Release Notes for Cisco Intrusion Prevention System 7.1(3)E4

Published: December 5, 2011, OL-25881-01

Revised: November 9, 2013

Contents

- IPS File List, page 2
- Supported Platforms, page 3
- Supported Servers, page 3
- ROMMON and TFTP, page 4
- IPS Management and Event Viewers, page 4
- New and Changed Information, page 5
- AC Power Supply in the IPS 4300 Series V01 and V02 Chassis, page 6
- The IDM and JRE 1.7, page 6
- The ASA 5500-X IPS SSP and Memory Usage, page 6
- The Sensor and Jumbo Packet Frame Size, page 7
- The ASA IPS Modules and Jumbo Packets, page 7
- Obtaining Software, page 7
- Upgrading to IPS 7.1(3)E4, page 9
- Reimaging the Sensor, page 12
- Licensing the Sensor, page 25
- Initializing the Sensor, page 29
- Logging In to the IDM, page 49
- Installing or Upgrading the IME, page 50
- Enabling Anomaly Detection, page 52

Cisco Systems, Inc.
www.cisco.com

- Disabling Anomaly Detection, page 54
- Cisco Security Intelligence Operations, page 55
- Restrictions and Limitations, page 56
- Caveats, page 57
- Related Documentation, page 59
- Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request, page 60

IPS File List

The following files are part of Cisco IPS 7.1(3)E4:

- Readme
  - IPS-7.1-3-E4_readme.txt
- Minor Version Upgrade Files
  - IPS-4270_20-K9-7.1-3-E4.pkg
  - IPS-SSP_10-K9-7.1-3-E4.pkg
  - IPS-SSP_20-K9-7.1-3-E4.pkg
  - IPS-SSP_40-K9-7.1-3-E4.pkg
  - IPS-SSP_60-K9-7.1-3-E4.pkg
- System Image Files
  - IPS-4270_20-K9-sys-1.1-a-7.1-3-E4.img
  - IPS-4345-K9-sys-1.1-a-7.1-3-E4.img
  - IPS-4360-K9-sys-1.1-a-7.1-3-E4.img
  - IPS-SSP_5512-K9-sys-1.1-a-7.1-3-E4.aip
  - IPS-SSP_5515-K9-sys-1.1-a-7.1-3-E4.aip
  - IPS-SSP_5525-K9-sys-1.1-a-7.1-3-E4.aip
  - IPS-SSP_5545-K9-sys-1.1-a-7.1-3-E4.aip
  - IPS-SSP_5555-K9-sys-1.1-a-7.1-3-E4.aip
  - IPS-SSP_10-K9-sys-1.1-a-7.1-3-E4.img
  - IPS-SSP_20-K9-sys-1.1-a-7.1-3-E4.img
  - IPS-SSP_40-K9-sys-1.1-a-7.1-3-E4.img
  - IPS-SSP_60-K9-sys-1.1-a-7.1-3-E4.img
- Recovery Image Files
  - IPS-4270_20-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-4345-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-4360-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_5512-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_5515-K9-r-1.1-a-7.1-3-E4.pkg

  - IPS-SSP_5525-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_5545-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_5555-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_10-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_20-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_40-K9-r-1.1-a-7.1-3-E4.pkg
  - IPS-SSP_60-K9-r-1.1-a-7.1-3-E4.pkg

Supported Platforms

Cisco IPS 7.1(3)E4 is supported on the following platforms:

- IPS 4270-20
- IPS 4345
- IPS 4360
- ASA 5512-X IPS SSP
- ASA 5515-X IPS SSP
- ASA 5525-X IPS SSP
- ASA 5545-X IPS SSP
- ASA 5555-X IPS SSP
- ASA 5585-X IPS SSP-10
- ASA 5585-X IPS SSP-20
- ASA 5585-X IPS SSP-40
- ASA 5585-X IPS SSP-60

Supported Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- CSM - Apache Server (Tomcat)
- CSM - Apache Server (JRun)

ROMMON and TFTP

ROMMON uses TFTP to download an image and launch it. TFTP does not address network issues such as latency or error recovery. It does implement a limited packet integrity check so that packets arriving in sequence with the correct integrity value have an extremely low probability of error. But TFTP does not offer pipelining so the total transfer time is equal to the number of packets to be transferred times the network average RTT. Because of this limitation, we recommend that the TFTP server be located on the same LAN segment as the sensor. Any network with an RTT less than a 100 milliseconds should provide reliable delivery of the image. Be aware that some TFTP servers limit the maximum file size that can be transferred to ~32 MB.

