APPENDIX A

Troubleshooting

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

Bug Toolkit

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

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

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

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

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

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

Preventive Maintenance

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

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 A-3.
- 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 A-3.
- For more information about the service account, see Creating the Service Account, page A-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.

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

The current configuration is saved in a backup file.

Step 3 Display the backup configuration file.

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

The backup configuration file is displayed.

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

- To merge the backup configuration into the current configuration:

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

- To 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.

Options

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

- 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 If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must also 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

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

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

Note HTTP and HTTPS prompt for a password if a username is required to access the website. If you use HTTPS protocol, 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 12-2.

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.

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.

Note 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 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.

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

A valid username contains 1 to 64 alphanumeric characters. You can also use an underscore (_) or dash (-) in the username.

Step 4 Specify a password when prompted.

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 the following 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

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

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

- If you are using the CLI, 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 A-3.
- For the procedure for obtaining a list of the current users on the sensor, for the CLI refer to Showing User Status, for IDM refer to Configuring Users, and for IME refer to Configuring Users.
- For the procedures for reimaging a sensor, see Chapter 12, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for using the **setup** command to initialize the sensor, see Chapter 9, "Initializing the Sensor."
- For more information on obtaining IPS software and how to install it, see Obtaining Cisco IPS Software, page 11-1.
- 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 A-3.
- For the procedure for adding hosts to the SSH known hosts list, for the CLI refer to Adding Hosts to the SSH Known Hosts List, for IDM refer to Defining Known Host Keys, and for IME refer to Defining Known Host Keys.
- For the procedure for adding users, for the CLI refer to Adding and Removing Users, for IDM refer to Configuring Users, and for IME refer to Configuring Users.

Recovering the Password

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

Understanding Password Recovery

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

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

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

Table A-1 Password Recovery Methods According to Platform

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

Password Recovery for Appliances

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

- Using ROMMON, page A-9

Using the GRUB Menu

For 4200 series appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.

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

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance.

The following menu appears:

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

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

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **2: Cisco IPS Clear Password (cisco)**.

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

Using ROMMON

For IPS-4240 and IPS-4255 you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

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

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection).

The boot code either pauses for 10 seconds or displays something similar to one of the following:

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

Step 3 Enter the following commands to reset the password:

```
confreg 0x7
```

```
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Password Recovery for AIM-IPS

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

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

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

Step 4 Session in to AIM-IPS.

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

Example

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

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

Step 6 Reset AIM-IPS from the router console.

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

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

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

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

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

Password Recovery for AIP-SSM

You can reset the password to the default (**cisco**) for the AIP-SSM 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 7.2.2 or later.

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.
```

Resetting the Password Using the CLI

To reset the password on the AIP-SSM, follow these steps:

Step 1 Log into the adaptive security appliance and enter the following command to verify the module slot number:

```
asa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5510 Adaptive Security Appliance         ASA5510            JMX1135L097
  1 ASA 5500 Series Security Services Module-40  ASA-SSM-40         JAF1214AMRL

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 001b.d5e8.e0c8 to 001b.d5e8.e0cc  2.0          1.0(11)2     8.4(3)
  1 001e.f737.205f to 001e.f737.205f  1.0          1.0(14)5     7.0(7)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.0(7)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

Step 2 Reset the password for module 1.

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

Step 3 Press **Enter** to confirm.

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

Step 4 Verify the status of the module. Once the status reads Up, you can session to the AIP-SSM.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5500 Series Security Services Module-40  ASA-SSM-40         JAF1214AMRL

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 001e.f737.205f to 001e.f737.205f  1.0          1.0(14)5     7.0(7)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.0(7)E4

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

Step 5 Session to the AIP-SSM.

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

Step 6 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 7 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.
aip_ssm#
```

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.

Password Recovery for IDSM-2

To recover the password for the IDSM-2, you must install a special password recovery image file. This installation only resets the password, all other configuration remains intact. The password recovery image is version-dependent and can be found on the Cisco Download Software site. For IPS 6.*x*, download WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz. For IPS 7.*x*, download WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz.

FTP is the only supported protocol for image installations, so make sure you put the password recovery image file on an FTP server that is accessible to the switch. You must have administrative access to the Cisco 6500 series switch to recover the password on the IDSM-2.

During the password recovery image installation, the following message appears:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

This message is in error. Installing the password recovery image does not remove any configuration, it only resets the login account.

Once you have downloaded the password recovery image file, follow the instructions to install the system image file but substitute the password recovery image file for the system image file. The IDSM-2 should reboot in to the primary partition after installing the recovery image file. If it does not, enter the following command from the switch:

```
hw-module module module_number reset hdd:1
```

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

For More Information

- For the procedure for installing system images on the IDSM-2, see Installing the IDSM-2 System Image, page 12-26.
- For more information on downloading Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

Password Recovery for NME-IPS

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

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

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

Step 4 Session in to NME-IPS.

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

Example

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

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

Step 6 Reset NME-IPS from the router console.

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

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

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

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

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

Disabling Password Recovery

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

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

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 IDM or IME

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

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

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

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

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled. To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

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

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

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

Troubleshooting Password Recovery

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

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If you attempt password recovery, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as the AIM-IPS and NME-IPS bootloader, ROMMON, and the maintenance partition for IDSM-2, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.
- When performing password recovery on IDSM-2, you see the following message: `Upgrading will wipe out the contents on the storage media`. You can ignore this message. Only the password is reset when you use the specified password recovery image.

Time and the Sensor

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

Time Sources and the Sensor

The sensor requires a reliable time source. All events (alerts) must have the correct UTC and local time stamp, otherwise, you cannot correctly analyze the logs after an attack. When you initialize the sensor, you set up the time zones and summertime settings.

Note We recommend that you use an NTP server. 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.

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

- For appliances
  - Use the **clock set** command to set the time. This is the default.
  - Use NTP—You can configure the appliance to get its time from an NTP time synchronization source.

- For IDSM-2
  - The IDSM-2 can automatically synchronize its clock with the switch time. This is the default. The UTC time is synchronized between the switch and the IDSM-2. The time zone and summertime settings are not synchronized between the switch and the IDSM-2.

