Perform the following actions to troubleshoot loose connections on sensors:

- Make sure all power cords are securely connected.
- Make sure all cables are properly aligned and securely connected for all external and internal components.
- Remove and check all data and power cables for damage. Make sure no cables have bent pins or damaged connectors.
- Make sure each device is properly seated.
- If a device has latches, make sure they are completely closed and locked.
- Check any interlock or interconnect indicators that indicate a component is not connected properly.
- If problems continue, remove and reinstall each device, checking the connectors and sockets for bent pins or other damage.

The Analysis Engine is Busy

After you reimage a sensor, the Analysis Engine is busy rebuilding Regex tables and does not respond to new configurations. You can check whether the Analysis Engine is busy by using the **show statistics virtual-sensor** command. You receive the following error message if the Analysis Engine is busy:

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy rebuilding regex tables. This
may take a while.
sensor#
```

When the Analysis Engine is busy rebuilding Regex tables, you receive an error message if you try to update a configuration, for example, enabling or retiring a signature:

```
sensor# configure terminal
sensor(config)# service sig sig0
sensor(config-sig)# sig 2000 0
sensor(config-sig-sig)# status enabled
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# retired false
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
Error: editConfigDeltaSignatureDefinition : Analysis Engine is busy rebuilding regex
tables. This may take a while.
The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]: no
No changes were made to the configuration.
sensor(config)#
```

If you try to get the virtual sensor statistics immediately after you boot a sensor, you receive an error message. Although the sensor has rebuilt the cache files, the virtual sensor is not finished initializing.

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy.
sensor#
```

When you receive the errors that the Analysis Engine is busy, wait a while before trying to make configuration changes. Use the **show statistics virtual-sensor** command to find out when the Analysis Engine is available again.

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, page C-25
- Correcting a Misconfigured Access List, page C-27
- Duplicate IP Address Shuts Interface Down, page C-27

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:

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

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

```
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#
```

Step 3 Make sure the sensor IP address is unique. If the management interface detects that another device on the network has the same IP address, it does not come up.

```
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 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

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

```
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 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

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

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 workstation IP address, and the sensor is in front of the firewall, make sure that the sensor access list contains a permit entry for the workstation translated address.

For More Information

- For the procedures for changing the IP address, changing the access list, and enabling and disabling Telnet, see Configuring Network Settings, page 6-1.
- For the various ways to open a CLI session directly on the sensor, see Chapter 24, "Logging In to the Sensor."

Correcting a 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: 192.168.1.2/24,192.168.1.1 default: 10.1.9.201/24,10.1.9.1
      host-name: sensor-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. If the output says the command and control interface link status is down, there is a hardware issue or an IP address conflict.

```
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#
```

Step 3 Make sure the sensor cabling is correct.

Step 4 Make sure the IP address is correct.

For More Information

- To make sure the sensor cabling is correct, refer to your sensor chapter in *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.2*.
- For the procedure for making sure the IP address is correct, see Configuring Network Settings, page 6-1 .

The SensorApp and Alerting

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

- The SensorApp Not Running, page C-29
- Physical Connectivity, SPAN, or VACL Port Issue, page C-30
- Unable to See Alerts, page C-32
- Sensor Not Seeing Packets, page C-33
- Cleaning Up a Corrupted SensorApp Configuration, page C-35

The SensorApp Not Running

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

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

Step 1 Log in to the CLI.

Step 2 Determine the status of the Analysis Engine service and whether you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

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


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

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

Upgrade History:

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

Recovery Partition Version 1.1 - 7.2(1)E4

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

Step 3 If the 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 If you do not have the latest software updates, download them from Cisco.com. Read the Readme that accompanies the software upgrade for any known DDTS for the SensorApp or the Analysis Engine.

Step 5 If the Analysis Engine is still not running, enter **`show tech-support`** and save the output.

Step 6 Reboot the sensor.

Step 7 Enter **`show version`** after the sensor has stabilized to see if the issue is resolved.

Step 8 If the Analysis Engine still reads `Not Running`, contact TAC with the original **show tech support** command output.

For More Information

- For more information on IPS system architecture, see Appendix A, "System Architecture."
- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.

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:

- Make sure the sensing port is connected properly on the appliance.
- Make sure the sensing port is connected to the correct SPAN or VACL capture port on IDSM2.

Step 4 Verify the interface configuration:

- Make sure you have the interfaces configured properly.
- 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
```

For More Information

- For the procedure for properly installing the sensing interface on your sensor, refer to your sensor chapter in *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.2*.
- For the procedures for configuring interfaces on your sensor, see Chapter 7, "Configuring 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 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
- Make sure the sensing interface is in a virtual sensor

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:

- Check the cabling.
- 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 ...
```

For More Information

For the procedure for installing the sensor properly, refer to your sensor chapter in *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 7.2*.

Cleaning Up a Corrupted SensorApp Configuration

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

For More Information

For more information on IPS system architecture, see Appendix A, "System Architecture."

Blocking

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

- Troubleshooting Blocking, page C-36
- Verifying the ARC is Running, page C-37
- Verifying ARC Connections are Active, page C-38
- Device Access Issues, page C-40
- Verifying the Interfaces and Directions on the Network Device, page C-41
- Enabling SSH Connections to the Network Device, page C-42
- Blocking Not Occurring for a Signature, page C-42
- Verifying the Master Blocking Sensor Configuration, page C-43

Troubleshooting Blocking

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

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

To troubleshoot the ARC, follow these steps:

1. Verify that the ARC is running.
2. Verify that the ARC is connecting to the network devices.
3. Verify that the Event Action is set to Block Host for specific signatures.
4. Verify that the master blocking sensor is properly configured.

For More Information

- For the procedure to verify that the ARC is running, see Verifying the ARC is Running, page C-37.
- For the procedure to verify that the ARC is connecting, see Verifying ARC Connections are Active, page C-38.
- For the procedure to verify that the Event Action is set to Block Host, see Blocking Not Occurring for a Signature, page C-42.
- For the procedure to verify that the master blocking sensor is properly configured, see Verifying the Master Blocking Sensor Configuration, page C-43.
- For a discussion of ARC architecture, see Attack Response Controller, page A-12.

Verifying the ARC is Running

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

To verify that the ARC is running, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify that the MainApp is running.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

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


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

Upgrade History:

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

Recovery Partition Version 1.1 - 7.2(1)E4
```

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

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

For More Information

For more information on IPS system architecture, see Appendix A, "System Architecture."

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 the 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 the 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 2011 | include : nac
```

Step 4 Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

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


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

Upgrade History:

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

Recovery Partition Version 1.1 - 7.2(1)E4

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

Note If you do not have the latest software updates, download them from Cisco.com. Read the Readme that accompanies the software upgrade for any known DDTS for the ARC.

Step 5 Make sure the configuration settings for each device are correct (the username, password, and IP address).

Step 6 Make sure the interface and directions for each network device are correct.

Step 7 If the network device is using SSH-3DES, make sure that you have enabled SSH connections to the device.

Step 8 Verify that each interface and direction on each controlled device is correct.

For More Information

- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.
- For more information about configuring devices, see Device Access Issues, page C-40.
- For the procedure for verifying the interfaces and directions for each network device, see Verifying the Interfaces and Directions on the Network Device, page C-41.
- For the procedure for enabling SSH, see Enabling SSH Connections to the Network Device, page C-42.

Device Access Issues

The 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 and direction on each network device is correct.

For More Information

For the procedure for verifying the interfaces and directions for each network device, see Verifying the Interfaces and Directions on the Network Device, page C-41.

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 To perform a manual block, choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Time-Based Actions > Host Blocks**.

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 router ACL. 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-3DES as the communication protocol for the network device, you must make sure you have enabled it on the device.

To enable SSH-3DES 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-3DES.

```
sensor(config)# ssh-3des 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 a master blocking sensor configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 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 3 If the master blocking sensor does not show up in the statistics, you need to add it.

Step 4 Initiate a manual block to a bogus host IP address to make sure the master blocking sensor is initiating blocks.

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

Step 5 Exit network access general submode.

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

Step 6 Press **Enter** to apply the changes or type **no** to discard them.

Step 7 Verify that the block shows up in the ARC statistics.

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

Step 8 Log in to the CLI of the master blocking sensor host, 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 9 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
```

For More Information

For the procedure to configure the sensor to be a master blocking sensor, see Configuring the Master Blocking Sensor, page 16-23.

Logging

This section describes debug logging, and contains the following topics:

- Understanding Debug Logging, page C-45
- Enabling Debug Logging, page C-45
- Zone Names, page C-49
- Directing cidLog Messages to SysLog, page C-50

Understanding Debug Logging

TAC may suggest that you turn on debug logging for troubleshooting purposes. Logger 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.

