



## Troubleshooting

---

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

- [Cisco Bug Search Tool, page E-1](#)
- [Preventive Maintenance, page E-2](#)
- [Disaster Recovery, page E-6](#)
- [Recovering the Password, page E-7](#)
- [Time Sources and the Sensor, page E-11](#)
- [Advantages and Restrictions of Virtualization, page E-13](#)
- [Supported MIBs, page E-13](#)
- [When to Disable Anomaly Detection, page E-14](#)
- [Troubleshooting Global Correlation, page E-15](#)
- [The Analysis Engine Not Responding, page E-16](#)
- [Troubleshooting RADIUS Authentication, page E-17](#)
- [Troubleshooting External Product Interfaces, page E-17](#)
- [Troubleshooting the Appliance, page E-18](#)
- [Troubleshooting the IDM, page E-49](#)
- [Troubleshooting the IME, page E-52](#)
- [Gathering Information, page E-53](#)

## Cisco Bug Search Tool

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

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

Check out Bug Search Tools & Resources on Cisco.com. For more details on the tool overview and factionalists, check out the help page, located at this URL:

<http://www.cisco.com/web/applicat/cbsshelp/help.html>.

# Preventive Maintenance

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

- [Understanding Preventive Maintenance, page E-2](#)
- [Creating and Using a Backup Configuration File, page E-2](#)
- [Backing Up and Restoring the Configuration File Using a Remote Server, page E-3](#)
- [Creating the Service Account, page E-5](#)

## Understanding Preventive Maintenance

The following actions will help you maintain your sensor:

- Back up a good configuration. If your current configuration becomes unusable, you can replace it with the backup version.
- Save your backup configuration to a remote system.
- Always back up your configuration before you do a manual upgrade. If you have auto upgrades configured, make sure you do periodic backups.
- Create a service account. A service account is needed for special debug situations directed by TAC.



### Caution

You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. Analyze your situation to decide if you want a service account existing on the system.

### For More Information

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

## Creating and Using a Backup Configuration File

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

To back up your current configuration, follow these steps:

- 
- Step 1** Log in to the CLI using an account with administrator privileges.
- Step 2** Save the current configuration. The current configuration is saved in a backup file.
- ```
sensor# copy current-config backup-config
```
- Step 3** Display the backup configuration file. The backup configuration file is displayed.

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

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

- Merge the backup configuration into the current configuration.

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

- Overwrite the current configuration with the backup configuration.

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

## Backing Up and Restoring the Configuration File Using a Remote Server



### Note

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

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

The following options apply:

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

This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.

- **source\_url**—The location of the source file to be copied. It can be a URL or keyword.
- **destination\_url**—The location of the destination file to be copied. It can be a URL or a keyword.
- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.
- **backup-config**—The storage location for the configuration backup.

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

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

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

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



### Note

You are prompted for a password.

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

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

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




---

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

---

- http:—Source URL for the web server. The syntax for this prefix is:  
http://[[username@]location][[/directory]]/filename




---

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

---

- https:—Source URL for the web server. The syntax for this prefix is:  
https://[[username@]location][[/directory]]/filename




---

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

---

**Caution**


---

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

---

**Backing Up the Current Configuration to a Remote Server**

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

---

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

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

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

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

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

---

**Restoring the Current Configuration From a Backup File**

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

---

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

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

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

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

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

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

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

#### For More Information

For a list of supported HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page D-3](#).

## Creating the Service Account

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

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



#### Caution

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



#### Caution

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



#### Note

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

To create the service account, follow these steps:

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

- Step 2** Enter configuration mode.

```
sensor# configure terminal
```

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

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

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

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

**Step 5** Exit configuration mode.

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

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

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

---

## Disaster Recovery

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

- If you are using the CLI, IDM, or IME for configuration, copy the current configuration from the sensor to an FTP or SCP server any time a change has been made.
- You should note the specific software version for that configuration. You can apply the copied configuration only to a sensor of the same version.
- You also need the list of user IDs that have been used on that sensor. The list of user IDs and passwords are not saved in the configuration.

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

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



---

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

---

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



**Warning**

---

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

---

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

**For More Information**

- For the procedure for backing up a configuration file, see [Creating and Using a Backup Configuration File, page E-2](#).
- For the procedures for reimaging a sensor, see [Chapter D, “Upgrading, Downgrading, and Installing System Images.”](#)
- For the procedure for using the **setup** command to initialize the sensor, see [Appendix B, “Initializing the Sensor.”](#)
- For more information on obtaining IPS software and how to install it, see [Obtaining Cisco IPS Software, page C-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 E-3](#).
- For the procedure for adding hosts to the SSH known hosts list, refer to [Adding Hosts to the SSH Known Hosts Lists](#).
- For the procedure for adding users and obtaining a list of the current users on the sensor, refer to [Configuring User Parameters](#).

## Recovering the Password

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

- [Understanding Password Recovery, page E-8](#)
- [Recovering the Password for the Appliance, page E-8](#)
- [Disabling Password Recovery, page E-10](#)
- [Verifying the State of Password Recovery, page E-11](#)

- [Troubleshooting Password Recovery, page E-11](#)

## Understanding Password Recovery



### Note

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

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

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

**Table E-1 Password Recovery Methods According to Platform**

| Platform            | Description               | Recovery Method       |
|---------------------|---------------------------|-----------------------|
| 4300 series sensors | Standalone IPS appliances | GRUB prompt or ROMMON |
| 4500 series sensors |                           |                       |

## Recovering the Password for the Appliance

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

- [Using the GRUB Menu, page E-8](#)
- [Using ROMMON, page E-9](#)

### Using the GRUB Menu



### Note

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

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

To recover the password on appliances, follow these steps:

**Step 1** Reboot the appliance to see the GRUB menu.

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

Use the ^ and v keys to select which entry is highlighted.  
Press enter to boot the selected OS, 'e' to edit the



Commands before booting, or 'c' for a command-line.

Highlighted entry is 0:

**Step 2** Press any key to pause the boot process.

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



**Note**

## Using ROMMON

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



**Note**

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

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

**Step 1** Reboot the appliance.

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

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

**Step 3** Enter the following commands to reset the password:

```
confreg 0x7
boot
```

Sample ROMMON session:

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

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

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

```
confreg 0
```

---

## 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 the IDM or IME

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

---

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

**Step 2** Choose **Configuration > sensor\_name > Sensor Setup > Network**.

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

---

## Verifying the State of Password Recovery

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

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

---

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

**Step 2** Enter service host submode.

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

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

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

---

## Troubleshooting Password Recovery

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

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

## Time Sources and the Sensor

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

- [Time Sources and the Sensor, page E-12](#)
- [Correcting Time on the Sensor, page E-12](#)
- [Correcting Time on the Sensor, page E-12](#)

## Time Sources and the Sensor

**Note**

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

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

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

**Note**

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

**For More Information**

For the procedure for configuring NTP, refer to [Configuring NTP](#).

## 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 E-83](#).

# 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 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520

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

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

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

**Note**

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

**Note**

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

## When to Disable Anomaly Detection

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

To disable anomaly detection, follow these steps:

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

**Step 2** Enter analysis engine submode.

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

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

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

**Step 4** Disable anomaly detection operational mode.

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

**Step 5** Exit analysis engine submode.

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

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

### For More Information

For more information about Worms, refer to [Worms](#).

# Troubleshooting Global Correlation

Make sure you observe the following when configuring global correlation:

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

## For More Information

- For detailed information about Global Correlation features and how to configure them, for IDM refer to [Configuring Global Correlation](#), for IME refer to [Configuring Global Correlation](#), and for the CLI refer to [Configuring Global Correlation](#).
- For the procedure for adding a DNS server to support Global Correlation, for IDM refer to [Configuring Network Settings](#), for IME refer to [Configuring Network Settings](#), and for the CLI, refer to [Configuring the DNS and Proxy Servers for Global Correlation](#).
- For the procedure for obtaining and installing the IPS license key, for IDM refer to [Configuring Licensing](#), for IME refer to [Configuring Licensing](#), and for the CLI, refer to [Installing the License Key](#).