    Note Be sure to set the time zone and summertime settings on both the switch and IDSM-2 to ensure that the UTC time settings are correct. The local time of IDSM-2 could be incorrect if the time zone and/or summertime settings do not match between IDSM-2 and the switch.

  - Use NTP—You can configure IDSM-2 to get its time from an NTP time synchronization source.
- For AIM-IPS and NME-IPS
  - AIM-IPS and NME-IPS can automatically synchronize their clock with the clock in the router chassis in which they are installed (parent router). This is the default. The UTC time is synchronized between the parent router and AIM-IPS and NME-IPS. The time zone and summertime settings are not synchronized between the parent router and AIM-IPS and NME-IPS.

    Note Be sure to set the time zone and summertime settings on both the parent router and AIM-IPS and NME-IPS to ensure that the UTC time settings are correct. The local time of AIM-IPS and NME-IPS could be incorrect if the time zone and/or summertime settings do not match between AIM-IPS and NME-IPS and the router.

  - Use NTP—You can configure AIM-IPS and NME-IPS to get their time from an NTP time synchronization source, such as a Cisco router, other than the parent router.
- For AIP-SSM
  - AIP-SSM can automatically synchronize its clock with the clock in the adaptive security appliance in which it is installed. This is the default. The UTC time is synchronized between the adaptive security appliance and AIP-SSM. The time zone and summertime settings are not synchronized between the adaptive security appliance and AIP-SSM.

    Note Be sure to set the time zone and summertime settings on both the adaptive security appliance and AIP-SSM to ensure that the UTC time settings are correct. The local time of AIP-SSM could be incorrect if the time zone and/or summertime settings do not match between AIP-SSM and the adaptive security appliance.

  - Use NTP—You can configure AIP-SSM to get its time from an NTP time synchronization source, such as a Cisco router other than the parent router.

For More Information

For the procedure for configuring NTP, for the CLI refer to Configuring NTP, for IDM refer to Configuring NTP, and for IME refer to Configuring NTP.

Synchronizing IPS Module Clocks with Parent Device Clocks

All IPS modules (AIM-IPS, AIP-SSM, IDSM-2, and NME-IPS) synchronize their system clocks to the parent chassis clock (switch, router, or security appliance) each time the module boots up and any time the parent chassis clock is set. The module clock and parent chassis clock tend to drift apart over time. The difference can be as much as several seconds per day. To avoid this problem, make sure that both the module clock and the parent clock are synchronized to an external NTP server. If only the module clock or only the parent chassis clock is synchronized to an NTP server, the time drift occurs.

Verifying the Sensor is Synchronized with the NTP Server

In IPS 6.1, you cannot apply an incorrect NTP configuration, such as an invalid NTP key value or ID, to the sensor. If you try to apply an incorrect configuration, you receive an error message. To verify the NTP configuration, use the **show statistics host** command to gather sensor statistics. The NTP statistics section provides NTP statistics including feedback on sensor synchronization with the NTP server.

To verify the NTP configuration, follow these steps:

Step 1 Log in to the sensor.

Step 2 Generate the host statistics.

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

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

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

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

Correcting Time on the Sensor

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

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

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

To ensure the integrity of the time stamp on the event records, you must clear the event archive of the older events by using the **clear events** command.

Note You cannot remove individual events.

For More Information

For the procedure for clearing events, see Clearing Events, page A-94.

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:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS 4270-20
- AIP-SSM

IDSM-2 supports virtualization with the exception of VLAN groups on inline interface pairs. AIM-IPS and NME-IPS do not support virtualization.

Supported MIBs

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
- 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 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, refer to Worms.

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

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 POSFP 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, refer to Configuring External Product Interfaces.
- For more information on working with OS maps, for the CLI refer to Adding, Editing, Deleting, and Moving Configured OS Maps, for IDM refer to Adding, Editing, Deleting, and Moving Configured OS Maps, and for IME refer to Adding, Editing, Deleting, and Moving Configured OS Maps.
- For more information on working with OS identifications, for the CLI refer to Displaying and Clearing OS Identifications, for IDM refer to OS Identifications, and for IME refer to OS Identifications.
- For the procedure for adding trusted hosts, for the CLI refer to Adding TLS Trusted Hosts, for IDM refer to Adding Trusted Hosts, and for IME refer to Adding Trusted Hosts.

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 **Monitoring > Sensor Monitoring > Support Information > Statistics** in IDM and check the Interface state line in the response, or choose **Configuration > *sensor_name* > Sensor Monitoring > Support Information > Statistics** in 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 CSA MC using the browser.
- Check Event Store for CSA MC subscription errors.

For More Information

- For the procedure for adding trusted hosts:
  - For the CLI, refer to Adding TLS Trusted Hosts
  - For IDM, refer to Adding Trusted Hosts
  - For IME, refer to Adding Trusted Hosts
- For the procedure for displaying events, see Displaying Events, page A-91.

Troubleshooting the 4200 Series Appliance

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

This section contains information to troubleshoot the 4200 series appliance. It contains the following topics:

Hardware Bypass Link Status Changes and Drops

Note Hardware bypass is available on the 4GE bypass interface card, which is supported on IPS 4260 and IPS 4270-20.

Properly configuring and deploying hardware bypass protects against complete link failure if the IPS appliance experiences a power loss, critical hardware failure, or is rebooted; however, a link status change still occurs when hardware bypass engages (and again when it disengages).

During engagement, the interface card disconnects both physical connections from itself and bridges them together. The interfaces of the connected devices can then negotiate the link and traffic forwarding can resume. Once the appliance is back online, hardware bypass disengages and the interface card interrupts the bypass and reconnects the links back to itself. The interface card then negotiates both links and traffic resumes.

There is no built-in way to completely avoid link status changes and drops. However, you can greatly reduce the interruption time (in some cases to sub-second times) by doing the following:

- Make sure you use CAT 5e/6-certified cabling for all connections.
- Make sure the interfaces of the connected devices are configured to match the interfaces of the appliance for speed/duplex negotiation (auto/auto).
- Enable portfast on connected switchports to reduce spanning-tree forwarding delays.