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 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 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)#
```

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:

For More Information

For a list of what each zone name refers to, see Zone Names, page C-49.

Zone Names

Table C-2 lists the debug logger zone names:

Table C-2 Debug Logger Zone Names

Zone Name	Description
AD	Anomaly Detection zone
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
cplane	Control Plane zone
csi	CIDS Servlet Interface[1]
ctlTransSource	Outbound control transactions zone
intfc	Interface zone
nac	ARC zone
rep	Reputation zone
sched	Automatic update scheduler zone
sensorApp	AnalysisEngine zone
tls	SSL and TLS zone

[1] The CIDS servlet interface is the interface layer between the CIDS web server and the servlets.

For More Information

To learn more about the IPS Logger service, see Logger, page A-19.

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

Note There is only one sensing interface on the ASA IPS modules (ASA 5500-X IPS SSP and ASA 5585-X IPS SSP), so you cannot designate an alternate TCP reset interface.

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

Note TCP Resets are not supported over MPLS links or the following tunnels: GRE, IPv4 in IPv4, IPv6 in IPv4, or IPv4 in IPv6.

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 alarms 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 more information.

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:

- Upgrading, page C-52
- Which Updates to Apply and Their Prerequisites, page C-53
- Issues With Automatic Update, page C-53
- Updating a Sensor with the Update Stored on the Sensor, page C-54

Upgrading

When you upgrade an IPS sensor, you may receive an error that the Analysis Engine is not running:

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-7.2.-1-E4.pkg
Password: ********
Warning: Executing this command will apply a major version upgrade to the application
partition. The system may be rebooted to complete the upgrade.
Continue with upgrade?: yes
Error: AnalysisEngine is not running. Please reset box and attempt upgrade again.
```

If you receive this error, you must get the Analysis Engine running before trying to upgrade again. This error is often caused by a defect in the currently running version. Try rebooting the sensor, and after reboot, run the **setup** command and remove the interfaces from the virtual sensor vs0. When it is not monitoring traffic, Analysis Engine usually stays up and running. You can upgrade at this time. After the upgrade, add the interfaces back to the virtual sensor vs0 using the **setup** command.

Or you can use the system image file to reimage the sensor directly to the version you want. You can reimage a sensor and avoid the error because the reimage process does not check to see if the Analysis Engine is running.

Caution Reimaging using the system image file restores all configuration defaults.

For More Information

- For more information on running the **setup** command, see Chapter 25, "Initializing the Sensor."
- For more information on reimaging your sensor, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."

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:

- Signature updates require the minimum version and engine version listed in the filename.
- Engine updates require the major or minor version in the engine update filename. Service packs require the correct minor version.
- Minor versions require the correct major version.
- Major versions require the previous major version.

For More Information

To understand how to interpret the IPS software filenames, see IPS Software Versioning, page 26-3.

Issues With Automatic Update

The following list provides suggestions for troubleshooting automatic updates:

- 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.
  - Use the **upgrade** command to manually upgrade the sensor.
  - 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.
- 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.

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.
- Make sure the passwords are 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.

For More Information

- For the procedure for creating the service account, see Creating the Service Account, page C-5.
- For the procedure for reimaging your sensor, see Chapter 27, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for adding hosts to the SSH known hosts list, see Defining Known Host RSA1 Keys, page 15-9.
- For the procedure for determining the software version, see Displaying Version Information, page C-80.

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.

Step 3 FTP or SCP the update file to the sensor /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 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: *****
```

For More Information

For the procedure for obtaining Cisco IPS software, see Obtaining Cisco IPS Software, page 26-1.

Troubleshooting the IDM

Tip Before troubleshooting the IDM, 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.

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

Note The IDM is part of the IME configuration, so these troubleshooting procedures also apply to the IME.

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 the IDM. It contains the following topics:

- Cannot Launch the IDM - Loading Java Applet Failed, page C-55
- Cannot Launch the IDM-the Analysis Engine Busy, page C-56
- The IDM, Remote Manager, or Sensing Interfaces Cannot Access Sensor, page C-56
- Signatures Not Producing Alerts, page C-57

Cannot Launch the 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 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 the IDM-the 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 the IDM.

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

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

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

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 192.168.1.2/24,192.168.1.1
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
```

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

For More Information

For the procedure for enabling and disabling Telnet on the sensor, and configuring the web server, see Configuring Network Settings, page 6-1 .

Signatures Not Producing Alerts

⚠ **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.

If you are not seeing any alerts when signatures are firing, make sure that you have configured Produce Alert as an event action. For example, if you choose Produce Alert, but later add another event action and do not add Produce Alert to the new configuration, alerts are not sent to the Event Store. To make sure you are getting alerts, check the statistics for the virtual sensor and the Event Store.

For More Information

- For more information about event actions, see Event Actions, page 12-7.
- For the procedure for configuring event actions, see Assigning Actions to Signatures, page 10-23.
- For the procedure for obtaining statistics about virtual sensor and Event Store, see Viewing Statistics, page 21-22.

Troubleshooting the IME

Tip Before troubleshooting the IME, 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 describes troubleshooting tools for the IME, and contains the following sections:

- Time Synchronization on the IME and the Sensor, page C-58
- Not Supported Error Message, page C-58

Time Synchronization on the IME and the Sensor

Symptom The IME displays `No Data Available` on the Events dashboard. A historical query does not return any events; however, events are coming in to the IME and they appear in the real-time event viewer.

Possible Cause The time is not synchronized between the sensor and the IME local server. The IME dashboards use a time relative to the IME local time. If these times are not synchronized, the query does not return any results. When you add a sensor to the IME, it checks for the time synchronization and warns you to correct it if is in wrong. The IME also displays a clock warning in Home > Devices > Device List to warn you about problems with synchronization.

Recommended Action Change the time settings on the sensor or the IME local server. In most cases, the time change is required for the sensor because it is configured with the incorrect or default time.

For More Information

- For more information on time and the sensor, see Time Sources and the Sensor, page C-15.
- For the procedure for changing the time on the sensor, see Correcting Time on the Sensor, page C-17.

Not Supported Error Message

Symptom The IME displays `Not Supported` in the device list table and in some gadgets, and no data is included.

Possible Cause Click **Details** to see an explanation for this message. The IME needs IPS 6.1 or later to obtain certain information. The IME still operates with event monitoring and reporting for IPS 5.0 and later and specific IOS IPS versions, but some functions, such as health information and integrated configuration, are not available.

Recommended Action Upgrade to IPS 6.1 or later.

Troubleshooting the ASA 5500-X IPS SSP

Tip Before troubleshooting the ASA 5500-X IPS SSP, check the Caveats section of the Readme for the software version installed on your sensor to see if you are dealing with a known issue.

This section contains troubleshooting information specific to the ASA 5500-X IPS SSP, and contains the following topics:

Failover Scenarios

The following failover scenarios apply to the ASA 5500-X series in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on theASA 5500-X IPS SSP.

Single ASA in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a configuration change or signature/signature engine update, traffic is passed through the ASA without being inspected.
- If the ASA is configured in fail-open mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA in Fail-Close Mode

- If the ASA is configured in fail-close mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the ASA.
- If the ASA is configured in fail-close mode for the ASA 5500-X IPS SSP, and the ASA 5500-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASAs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the ASA 5500-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is still passed through the active ASA without being inspected. Failover is not triggered.
- If the ASAs are configured in fail-open mode, and if the ASA 5500-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500-X IPS SSP that was previously the standby ASA 5500-X IPS SSP.

Two ASAs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5500-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the active ASA. No failover is triggered.
- If the ASAs are configured in fail-close mode, and if the ASA 5500-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5500-X IPS SSP that was previously the standby for the ASA 5500-X IPS SSP.

Configuration Examples

Use the following configuration for the primary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Use the following configuration for the secondary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Health and Status Information

To see the general health of the ASA 5500-X IPS SSP, use the **show module ips details** command.

```
asa# show module ips details
Getting details from the Service Module, please wait...

Card Type:          IPS 5555 Intrusion Prevention System
Model:              IPS5555
Hardware version:   N/A
Serial Number:      FCH1504V0CW
Firmware version:   N/A
Software version:   7.2.(1)E4
MAC Address Range:  503d.e59c.7ca0 to 503d.e59c.7ca0
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data Plane Status:  Up
Status:             Up
License:            IPS Module  Enabled  perpetual
Mgmt IP addr:       192.168.1.2
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.168.1.1
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

The output shows that the ASA 5500-X IPS SSP is up. If the status reads `Down`, you can reset it using the **sw-module module 1 reset** command.

If you have problems with reimaging the ASA 5500-X IPS SSP, use the **debug module-boot** command to see the output as it 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 **sw-module module ips recover** command again to reimage the module.