# The Analysis Engine Not Responding

**Error Message** Output from show statistics analysis-engine  
 Error: getAnalysisEngineStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

**Error Message** Output from show statistics anomaly-detection  
 Error: getAnomalyDetectionStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

**Error Message** Output from show statistics denied-attackers  
 Error: getDeniedAttackersStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

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

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

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

- 
- Step 1** Log in to the sensor.
- Step 2** Verify that the Analysis Engine is not running, Check to see if the Analysis Engine reads Not Running.
- ```

sensor# show version

-----
MainApp          C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
AnalysisEngine   C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Not Running
CollaborationApp C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CLI              C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
  
```
- Step 3** Enter **show tech-support** and save the output.
- Step 4** Reboot the sensor.
- Step 5** Enter **show version** after the sensor has stabilized to see if the issue is resolved.
- Step 6** If the Analysis Engine still reads Not Running, contact TAC with the original **show tech support** command output.
-



# Troubleshooting RADIUS Authentication

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

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

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

## For More Information

For detailed information about RADIUS authentication, for the IDM and IME refer to [Configuring Authentication and Users](#), and for the CLI, refer to [Configuring Authentication and User Parameters](#).

# Troubleshooting External Product Interfaces

This section lists issues that can occur with external product interfaces and provides troubleshooting tips. For more information on external product interfaces, refer to [Configuring External Product Interfaces](#). This section contains the following topics:

- [External Product Interfaces Issues, page E-17](#)
- [External Product Interfaces Troubleshooting Tips, page E-18](#)

## External Product Interfaces Issues

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

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

- The sensor must recognize each CSA MC host X.509 certificate. You must add them as a trusted host.
- You can configure a maximum of two external product devices.

#### For More Information

- For more information on working with OS maps and identifications, refer to [Adding, Editing, Deleting, and Moving Configured OS Maps](#) and [Adding, Editing, Deleting, and Moving Configured OS Maps](#).
- For the procedure for adding trusted hosts, refer to [Adding TLS 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 the IDM and check the Interface state line in the response, or choose **Configuration > sensor\_name > Sensor Monitoring > Support Information > Statistics** in the IME, and check the Interface state line in the response.
- Make sure you have added the CSA MC IP address to the trusted hosts. If you forgot to add it, add it, wait a few minutes and then check again.
- Confirm subscription login information by opening and closing a subscription on the CSA MC using the browser.
- Check the Event Store for the CSA MC subscription errors.

#### For More Information

- For the procedure for adding trusted hosts, refer to [Adding TLS Trusted Hosts](#).
- For the procedure for displaying events, refer to [Displaying Events](#).

## Troubleshooting the Appliance

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

- [Troubleshooting Loose Connections](#), page E-19
- [Analysis Engine is Busy](#), page E-19
- [Communication Problems](#), page E-20
- [The SensorApp and Alerting](#), page E-24
- [Blocking](#), page E-31
- [Logging](#), page E-40
- [TCP Reset Not Occurring for a Signature](#), page E-45
- [Software Upgrades](#), page E-47



#### 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.

---

## Troubleshooting Loose Connections

Perform the following actions to troubleshoot loose connections on sensors:

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

## Analysis Engine is Busy

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

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

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

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

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

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

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

## Communication Problems

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

- [Cannot Access the Sensor CLI Through Telnet or SSH, page E-20](#)
- [Correcting a Misconfigured Access List, page E-22](#)
- [Duplicate IP Address Shuts Interface Down, page E-23](#)

### Cannot Access the Sensor CLI Through Telnet or SSH

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

- 
- Step 1** Log in to the sensor CLI through a console, terminal, or module session.
  - Step 2** Make sure that the sensor management interface is enabled. The management interface is the interface in the list with the status line `Media Type = TX`. If the Link Status is `Down`, go to Step 3. If the Link Status is `Up`, go to Step 5.

```

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

```

Link Speed = Auto_100
Link Duplex = Auto_Full
Total Packets Received = 944333
Total Bytes Received = 83118358
Total Multicast Packets Received = 0
Total Receive Errors = 0
Total Receive FIFO Overruns = 0
Total Packets Transmitted = 397633
Total Bytes Transmitted = 435730956
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0
sensor#

```

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

```

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

```

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

Current Configuration:

```

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

```

- Step 4** Make sure the management port is connected to an active network connection. If the management port is not connected to an active network connection, the management interface does not come up.

- Step 5** Make sure the IP address of the workstation that is trying to connect to the sensor is permitted in the sensor access list. If the workstation network address is permitted in the sensor access list, go to Step 6.

```

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

```

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

Current Configuration:

```

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

```

--MORE--

- Step 6** Add a permit entry for the workstation network address, save the configuration, and try to connect again.
- Step 7** Make sure the network configuration allows the workstation to connect to the sensor. If the sensor is protected behind a firewall and the workstation is in front of the firewall, make sure the firewall is configured to allow the workstation to access the sensor. Or if the workstation is behind a firewall that is performing network address translation on the workstation IP address, and the sensor is in front of the firewall, make sure that the sensor access list contains a permit entry for the workstation translated address.

#### For More Information

- For the procedures for changing the IP address, changing the access list, and enabling and disabling Telnet, refer to [Configuring Network Settings](#).
- For the various ways to open a CLI session directly on the sensor, see [Appendix A, “Logging In to the Sensor.”](#)

## Correcting a Misconfigured Access List

To correct a misconfigured access list, follow these steps:

- Step 1** Log in to the CLI.

- Step 2** View your configuration to see the access list.

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

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

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

- Step 4** Verify the settings.

```
sensor(config-hos-net)# show settings
network-settings
-----
host-ip: 192.168.1.2/24,192.168.1.1 default: 10.1.9.201/24,10.1.9.1
host-name: sensor-238 default: sensor
telnet-option: enabled default: disabled
access-list (min: 0, max: 512, current: 3)
-----
network-address: 10.0.0.0/8
-----
network-address: 64.0.0.0/8
-----
network-address: 171.69.70.0/24
-----
```

```

ftp-timeout: 300 seconds <defaulted>
login-banner-text: <defaulted>
-----
sensor(config-hos-net)#

```

## Duplicate IP Address Shuts Interface Down

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

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

- 
- Step 1** Log in to the CLI.
  - Step 2** Determine whether the interface is up. If the output says the command and control interface link status is down, there is a hardware issue or an IP address conflict.

```

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

```

```
Total Packets Transmitted = 219260
Total Bytes Transmitted = 103668610
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0
sensor#
```

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

**Step 4** Make sure the IP address is correct.

---

#### For More Information

- To make sure the sensor cabling is correct, refer to the chapter for your sensor in this document.
- For the procedure for making sure the IP address is correct, refer to [Configuring Network Settings](#).

## The SensorApp and Alerting

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

- [The SensorApp Is Not Running](#), page E-24
- [Physical Connectivity, SPAN, or VACL Port Issue](#), page E-26
- [Unable to See Alerts](#), page E-27
- [Sensor Not Seeing Packets](#), page E-29
- [Cleaning Up a Corrupted SensorApp Configuration](#), page E-30

## The SensorApp Is Not Running

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

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

---

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

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

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S741.0          2013-09-10
  Threat Profile Version 2
OS Version:          2.6.29.1
Platform:            IPS-4360
Serial Number:       FGL1702401M
Licensed, expires:   21-Nov-2014 UTC
Sensor up-time is 22:09.
Using 14372M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.6M out of 376.4M bytes of available disk space (24% usage)
```



```
boot is using 63.1M out of 70.2M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)
```

```
MainApp          C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
AnalysisEngine  C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CollaborationApp C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CLI             C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
```

Upgrade History:

```
IPS-K9-7.3-1-E4  11:22:07 UTC Sat Jan 19 2013
```

Recovery Partition Version 1.1 - 7.3(1)E4

Host Certificate Valid from: 09-Oct-2014 to 09-Oct-2016

sensor#

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

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

originator:

hostId: sensor

appName: sensorApp

appInstanceId: 1045

time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC

errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.