For More Information

- For more information about hardware bypass on IPS-4260, see Hardware Bypass, page 3-4.
- For more information about hardware bypass on IPS 4270-20, see Hardware Bypass, page 4-5.

Troubleshooting Loose Connections

Perform the following actions to troubleshoot loose connections on a sensor:

- 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.

Analysis Engine is Busy

After you reimage a sensor, Analysis Engine is busy rebuilding Regex tables and does not respond to new configurations. You can check whether Analysis Engine is busy by using the **show statistics virtual-sensor** command. You receive the following error message if 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 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 Analysis Engine is busy, wait a while before trying to make configuration changes. Use the **show statistics virtual-sensor** command to find out when Analysis Engine is available again.

Connecting IPS-4240 to a Cisco 7200 Series Router

When an IPS-4240 is connected directly to a 7200 series router and both the IPS-4240 and the router interfaces are hard-coded to speed 100 with duplex Full, the connection does not work. If you set IPS-4240 to speed Auto and duplex Auto, it connects to the router but only at speed 100 and duplex Half.

To connect correctly at speed 100 and duplex Full, set the interfaces of both IPS-4240 and the router to speed Auto and duplex Auto. Also, if either interface is hard-coded, you must make the connection using a crossover cable.

Communication Problems

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

Cannot Access the Sensor CLI Through Telnet or SSH

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

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.

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

```
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

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

Step 3 Make sure the sensor IP address is unique.

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

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


Current Configuration:


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

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

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.

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

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


Current Configuration:


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

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

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 procedure for enabling and disabling Telnet on the sensor, refer to Enabling and Disabling Telnet.
- For the various ways to open a CLI session directly on the sensor, see Chapter 10, "Logging In to the Sensor."
- For the procedure for changing the IP address, refer to Changing the IP Address, Netmask, and Gateway.
- For the procedure for changing the access list, see Correcting a Misconfigured Access List, page A-27.

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: 10.89.149.238/25,10.89.149.254 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.

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

```
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

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

Step 3 Make sure the 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 the chapter for your sensor in *Installing Cisco Intrusion Prevention System Appliances and Module 6.1*.
- For the procedure for making sure the IP address is correct, refer to Changing the IP Address, Netmask, and Gateway.

SensorApp and Alerting

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

SensorApp Not Running

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

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

Step 1 Log in to the CLI.

Step 2 Determine the status of the Analysis Engine service.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E1

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S329.0                  2008-04-16
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          JAB0948035P
License expired:        11-Apr-2008 UTC
Sensor up-time is 7 days.
Using 1018015744 out of 2093600768 bytes of available memory (48% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 39.7M out of 166.6M bytes of available disk space (25% usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   Running
AnalysisEngine   M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   NotRunning
CLI              M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500

Upgrade History:

  IPS-K9-6.1-1-E1   01:16:00 UTC Fri Apr 25 2008

Recovery Partition Version 1.1 - 6.1(1)E1

Host Certificate Valid from: 29-Jun-2008 to 30-Jun-2010

sensor#
```

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

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

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

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

Step 4 Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E1

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S329.0                  2008-04-16
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          JAB0948035P
License expired:        11-Apr-2008 UTC
Sensor up-time is 7 days.
Using 1018015744 out of 2093600768 bytes of available memory (48% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 39.7M out of 166.6M bytes of available disk space (25% usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   Running
AnalysisEngine   M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500   NotRunning
CLI              M-2008_APR_24_19_16   (Release)   2008-04-24T19:49:05-0500

Upgrade History:

  IPS-K9-6.1-1-E1   01:16:00 UTC Fri Apr 25 2008

Recovery Partition Version 1.1 - 6.1(1)E1

Host Certificate Valid from: 29-Jun-2008 to 30-Jun-2010

sensor#
```

If you do not have the latest software updates, download them from Cisco.com.

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

For More Information

- For more information on IPS system architecture, refer to System Architecture.
- For the procedure for obtaining the latest Cisco IPS software, see Obtaining Cisco IPS Software, page 11-1.

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:

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

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

Step 4 Verify the interface configuration:

a. Make sure you have the interfaces configured properly.

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

Refer to your switch documentation for the procedure.

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

```
sensor# show interfaces
```

For More Information

- For the procedure for properly installing the sensing interface on your sensor, refer to the chapter on your appliance in *Installing Cisco Intrusion Prevention System Appliances and Modules 6.1*.
- For the procedure for connecting SPAN and VACL capture ports on IDSM-2, refer to Configuring IDSM-2.
- For the procedures for configuring interfaces on your sensor, for the CLI refer to Configuring Interfaces, for IDM refer to Configuring Interfaces, and for IME refer to 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 be sent to the Event Store. Every time you configure a signature, the new configuration overwrites the old one, so make sure you have configured all the event actions you want for each signature.

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

a. Check the cabling.

b. Enable the interface.

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

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

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 3
```

```
Total Bytes Received = 900
Total Multicast Packets Received = 3
Total Broadcast Packets Received = 0
Total Jumbo Packets Received = 0
Total Undersize Packets Received = 0
Total Receive Errors = 0
Total Receive FIFO Overruns = 0
Total Packets Transmitted = 0
Total Bytes Transmitted = 0
Total Multicast Packets Transmitted = 0
Total Broadcast Packets Transmitted = 0
Total Jumbo Packets Transmitted = 0
Total Undersize Packets Transmitted = 0
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0 ...
```

For More Information

For information on installing the sensor properly, refer to your sensor chapter in *Installing Cisco Intrusion Prevention System Appliances and Modules 6.1*.

Cleaning Up a Corrupted SensorApp Configuration

If the SensorApp configuration has become corrupted and SensorApp cannot run, you must delete it entirely and restart SensorApp. To delete the SensorApp configuration, follow these steps:

Step 1 Log in to the service account.

Step 2 Su to root.

Step 3 Stop the IPS applications.

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

Step 4 Replace the virtual sensor file.

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

Step 5 Remove the cache files.

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

Step 6 Exit the service account.

Step 7 Log in to the sensor CLI.

Step 8 Start the IPS services.