```
asa-ips# sw-module module ips recover configure image
disk0:/IPS-SSP_5555-K9-sys-1.1-a-7.2.-1-E4.aip
Image URL [tftp://192.0.2.1/IPS-5545-K9-sys-1.1-a-7.2.-1-E4.aip]:
Port IP Address [192.0.2.226]:
VLAN ID [0]:
Gateway IP Address [192.0.2.254]:

asa-ips# debug module-boot
debug module-boot  enabled at level 1
asa-ips# sw-module module ips reload

Reload module ips? [confirm]
Reload issued for module ips.
asa-ips# Mod-ips 228> ***
Mod-ips 229> *** EVENT: The module is reloading.
Mod-ips 230> *** TIME: 08:07:36 CST Jan 17 2012
Mod-ips 231> ***
Mod-ips 232> Mod-ips 233> The system is going down NOW!
Mod-ips 234> Sending SIGTERM to all processes
Mod-ips 235> Sending SIGKILL to all processes
Mod-ips 236> Requesting system reboot
Mod-ips 237> e1000 0000:00:07.0: PCI INT A disabled
Mod-ips 238> e1000 0000:00:06.0: PCI INT A disabled
Mod-ips 239> e1000 0000:00:05.0: PCI INT A disabled
Mod-ips 240> Restarting system.
Mod-ips 241> machine restart
Mod-ips 242> IVSHMEM: addr = 4093640704 size = 67108864
Mod-ips 243>   Booting 'Cisco IPS'
Mod-ips 244> root (hd0,0)
Mod-ips 245>  Filesystem type is ext2fs, partition type 0x83
Mod-ips 246> kernel /ips-2.6.ld ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
init
Mod-ips 247> fs=runtime-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepag
Mod-ips 248> es=3223
Mod-ips 249>    [Linux-bzImage, setup=0x2c00, size=0x2bad80]
Mod-ips 250> Linux version 2.6.29.1 (ipsbuild@seti-teambuilder-a) (gcc version 4.3.2
(crosstool
Mod-ips 251> -NG-1.4.1) ) #56 SMP Tue Dec 6 00:46:11 CST 2011
Mod-ips 252> Command line: ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
initfs=runti
Mod-ips 253> me-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepages=3223
Mod-ips 254> KERNEL supported cpus:
Mod-ips 255>   Intel GenuineIntel
Mod-ips 256>   AMD AuthenticAMD
Mod-ips 257>   Centaur CentaurHauls
Mod-ips 258> BIOS-provided physical RAM map:
Mod-ips 259>  BIOS-e820: 0000000000000000 - 000000000009f400 (usable)
Mod-ips 260>  BIOS-e820: 000000000009f400 - 00000000000a0000 (reserved)
Mod-ips 261>  BIOS-e820: 00000000000f0000 - 0000000000100000 (reserved)
Mod-ips 262>  BIOS-e820: 0000000000100000 - 00000000dfffd000 (usable)
Mod-ips 263>  BIOS-e820: 00000000dfffd000 - 00000000e0000000 (reserved)
Mod-ips 264>  BIOS-e820: 00000000fffbc000 - 0000000100000000 (reserved)
Mod-ips 265>  BIOS-e820: 0000000100000000 - 0000000201400000 (usable)
```

```
Mod-ips 266> DMI 2.4 present.
Mod-ips 267> last_pfn = 0x201400 max_arch_pfn = 0x100000000
Mod-ips 268> last_pfn = 0xdfffd max_arch_pfn = 0x100000000
Mod-ips 269> init_memory_mapping: 0000000000000000-00000000dfffd000
Mod-ips 270> last_map_addr: dfffd000 end: dfffd000
Mod-ips 271> init_memory_mapping: 0000000100000000-0000000201400000
Mod-ips 272> last_map_addr: 201400000 end: 201400000
Mod-ips 273> ACPI: RSDP 000F88D0, 0014 (r0 BOCHS )
Mod-ips 274> ACPI: RSDT DFFFDD00, 0034 (r1 BOCHS  BXPCRSDT        1 BXPC        1)
Mod-ips 275> ACPI: FACP DFFFFD90, 0074 (r1 BOCHS  BXPCFACP        1 BXPC        1)
Mod-ips 276> FADT: X_PM1a_EVT_BLK.bit_width (16) does not match PM1_EVT_LEN (4)
Mod-ips 277> ACPI: DSDT DFFFDF10, 1E22 (r1   BXPC   BXDSDT        1 INTL 20090123)
Mod-ips 278> ACPI: FACS DFFFFD40, 0040
Mod-ips 279> ACPI: SSDT DFFFDE90, 0079 (r1 BOCHS  BXPCSSDT        1 BXPC        1)
Mod-ips 280> ACPI: APIC DFFFDD80, 0090 (r1 BOCHS  BXPCAPIC        1 BXPC        1)
Mod-ips 281> ACPI: HPET DFFFDD40, 0038 (r1 BOCHS  BXPCHPET        1 BXPC        1)
Mod-ips 282> No NUMA configuration found
Mod-ips 283> Faking a node at 0000000000000000-0000000201400000
Mod-ips 284> Bootmem setup node 0 0000000000000000-0000000201400000
Mod-ips 285>   NODE_DATA [0000000000011000 - 000000000001ffff]
Mod-ips 286>   bootmap [0000000000020000 -  000000000006027f] pages 41
Mod-ips 287> (6 early reservations) ==> bootmem [0000000000 - 0201400000]
Mod-ips 288>   #0 [0000000000 - 0000001000]   BIOS data page ==> [0000000000 - 0000001000]
Mod-ips 289>   #1 [0000006000 - 0000008000]       TRAMPOLINE ==> [0000006000 - 0000008000]
Mod-ips 290>   #2 [0000200000 - 0000d55754]    TEXT DATA BSS ==> [0000200000 - 0000d55754]
Mod-ips 291>   #3 [000009f400 - 0000100000]    BIOS reserved ==> [000009f400 - 0000100000]
Mod-ips 292>   #4 [0000008000 - 000000c000]          PGTABLE ==> [0000008000 - 000000c000]
Mod-ips 293>   #5 [000000c000 - 0000011000]          PGTABLE ==> [000000c000 - 0000011000]
Mod-ips 294> found SMP MP-table at [ffff8800000f8920] 000f8920
Mod-ips 295> Zone PFN ranges:
Mod-ips 296>   DMA      0x00000000 -> 0x00001000
Mod-ips 297>   DMA32    0x00001000 -> 0x00100000
Mod-ips 298>   Normal   0x00100000 -> 0x00201400
Mod-ips 299> Movable zone start PFN for each node
Mod-ips 300> early_node_map[3] active PFN ranges
Mod-ips 301>     0: 0x00000000 -> 0x0000009f
Mod-ips 302>     0: 0x00000100 -> 0x000dfffd
Mod-ips 303>     0: 0x00100000 -> 0x00201400
Mod-ips 304> ACPI: PM-Timer IO Port: 0xb008
Mod-ips 305> ACPI: LAPIC (acpi_id[0x00] lapic_id[0x00] enabled)
Mod-ips 306> ACPI: LAPIC (acpi_id[0x01] lapic_id[0x01] enabled)
Mod-ips 307> ACPI: LAPIC (acpi_id[0x02] lapic_id[0x02] enabled)
Mod-ips 308> ACPI: LAPIC (acpi_id[0x03] lapic_id[0x03] enabled)
Mod-ips 309> ACPI: LAPIC (acpi_id[0x04] lapic_id[0x04] enabled)
Mod-ips 310> ACPI: LAPIC (acpi_id[0x05] lapic_id[0x05] enabled)
Mod-ips 311> ACPI: IOAPIC (id[0x06] address[0xfec00000] gsi_base[0])
Mod-ips 312> IOAPIC[0]: apic_id 6, version 0, address 0xfec00000, GSI 0-23
Mod-ips 313> ACPI: INT_SRC_OVR (bus 0 bus_irq 5 global_irq 5 high level)
Mod-ips 314> ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high level)
Mod-ips 315> ACPI: INT_SRC_OVR (bus 0 bus_irq 10 global_irq 10 high level)
Mod-ips 316> ACPI: INT_SRC_OVR (bus 0 bus_irq 11 global_irq 11 high level)
Mod-ips 317> Using ACPI (MADT) for SMP configuration information
Mod-ips 318> ACPI: HPET id: 0x8086a201 base: 0xfed00000
Mod-ips 319> SMP: Allowing 6 CPUs, 0 hotplug CPUs
Mod-ips 320> Allocating PCI resources starting at e2000000 (gap: e0000000:1ffbc000)
Mod-ips 321> NR_CPUS:32 nr_cpumask_bits:32 nr_cpu_ids:6 nr_node_ids:1
Mod-ips 322> PERCPU: Allocating 49152 bytes of per cpu data
Mod-ips 323> Built 1 zonelists in Zone order, mobility grouping on.  Total pages: 1939347
Mod-ips 324> Policy zone: Normal
Mod-ips 325> Kernel command line: ro initfsDev=/dev/hda1 init=loader.run rootrw=/dev/hda2
initf
Mod-ips 326> s=runtime-image.cpio.bz2 hda=nodma console=ttyS0 plat=saleen htlblow=1
hugepages=3
Mod-ips 327> 223
```