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

**Step 4** If you do not have the latest software updates, download them from Cisco.com. Read the Readme that accompanies the software upgrade for any known DDTS for the SensorApp or the Analysis Engine.

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

**Step 6** Reboot the sensor.

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

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

#### For More Information

- For more information on IPS system architecture, refer to [System Architecture](#).
- For the procedure for obtaining the latest Cisco IPS software, see [Obtaining Cisco IPS Software, page C-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.

**Step 4** Verify the interface configuration:

- Make sure you have the interfaces configured properly.
- Verify the SPAN and VACL capture port configuration on the Cisco switch. Refer to your switch documentation for the procedure.

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

```
sensor# show interfaces
```

---

#### For More Information

- For the procedure for properly installing the sensing interface on your sensor, refer to the chapter on your appliance in this document.
- For the procedures for configuring interfaces on your sensor, 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 sent to the Event Store. Every time you configure a signature, the new configuration overwrites the old one, so make sure you have configured all the event actions you want for each signature.

---

- Make sure the sensor is seeing packets
- Make sure that alerts are being generated
- Make sure the sensing interface is in a virtual sensor

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

---

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

**Step 2** Make sure the signature is enabled.

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

**Step 3** Make sure you have Produce Alert configured.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer      Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
```

```

sensor(config-sig-sig-nor)# show settings
normalizer
-----
event-action: produce-alert default: produce-alert|deny-connection-inline
edit-default-sigs-only
-----
sensor#

```

**Step 4** Make sure the sensor is seeing packets.

```

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

```

**Step 5** Check for alerts.

```

sensor# show statistics virtual-sensor
SigEvent Preliminary Stage Statistics
Number of Alerts received = 0
Number of Alerts Consumed by AlertInterval = 0
Number of Alerts Consumed by Event Count = 0
Number of FireOnce First Alerts = 0
Number of FireOnce Intermediate Alerts = 0
Number of Summary First Alerts = 0
Number of Summary Intermediate Alerts = 0
Number of Regular Summary Final Alerts = 0
Number of Global Summary Final Alerts = 0
Number of Alerts Output for further processing = 0alertDetails: Traffic Source: int0 ;

```

---

## Sensor Not Seeing Packets

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

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

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

**Step 2** Make sure the interfaces are up and receiving packets.

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

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

- Check the cabling.
- Enable the interface.

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

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

```

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

---

**For More Information**

For the procedure for installing the sensor properly, refer to your sensor chapter in this document.

## Cleaning Up a Corrupted SensorApp Configuration

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

To delete the SensorApp configuration, follow these steps:

- 
- Step 1** Log in to the service account.
  - Step 2** Su to root.
  - Step 3** Stop the IPS applications.  
`/etc/init.d/cids stop`
  - Step 4** Replace the virtual sensor file.  
`cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml /usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml`
  - Step 5** Remove the cache files.  
`rm /usr/cids/idsRoot/var/virtualSensor/*.pmz`
  - Step 6** Exit the service account.
  - Step 7** Log in to the sensor CLI.

**Step 8** Start the IPS services.

```
sensor# cids start
```

**Step 9** Log in to an account with administrator privileges.

**Step 10** Reboot the sensor.

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

---

### For More Information

For more information on IPS system architecture, refer to [System Architecture](#).

## Blocking

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

- [Troubleshooting Blocking, page E-31](#)
- [Verifying ARC is Running, page E-32](#)
- [Verifying ARC Connections are Active, page E-33](#)
- [Device Access Issues, page E-35](#)
- [Verifying the Interfaces and Directions on the Network Device, page E-36](#)
- [Enabling SSH Connections to the Network Device, page E-37](#)
- [Blocking Not Occurring for a Signature, page E-37](#)
- [Verifying the Master Blocking Sensor Configuration, page E-38](#)

## Troubleshooting Blocking

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



### Note

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

---

To troubleshoot the ARC, follow these steps:

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

**For More Information**

- For the procedure to verify that ARC is running, see [Verifying ARC is Running, page E-32](#).
- For the procedure to verify that ARC is connecting, see [Verifying ARC Connections are Active, page E-33](#).
- For the procedure to verify that the Event Action is set to Block Host, see [Blocking Not Occurring for a Signature, page E-37](#).
- For the procedure to verify that the master blocking sensor is properly configured, see [Verifying the Master Blocking Sensor Configuration, page E-38](#).
- For a discussion of ARC architecture, refer to [Attack Response Controller](#).

## Verifying ARC is Running

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

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

- Step 1** Log in to the CLI.
- Step 2** Verify that the MainApp is running.

```

sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S741.0          2013-09-10
  Threat Profile Version 2
OS Version:          2.6.29.1
Platform:            IPS-4360
Serial Number:       FGL1702401M
Licensed, expires:   21-Nov-2014 UTC
Sensor up-time is 22:09.
Using 14372M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.6M out of 376.4M bytes of available disk space (24% usage)
boot is using 63.1M out of 70.2M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

MainApp          C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
AnalysisEngine   C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CollaborationApp C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CLI              C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600

Upgrade History:

  IPS-K9-7.3-1-E4   11:22:07 UTC Sat Jan 19 2013

Recovery Partition Version 1.1 - 7.3(1)E4

Host Certificate Valid from: 09-Oct-2014 to 09-Oct-2016
    
```



```
sensor#
```

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

### For More Information

For more information on IPS system architecture, 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 the ARC is connecting. Check the State section of the output to verify that all devices are connecting.

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

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

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

### Example

```
sensor# show events error 00:00:00 Apr 01 2011 | include : nac
```

- Step 4** Make sure you have the latest software updates.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

Host:
  Realm Keys          key1.0
```

```
Signature Definition:
  Signature Update      S741.0      2013-09-10
  Threat Profile Version 2
OS Version:           2.6.29.1
Platform:             IPS-4360
Serial Number:        FGL1702401M
Licensed, expires:    21-Nov-2014 UTC
Sensor up-time is 22:09.
Using 14372M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.6M out of 376.4M bytes of available disk space (24% usage)
boot is using 63.1M out of 70.2M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)
```

```
MainApp      C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
AnalysisEngine C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CollaborationApp C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CLI          C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
```

#### Upgrade History:

```
IPS-K9-7.3-1-E4  11:22:07 UTC Sat Jan 19 2013
```

```
Recovery Partition Version 1.1 - 7.3(1)E4
```

```
Host Certificate Valid from: 09-Oct-2014 to 09-Oct-2016
```

```
sensor#
```




---

**Note** If you do not have the latest software updates, download them from [Cisco.com](http://Cisco.com). Read the Readme that accompanies the software upgrade for any known DDTs for the ARC.

---

- Step 5** Make sure the configuration settings for each device are correct (the username, password, and IP address).
- Step 6** Make sure the interface and directions for each network device are correct.
- Step 7** If the network device is using SSH-3DES, make sure that you have enabled SSH connections to the device.
- Step 8** Verify that each interface and direction on each controlled device is correct.

#### For More Information

- For the procedure for obtaining the latest Cisco IPS software, see [Obtaining Cisco IPS Software, page C-1](#).
- For more information about configuring devices, see [Device Access Issues, page E-35](#).
- For the procedure for verifying the interfaces and directions for each network device, see [Verifying the Interfaces and Directions on the Network Device, page E-36](#).
- For the procedure for enabling SSH, see [Enabling SSH Connections to the Network Device, page E-37](#).

## Device Access Issues

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

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 E-36](#).

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

To enable SSH-3DES connections to the network device, follow these steps:

- Step 1** Log in to the CLI.
- Step 2** Enter configuration mode.
- ```
sensor# configure terminal
```
- Step 3** Enable SSH-3DES.
- ```
sensor(config)# ssh-3des host blocking_device_ip_address
```
- Step 4** Type **yes** when prompted to accept the device.
- 

## Blocking Not Occurring for a Signature

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

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

- Step 1** Log in to the CLI.
- Step 2** Enter signature definition submode.
- ```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

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



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

---

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

```

edit-default-sigs-only
-----
default-signatures-only
-----
specify-service-ports
-----
no
-----
-----
specify-tcp-max-mss
-----
no
-----
-----
specify-tcp-min-mss
-----
no
-----
-----
--MORE--
    
```

**Step 4** Exit signature definition submenu.

```

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

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

## Verifying the Master Blocking Sensor Configuration

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

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

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

**Step 2** View the ARC statistics and verify that the master blocking sensor entries are in the statistics.