```
sensor# cids start
```

Step 9 Log in to an account with administrator privileges.

Step 10 Reboot the sensor.

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

For More Information

For more information on IPS system architecture, refer to System Architecture.

Blocking

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

Troubleshooting Blocking

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

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

To troubleshoot ARC, follow these steps:

1. Verify that ARC is running.
2. Verify that 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 ARC is running, see Verifying ARC is Running, page A-38.
- For the procedure to verify that ARC is connecting, see Verifying ARC Connections are Active, page A-39.
- For the procedure to verify that the Event Action is set to Block Host, see Blocking Not Occurring for a Signature, page A-43.
- For the procedure to verify that the master blocking sensor is properly configured, see Verifying the Master Blocking Sensor Configuration, page A-44.
- For a discussion of ARC architecture, see Attack Response Controller.

Verifying ARC is Running

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

Step 1 Log in to the CLI.

Step 2 Verify that MainApp is running.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(1)E1.1

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S294.0                  2007-08-02
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          P300000220
No license present
Sensor up-time is 6 days.
Using 1026641920 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 38.4M out of 166.6M bytes of available disk space (24% usage)
boot is using 38.0M out of 68.5M bytes of available disk space (58% usage)


MainApp          N-2007_SEP_20_16_44   (Release)   2007-09-20T17:10:01-0500   Running
AnalysisEngine   N-2007_SEP_20_16_44   (Release)   2007-09-20T17:10:01-0500   Running
CLI              N-2007_SEP_20_16_44   (Release)   2007-09-20T17:10:01-0500


Upgrade History:

  IPS-K9-6.0-1-E1.1   16:44:00 UTC Thu Sep 20 2007

Recovery Partition Version 1.1 - 6.0(1)E1.1

sensor#
```

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

For More Information

For more information on IPS system architecture, refer to 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 ARC is connecting.

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

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

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

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

Example

```
sensor# show events error 00:00:00 Apr 01 2007 | include : nac
```

Step 4 Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(1)E1.1

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S294.0                  2007-08-02
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          P300000220
```

```
No license present
Sensor up-time is 6 days.
Using 1026641920 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 38.4M out of 166.6M bytes of available disk space (24% usage)
boot is using 38.0M out of 68.5M bytes of available disk space (58% usage)


MainApp          N-2007_SEP_20_16_44   (Release)   2007-09-20T17:10:01-0500   Running
AnalysisEngine   N-2007_SEP_20_16_44   (Release)   2007-09-20T17:10:01-0500   Running
CLI              N-2007_SEP_20_16_44   (Release)   2007-09-20T17:10:01-0500


Upgrade History:

  IPS-K9-6.0-1-E1.1   16:44:00 UTC Thu Sep 20 2007

Recovery Partition Version 1.1 - 6.0(1)E1.1

sensor#
```

Note If you do not have the latest software updates, download them from Cisco.com.

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

Step 6 Make sure the configuration settings for each device are correct (the username, password, and IP address).

Step 7 Make sure the interface and directions for each network device are correct.

Step 8 If the network device is using SSH-DES or SSH-3DES, make sure that you have enabled SSH connections to the device.

Step 9 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 11-1.
- For more information about configuring devices, see Device Access Issues, page A-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 A-42.
- For the procedure for enabling SSH, see Enabling SSH Connections to the Network Device, page A-43.

Device Access Issues

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

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

To troubleshoot device access issues, follow these steps:

Step 1 Log in to the CLI.

Step 2 Verify the IP address for the managed devices.

```
sensor# configure terminal
sensor (config)# service network-access
sensor(config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ------------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
   ------------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ------------------------------------------------
   ------------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.54
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ------------------------------------------------
            interface-name: fa0/0
            direction: in
            ------------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
```

```
   -----------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   -----------------------------------------------
   -----------------------------------------------
sensor(config-net)#
```

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

a. Log in to the service account.

b. Telnet or SSH to the network device to verify the configuration.

c. Make sure you can reach the device.

d. Verify the username and password.

Step 4 Verify that each interface 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 A-42.

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 using IDM, choose **Monitoring > Sensor Monitoring > Time-Based Actions > Host Blocks**. To perform a manual block using IME, 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-DES or SSH-3DES as the communication protocol for the network device, you must make sure you have enabled it on the device.

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

Step 1 Log in to the CLI.

Step 2 Enter configuration mode.

```
sensor# configure terminal
```

Step 3 Enable SSH.

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

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

Blocking Not Occurring for a Signature

If blocking is not occurring for a specific signature, check that the event action is set to block the host. To make sure blocking is occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter signature definition submode.

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

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

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

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
         default-signatures-only
         -----------------------------------------------
```

```
                specify-service-ports
                ---------------------------------------------
                   no
                   ---------------------------------------------
                   ---------------------------------------------
                ---------------------------------------------
                specify-tcp-max-mss
                ---------------------------------------------
                   no
                   ---------------------------------------------
                   ---------------------------------------------
                ---------------------------------------------
                specify-tcp-min-mss
                ---------------------------------------------
                   no
                   ---------------------------------------------
                   ---------------------------------------------
--MORE--
```

Step 4 Exit signature definition submode.

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

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

Verifying the Master Blocking Sensor Configuration

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

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

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

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

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

Step 3 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 4 Exit network access general submode.

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

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

Step 6 Verify that the block shows up in the ARC statistics.

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

Step 7 Log in to the 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 8 If the remote master blocking sensor is using TLS for web access, make sure the forwarding sensor is configured as a TLS host.

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

For More Information

For the procedure to configure the sensor to be a master blocking sensor, for the CLI refer to Configuring the Sensor to be a Master Blocking Sensor, for IDM refer to Configuring the Master Blocking Sensor, and for IME refer to Configuring the Master Blocking Sensor.

Logging

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

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 To enable debug logging for all zones.

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

Step 9 To turn on individual zone control.

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

Step 10 Exit master zone control.

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

Step 11 View the zone names.

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

```
      zone-name: tls
      severity: warning <defaulted>
   ------------------------------------------------
sensor(config-log)#
```

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 A-50.

Zone Names

Table A-2 lists the debug logger zone names:

Table A-2 Debug Logger Zone Names

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

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

For More Information

For more information on the IPS Logger service, refer to Logger.