```
Mod-ips 328> hugetlb_lowmem_setup: Allocated 2097152 huge pages (size=0x200000) from
lowmem are
Mod-ips 329> a at 0xffff88002ee00000 phys addr 0x000000002ee00000
Mod-ips 330> Initializing CPU#0
Mod-ips 331> PID hash table entries: 4096 (order: 12, 32768 bytes)
Mod-ips 332> Fast TSC calibration using PIT
Mod-ips 333> Detected 2792.965 MHz processor.
Mod-ips 334> Console: colour VGA+ 80x25
Mod-ips 335> console [ttyS0] enabled
Mod-ips 336> Checking aperture...
Mod-ips 337> No AGP bridge found
Mod-ips 338> PCI-DMA: Using software bounce buffering for IO (SWIOTLB)
Mod-ips 339> Placing 64MB software IO TLB between ffff880020000000 - ffff880024000000
Mod-ips 340> software IO TLB at phys 0x20000000 - 0x24000000
Mod-ips 341> Memory: 7693472k/8409088k available (3164k kernel code, 524688k absent,
190928k re
Mod-ips 342> served, 1511k data, 1032k init)
Mod-ips 343> Calibrating delay loop (skipped), value calculated using timer frequency..
5585.93
Mod-ips 344>  BogoMIPS (lpj=2792965)
Mod-ips 345> Dentry cache hash table entries: 1048576 (order: 11, 8388608 bytes)
Mod-ips 346> Inode-cache hash table entries: 524288 (order: 10, 4194304 bytes)
Mod-ips 347> Mount-cache hash table entries: 256
Mod-ips 348> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 349> CPU: L2 cache: 4096K
Mod-ips 350> CPU 0/0x0 -> Node 0
Mod-ips 351> Freeing SMP alternatives: 29k freed
Mod-ips 352> ACPI: Core revision 20081204
Mod-ips 353> Setting APIC routing to flat
Mod-ips 354> ..TIMER: vector=0x30 apic1=0 pin1=0 apic2=-1 pin2=-1
Mod-ips 355> CPU0: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 356> Booting processor 1 APIC 0x1 ip 0x6000
Mod-ips 357> Initializing CPU#1
Mod-ips 358> Calibrating delay using timer specific routine.. 5585.16 BogoMIPS
(lpj=2792581)
Mod-ips 359> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 360> CPU: L2 cache: 4096K
Mod-ips 361> CPU 1/0x1 -> Node 0
Mod-ips 362> CPU1: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 363> checking TSC synchronization [CPU#0 -> CPU#1]:
Mod-ips 364> Measured 1453783140569731 cycles TSC warp between CPUs, turning off TSC
clock.
Mod-ips 365> Marking TSC unstable due to check_tsc_sync_source failed
Mod-ips 366> Booting processor 2 APIC 0x2 ip 0x6000
Mod-ips 367> Initializing CPU#2
Mod-ips 368> Calibrating delay using timer specific routine.. 5580.51 BogoMIPS
(lpj=2790259)
Mod-ips 369> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 370> CPU: L2 cache: 4096K
Mod-ips 371> CPU 2/0x2 -> Node 0
Mod-ips 372> CPU2: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 373> Booting processor 3 APIC 0x3 ip 0x6000
Mod-ips 374> Initializing CPU#3
Mod-ips 375> Calibrating delay using timer specific routine.. 5585.18 BogoMIPS
(lpj=2792594)
Mod-ips 376> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 377> CPU: L2 cache: 4096K
Mod-ips 378> CPU 3/0x3 -> Node 0
Mod-ips 379> CPU3: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 380> Booting processor 4 APIC 0x4 ip 0x6000
Mod-ips 381> Initializing CPU#4
Mod-ips 382> Calibrating delay using timer specific routine.. 5585.15 BogoMIPS
(lpj=2792579)
Mod-ips 383> CPU: L1 I cache: 32K, L1 D cache: 32K
```

```
Mod-ips 384> CPU: L2 cache: 4096K
Mod-ips 385> CPU 4/0x4 -> Node 0
Mod-ips 386> CPU4: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 387> Booting processor 5 APIC 0x5 ip 0x6000
Mod-ips 388> Initializing CPU#5
Mod-ips 389> Calibrating delay using timer specific routine.. 5585.21 BogoMIPS
(lpj=2792609)
Mod-ips 390> CPU: L1 I cache: 32K, L1 D cache: 32K
Mod-ips 391> CPU: L2 cache: 4096K
Mod-ips 392> CPU 5/0x5 -> Node 0
Mod-ips 393> CPU5: Intel QEMU Virtual CPU version 0.12.5 stepping 03
Mod-ips 394> Brought up 6 CPUs
Mod-ips 395> Total of 6 processors activated (33507.17 BogoMIPS).
Mod-ips 396> net_namespace: 1312 bytes
Mod-ips 397> Booting paravirtualized kernel on bare hardware
Mod-ips 398> NET: Registered protocol family 16
Mod-ips 399> ACPI: bus type pci registered
Mod-ips 400> dca service started, version 1.8
Mod-ips 401> PCI: Using configuration type 1 for base access
Mod-ips 402> mtrr: your CPUs had inconsistent variable MTRR settings
Mod-ips 403> mtrr: your CPUs had inconsistent MTRRdefType settings
Mod-ips 404> mtrr: probably your BIOS does not setup all CPUs.
Mod-ips 405> mtrr: corrected configuration.
Mod-ips 406> bio: create slab <bio-0> at 0
Mod-ips 407> ACPI: Interpreter enabled
Mod-ips 408> ACPI: (supports S0 S5)
Mod-ips 409> ACPI: Using IOAPIC for interrupt routing
Mod-ips 410> ACPI: No dock devices found.
Mod-ips 411> ACPI: PCI Root Bridge [PCI0] (0000:00)
Mod-ips 412> pci 0000:00:01.3: quirk: region b000-b03f claimed by PIIX4 ACPI
Mod-ips 413> pci 0000:00:01.3: quirk: region b100-b10f claimed by PIIX4 SMB
Mod-ips 414> IVSHMEM: addr = 4093640704 size = 67108864
Mod-ips 415> ACPI: PCI Interrupt Link [LNKA] (IRQs 5 *10 11)
Mod-ips 416> ACPI: PCI Interrupt Link [LNKB] (IRQs 5 *10 11)
Mod-ips 417> ACPI: PCI Interrupt Link [LNKC] (IRQs 5 10 *11)
Mod-ips 418> ACPI: PCI Interrupt Link [LNKD] (IRQs 5 10 *11)
Mod-ips 419> SCSI subsystem initialized
Mod-ips 420> usbcore: registered new interface driver usbfs
Mod-ips 421> usbcore: registered new interface driver hub
Mod-ips 422> usbcore: registered new device driver usb
Mod-ips 423> PCI: Using ACPI for IRQ routing
Mod-ips 424> pnp: PnP ACPI init
Mod-ips 425> ACPI: bus type pnp registered
Mod-ips 426> pnp: PnP ACPI: found 9 devices
Mod-ips 427> ACPI: ACPI bus type pnp unregistered
Mod-ips 428> NET: Registered protocol family 2
Mod-ips 429> IP route cache hash table entries: 262144 (order: 9, 2097152 bytes)
Mod-ips 430> TCP established hash table entries: 524288 (order: 11, 8388608 bytes)
Mod-ips 431> TCP bind hash table entries: 65536 (order: 8, 1048576 bytes)
Mod-ips 432> TCP: Hash tables configured (established 524288 bind 65536)
Mod-ips 433> TCP reno registered
Mod-ips 434> NET: Registered protocol family 1
Mod-ips 435> Adding htlb page ffff88002ee00000 phys 000000002ee00000 page ffffe20000a41000
Mod-ips 436> HugeTLB registered 2 MB page size, pre-allocated 3223 pages
Mod-ips 437> report_hugepages: Using 1 pages from low memory at ffff88002ee00000 HugeTLB
FS
Mod-ips 438> msgmni has been set to 15026
Mod-ips 439> alg: No test for stdrng (krng)
Mod-ips 440> io scheduler noop registered
Mod-ips 441> io scheduler anticipatory registered
Mod-ips 442> io scheduler deadline registered
Mod-ips 443> io scheduler cfq registered (default)
Mod-ips 444> pci 0000:00:00.0: Limiting direct PCI/PCI transfers
Mod-ips 445> pci 0000:00:01.0: PIIX3: Enabling Passive Release
```