```

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

- Step 3** If the master blocking sensor does not show up in the statistics, you need to add it.
- Step 4** Initiate a manual block to a bogus host IP address to make sure the master blocking sensor is initiating blocks.

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

- Step 5** Exit network access general submode.

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

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

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

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

- Step 8** Log in to the CLI of the master blocking sensor host, and using the **show statistics network-access** command, verify that the block also shows up in the master blocking sensor ARC statistics.

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

- Step 9** If the remote master blocking sensor is using TLS for web access, make sure the forwarding sensor is configured as a TLS host.

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

### For More Information

For the procedure to configure the sensor to be a master blocking sensor, refer to [Configuring the Sensor to be a Master Blocking Sensor](#).

# 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. This section contains the following topics:

- [Enabling Debug Logging, page E-40](#)
- [Zone Names, page E-44](#)
- [Directing cidLog Messages to SysLog, page E-44](#)

## Enabling Debug Logging



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

To enable debug logging, follow these steps:

- Step 1** Log in to the service account.
- Step 2** Edit the log.conf file to increase the size of the log to accommodate the additional log statements.
- ```
vi /usr/cids/idsRoot/etc/log.conf
```
- Step 3** Change `fileMaxSizeInK=500` to `fileMaxSizeInK=5000`.
- Step 4** Locate the zone and CID section of the file and set the severity to debug.
- ```
severity=debug
```
- Step 5** Save the file, exit the vi editor, and exit the service account.
- Step 6** Log in to the CLI as administrator.
- Step 7** Enter master control submode.
- ```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```
- Step 8** Enable debug logging for all zones.
- ```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
master-control
-----
enable-debug: true default: false
individual-zone-control: false <defaulted>
-----
sensor(config-log-mas)#
```
- Step 9** Turn on individual zone control.
- ```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
master-control
-----
enable-debug: true default: false
individual-zone-control: true default: false
```



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

**Step 10** Exit master zone control.

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

**Step 11** View the zone names.

```
sensor(config-log)# show settings
master-control
-----
enable-debug: false <defaulted>
individual-zone-control: true default: false
-----
zone-control (min: 0, max: 999999999, current: 14)
-----
<protected entry>
zone-name: AuthenticationApp
severity: warning <defaulted>
<protected entry>
zone-name: Cid
severity: debug <defaulted>
<protected entry>
zone-name: Cli
severity: warning <defaulted>
<protected entry>
zone-name: IdapiCtlTrans
severity: warning <defaulted>
<protected entry>
zone-name: IdsEventStore
severity: warning <defaulted>
<protected entry>
zone-name: MpInstaller
severity: warning <defaulted>
<protected entry>
zone-name: cmgr
severity: warning <defaulted>
<protected entry>
zone-name: cplane
severity: warning <defaulted>
<protected entry>
zone-name: csi
severity: warning <defaulted>
<protected entry>
zone-name: ctlTransSource
severity: warning <defaulted>
<protected entry>
zone-name: intf
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: intf
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: intfci
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 E-44](#).

## Zone Names

Table E-2 lists the debug logger zone names:

**Table E-2** *Debug Logger Zone Names*

Zone Name	Description
AD	Anomaly Detection zone
AuthenticationApp	Authentication zone
Cid	General logging zone
Cli	CLI zone
IdapiCtlTrans	All control transactions zone
IdsEventStore	Event Store zone
csi	CIDS Servlet Interface <sup>1</sup>
ctlTransSource	Outbound control transactions zone
intfc	Interface zone
nac	ARC zone
rep	Reputation zone
sched	Automatic update scheduler zone
sensorApp	AnalysisEngine zone
tls	SSL and TLS zone

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

### For More Information

To learn more about the IPS Logger service, 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

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



**Note**

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

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

- Step 1** Log in to the CLI.
- Step 2** Make sure the event action is set to TCP reset.

```

sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
atomic-ip
-----

```

```

event-action: produce-alert|reset-tcp-connection default: produce-alert
fragment-status: any <defaulted>
specify-l4-protocol
-----
no
-----
-----
specify-ip-payload-length
-----
no
-----
-----
specify-ip-header-length
-----
no
-----
-----
specify-ip-tos
-----
--MORE--

```

**Step 3** Exit signature definition submode.

```

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

```

**Step 4** Press **Enter** to apply the changes or type **no** to discard them.**Step 5** Make sure the correct alarms are being generated.

```

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

```

**Step 6** Make sure the switch is allowing incoming TCP reset packet from the sensor. Refer to your switch documentation for more information.**Step 7** Make sure the resets are being sent.

```

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

```

## Software Upgrades

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

- [Upgrading and Analysis Engine, page E-47](#)
- [Which Updates to Apply and Their Prerequisites, page E-47](#)
- [Issues With Automatic Update, page E-48](#)
- [Updating a Sensor with the Update Stored on the Sensor, page E-49](#)

### Upgrading and Analysis Engine

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

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-7.1-2-E4.pkg
Password: *****
Warning: Executing this command will apply a major version upgrade to the application
partition. The system may be rebooted to complete the upgrade.
Continue with upgrade?: yes
Error: AnalysisEngine is not running. Please reset box and attempt upgrade again.
```

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

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



#### Caution

---

Reimaging using the system image file restores all configuration defaults.

---

#### For More Information

- For more information on running the **setup** command, see [Appendix B, “Initializing the Sensor.”](#)
- For more information on reimaging your sensor, see [Chapter D, “Upgrading, Downgrading, and Installing System Images.”](#)

### Which Updates to Apply and Their Prerequisites

You must have the correct service pack and minor and major version of the software. If you are having trouble with applying new software, make sure that you are applying the proper updates with the proper prerequisites:

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

**For More Information**

To understand how to interpret the IPS software filenames, see [IPS Software Versioning, page C-3](#).

**Issues With Automatic Update**

The following list provides suggestions for troubleshooting automatic updates:

- Run TCPDUMP:
  - Create a service account. **Su** to root and run TCPDUMP on the command and control interface to capture packets between the sensor and the FTP server.
  - Use the **upgrade** command to manually upgrade the sensor.
  - Look at the TCPDUMP output for errors coming back from the FTP server.
- Make sure the sensor is in the correct directory. The directory must be specified correctly. This has caused issues with Windows FTP servers. Sometimes an extra “/” or even two “/” are needed in front of the directory name. To verify this, use the same FTP commands you see in the TCPDUMP output through your own FTP connection.
- You must use the Windows FTP server setup option to emulate UNIX file structure and not MS-DOS file structure.
- If you are using SCP, make sure you have added the SSH host key to the known hosts list.

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

- Determine which IPS software version your sensor has.
- Make sure the passwords are configured for automatic update. Make sure they match the same passwords used for manual update.
- Make sure that the filenames in the FTP server are exactly what you see on Downloads on Cisco.com. This includes capitalization. Some Windows FTP servers allow access to the file with the incorrect capitalization but the sensor ultimately rejects the file because the name has changed.
- If necessary, run TCPDUMP on automatic update. You can compare the successful manual update with the unsuccessful automatic update and troubleshoot from there.

**For More Information**

- For the procedure for creating the service account, see [Creating the Service Account, page E-5](#).
- For the procedure for reimaging your sensor, see [Chapter D, “Upgrading, Downgrading, and Installing System Images.”](#)
- For the procedure for adding hosts to the SSH known hosts list, refer to [Adding Hosts to the SSH Known Hosts List](#).
- For the procedure for determining the software version, see [Displaying Version Information, page E-59](#).



## 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 C-1](#).

## Troubleshooting the IDM

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

- [Cannot Launch IDM - Loading Java Applet Failed, page E-50](#)
- [Cannot Launch the IDM-the Analysis Engine Busy, page E-50](#)
- [The IDM, Remote Manager, or Sensing Interfaces Cannot Access the Sensor, page E-51](#)
- [Signatures Not Producing Alerts, page E-52](#)

## 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 are installed on the machine on which you are launching the IDM.

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

To clear the cache, follow these steps:

- 
- Step 1** Close all browser windows.
  - Step 2** If you have Java Plug-in 1.3.x installed:
    - a. Click **Start > Settings > Control Panel > Java Plug-in 1.3.x**.
    - b. Click the **Advanced** tab.
    - c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.
    - d. Click the **Cache** tab.
    - e. Click **Clear**.
  - Step 3** If you have Java Plug-in 1.4.x installed:
    - a. Click **Start > Settings > Control Panel > Java Plug-in 1.4.x**.
    - b. Click the **Advanced** tab.
    - c. Under Java Runtime Environment, select **JRE 1.3.x** from the drop-down menu.
    - d. Click the **Cache** tab.
    - e. Click the **Browser** tab.
    - f. Deselect all browser check boxes.
    - g. Click **Clear Cache**.
  - Step 4** Delete the temp files and clear the history in the browser.
- 

## Cannot Launch the IDM-the Analysis Engine Busy

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

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

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

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

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

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