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

If you do not have the event action set to reset, the TCP reset does not occur for a specific signature. To troubleshoot a reset not occurring for a specific signature, follow these steps:

Step 1 Log in to the CLI.

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

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

Step 3 Exit signature definition submode.

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

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

Step 5 Make sure the correct 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 to 6.*x*

If you try to upgrade a sensor to IPS 6.*x*, you may receive an error that Analysis Engine is not running:

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-6.1-1-E1.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 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 to 6.*x* at this time. After the upgrade to 6.*x*, add the interfaces back to the virtual sensor vs0 using the **setup** command.

Or you can use the system image file to reimage directly to IPS 6.*x*. You can reimage a 5.*x* sensor to 6.*x* because the reimage process does not check to see if 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 9, "Initializing the Sensor."
- For more information on reimaging your sensor, see Chapter 12, "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

For more information on how to interpret the IPS software filenames, see IPS Software Versioning, page 11-3.

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, refer to Creating the Service Account.
- For the procedure for reimaging your sensor, see Chapter 12, "Upgrading, Downgrading, and Installing System Images."
- For the procedure for adding hosts to the SSH known hosts list, for the CLI refer to Adding Hosts to the SSH Known Hosts List, for IDM refer to Defining Known Host Keys, and for IME refer to Defining Known Host Keys.

- For the procedure for determining the software version, see Displaying Version Information, page A-76.

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 11-1.

Troubleshooting IDM

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

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

This section contains troubleshooting procedures for IDM, and contains the following topics:

Cannot Launch IDM - Loading Java Applet Failed

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

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

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

To clear the cache, follow these steps:

Step 1 Close all browser windows.

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

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

b. Click the **Advanced** tab.

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

d. Click the **Cache** tab.

e. Click **Clear**.

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

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

b. Click the **Advanced** tab.

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

d. Click the **Cache** tab.

e. Click the **Browser** tab.

f. Deselect all browser check boxes.

g. Click **Clear Cache**.

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

Cannot Launch IDM-Analysis Engine Busy

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

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

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

IDM, Remote Manager, or Sensing Interfaces Cannot Access Sensor

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

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, refer to Enabling and Disabling Telnet.
- For the procedure for configuring the web server, refer to Changing Web Server Settings.

Signatures Not Producing Alerts

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

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.

To make sure you are getting alerts, check the statistics for the virtual sensor and Event Store.

For More Information

- For more information about event actions, refer to Event Actions.
- For the procedure for configuring event actions, for the CLI refer to Assigning Actions to Signatures, for IDM refer to Assigning Actions to Signatures, and for IME refer to Assigning Actions to Signatures.
- For the procedure for obtaining statistics about virtual sensor and Event Store, see Displaying Statistics, page A-79.

Troubleshooting IME

This section describes troubleshooting tools for IME, and contains the following sections:

Time Synchronization on IME and the Sensor

Symptom IME displays `No Data Available` on the Events dashboard. A historical query does not return any events; however, events are coming in to 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 IME, it checks for the time synchronization and warns you to correct it if is in wrong. 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 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 A-16.
- For the procedure for changing the time on the sensor, see Correcting Time on the Sensor, page A-19.

Not Supported Error Message

Symptom 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. IME needs IPS 6.1 or later to obtain certain information. 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.

Troubleshooting IDSM-2

Note IDSM-2 has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the 4200 Series Appliance, page A-23.

This section pertains specifically to troubleshooting IDSM-2, and contains the following topics:

Diagnosing IDSM-2 Problems

Use the following list to diagnose IDSM-2 problems:

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

  During physical handling of the module, the connector can come loose from the base card, and cause the daughter card and the base card to lose contact with each other. A loose ribbon cable connector causes an on-line diagnostic error on ports 7 and 8. The module cannot operate when this condition exists. For more information, refer to Partner Field Notice 29877.

- Some IDSM-2s were shipped with faulty DIMMs. For the procedure for checking IDSM-2 for faulty memory, refer to Partner Field Notice 29837.

- The hard-disk drive fails to read or write.

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

  – An inability to log in

  - I/O errors to the console when doing read/write operations (the **ls** command)
  - Commands do not execute properly (cannot find the path to the executable)

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

- SensorApp either crashes or takes 99% of the CPU when IP logging is enabled for stream-based signatures (1300 series). For the workaround, refer to CSCed32093.
- IDSM-2 appears to lock up and remote access is prohibited (SSH, Telnet, IDM, Event Server, Control Transaction Server, and IP log Server).

  This defect is related to using SWAP. IDSM-2 responds to pings. Apply the 4.1(4) service pack to resolve this issue. For more information, refer to CSCed54146.
- Shortly after you upgrade IDSM-2 or you tune a signature with VMS, IDSM-2 becomes unresponsive and often produces a SensorApp core file. Apply the 4.1(4b) patch to fix this issue.
- Confirm that IDSM-2 has the supported configurations.

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

For More Information

- For information about the Bug Toolkit and how to access it, see Bug Toolkit, page A-1.
- For a table listing the supported IDSM-2 configurations, see Minimum Supported IDSM-2 Configurations, page A-60.

Minimum Supported IDSM-2 Configurations

Note The following matrix is not intended to recommend any particular version, but rather lists the earliest supported versions.

Table A-3 lists the minimum supported configurations for IDSM-2.

Table A-3 Minimum Catalyst 6500 Software Version for IDSM-2 Feature Support

Catalyst/IDSM-2 Feature	Catalyst Software				Cisco IOS Software			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL capture[1]	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
ECLB with VACL capture[2]	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
Inline interface pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1

Table A-3 Minimum Catalyst 6500 Software Version for IDSM-2 Feature Support (continued)

Catalyst/IDSM-2 Feature	Catalyst Software				Cisco IOS Software			
ECLB with inline interface pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
Inline VLAN pairs	8.4(1)	8.4(1)	8.4(1)	8.4(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
ECLB with inline VLAN pairs	8.5(1)	8.5(1)	8.5(1)	8.5(1)	N/A	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. Requires PFC2/3 or MSFC2/3.
2. Requires PFC2/3 or MSFC2/3.