```
Mod-ips 446> pci 0000:00:01.0: Activating ISA DMA hang workarounds
Mod-ips 447> pci_hotplug: PCI Hot Plug PCI Core version: 0.5
Mod-ips 448> pciehp: PCI Express Hot Plug Controller Driver version: 0.4
Mod-ips 449> acpiphp: ACPI Hot Plug PCI Controller Driver version: 0.5
Mod-ips 450> acpiphp_glue: can't get bus number, assuming 0
Mod-ips 451> decode_hpp: Could not get hotplug parameters. Use defaults
Mod-ips 452> acpiphp: Slot [1] registered
Mod-ips 453> acpiphp: Slot [2] registered
Mod-ips 454> acpiphp: Slot [3] registered
Mod-ips 455> acpiphp: Slot [4] registered
Mod-ips 456> acpiphp: Slot [5] registered
Mod-ips 457> acpiphp: Slot [6] registered
Mod-ips 458> acpiphp: Slot [7] registered
Mod-ips 459> acpiphp: Slot [8] registered
Mod-ips 460> acpiphp: Slot [9] registered
Mod-ips 461> acpiphp: Slot [10] registered
Mod-ips 462> acpiphp: Slot [11] registered
Mod-ips 463> acpiphp: Slot [12] registered
Mod-ips 464> acpiphp: Slot [13] registered
Mod-ips 465> acpiphp: Slot [14] registered
Mod-ips 466> acpiphp: Slot [15] registered
Mod-ips 467> acpiphp: Slot [16] registered
Mod-ips 468> acpiphp: Slot [17] registered
Mod-ips 469> acpiphp: Slot [18] registered
Mod-ips 470> acpiphp: Slot [19] registered
Mod-ips 471> acpiphp: Slot [20] registered
Mod-ips 472> acpiphp: Slot [21] registered
Mod-ips 473> acpiphp: Slot [22] registered
Mod-ips 474> acpiphp: Slot [23] registered
Mod-ips 475> acpiphp: Slot [24] registered
Mod-ips 476> acpiphp: Slot [25] registered
Mod-ips 477> acpiphp: Slot [26] registered
Mod-ips 478> acpiphp: Slot [27] registered
Mod-ips 479> acpiphp: Slot [28] registered
Mod-ips 480> acpiphp: Slot [29] registered
Mod-ips 481> acpiphp: Slot [30] registered
Mod-ips 482> acpiphp: Slot [31] registered
Mod-ips 483> shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
Mod-ips 484> fakephp: Fake PCI Hot Plug Controller Driver
Mod-ips 485> fakephp: pci_hp_register failed with error -16
Mod-ips 486> fakephp: pci_hp_register failed with error -16
Mod-ips 487> fakephp: pci_hp_register failed with error -16
Mod-ips 488> fakephp: pci_hp_register failed with error -16
Mod-ips 489> fakephp: pci_hp_register failed with error -16
Mod-ips 490> fakephp: pci_hp_register failed with error -16
Mod-ips 491> fakephp: pci_hp_register failed with error -16
Mod-ips 492> processor ACPI_CPU:00: registered as cooling_device0
Mod-ips 493> processor ACPI_CPU:01: registered as cooling_device1
Mod-ips 494> processor ACPI_CPU:02: registered as cooling_device2
Mod-ips 495> processor ACPI_CPU:03: registered as cooling_device3
Mod-ips 496> processor ACPI_CPU:04: registered as cooling_device4
Mod-ips 497> processor ACPI_CPU:05: registered as cooling_device5
Mod-ips 498> hpet_acpi_add: no address or irqs in _CRS
Mod-ips 499> Non-volatile memory driver v1.3
Mod-ips 500> Linux agpgart interface v0.103
Mod-ips 501> ipmi message handler version 39.2
Mod-ips 502> ipmi device interface
Mod-ips 503> IPMI System Interface driver.
Mod-ips 504> ipmi_si: Unable to find any System Interface(s)
Mod-ips 505> IPMI SMB Interface driver
Mod-ips 506> IPMI Watchdog: driver initialized
Mod-ips 507> Copyright (C) 2004 MontaVista Software - IPMI Powerdown via sys_reboot.
Mod-ips 508> Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
Mod-ips 509> ?serial8250: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
```

```
Mod-ips 510> serial8250: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
Mod-ips 511> 00:06: ttyS0 at I/O 0x3f8 (irq = 4) is a 16550A
Mod-ips 512> 00:07: ttyS1 at I/O 0x2f8 (irq = 3) is a 16550A
Mod-ips 513> brd: module loaded
Mod-ips 514> loop: module loaded
Mod-ips 515> lpc: version 0.1 (Nov 10 2011)
Mod-ips 516> tun: Universal TUN/TAP device driver, 1.6
Mod-ips 517> tun: (C) 1999-2004 Max Krasnyansky <maxk@qualcomm.com>
Mod-ips 518> Uniform Multi-Platform E-IDE driver
Mod-ips 519> piix 0000:00:01.1: IDE controller (0x8086:0x7010 rev 0x00)
Mod-ips 520> piix 0000:00:01.1: not 100native mode: will probe irqs later
Mod-ips 521>     ide0: BM-DMA at 0xc000-0xc007
Mod-ips 522>     ide1: BM-DMA at 0xc008-0xc00f
Mod-ips 523> hda: QEMU HARDDISK, ATA DISK drive
Mod-ips 524> Clocksource tsc unstable (delta = 2851415955127 ns)
Mod-ips 525> hda: MWDMA2 mode selected
Mod-ips 526> hdc: QEMU DVD-ROM, ATAPI CD/DVD-ROM drive
Mod-ips 527> hdc: MWDMA2 mode selected
Mod-ips 528> ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
Mod-ips 529> ide1 at 0x170-0x177,0x376 on irq 15
Mod-ips 530> ide_generic: please use "probe_mask=0x3f" module parameter for probing all
legacy
Mod-ips 531> ISA IDE ports
Mod-ips 532> ide-gd driver 1.18
Mod-ips 533> hda: max request size: 512KiB
Mod-ips 534> hda: 7815168 sectors (4001 MB) w/256KiB Cache, CHS=7753/255/63
Mod-ips 535> hda: cache flushes supported
Mod-ips 536>  hda: hda1 hda2 hda3 hda4
Mod-ips 537> Driver 'sd' needs updating - please use bus_type methods
Mod-ips 538> Driver 'sr' needs updating - please use bus_type methods
Mod-ips 539> ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
Mod-ips 540> ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
Mod-ips 541> uhci_hcd: USB Universal Host Controller Interface driver
Mod-ips 542> Initializing USB Mass Storage driver...
Mod-ips 543> usbcore: registered new interface driver usb-storage
Mod-ips 544> USB Mass Storage support registered.
Mod-ips 545> PNP: PS/2 Controller [PNP0303:KBD,PNP0f13:MOU] at 0x60,0x64 irq 1,12
Mod-ips 546> serio: i8042 KBD port at 0x60,0x64 irq 1
Mod-ips 547> serio: i8042 AUX port at 0x60,0x64 irq 12
Mod-ips 548> mice: PS/2 mouse device common for all mice
Mod-ips 549> rtc_cmos 00:01: rtc core: registered rtc_cmos as rtc0
Mod-ips 550> rtc0: alarms up to one day, 114 bytes nvram
Mod-ips 551> input: AT Translated Set 2 keyboard as /class/input/input0
Mod-ips 552> i2c /dev entries driver
Mod-ips 553> piix4_smbus 0000:00:01.3: SMBus Host Controller at 0xb100, revision 0
Mod-ips 554> device-mapper: ioctl: 4.14.0-ioctl (2008-04-23) initialised:
dm-devel@redhat.com
Mod-ips 555> cpuidle: using governor ladder
Mod-ips 556> usbcore: registered new interface driver usbhid
Mod-ips 557> usbhid: v2.6:USB HID core driver
Mod-ips 558> TCP cubic registered
Mod-ips 559> IPv6: Loaded, but is disabled by default. IPv6 may be enabled on individual
interf
Mod-ips 560> aces.
Mod-ips 561> NET: Registered protocol family 10
Mod-ips 562> NET: Registered protocol family 17
Mod-ips 563> NET: Registered protocol family 5
Mod-ips 564> rtc_cmos 00:01: setting system clock to 2012-01-17 14:06:34 UTC (1326809194)
Mod-ips 565> Freeing unused kernel memory: 1032k freed
Mod-ips 566> Write protecting the kernel read-only data: 4272k
Mod-ips 567> Loader init started...
Mod-ips 568> kjournald starting.  Commit interval 5 seconds
Mod-ips 569> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 570> input: ImExPS/2 Generic Explorer Mouse as /class/input/input1
```