```
sensor# setup
```

```
--- System Configuration Dialog ---
```

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

```
Current Configuration:
```

```
service host  
network-settings  
host-ip 192.168.1.2/24,192.168.1.1  
host-name sensor  
telnet-option enabled  
access-list 0.0.0.0/0  
ftp-timeout 300  
no login-banner-text  
exit  
time-zone-settings  
offset 0  
standard-time-zone-name UTC  
exit  
summertime-option disabled  
ntp-option disabled  
exit  
service web-server  
port 443  
exit
```

- Step 2** If network devices, such as routers, switches, or firewalls, are between the sensor and the workstation, make sure these devices are configured to allow the workstation to access the sensor web server port. All remote management communication is performed by the sensor web server.

### For More Information

For the procedure for enabling and disabling Telnet on the sensor, and configuring the web server, refer to [Changing Network Settings](#).

## Signatures Not Producing Alerts

**Caution**

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

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

**For More Information**

- For more information about event actions, refer to [Event Actions](#).
- For the procedure for configuring event actions, refer to [Assigning Actions to Signatures](#).
- For the procedure for obtaining statistics about virtual sensor and Event Store, refer to [Displaying Statistics](#).

## Troubleshooting the IME

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

- [Time Synchronization on the IME and the Sensor](#), page E-52
- [Not Supported Error Message](#), page E-53

## Time Synchronization on the IME and the Sensor

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

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

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

**For More Information**

- For more information on time and the sensor, see [Time Sources and the Sensor](#), page E-12.
- For the procedure for changing the time on the sensor, see [Correcting Time on the Sensor](#), page E-12.

## Not Supported Error Message

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

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

**Recommended Action** Upgrade to IPS 6.1 or later.

## 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 contains the following topics:

- [Health and Network Security Information, page E-53](#)
- [Tech Support Information, page E-54](#)
- [Version Information, page E-59](#)
- [Statistics Information, page E-63](#)
- [Interfaces Information, page E-75](#)
- [Events Information, page E-79](#)
- [cidDump Script, page E-83](#)
- [Uploading and Accessing Files on the Cisco FTP Site, page E-84](#)

## Health and Network Security Information



### Caution

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

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

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

- 
- Step 1** Log in to the CLI.
- Step 2** Show the health and security status of the sensor.

```
sensor# show health
Overall Health Status                Red
Health Status for Failed Applications Green
```

|   |             |
|---|-------------|
| Health Status for Signature Updates                   | Green       |
| Health Status for License Key Expiration              | Red         |
| Health Status for Running in Bypass Mode              | Green       |
| Health Status for Interfaces Being Down               | Red         |
| Health Status for the Inspection Load                 | Green       |
| Health Status for the Time Since Last Event Retrieval | Green       |
| Health Status for the Number of Missed Packets        | Green       |
| Health Status for the Memory Usage                    | Not Enabled |
| Health Status for Global Correlation                  | Red         |
| Health Status for Network Participation               | Not Enabled |
| <hr/>   |             |
| Security Status for Virtual Sensor vs0                | Green       |
| sensor#   |             |

## Tech Support Information

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

- [Understanding the show tech-support Command, page E-54](#)
- [Displaying Tech Support Information, page E-54](#)
- [Tech Support Command Output, page E-56](#)

### Understanding the show tech-support Command



#### Note

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

The **show tech-support** command captures all status and configuration information on the sensor and includes the current configuration, version information, and cidDump information. The output can be large, over 1 MB. You can transfer the output to a remote system. For the procedure for copying the output to a remote system, see [Displaying Tech Support Information, page E-54](#).



#### Note

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

### Displaying Tech Support Information



#### Note

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

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

The following parameters are optional:

- **page**—Displays the output, one page of information at a time. Press **Enter** to display the next line of output or use the spacebar to display the next page of information.
- **destination-url**—Indicates the information should be formatted as HTML and sent to the destination that follows this command. If you use this keyword, the output is not displayed on the screen.
- *destination\_url*—Indicates the information should be formatted as HTML. The URL specifies where the information should be sent. If you do not use this keyword, the information is displayed on the screen.
- You can specify the following destination types:
  - **ftp**—Destination URL for FTP network server. The syntax for this prefix is:  
`ftp://[[username@location]/relativeDirectory]/filename` or  
`ftp://[[username@location]//absoluteDirectory]/filename`
  - **scp**—Destination URL for the SCP network server. The syntax for this prefix is:  
`scp://[[username@]location]/relativeDirectory]/filename` or  
`scp://[[username@]location]//absoluteDirectory]/filename`

### Varlog Files

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

### Displaying Tech Support Information

To display tech support information, follow these steps:

- 
- Step 1** Log in to the CLI using an account with administrator privileges.
- Step 2** View the output on the screen. The system information appears on the screen, one page at a time. Press the spacebar to view the next page or press **Ctrl-C** to return to the prompt
- ```
sensor# show tech-support page
```
- Step 3** To send the output (in HTML format) to a file:
- a. Enter the following command, followed by a valid destination. The `password:` prompt appears.
 

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

Example

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

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```
  - b. Enter the password for this user account. The `Generating report:` message is displayed.
-

## Tech Support Command Output

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



### Note

This output example shows the first part of the command and lists the information for the interfaces, authentication, and the Analysis Engine.