Switch Commands for Troubleshooting

The following switch commands help you troubleshoot IDSM-2:

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

Status LED Off

If the status indicator is off on IDSM-2, you need to turn power on to IDSM-2.To determine the status of IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Verify that IDSM-2 is online.

Catalyst Software.

```
console> enable

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

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

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

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

Cisco IOS software.

```
router# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2    48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3    48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5     8  Intrusion Detection System             WS-SVC-IDSM-2      SAD0751059U
  6    16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7     2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9     1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 11     8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13     8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072405D8

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

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

Mod Online Diag Status
--- -------------------
```

```
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
router#
```

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

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

```
router# set module power up module_number
```

Status LED On But IDSM-2 Does Not Come Online

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

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

To enable IDSM-2, follow these steps:

Step 1 Log in to the console.

Step 2 Make sure IDSM-2 is enabled.

```
router# show module
```

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

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

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

```
router# reset module_number
```

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

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

```
router# show test module_number
```

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

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

For More Information

For the procedure for reimaging the application partition, see Chapter 12, "Upgrading, Downgrading, and Installing System Images."

Cannot Communicate With IDSM-2 Command and Control Port

If you cannot communicate with the IDSM-2 command and control port, the command and control port may not be in the correct VLAN. To communicate with the command and control port of IDSM-2, follow these steps:

Step 1 Log in to the console.

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

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

```
router# show configuration
```

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

Catalyst software.

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

# = 802.1X Authenticated Port Name.

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


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

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

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

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

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

Cisco IOS software.

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

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
```

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


router#
```

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

For More Information

For the procedure for configuring the switch for command and control access to IDSM-2, see Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM-2.

Using the TCP Reset Interface

The IDSM2 has a TCP reset interface—port 1. The IDSM2 has a specific TCP reset interface because it cannot send TCP resets on its sensing ports.

If you have reset problems with the IDSM2, and the switch is running Catalyst software, try the following:

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

Note In Cisco IOS when the IDSM2 is in promiscuous mode, the IDSM2 ports are always dot1q trunk ports (even when monitoring only 1 VLAN), and the TCP reset port is automatically set to a trunk port and is not configurable.

For More Information

For more information, refer to Configuring IDSM-2.

Connecting a Serial Cable to IDSM-2

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

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

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

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

Step 3 Configure the terminal server port to be 19200 baud, 8 bits, no parity. You can now log directly in to IDSM-2.

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

Troubleshooting AIP-SSM

Note AIP-SSM has the same software architecture as the 4200 series sensors. You can use the same troubleshooting tools as outlined in Troubleshooting the 4200 Series Appliance, page A-23.

The following section contains information for troubleshooting AIP-SSM, and contains the following topics:

Health and Status Information

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

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

```
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

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

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

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

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

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

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

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

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

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

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
asa(config)# debug module-boot
debug module-boot  enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

```
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2005
Slot-1 141> Platform ASA-SSM-10
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2005
Slot-1 161> Platform ASA-SSM-10
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

Failover Scenarios

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

Single ASA in Fail-Open Mode

- If the ASA is configured in fail-open mode for the AIP-SSM, and the AIP-SSM 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 AIP-SSM, and the AIP-SSM 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 AIP-SSM, and the AIP-SSM 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 AIP-SSM, and the AIP-SSM 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 AIP-SSM 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 AIP-SSM on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the AIP-SSM that was previously the standby module.

Two ASAs in Fail-Close Mode

- If the ASAs are configured in fail-close mode, and if the AIP-SSM 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 AIP-SSM on the active ASA experiences a SensorApp crash or a service pack upgrade, failover is triggered and traffic passes through the module that was previously the standby for the AIP-SSM.

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
```

AIP-SSM and the Data Plane

Symptom The AIP-SSM data plane is kept in the Up state while applying signature updates. You can check the AIP-SSM data plane status by using the **show module** command during signature updates.

Possible Cause Bypass mode is set to off. The issue is seen when updating signatures, and when you use either CSM or IDM to apply signature updates. This issue is not seen when upgrading IPS system software.

AIM-IPS and the Normalizer Engine

The majority of the features in the Normalizer engine are not used on the AIP-SSM, 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

For More Information

For detailed information about the Normalizer engine, refer to Normalizer Engine.

TCP Reset Differences Between IPS Appliances and AIP-SSM

The IPS appliance sends TCP reset packets to both the attacker and victim when reset-tcp-connection is selected. The IPS appliance sends a TCP reset packet only to the victim under the following circumstances:

- When a deny-packet-inline or deny-connection-inline is selected
- When TCP-based signatures and reset-tcp-connection have NOT been selected

In the case of the AIP-SSM, the TCP reset request is sent to the ASA, and then the ASA sends the TCP reset packets. The ASA sends TCP reset packets to both the attacker and victim when the reset-tcp-connection is selected. When deny-packet-inline or deny-connection-inline is selected, the ASA sends the TCP reset packet to either the attacker or victim depending on the configuration of the signature. Signatures configured to swap the attacker and victim when reporting the alert can cause the ASA to send the TCP reset packet to the attacker.

For More Information

For detailed information about event actions, refer to Event Actions.

Troubleshooting AIM-IPS and NME-IPS

This section contains information for troubleshooting the IPS network modules, AIM-IPS and NME-IPS. It contains the following sections:

Interoperability With Other IPS Network Modules

The Cisco access routers only support one IDS/IPS module per router. If you have more than one IDS/IPS module installed, the most capable card is enabled. The most capable hierarchy is:

1. NME-IPS
2. AIM-IPS
3. NM-CIDS

This means, for example, that if all modules are installed, NME-IPS disables all other modules. AIM-IPS disables all NM-CIDS. If there are multiple modules with the same level of capability, the first one discovered is enabled and all others are disabled.

You cannot bring up, enable, or configure a disabled module. To bring up a less capable module, you must remove the more capable module from the router and reboot. Disabled modules are reported in the **show diag** command output. The state of the module is reported as present but disabled.

If the most capable module slot and port do not match the **interface ids slot/port** configuration command, the most capable module is disabled with the following warning:

```
The module in slot x will be disabled and configuration ignored.
```

The correct slot/port number are displayed so that you can change the configuration.