```
Mod-ips 571> 51216 blocks
Mod-ips 572> Checking rootrw fs: corrected filesystem
Mod-ips 573> kjournald starting.  Commit interval 5 seconds
Mod-ips 574> EXT3 FS on hda2, internal journal
Mod-ips 575> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 576> mkdir: cannot create directory '/lib/modules': File exists
Mod-ips 577> init started: BusyBox v1.13.1 (2011-11-01 07:21:34 CDT)
Mod-ips 578> starting pid 678, tty '': '/etc/init.d/rc.init'
Mod-ips 579> Checking system fs: no errors
Mod-ips 580> kjournald starting.  Commit interval 5 seconds
Mod-ips 581> EXT3-fs: mounted filesystem with ordered data mode.
Mod-ips 582> /etc/init.d/rc.init: line 102: /proc/sys/vm/bdflush: No such file or
directory
Mod-ips 583> starting pid 728, tty '': '/etc/init.d/rcS'
Mod-ips 584> Initializing random number generator... done.
Mod-ips 585> Starting network... ifconfig lo 127.0.0.1 netmask 255.255.255.255 up
Mod-ips 586> starting inetd
Mod-ips 587> done
Mod-ips 588> Starting sshd:
Mod-ips 589> Starting nscd:
Mod-ips 590> Set Irq Affinity ... cpus:
Mod-ips 591> Checking kernel allocated memory: EXT3 FS on hda1, internal journal
Mod-ips 592> [  OK  ]
Mod-ips 593> Unloading REGEX-CP drivers ...
Mod-ips 594> Loading REGEX-CP drivers ...
Mod-ips 595> ACPI: PCI Interrupt Link [LNKD] enabled at IRQ 11
Mod-ips 596> cpp_user_kvm 0000:00:04.0: PCI INT A -> Link[LNKD] -> GSI 11 (level, high) ->
IRQ
Mod-ips 597> 11
Mod-ips 598> Detected cpp_user_kvm device with 33554432 bytes of shared memory
Mod-ips 599> Device 0: model=LCPX8640, cpc=T2005, cpe0=None, cpe1=None
Mod-ips 600> Load cidmodcap:
Mod-ips 601> Create node:
Mod-ips 602> ln: /etc/modprobe.conf: File exists
Mod-ips 603> Shutting down network... ifconfig lo down
Mod-ips 604> ifconfig lo down
Mod-ips 605> done
Mod-ips 606> Load ihm:
Mod-ips 607> Create node:
Mod-ips 608> Load kvm_ivshmem: IVSHMEM: writing 0x0 to 0xc86cf8
Mod-ips 609> IVSHMEM: IntrMask write(w) val = 0xffff
Mod-ips 610> Create node:
Mod-ips 611> Create node:
Mod-ips 612> Create node:
Mod-ips 613> Set Irq Affinity ... cpus: 6
Mod-ips 614> Starting network... ifconfig lo 127.0.0.1 netmask 255.255.255.255 up
Mod-ips 615> done
Mod-ips 616> Creating boot.info[  OK  ]
Mod-ips 617> Checking for system modifications since last boot[  OK  ]
Mod-ips 618> Checking model identification[  OK  ]
Mod-ips 619> Model: ASA-5555
Mod-ips 620> Model=ASA-5555
Mod-ips 621> Unable to set speed and duplex for user mode interfaces
Mod-ips 622> interface type 0x8086:0x100e at pci address 0:6.0(0) is currently named eth1
Mod-ips 623> Renaming eth1 --> ma0_0
Mod-ips 624> interface type 0x8086:0x100e at pci address 0:7.0(0) is currently named po0_0
Mod-ips 625> interface type 0x8086:0x100e at pci address 0:5.0(0) is currently named eth0
Mod-ips 626> Renaming eth0 --> sy0_0
Mod-ips 627> Initializing access list
Mod-ips 628> MGMT_INTFC_CIDS_NAME Management0/0
Mod-ips 629> MGMT_INTFC_OS_NAME ma0_0
Mod-ips 630> SYSTEM_PCI_IDS 0x0030,0x0028
Mod-ips 631> Load rebootkom:
Mod-ips 632> root: Starting SSM controlplane
```

```
Mod-ips 633> Starting CIDS:
Mod-ips 634> starting pid 1718, tty '/dev/ttyS0': '/sbin/getty -L ttyS0 9600 vt100'
```

The ASA 5500-X IPS SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5500-X IPS SSP, because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0
- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

The ASA 5500-X IPS SSP and Memory Usage

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

Note Make sure you have the Memory Usage option in the sensor health metrics enabled.

Table C-3 lists the Yellow Threshold and the Red Threshold health values.

Table C-3 ASA 5500-X IPS SSP Memory Usage Values

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

The ASA 5500-X IPS SSP and Jumbo Packets

The jumbo packet count in the **show interface** command output from the lines `Total Jumbo Packets Received` and `Total Jumbo Packets Transmitted` for ASA IPS modules may be larger than expected due to some packets that were almost jumbo size on the wire being counted as jumbo size by the IPS. This miscount is a result of header bytes added to the packet by the ASA before the packet is transmitted to the IPS. For IPv4, 58 bytes of header data are added. For IPv6, 78 bytes of header data are added. The ASA removes the added IPS header before the packet leaves the ASA.

Reloading IPS Messages

The following messages generated during some IPS signature and global correlation updates for IPS 7.1 and later on the ASA 5500-X IPS SSP can cause confusion since the IPS is not reloading:

```
ASA5585-SSP-IPS20 Module in slot 1, application up "IPS", version "7.1(1)E4" Normal 
Operation
ASA5585-SSP-IPS20 Module in slot 1, application reloading "IPS", version "7.1(1)E4" Config 
Change
```

These messages are generated during some, but not all, of the global correlation updates that are attempted every five minutes. This is expected behavior. There is a global correlation check every five minutes, but there may not be an update available, thus the message appears every hour or so. When a global correlation update actually takes place, a message is sent from the IPS to the ASA indicating that a configuration change is taking place.

Troubleshooting the ASA 5585-X IPS SSP

Tip Before troubleshooting the ASA 5585-X IPS SSP, check the Caveats section of the Readme for the software version installed on your sensor to see if you are dealing with a known issue.

This section contains troubleshooting information specific to the ASA 5585-X IPS SSP, and contains the following topics:

Failover Scenarios

The following failover scenarios apply to the ASA 5585-X in the event of configuration changes, signature/signature engine updates, service packs, and SensorApp crashes on the ASA 5585-X IPS SSP.

Single ASA 5585-X in Fail-Open Mode

- If the ASA is configured in fail-open mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a configuration change or signature/signature engine update, traffic is passed through the ASA without being inspected.
- If the ASA is configured in fail-open mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is passed through the ASA without being inspected.

Single ASA 5585-X in Fail-Close Mode

- If the ASA is configured in fail-close mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the ASA.
- If the ASA is configured in fail-close mode for the ASA 5585-X IPS SSP, and the ASA 5585-X IPS SSP experiences a SensorApp crash or a service pack upgrade, traffic is stopped from passing through the ASA.

Two ASA 5585-Xs in Fail-Open Mode

- If the ASAs are configured in fail-open mode and if the ASA 5585-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is still passed through the active ASA without being inspected. Failover is not triggered.
- If the ASAs are configured in fail-open mode, and if the ASA 5585-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5585-X IPS SSP that was previously the standby ASA 5585-X IPS SSP.

Two ASA 5585-Xs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the ASA 5585-X IPS SSP on the active ASA experiences a configuration change or a signature/signature engine update, traffic is stopped from passing through the active ASA. No failover is triggered.
- If the ASAs are configured in fail-close mode, and if the ASA 5585-X IPS SSP on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the ASA 5585-X IPS SSP that was previously the standby for the ASA 5585-X IPS SSP.

Configuration Examples

Use the following configuration for the primary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Use the following configuration for the secondary ASA:

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

Traffic Flow Stopped on IPS Switchports

Problem Traffic on any port located on the ASA 5585-X IPS SSP (1/x) no longer passes through the adaptive security appliance when the ASA 5585-X IPS SSP is reset or shut down. This affects all traffic through these ports regardless of whether or not the traffic would have been monitored by the IPS. The link on the ports will link down when the ASA 5585-X IPS SSP is reset or shut down.

Possible Cause Using the ports located on the ASA 5585-X IPS SSP (1/x), and resetting or shutting it down via any mechanism.

Solution Use the ports on the adaptive security appliance (0/x) instead because those ports do not lose their link when the ASA 5585-X IPS SSP is reset or shut down.

Health and Status Information

To see the general health of the ASA 5585-X IPS SSP, use the **show module 1 details** command.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.2.(1)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa
```

The output shows that the ASA 5585-X IPS SSP is up. If the status reads `Down`, you can reset it 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# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2.(1)E4
Data plane Status:  Not Applicable
Status:             Shutting Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2.(1)E4
Data plane Status:  Not Applicable
Status:             Down
asa# show module 1 details
Getting details from the Service Module, please wait...
Unable to read details from slot 1
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Not Applicable
App. Status Desc:   Not Applicable
App. version:       7.2.(1)E4
Data plane Status:  Not Applicable
Status:             Init
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
```

```
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Reload
App. Status Desc:   Starting up
App. version:       7.2.(1)E4
Data plane Status:  Down
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-20 with 8GE
Model:              ASA5585-SSP-IPS20
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(7)0
Software version:   7.2.(1)E4
MAC Address Range:  5475.d029.7f9c to 5475.d029.7fa7
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.2.(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.3
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
Mgmt Access List:   0.0.0.0/0
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

If you have problems with reimaging the ASA 5585-X IPS SSP, use the **debug module-boot** command to see the output as it 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 reimage the module.

```
ips-ssp# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.10.10.10//IPS-SSP_20-K9-sys-1.1-a-7.2.-1-E4.img
Port IP Address [0.0.0.0]: 10.10.10.11
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.10.10.254

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 2010
Slot-1 141> Platform ASA5585-SSP-IPS20
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=192.0.2.3
Slot-1 147>   SERVER=192.0.2.15
Slot-1 148>   GATEWAY=192.0.2.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSP-K9-sys-1.1-a-7.2.-1.1.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-SSP_10-K9-sys-1.1-a-7.2.-0.1.img@192.0.2.15 via 192.0.2.254
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 2010
Slot-1 161> Platform ASA5585-SSP-IPS20
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=192.0.2.3
Slot-1 167>   SERVER=192.0.2.15
Slot-1 168>   GATEWAY=192.0.2.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSP_10-K9-sys-1.1-a-7.2.-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-SSP_10-K9-sys-1.1-a-7.2.-0.1.img@192.0.2.15 via 192.0.2.254
```

The ASA 5585-X IPS SSP and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the ASA 5585-X IPS SSP, because the ASA itself handles the normalization. Packets on the ASA IPS modules go through a special path in the Normalizer that only reassembles fragments and puts packets in the right order for the TCP stream. The Normalizer does not do any of the normalization that is done on an inline IPS appliance, because that causes problems in the way the ASA handles the packets.