```

sensor# show tech-support page
System Status Report
This Report was generated on Thu Oct 17 14:35:52 2013.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S741.0          2013-09-10
  Threat Profile Version 2
OS Version:          2.6.29.1
Platform:            IPS-4345-K9
Serial Number:       FGL170340DR
No license present
Sensor up-time is 3 days.
Using 6282M out of 7864M bytes of available memory (79% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.2M out of 376.4M bytes of available disk space (24% usage)
boot is using 62.9M out of 70.2M bytes of available disk space (94% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

MainApp              C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
AnalysisEngine       C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CollaborationApp     C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600
Running
CLI                  C-2013_12_16_14_00_7_3_0_143  (Release)  2013-12-16T14:06:20-0600

Upgrade History:

  IPS-K9-7.3-1-E4   14:16:07 UTC Sat Jan 26 2013

Recovery Partition Version 1.1 - 7.3(1)E4

Host Certificate Valid from: 13-Oct-2013 to 14-Oct-2015

Output from show interfaces
Interface Statistics
  Total Packets Received = 141568
  Total Bytes Received = 13807286
  Missed Packet Percentage = 0
  Current Bypass Mode = Off
MAC statistics from interface GigabitEthernet0/0
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0

```



```
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 Management0/0
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 = 428857
Total Bytes Received = 29967463
Total Multicast Packets Received = 0
Total Receive Errors = 0
Total Receive FIFO Overruns = 0
Total Packets Transmitted = 5303
Total Bytes Transmitted = 1040574
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/1
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/2
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/3
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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
--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 E-59](#)
- [Displaying Version Information, page E-59](#)

## 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.



### Note

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



### Note

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

To display the version and configuration, follow these steps:

- Step 1** Log in to the CLI.
- Step 2** View version information.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

Host:
  Realm Keys                key1.0
Signature Definition:
  Signature Update          S741.0      2013-09-10
  Threat Profile Version    2
```

```

OS Version:                2.6.29.1
Platform:                  IPS-4360
Serial Number:             FGL1702401M
Licensed, expires:        21-Nov-2014 UTC
Sensor up-time is 22:09.
Using 14372M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.6M out of 376.4M bytes of available disk space (24% usage)
boot is using 63.1M out of 70.2M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

```

```

MainApp                    C-2013_12_16_14_00_7_3_0_143   (Release)  2013-12-16T14:06:20-0600
Running
AnalysisEngine             C-2013_12_16_14_00_7_3_0_143   (Release)  2013-12-16T14:06:20-0600
Running
CollaborationApp          C-2013_12_16_14_00_7_3_0_143   (Release)  2013-12-16T14:06:20-0600
Running
CLI                        C-2013_12_16_14_00_7_3_0_143   (Release)  2013-12-16T14:06:20-0600

```

## Upgrade History:

```
IPS-K9-7.3-1-E4   11:22:07 UTC Sat Jan 19 2013
```

```
Recovery Partition Version 1.1 - 7.3(1)E4
```

```
Host Certificate Valid from: 09-Oct-2014 to 09-Oct-2016
```

```
sensor#
```




---

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

---

**Step 3** View configuration information.


---

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

---

```

sensor# more current-config
! -----
! Current configuration last modified Fri Oct 10 09:41:17 2014
! -----
! Version 7.3(1)
! Host:
!   Realm Keys                key1.0
! Signature Definition:
!   Signature Update          S741.0   2013-09-10
!   Threat Profile Version    2
! -----
service interface
physical-interfaces GigabitEthernet0/0
no description
admin-state disabled
duplex auto
speed auto
default-vlan 6
alt-tcp-reset-interface none
subinterface-type inline-vlan-pair
subinterface 255
vlan1 100

```

```
vlan2 101
exit
lacp
channel-id 5
mode passive
exit
exit
exit
physical-interfaces GigabitEthernet0/1
no description
admin-state disabled
duplex auto
speed auto
default-vlan 7
alt-tcp-reset-interface none
subinterface-type inline-vlan-pair
subinterface 200
vlan1 200
vlan2 201
exit
lacp
mode passive
exit
exit
exit
physical-interfaces GigabitEthernet0/2
admin-state disabled
exit
physical-interfaces GigabitEthernet0/3
admin-state disabled
exit
physical-interfaces GigabitEthernet0/4
admin-state disabled
exit
physical-interfaces GigabitEthernet0/5
admin-state disabled
exit
physical-interfaces TenGigabitEthernet0/0 no description admin-state disabled duplex auto
speed auto default-vlan 0 alt-tcp-reset-interface none subinterface-type inline-vlan-pair
subinterface 1
vlan1 100
vlan2 101
exit
lacp
channel-id 120
mode passive
exit
exit
exit
physical-interfaces TenGigabitEthernet0/1 admin-state disabled exit physical-interfaces
TenGigabitEthernet0/2 no description admin-state enabled duplex auto speed auto
default-vlan 0 alt-tcp-reset-interface none subinterface-type inline-vlan-pair
subinterface 120
vlan1 100
vlan2 101
exit
lacp
channel-id 130
mode passive
exit
exit
exit
physical-interfaces TenGigabitEthernet0/3 admin-state enabled exit inline-interfaces P0 no
description
```

```

interface1 GigabitEthernet0/2
interface2 GigabitEthernet0/3
exit
lACP-system-priority 400
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.106.188.162/24,10.106.188.1
host-name QA-4510-B-C2017-188-162
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
exit
time-zone-settings
offset 330
standard-time-zone-name GMT+05:30
exit
exit
! -----
service logger
exit
! -----
service network-access
exit
! -----
service notification
exit
! -----
service signature-definition sig0
exit
! -----
service signature-definition sig1
exit
! -----
service ssh-known-hosts
rsa-keys 10.106.133.24
pubkey
AAAAB3NzaC1yc2EAAAABIwAAAQEAwNaZXSq/sQvm+Gf2CW+tB+AtgYCl7RRNKReUgwWNA1GWIGmyUEBE0qNKlofon+
UjTdFWA9nUs5PADGpDbL1DGw9zLdIVu2EzWgi5CC940TQKpPubsixVzxY/QTRGvJ1MSIZTwJMcMWNLC5H22TYhvvcb
mhWAIYdbeAR07otANYRvgSlRuNbJ/I6fHfrVv5aI01psY9+RsZxzXmgtcFhOjcdYK84DTy3PEbMLZw3wDQoQxK/4+h
84RapRskvZ9IM1GFGwLwkgdWN14pygaBSESSgImUt4KODiWhEeCPHIuJz00LfpDr/pPcCp8FTd4LIe0RnrvfLdzX4cx
2gUbOgpNtQ==
exit
exit
! -----
service trusted-certificates
exit
! -----
service web-server
exit
! -----
service anomaly-detection ad0
exit
! -----
service external-product-interface
exit
! -----

```

```
service health-monitor
exit
! -----
service global-correlation
exit
! -----
service aaa
exit
! -----
service threat-profile sig1
threat-profile Edge
exit
! -----
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 255 physical-interface
GigabitEthernet0/1 subinterface-number 200 physical-interface TenGigabitEthernet0/0
subinterface-number 1 physical-interface TenGigabitEthernet0/2 subinterface-number 120
logical-interface P0 subinterface-number 0 exit virtual-sensor vs1 description Custom VS
physical-interface TenGigabitEthernet0/1 subinterface-number 0 exit 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, page E-63](#)
- [Displaying Statistics, page E-64](#)

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

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

**Note**

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

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

**Note**

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

To display statistics for the sensor, follow these steps:

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

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

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
Number of seconds since service started = 318375
Processing Load Percentage
  Thread    5 sec   1 min   5 min
  0          1       1       1
  1          1       1       1
  2          1       1       1
  3          1       1       1
  Average   1       1       1

The rate of TCP connections tracked per second = 0
The rate of packets per second = 0
The rate of bytes per second = 0
Receiver Statistics
  Total number of packets processed since reset = 0
```



```

Total number of IP packets processed since reset = 0
Transmitter Statistics
  Total number of packets transmitted = 129766
  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
Inspection Stats

```