Caution You cannot upgrade an NM-CIDS to NME-IPS. For more information on NM-CIDS, refer to Introducing NM-CIDS and Installing NM-CIDS.

Gathering Information

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

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

Health and Network Security Information

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

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

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

Step 1 Log in to the CLI.

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

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

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

Tech Support Information

The **show tech-support** command is useful for capturing all sensor status and configuration information. This section describes the **show tech-support** command, and contains the following topics:

Understanding 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.

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 A-73.

Displaying Tech Support Information

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

The following parameters are optional:

- **page**—Displays the output, one page of information at a time.

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

To display tech support information, follow these steps:

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

Step 2 View the output on the screen.

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

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

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

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

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

You can specify the following destination types:

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

For example, to send the tech support output to the file `/absolute/reports/sensor1Report.html`:

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

The `password:` prompt appears.

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

Tech Support Command Output

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

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

```
sensor# show tech-support page

System Status Report
This Report was generated on Mon Jun 23 19:49:30 2008.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E2

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S340.0                  2008-06-19
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          P300000220
Licensed, expires:      31-Dec-2009 UTC
Sensor up-time is 25 days.
Using 1052807168 out of 2093600768 bytes of available memory (50% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 41.1M out of 166.6M bytes of available disk space (26%
 usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          M-2008_APR_24_19_16    (Release)   2008-04-24T19:49:05-0500   Running
```

```
AnalysisEngine   ME-2008_JUN_05_18_26   (Release)   2008-06-05T18:55:02-0500   Running
CLI              M-2008_APR_24_19_16    (Release)   2008-04-24T19:49:05-0500


Upgrade History:

* IPS-engine-E2-req-6.1-1   20:39:12 UTC Fri Jun 20 2008
  IPS-sig-S340-req-E2.pkg   20:42:45 UTC Fri Jun 20 2008

Recovery Partition Version 1.1 - 6.1(1)E1

Host Certificate Valid from: 28-May-2008 to 29-May-2010


Output from show interfaces
Interface Statistics
   Total Packets Received = 7561053
   Total Bytes Received = 620005608
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
   Interface function = Command-control interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 7115688
   Total Bytes Received = 807518285
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 4988611
   Total Bytes Transmitted = 1004944745
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/1
   Interface function = Sensing interface
   Description =
   Media Type = backplane
   Default Vlan = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   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 = 7561056
   Total Bytes Received = 620005854
   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 = 7561056
   Total Bytes Transmitted = 620006592
   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

Output from show statistics authentication
General
   totalAuthenticationAttempts = 1105
   failedAuthenticationAttempts = 5

Output from show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 256036
--MORE--
```

Version Information

The **show version** command is useful for obtaining sensor information. This section describes the **show version** command, and contains the following topics:

- Understanding the show version Command, page A-76
- Displaying Version Information, page A-76

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 IDM, choose **Monitoring > Sensor Monitoring > Support Information > Diagnostics Report.** 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.

To display the version and configuration, follow these steps:

Step 1 Log in to the CLI.

Step 2 View version information.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E1
```

```
Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S323.0                  2008-03-24
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS-4240-K9
Serial Number:          P3000000652
No license present
Sensor up-time is 4 days.
Using 1421475840 out of 1984548864 bytes of available memory (71% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 41.0M out of 166.8M bytes of available disk space (26%
 usage)
boot is using 40.4M out of 68.6M bytes of available disk space (62% usage)


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


Upgrade History:

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

Recovery Partition Version 1.1 - 6.1(1)E1

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

sensor#
```

Note If the –-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 Thu Apr 24 16:21:25 2008
! ------------------------------
! Version 6.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S323.0   2008-03-24
!     Virus Update        V1.2     2005-11-24
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
```

```
service host
network-settings
host-ip 10.89.147.45/25,10.89.147.126
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

Statistics Information

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

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

Displaying Statistics

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

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

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

To display statistics for the sensor, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display the statistics for Analysis Engine.

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1421127
   Measure of the level of current resource utilization = 0
```

```
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 0
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 0
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 0
sensor#
```

Step 3 Display the statistics for anomaly detection.

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

```
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor-4240#
```

Step 4 Display the statistics for authentication.

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

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

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


   Denied Attackers with percent denied and hit count for each.


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


   Denied Attackers with percent denied and hit count for each.


sensor#
```

Step 6 Display the statistics for Event Server.

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

Step 7 Display the statistics for Event Store.

```
sensor# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
```

```
sensor#
```

Step 8 Display the statistics for the host.

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

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
sensor#
```

Step 9 Display the statistics for the logging application.

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

Step 10 Display the statistics for ARC.

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 10.89.150.138
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 10.89.150.171
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 10.89.150.219
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
```

```
   NetDevice
      IP = 10.89.150.250
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

Step 11 Display the statistics for the notification application.

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

Step 12 Display the statistics for the SDEE server.

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

Step 13 Display the statistics for the transaction server.

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

```
   failedControlTransactions = 0
sensor#
```