The following Normalizer engine signatures are not supported:

- 1300.0
- 1304.0
- 1305.0
- 1307.0
- 1308.0
- 1309.0
- 1311.0
- 1315.0
- 1316.0
- 1317.0
- 1330.0

- 1330.1
- 1330.2
- 1330.9
- 1330.10
- 1330.12
- 1330.14
- 1330.15
- 1330.16
- 1330.17
- 1330.18

The ASA 5585-X IPS SSP and Jumbo Packets

The jumbo packet count in the **show interface** command output from the lines `Total Jumbo Packets Received` and `Total Jumbo Packets Transmitted` for ASA IPS modules may be larger than expected due to some packets that were almost jumbo size on the wire being counted as jumbo size by the IPS. This miscount is a result of header bytes added to the packet by the ASA before the packet is transmitted to the IPS. For IPv4, 58 bytes of header data are added. For IPv6, 78 bytes of header data are added. The ASA removes the added IPS header before the packet leaves the ASA.

Reloading IPS Messages

The following messages generated during some IPS signature and global correlation updates for IPS 7.1 and later on the ASA 5585-X IPS SSP can cause confusion since the IPS is not reloading:

```
ASA5585-SSP-IPS20 Module in slot 1, application up "IPS", version "7.1(1)E4" Normal
Operation
ASA5585-SSP-IPS20 Module in slot 1, application reloading "IPS", version "7.1(1)E4" Config
Change
```

These messages are generated during some, but not all, of the global correlation updates that are attempted every five minutes. This is expected behavior. There is a global correlation check every five minutes, but there may not be an update available, thus the message appears every hour or so. When a global correlation update actually takes place, a message is sent from the IPS to the ASA indicating that a configuration change is taking place.

Gathering Information

This section describes how to gather troubleshooting information about your sensor, and contains the following topics:

- Understanding Information Gathering, page C-76
- Health and Network Security Information, page C-76
- Tech Support Information, page C-77
- Version Information, page C-80

- Statistics Information, page C-83
- Interfaces Information, page C-95
- Events Information, page C-97
- cidDump Script, page C-101
- Uploading and Accessing Files on the Cisco FTP Site, page C-101

Understanding Information Gathering

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 information of the sensor, or you can use the other individual commands listed in this section for specific information.

Health and Network Security Information

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

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

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

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

Step 1 Log in to the CLI.

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

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

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

Tech Support Information

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

- Understanding the show tech-support Command, page C-77
- Displaying Tech Support Information, page C-77
- Tech Support Command Output, page C-78

Understanding the show tech-support Command

Note The /var/log/messages file is now persistent across reboots and the information is displayed in the output of the **show tech-support** command.

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.

To get the same information from IME, choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information > System Information**.

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

For More Information

For the procedure for copying the output to a remote system, see Displaying Tech Support Information, page C-77.

Displaying Tech Support Information

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

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

The following parameters are optional:

- **page**—Displays the output, one page of information at a time. Press **Enter** to display the next line of output or use the spacebar to display the next page of information.
- **destination-url**—Indicates the information should be formatted as HTML and sent to the destination that follows this command. If you use this keyword, the output is not displayed on the screen.
- *destination_url*—Indicates the information should be formatted as HTML.The URL specifies where the information should be sent. If you do not use this keyword, the information is displayed on the screen.

- You can specify the following destination types:
  - **ftp:**—Destination URL for FTP network server. The syntax for this prefix is:
    `ftp://[[username@location]/relativeDirectory]/filename` or
    `ftp://[[username@location]//absoluteDirectory]/filename`
  - **scp:**—Destination URL for the SCP network server. The syntax for this prefix is:
    `scp://[[username@]location]/relativeDirectory]/filename` or
    `scp://[[username@]location]//absoluteDirectory]/filename`

Varlog Files

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

Displaying Tech Support Information

To display tech support information, follow these steps:

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

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

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

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

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

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

Example

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

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

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

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, authentication, and the Analysis Engine.

```
sensor# show tech-support page
System Status Report
This Report was generated on Mon Apr 22 18:31:33 2013.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4
```

```
Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S697.0            2013-02-15
OS Version:             2.6.29.1
Platform:               IPS4360
Serial Number:          FCH1504V0CF
Licensed, expires:      18-Sep-2013 UTC
Sensor up-time is 9:46.
Using 14389M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 87.3M out of 376.1M bytes of available disk space (24% usage)
boot is using 61.2M out of 70.1M bytes of available disk space (92% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


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

Upgrade History:

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

Recovery Partition Version 1.1 - 7.2(1)E4

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


Output from show interfaces
Interface Statistics
   Total Packets Received = 92475
   Total Bytes Received = 8216738
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
   Interface function = Sensing interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Inline Mode = Paired with interface GigabitEthernet0/1
   Pair Status = Up
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Up
   Admin Enabled Status = Enabled
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Missed Packet Percentage = 0
   Total Packets Received = 90664
   Total Bytes Received = 7789276
   Total Multicast Packets Received = 70475
   Total Broadcast Packets Received = 2190
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 1301
   Total Bytes Transmitted = 298432
   Total Multicast Packets Transmitted = 1258
   Total Broadcast Packets Transmitted = 16
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description =
--MORE--
```

Version Information

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

- Understanding the show version Command, page C-80
- Displaying Version Information, page C-80

Understanding the show version Command

The **show version** command shows the basic sensor information 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 To get the same information from IME, choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information > Diagnostics Report**.

Displaying Version Information

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

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

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

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View version information.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.2(1)E4

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


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

Upgrade History:

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

Recovery Partition Version 1.1 - 7.2(1)E4

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

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

Step 3 View configuration information.

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

```
sensor# more current-config
! ------------------------------
! Current configuration last modified Fri Apr 19 19:01:05 2013
! ------------------------------
! Version 7.2(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S697.0   2013-02-15
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
inline-interfaces pair0
interface1 GigabitEthernet0/0
interface2 GigabitEthernet0/1
exit
bypass-mode auto
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.106.133.159/23,10.106.132.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
websession-inactivity-timeout 3600
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
```

```
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service aaa
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
logical-interface pair0
exit
exitsensor#
```

Statistics Information

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

- Understanding the show statistics Command, page C-83
- Displaying Statistics, page C-84

Understanding the show statistics Command

The **show statistics** command provides a snapshot of the state of the sensor 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 To get the same information from IME, choose **Configuration >** ***sensor_name*** **> Sensor Monitoring > Support Information >Statistics**.

Displaying Statistics

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

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

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

For the IPS 4510 and IPS 4520, at the end of the command output, there are extra details for the Ethernet controller statistics, such as the total number of packets received at the Ethernet controller, the total number of packets dropped at the Ethernet controller under high load conditions, and the total packets transmitted including the customer traffic packets and the internal keepalive packet count.

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

To display statistics for the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the statistics for the Analysis Engine.

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

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

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

GlobalCorrelationStats
   SwVersion = 7.1(4.70)E4
   SigVersion = 645.0
   DatabaseRecordCount = 0
   DatabaseVersion = 0
   RuleVersion = 0
   ReputationFilterVersion = 0
   AlertsWithHit = 0
   AlertsWithMiss = 0
   AlertsWithModifiedRiskRating = 0
   AlertsWithGlobalCorrelationDenyAttacker = 0
   AlertsWithGlobalCorrelationDenyPacket = 0
   AlertsWithGlobalCorrelationOtherAction = 0
   AlertsWithAuditRepDenies = 0
   ReputationForcedAlerts = 0
   EventStoreInsertTotal = 0
   EventStoreInsertWithHit = 0
   EventStoreInsertWithMiss = 0
   EventStoreDenyFromGlobalCorrelation = 0
   EventStoreDenyFromOverride = 0
   EventStoreDenyFromOverlap = 0
   EventStoreDenyFromOther = 0
   ReputationFilterDataSize = 0
   ReputationFilterPacketsInput = 0
   ReputationFilterRuleMatch = 0
```

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

Step 3 Display the statistics for anomaly detection.

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor#
```

Step 4 Display the statistics for authentication.

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

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

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


   Denied Attackers with percent denied and hit count for each.


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


   Denied Attackers with percent denied and hit count for each.


sensor#
```

Step 6 Display the statistics for the Event Server.

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

Step 7 Display the statistics for the Event Store.

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

Step 8 Display the statistics for global correlation.