```

GlobalCorrelationStats
  SwVersion = 7.3(0.119)E4
  SigVersion = 741.0
  DatabaseRecordCount = 0
  DatabaseVersion = 0
  RuleVersion = 0
  ReputationFilterVersion = 0
  AlertsWithHit = 0
  AlertsWithMiss = 0
  AlertsWithModifiedRiskRating = 0
  AlertsWithGlobalCorrelationDenyAttacker = 0
  AlertsWithGlobalCorrelationDenyPacket = 0
  AlertsWithGlobalCorrelationOtherAction = 0
  AlertsWithAuditRepDenies = 0
  ReputationForcedAlerts = 0
  EventStoreInsertTotal = 0
  EventStoreInsertWithHit = 0
  EventStoreInsertWithMiss = 0
  EventStoreDenyFromGlobalCorrelation = 0
  EventStoreDenyFromOverride = 0
  EventStoreDenyFromOverlap = 0
  EventStoreDenyFromOther = 0
  ReputationFilterDataSize = 0
  ReputationFilterPacketsInput = 0
  ReputationFilterRuleMatch = 0
  DenyFilterHitsNormal = 0
  DenyFilterHitsGlobalCorrelation = 0
  SimulatedReputationFilterPacketsInput = 0
  SimulatedReputationFilterRuleMatch = 0
  SimulatedDenyFilterInsert = 0
  SimulatedDenyFilterPacketsInput = 0
  SimulatedDenyFilterRuleMatch = 0
  TcpDeniesDueToGlobalCorrelation = 0
  TcpDeniesDueToOverride = 0
  TcpDeniesDueToOverlap = 0
  TcpDeniesDueToOther = 0
  SimulatedTcpDeniesDueToGlobalCorrelation = 0
  SimulatedTcpDeniesDueToOverride = 0

```

```

SimulatedTcpDeniesDueToOverlap = 0
SimulatedTcpDeniesDueToOther = 0
LateStageDenyDueToGlobalCorrelation = 0
LateStageDenyDueToOverride = 0
LateStageDenyDueToOverlap = 0
LateStageDenyDueToOther = 0
SimulatedLateStageDenyDueToGlobalCorrelation = 0
SimulatedLateStageDenyDueToOverride = 0
SimulatedLateStageDenyDueToOverlap = 0
SimulatedLateStageDenyDueToOther = 0
AlertHistogram
RiskHistogramEarlyStage
RiskHistogramLateStage
ConfigAggressiveMode = 0
ConfigAuditMode = 0
RegexAccelerationStats
  Status = Enabled
  DriverVersion = 6.3.1
  Devices = 1
  Agents = 12
  Flows = 7
  Channels = 0
  SubmittedJobs = 193
  CompletedJobs = 193
  SubmittedBytes = 2836764
  CompletedBytes = 0
  TCPFlowsWithoutLCB = 0
  UDPFlowsWithoutLCB = 0
  TCPMissedPacketsDueToUpdate = 0
  UDPMissedPacketsDueToUpdate = 0
  MemorySize = 1073741824
  HostDirectMemSize = 0
MaliciousSiteDenyHitCounts
MaliciousSiteDenyHitCountsAUDIT
Ethernet Controller Statistics
  Total Packets Received = 0
  Total Received Packets Dropped = 0
  Total Packets Transmitted = 13643"
sensor#

```

### Step 3 Display the statistics for anomaly detection.

```

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

```

```

Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
Internal Zone
  TCP Protocol
  UDP Protocol
  Other Protocol
External Zone
  TCP Protocol
  UDP Protocol
  Other Protocol
Illegal Zone
  TCP Protocol
  UDP Protocol
  Other Protocol
sensor#

```

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

```

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

```

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

```

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

  Denied Attackers with percent denied and hit count for each.

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

  Denied Attackers with percent denied and hit count for each.

sensor#

```

**Step 6** Display the statistics for the Event Server.

```

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

```

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

```

sensor# show statistics event-store
EEvent store statistics
  General information about the event store
    The current number of open subscriptions = 2
    The number of events lost by subscriptions and queries = 0
    The number of filtered events not written to the event store = 850763
    The number of queries issued = 0
    The number of times the event store circular buffer has wrapped = 0
  Number of events of each type currently stored
    Status events = 4257

```

```

Shun request events = 0
Error events, warning = 669
Error events, error = 8
Error events, fatal = 0
Alert events, informational = 0
Alert events, low = 0
Alert events, medium = 0
Alert events, high = 0
Alert events, threat rating 0-20 = 0
Alert events, threat rating 21-40 = 0
Alert events, threat rating 41-60 = 0
Alert events, threat rating 61-80 = 0
Alert events, threat rating 81-100 = 0
Cumulative number of each type of event
Status events = 4257
Shun request events = 0
Error events, warning = 669
Error events, error = 8
Error events, fatal = 0
Alert events, informational = 0
Alert events, low = 0
Alert events, medium = 0
Alert events, high = 0
Alert events, threat rating 0-20 = 0
Alert events, threat rating 21-40 = 0
Alert events, threat rating 41-60 = 0
Alert events, threat rating 61-80 = 0
Alert events, threat rating 81-100 = 0
sensor#

```

**Step 8** Display the statistics for global correlation.

```

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

```

**Step 9** Display the statistics for the host.

```

sensor# show statistics host
General Statistics
  Last Change To Host Config (UTC) = 15-Oct-2013 09:11:13
  Command Control Port Device = Management0/0
Network Statistics
  = ma0_0      Link encap:Ethernet  HWaddr 00:06:F6:2B:48:4C

```

```

    =          inet addr:10.106.132.150  Bcast:10.106.133.255  Mask:255.255.254
.0
    =          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    =          RX packets:429575 errors:0 dropped:0 overruns:0 frame:0
    =          TX packets:5492 errors:0 dropped:0 overruns:0 carrier:0
    =          collisions:0 txqueuelen:100
    =          RX bytes:30017118 (28.6 MiB)  TX bytes:1064828 (1.0 MiB)
    =          Base address:0xe000 Memory:fb800000-fb820000
NTP Statistics
  status = Not applicable
Memory Usage
  usedBytes = 6630588416
  freeBytes = 1615556608
  totalBytes = 8246145024
CPU Statistics
  Note: CPU Usage statistics are not a good indication of the sensor processing
  load. The Inspection Load Percentage in the output of 'show inspection-load' sh
  ould be used instead.
  Usage over last 5 seconds = 100
  Usage over last minute = 100
  Usage over last 5 minutes = 99
  Usage over last 5 seconds = 2
  Usage over last minute = 1
  Usage over last 5 minutes = 1
  Usage over last 5 seconds = 100
  Usage over last minute = 100
  Usage over last 5 minutes = 100
  Usage over last 5 seconds = 100
  Usage over last minute = 100
  Usage over last 5 minutes = 100
Memory Statistics
  Memory usage (bytes) = 6630588416
  Memory free (bytes) = 1615556608
Auto Update Statistics
  lastDirectoryReadAttempt = N/A
  lastDownloadAttempt = N/A
  lastInstallAttempt = N/A
  nextAttempt = N/A
Auxiliary Processors Installed
sensor#

```

**Step 10** Display the statistics for the logging application.

```

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

```

**Step 11** Display the statistics for the ARC.

```

sensor# show statistics network-access

```

```

Current Configuration
  LogAllBlockEventsAndSensors = true
  EnableNvramWrite = false
  EnableAclLogging = false
  AllowSensorBlock = false
  BlockMaxEntries = 11
  MaxDeviceInterfaces = 250
NetDevice
  Type = PIX
  IP = 10.89.150.171
  NATAddr = 0.0.0.0
  Communications = ssh-3des
NetDevice
  Type = PIX
  IP = 192.0.2.4
  NATAddr = 0.0.0.0
  Communications = ssh-3des
NetDevice
  Type = PIX
  IP = 192.0.2.5
  NATAddr = 0.0.0.0
  Communications = telnet
NetDevice
  Type = Cisco
  IP = 192.0.2.6
  NATAddr = 0.0.0.0
  Communications = telnet
  BlockInterface
    InterfaceName = ethernet0/1
    InterfaceDirection = out
    InterfacePostBlock = Post_Acl_Test
  BlockInterface
    InterfaceName = ethernet0/1
    InterfaceDirection = in
    InterfacePreBlock = Pre_Acl_Test
    InterfacePostBlock = Post_Acl_Test
NetDevice
  Type = CAT6000_VACL
  IP = 192.0.2.1
  NATAddr = 0.0.0.0
  Communications = telnet
  BlockInterface
    InterfaceName = 502
    InterfacePreBlock = Pre_Acl_Test
  BlockInterface
    InterfaceName = 507
    InterfacePostBlock = Post_Acl_Test
State
  BlockEnable = true
NetDevice
  IP = 192.0.2.3
  AclSupport = Does not use ACLs
  Version = 6.3
  State = Active
  Firewall-type = PIX
NetDevice
  IP = 192.0.2.7
  AclSupport = Does not use ACLs
  Version = 7.0
  State = Active
  Firewall-type = ASA
NetDevice
  IP = 102.0.2.8
  AclSupport = Does not use ACLs

```