Step 14 Display the statistics for a virtual sensor.

```
sensor# show statistics virtual-sensor vs0
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1421711
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset =
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 0
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 0
         The average bytes per packet since reset = 0
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 0
         Number of Denied Attacker Victim Pairs Inserted = 0
         Number of Denied Attacker Service Pairs Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 0
      Denied Attackers and hit count for each.
      Denied Attackers with percent denied and hit count for each.


      The Signature Database Statistics.
         The Number of each type of node active in the system (can not be reset
            Total nodes active = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The number of each type of node inserted since reset
            Total nodes inserted = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The rate of nodes per second for each time since reset
            Nodes per second = 0
            TCP nodes keyed on both IP addresses and both ports per second = 0
            UDP nodes keyed on both IP addresses and both ports per second = 0
            IP nodes keyed on both IP addresses per second = 0
         The number of root nodes forced to expire because of memory constraint
            TCP nodes keyed on both IP addresses and both ports = 0
         Packets dropped because they would exceed Database insertion rate 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 Initial fragment missing since last reset = 0
      Fragments hitting the max partial dgrams limit since last reset = 0
      Fragments too small since last reset = 0
      Too many fragments per dgram limit since last reset = 0
      Number of datagram reassembly timeout since last reset = 0
      Too many fragments claiming to be the last since last reset = 0
      Fragments with bad fragment flags since last reset = 0
   TCP Normalizer stage statistics
      Packets Input = 0
      Packets Modified = 0
      Dropped packets from queue = 0
      Dropped packets due to deny-connection = 0
      Current Streams = 0
      Current Streams Closed = 0
      Current Streams Closing = 0
      Current Streams Embryonic = 0
      Current Streams Established = 0
      Current Streams Denied = 0
   Statistics for the TCP Stream Reassembly Unit
      Current Statistics for the TCP Stream Reassembly Unit
         TCP streams currently in the embryonic state = 0
         TCP streams currently in the established state = 0
         TCP streams currently in the closing state = 0
         TCP streams currently in the system = 0
         TCP Packets currently queued for reassembly = 0
      Cumulative Statistics for the TCP Stream Reassembly Unit since reset
         TCP streams that have been tracked since last reset = 0
         TCP streams that had a gap in the sequence jumped = 0
         TCP streams that was abandoned due to a gap in the sequence = 0
         TCP packets that arrived out of sequence order for their stream = 0
         TCP packets that arrived out of state order for their stream = 0
         The rate of TCP connections tracked per second since reset = 0
   SigEvent Preliminary Stage Statistics
      Number of Alerts received = 0
      Number of Alerts Consumed by AlertInterval = 0
      Number of Alerts Consumed by Event Count = 0
      Number of FireOnce First Alerts = 0
      Number of FireOnce Intermediate Alerts = 0
      Number of Summary First Alerts = 0
      Number of Summary Intermediate Alerts = 0
      Number of Regular Summary Final Alerts = 0
      Number of Global Summary Final Alerts = 0
      Number of Active SigEventDataNodes = 0
      Number of Alerts Output for further processing = 0
   SigEvent Action Override Stage Statistics
      Number of Alerts received to Action Override Processor = 0
      Number of Alerts where an override was applied = 0
      Actions Added
         deny-attacker-inline = 0
         deny-attacker-victim-pair-inline = 0
         deny-attacker-service-pair-inline = 0
         deny-connection-inline = 0
         deny-packet-inline = 0
         modify-packet-inline = 0
         log-attacker-packets = 0
         log-pair-packets = 0
```

```
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
                request-rate-limit = 0
          SigEvent Action Filter Stage Statistics
             Number of Alerts received to Action Filter Processor = 0
             Number of Alerts where an action was filtered = 0
             Number of Filter Line matches = 0
             Number of Filter Line matches causing decreased DenyPercentage = 0
             Actions Filtered
                deny-attacker-inline = 0
                deny-attacker-victim-pair-inline = 0
                deny-attacker-service-pair-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
                request-rate-limit = 0
          SigEvent Action Handling Stage Statistics.
             Number of Alerts received to Action Handling Processor = 0
             Number of Alerts where produceAlert was forced = 0
             Number of Alerts where produceAlert was off = 0
             Actions Performed
                deny-attacker-inline = 0
                deny-attacker-victim-pair-inline = 0
                deny-attacker-service-pair-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
--MORE--
```

Step 15 Display the statistics for Web Server.

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

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

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

The statistics were retrieved and cleared.

Step 17 Verify that the statistics have been cleared.

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

The statistics all begin from 0.

Interfaces Information

The **show interfaces** command is useful for gathering information on the sensing and command and control interfaces. This section describes the **show interfaces** command, and contains the following topics:

Understanding the show interfaces Command

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

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

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

Interfaces Command Output

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

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
   Total Transmit Errors = 0
```

```
   Total Transmit FIFO Overruns = 0
sensor#
```

Events Information

You can use the **show events** command to view the alerts generated by SensorApp and errors generated by an application. This section describes the **show events** command, and contains the following topics:

Sensor Events

There are five types of events:

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

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

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.

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] | **log** | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] command to display events from Event Store.

Events are displayed beginning at the start time. If you do not specify a start time, events are displayed beginning at the current time. If you do not specify an event type, all events are displayed.

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

The following options apply:

- **alert**—Displays alerts. Provides notification of some suspicious activity that may indicate an attack is in process or has been attempted. Alert events are generated by Analysis Engine whenever a signature is triggered by network activity.

  If no level is selected (informational, low, medium, or high), all alert events are displayed.
- **include-traits**—Displays alerts that have the specified traits.
- **exclude-traits**—Does not display alerts that have the specified traits.
- **traits**—Trait bit position in decimal (0 to 15).
- **min-threat-rating**—Displays events with a threat rating above or equal to this value. The default is 0. The valid range is 0 to 100.
- **max-threat-rating**—Displays events with a threat rating below or equal to this value. The default is 100. The valid range is 0 to 100.
- **error**—Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
- **log**—Displays log events. Log events are generated when a transaction is received and responded to by an application. Contains information about the request, response, success or failure of the transaction.
- **NAC**—Displays ARC (block) requests.

  Note ARC is formerly known as NAC. This name change has not been completely implemented throughout IDM, IME, and the CLI for Cisco IPS 6.1.
- **status**—Displays status events.
- **past**—Displays events starting in the past for the specified hours, minutes, and seconds.
- *hh:mm:ss*—Hours, minutes, and seconds in the past to begin the display.

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

To display events from Event Store, follow these steps:

Step 1 Log in to the CLI.

Step 2 Display all events starting now.

```
sensor# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

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

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

```
sensor# show events NAC 10:00:00 Feb 9 2008
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2008/02/09 10:33:31 2008/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

Step 4 Display errors with the warning level starting at 10.00 a.m. on February 9, 2008:

```
sensor# show events error warning 10:00:00 Feb 9 2008
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2008/01/07 04:49:25 2008/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

Step 5 Display alerts from the past 45 seconds.

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

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
```

```
    appName: sensorApp
    appInstanceId: 367
  time: 2008/03/02 14:15:59 2008/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


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

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

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

Clearing Events

Use the **clear events** command to clear Event Store. To clear events from Event Store, follow these steps:

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

Step 2 Clear Event Store.

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

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

cidDump Script

If you do not have access to IDM, 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 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 A-95.

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.