```
sensor# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
sensor#
```

Step 9 Display the statistics for the host.

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

Step 10 Display the statistics for the logging application.

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
```

```
sensor#
```

Step 11 Display the statistics for the ARC.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.4
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.5
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 192.0.2.6
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 192.0.2.1
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 192.0.2.3
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 192.0.2.7
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 102.0.2.8
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 192.0.2.9
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 192.0.2.10
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 203.0.113.1
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.2
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 203.0.113.9
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

Step 12 Display the statistics for the notification application.

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

Step 13 Display the statistics for OS identification.

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

Step 14 Display the statistics for the SDEE server.

```
sensor# show statistics sdee-server
General
```

```
   Open Subscriptions = 1
   Blocked Subscriptions = 1
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
   sub-4-d074914f
      State = Read Pending
      Last Read Time = 23:54:16 UTC Wed Nov 30 2011
      Last Read Time (nanoseconds) = 1322697256078549000
sensor#
```

Step 15 Display the statistics for the transaction server.

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

Step 16 Display the statistics for a virtual sensor.

```
sensor# show statistics virtual-sensor vs0
Statistics for Virtual Sensor vs0
      Name of current Signature-Defintion instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1151770
         MemoryAlloPercent = 23
         MemoryUsedPercent = 22
         MemoryMaxCapacity = 3500000
         MemoryMaxHighUsed = 4193330
         MemoryCurrentAllo = 805452
         MemoryCurrentUsed = 789047
         Processing Load Percentage = 1
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total IPv4 packets processed since reset = 0
         Total IPv6 packets processed since reset = 0
         Total IPv6 AH packets processed since reset = 0
         Total IPv6 ESP packets processed since reset = 0
         Total IPv6 Fragment packets processed since reset = 0
         Total IPv6 Routing Header packets processed since reset = 0
         Total IPv6 ICMP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset = 0
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total GRE Packets processed since reset = 0
         Total GRE Fragment Packets processed since reset = 0
         Total GRE Packets skipped since reset = 0
         Total GRE Packets with Bad Header skipped since reset = 0
         Total IpIp Packets with Bad Header skipped since reset = 0
         Total Encapsulated Tunnel Packets with Bad Header skipped since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total cross queue TCP packets processed since reset = 0
         Total cross queue UDP packets processed since reset = 0
         Packets dropped due to regex resources unavailable since reset = 0
         Total number of bytes processed since reset = 0
```

```
   The rate of packets per second since reset = 0
   The rate of bytes per second since reset = 0
   The average bytes per packet since reset = 0
Denied Address Information
   Number of Active Denied Attackers = 0
   Number of Denied Attackers Inserted = 0
   Number of Denied Attacker Victim Pairs Inserted = 0
   Number of Denied Attacker Service Pairs Inserted = 0
   Number of Denied Attackers Total Hits = 0
   Number of times max-denied-attackers limited creation of new entry = 0
   Number of exec Clear commands during uptime = 0
Denied Attackers and hit count for each.
Denied Attackers with percent denied and hit count for each.


The Signature Database Statistics.
   The Number of each type of node active in the system
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The number of each type of node inserted since reset
      Total nodes inserted = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The rate of nodes per second for each time since reset
      Nodes per second = 0
      TCP nodes keyed on both IP addresses and both ports per second = 0
      UDP nodes keyed on both IP addresses and both ports per second = 0
      IP nodes keyed on both IP addresses per second = 0
   The number of root nodes forced to expire because of memory constraints
      TCP nodes keyed on both IP addresses and both ports = 0
   Packets dropped because they would exceed Database insertion rate limits = 0
Fragment Reassembly Unit Statistics for this Virtual Sensor
   Number of fragments currently in FRU = 0
   Number of datagrams currently in FRU = 0
   Number of fragments received since reset = 0
   Number of fragments forwarded since reset = 0
   Number of fragments dropped since last reset = 0
   Number of fragments modified since last reset = 0
   Number of complete datagrams reassembled since last reset = 0
   Fragments hitting too many fragments condition since last reset = 0
   Number of overlapping fragments since last reset = 0
   Number of Datagrams too big since last reset = 0
   Number of overwriting fragments since last reset = 0
   Number of Inital fragment missing since last reset = 0
   Fragments hitting the max partial dgrams limit since last reset = 0
   Fragments too small since last reset = 0
   Too many fragments per dgram limit since last reset = 0
   Number of datagram reassembly timeout since last reset = 0
   Too many fragments claiming to be the last since last reset = 0
   Fragments with bad fragment flags since last reset = 0
TCP Normalizer stage statistics
   Packets Input = 0
   Packets Modified = 0
   Dropped packets from queue = 0
   Dropped packets due to deny-connection = 0
   Duplicate Packets = 0
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
```

```
         Current Streams Denied = 0
         Total SendAck Limited Packets = 0
         Total SendAck Limited Streams = 0
         Total SendAck Packets Sent = 0
      Statistics for the TCP Stream Reassembly Unit
         Current Statistics for the TCP Stream Reassembly Unit
            TCP streams currently in the embryonic state = 0
            TCP streams currently in the established state = 0
            TCP streams currently in the closing state = 0
            TCP streams currently in the system = 0
            TCP Packets currently queued for reassembly = 0
         Cumulative Statistics for the TCP Stream Reassembly Unit since reset
            TCP streams that have been tracked since last reset = 0
            TCP streams that had a gap in the sequence jumped = 0
            TCP streams that was abandoned due to a gap in the sequence = 0
            TCP packets that arrived out of sequence order for their stream = 0
            TCP packets that arrived out of state order for their stream = 0
            The rate of TCP connections tracked per second since reset = 0
      SigEvent Preliminary Stage Statistics
         Number of Alerts received = 0
         Number of Alerts Consumed by AlertInterval = 0
         Number of Alerts Consumed by Event Count = 0
         Number of FireOnce First Alerts = 0
         Number of FireOnce Intermediate Alerts = 0
         Number of Summary First Alerts  = 0
         Number of Summary Intermediate Alerts  = 0
         Number of Regular Summary Final Alerts  = 0
         Number of Global Summary Final Alerts  = 0
         Number of Active SigEventDataNodes  = 0
         Number of Alerts Output for further processing = 0
--MORE--
```

Step 17 Display the statistics for the web server.

```
sensor# show statistics web-server
listener-443
   session-11
      remote host = 64.101.182.167
      session is persistent = no
      number of requests serviced on current connection = 1
      last status code = 200
      last request method = GET
      last request URI = cgi-bin/sdee-server
      last protocol version = HTTP/1.1
      session state = processingGetServlet
   number of server session requests handled = 957134
   number of server session requests rejected = 0
   total HTTP requests handled = 365871
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 12
   number of busy allocated session objects = 1
summarized log messages
   number of TCP socket failure messages logged = 0
   number of TLS socket failure messages logged = 0
   number of TLS protocol failure messages logged = 0
   number of TLS connection failure messages logged = 595015
   number of TLS crypto warning messages logged = 0
   number of TLS expired certificate warning messages logged = 0
   number of receipt of TLS fatal alert message messages logged = 594969
crypto library version = 6.2.1.0
sensor#
```

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

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

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

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

Interfaces Information

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

- Understanding the show interfaces Command, page C-95
- Interfaces Command Output, page C-96

Understanding the show interfaces Command

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

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

- Sensor Events, page C-97
- Understanding the show events Command, page C-97
- Displaying Events, page C-97
- Clearing Events, page C-100

Sensor Events

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

Understanding the show events Command

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

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

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

Use the **show events** [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] command to display events from Event Store. Events are displayed beginning at the start time. If you do not specify a start time, events are displayed beginning at the current time. If you do not specify an event type, all events are displayed.

The following options apply:

- **alert**—Displays alerts. Provides notification of some suspicious activity that may indicate an attack is in process or has been attempted. Alert events are generated by the Analysis Engine whenever a signature is triggered by network activity. If no level is selected (informational, low, medium, or high), all alert events are displayed.
- **include-traits**—Displays alerts that have the specified traits.
- **exclude-traits**—Does not display alerts that have the specified traits.
- **traits**—Specifies the trait bit position in decimal (0 to 15).
- **min-threat-rating**—Displays events with a threat rating above or equal to this value. The default is 0. The valid range is 0 to 100.
- **max-threat-rating**—Displays events with a threat rating below or equal to this value. The default is 100. The valid range is 0 to 100.
- **error**—Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
- **NAC**—Displays the ARC (block) requests.

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

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

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

Displaying Events

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

Step 1 Log in to the CLI.

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

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

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

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

```
sensor# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

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

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

Step 5 Display alerts from the past 45 seconds.

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

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

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

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

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


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

Clearing Events

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

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

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

Step 2 Clear the Event Store.

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

Step 3 Enter `yes` to clear the events.

cidDump Script

If you do not have access to the IDM, the IME, 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 path of the cidDump file 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 More Information

For the procedure for putting a file on the Cisco FTP site, see Uploading and Accessing Files on the Cisco FTP Site, page C-101.

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.