```

    Version = 2.2
    State = Active
    Firewall-type = FWSM
NetDevice
  IP = 192.0.2.9
  AclSupport = uses Named ACLs
  Version = 12.2
  State = Active
NetDevice
  IP = 192.0.2.10
  AclSupport = Uses VACLs
  Version = 8.4
  State = Active
BlockedAddr
  Host
    IP = 203.0.113.1
    Vlan =
    ActualIp =
    BlockMinutes =
  Host
    IP = 203.0.113.2
    Vlan =
    ActualIp =
    BlockMinutes =
  Host
    IP = 203.0.113.4
    Vlan =
    ActualIp =
    BlockMinutes = 60
    MinutesRemaining = 24
  Network
    IP = 203.0.113.9
    Mask = 255.255.0.0
    BlockMinutes =
sensor#

```

**Step 12** Display the statistics for the notification application.

```

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

```

**Step 13** Display the statistics for OS identification.

```

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

```

**Step 14** Display the statistics for the SDEE server.

```

sensor# show statistics sdee-server
General
  Open Subscriptions = 1
  Blocked Subscriptions = 1
  Maximum Available Subscriptions = 5
  Maximum Events Per Retrieval = 500
Subscriptions

```

```

sub-4-d074914f
  State = Read Pending
  Last Read Time = 23:54:16 UTC Wed Nov 30 2011
  Last Read Time (nanoseconds) = 1322697256078549000
sensor#

```

**Step 15** Display the statistics for the transaction server.

```

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

```

**Step 16** Display the statistics for a virtual sensor.

```

sensor# show statistics virtual-sensor vs0

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 = 318712
  MemoryAlloPercent = 13
  MemoryUsedPercent = 13
  MemoryMaxCapacity = 5500000
  MemoryMaxHighUsed = 750721
  MemoryCurrentAllo = 769921
  MemoryCurrentUsed = 750721
  Inspection Load Percentage = 0
  Total packets processed since reset = 0
  Total IP packets processed since reset = 0
  Total IPv4 packets processed since reset = 0
  Total IPv6 packets processed since reset = 0
  Total IPv6 AH packets processed since reset = 0
  Total IPv6 ESP packets processed since reset = 0
  Total IPv6 Fragment packets processed since reset = 0
  Total IPv6 Routing Header packets processed since reset = 0
  Total IPv6 ICMP packets processed since reset = 0
  Total packets that were not IP processed since reset = 0
  Total TCP packets processed since reset = 0
  Total UDP packets processed since reset = 0
  Total ICMP packets processed since reset = 0
  Total packets that were not TCP, UDP, or ICMP processed since reset = 0
  Total ARP packets processed since reset = 0
  Total ISL encapsulated packets processed since reset = 0
  Total 802.1q encapsulated packets processed since reset = 0
  Total GRE Packets processed since reset = 0
  Total GRE Fragment Packets processed since reset = 0
  Total GRE Packets skipped since reset = 0
  Total GRE Packets with Bad Header skipped since reset = 0
  Total IpIp Packets with Bad Header skipped since reset = 0
  Total Encapsulated Tunnel Packets with Bad Header skipped since reset = 0
  Total packets with bad IP checksums processed since reset = 0
  Total packets with bad layer 4 checksums processed since reset = 0
  Total cross queue TCP packets processed since reset = 0
  Total cross queue UDP packets processed since reset = 0
  HTTP transfer encoding errors = 0
  HTTP content encoding errors = 0
  HTTP character encoding errors = 0
  HTTP connection out of sync = 0
  HTTP pipelining or persistence out of sync = 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.

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

```

```

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

```

**Step 17** Display the statistics for the web server.

```

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

```

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

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

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

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

---

## Interfaces Information

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, page E-75](#)
- [Interfaces Command Output, page E-76](#)

### 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 = 141600
  Total Bytes Received = 13821462
  Missed Packet Percentage = 0
  Current Bypass Mode = Off
MAC statistics from interface GigabitEthernet0/0
  Interface function = Sensing interface
  Description =
  Media Type = TX
  Default VLAN = 0
  Inline Mode = Unpaired
  Pair Status = N/A
  Hardware Bypass Capable = No
  Hardware Bypass Paired = N/A
  Link Status = Down
  Admin Enabled Status = Disabled
  Link Speed = N/A
  Link Duplex = N/A
  Missed Packet Percentage = 0
  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 Management0/0
  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 = 429895
  Total Bytes Received = 30039696
  Total Multicast Packets Received = 0
  Total Receive Errors = 0
  Total Receive FIFO Overruns = 0
  Total Packets Transmitted = 5567
  Total Bytes Transmitted = 1081130
```

```
Total Transmit Errors = 0
Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/1
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/2
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/3
Interface function = Sensing interface
```

```

Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/4
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/5
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired

```

```

Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
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 GigabitEthernet0/6
Interface function = Sensing interface
Description =
Media Type = TX
Default VLAN = 0
Inline Mode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Down
Admin Enabled Status = Disabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
--MORE--

```

## 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, page E-79](#)
- [Understanding the show events Command, page E-80](#)
- [Displaying Events, page E-80](#)
- [Clearing Events, page E-83](#)

## 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.

---



### Note

---

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

---

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

The following options apply:

- **alert**—Displays alerts. Provides notification of some suspicious activity that may indicate an attack is in process or has been attempted. Alert events are generated by the Analysis Engine whenever a signature is triggered by network activity. If no level is selected (informational, low, medium, or high), all alert events are displayed.
- **include-traits**—Displays alerts that have the specified traits.
- **exclude-traits**—Does not display alerts that have the specified traits.
- **traits**—Specifies the trait bit position in decimal (0 to 15).



- **min-threat-rating**—Displays events with a threat rating above or equal to this value. The default is 0. The valid range is 0 to 100.
- **max-threat-rating**—Displays events with a threat rating below or equal to this value. The default is 100. The valid range is 0 to 100.
- **error**—Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
- **NAC**—Displays the ARC (block) requests.



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

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



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

### Displaying Events

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

- Step 1** Log in to the CLI.
- Step 2** Display all events starting now. The feed continues showing all events until you press **Ctrl-C**.

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

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

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

```
sensor# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
```

```

srcAddr: 11.0.0.1
destAddr:
srcPort:
destPort:
protocol: numericType=0 other
timeoutMinutes: 40
evAlertRef: hostId=esendHost 123456789012345678
sensor#

```

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

```

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

```

**Step 5** Display alerts from the past 45 seconds.

```

sensor# show events alert past 00:00:45

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

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

```

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

```

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

```

```
appInstanceId: 2316
```

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

---

## Clearing Events

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

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

---

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

**Step 2** Clear the Event Store.

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

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

---

## cidDump Script

If you do not have access to the IDM, the IME, or the CLI, you can run the underlying script `cidDump` from the service account by logging in as root and running `/usr/cids/idsRoot/bin/cidDump`. The path of the `cidDump` file is `/usr/cids/idsRoot/htdocs/private/cidDump.html`. `cidDump` is a script that captures a large amount of information including the IPS processes list, log files, OS information, directory listings, package information, and configuration files.

To run the `cidDump` script, follow these steps:

---

**Step 1** Log in to the sensor service account.

**Step 2** **su** to **root** using the service account password.

**Step 3** Enter the following command.

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

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

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

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

---

**For More Information**

For the procedure for putting a file on the Cisco FTP site, see [Uploading and Accessing Files on the Cisco FTP Site, page E-84](#).

## 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.
-