IPS Management and Event Viewers

Use the following tools for configuring Cisco IPS 7.1(3)E4 sensors:

- Cisco IDM 7.1.3

  IDM 7.1.3 is included within the IPS 7.1(3)E4 files.

  IDM 7.1.3 is included within IME 7.2.1.

  IDM 7.1.3 requires JRE 1.6 or later.

  You can use IDM 7.1.3 to configure IPS 6.2, 7.0, and 7.1 sensors.

- Cisco IME 7.2.1

  You can use IME 7.2.1 to configure IPS 6.1, 6.2, 7.0, and 7.1 sensors. Although IME 7.2.1 supports the new platforms (IPS 4345, IPS 4360, and ASA 5500-X IPS SSP), they are not yet referenced in the online help.

- IPS CLI included in IPS 7.1.
- Cisco ASDM 6.3.4 and later.

Use the following tools for monitoring Cisco IPS 7.1(3)E4 sensors:

- IDM 7.1.3
- IME 7.2.1
- MARS minimum version 5.2 and latest version 6.0.5
- CSM 4.0 and later

Note CSM 4.0(2) does not support the IPS 4270-20.

Note You may need to configure viewers that are already configured to monitor the earlier version sensors to accept a new SSL certificate for the Cisco IPS 7.1 sensors.

New and Changed Information

Cisco IPS 7.1(3)E4 contains the following new and changed information:

- Support for the IPS 4345, IPS 4360, and the ASA 5500-X IPS SSP series.
- Although IME 7.2.1 supports the new platforms (IPS 4345, IPS 4360, and ASA 5500-X IPS SSP), the online help does not reference them.
- Contains signature update S605.
- Adds support for the IPS 4270-20 in addition to continuing support for the ASA 5585-X IPS SSP.
- Adds AAA RADIUS support to IPS 7.1(3)E4 and later.

  You can configure the IPS to use remote RADIUS servers to manage user accounts. This feature simplifies the operation of large IPS deployments.
- Adds the CLI idle timeout feature—You can now configure a CLI idle timeout feature, which times out the CLI if the session is inactive for more than the configured value.

  The CLI idle timeout feature enhances the security of the IPS. The CLI timeout feature is applicable only for sessions established through SSH, Telnet, and the console. Service account logins are not affected.
- Adds packet command restriction—You can configure packet command restriction for local and AAA RADIUS users.

  This feature is used to prevent users from arbitrarily executing **packet capture/display and iplog** commands. You configure the packet capture/display and iplog restrictions for AAA RADIUS users using a Cisco av-pair (**permit-packet-logging=true/false**) and for local users using a CLI configuration. By default there is no restriction to the commands. Only users with an administrator role can change the settings of the packet command restriction feature.
- Adds SNMP health monitoring—SNMP can now get health and security-related data.

  You can configure the sensor to send trap-related information for various health metrics. To receive sensor health information through SNMP, you must have sensor health metrics enabled.
- On systems that have both ASA and IPS, additional data is transferred along with the packets. In some cases, this causes the count of jumbo packets to be inflated by the backplane interfaces as viewed by the IPS. For the appropriate jumbo packet counts, refer to the ASA packet counts.

For More Information

- For more information about AAA RADIUS authentication, for the IDM see Configuring Authentication and Users, for the IME see Configuring Authentication and Users, and for the CLI see Configuring User Parameters.
- For more information about SNMP, for the IDM see Configuring SNMP, for the IME see Configuring SNMP, and for the CLI see Configuring SNMP.

AC Power Supply in the IPS 4300 Series V01 and V02 Chassis

The Cisco IPS 4300 series sensors with the AC power supply can restore the previous power state of the system if AC power is lost. Earlier IPS 4300s (V01) require you to turn on the power with the power switch. Newer IPS 4300s (V02) automatically turn on when you plug in the power cable.

To determine your version, do one of the following:

- At the CLI, enter the **show inventory** command and look for V01 or V02 in the output.
- On the back of the chassis, look at the VID PID label for V01 or V02.

The V01 chassis has the following limitations (these limitations do not apply to the V02 chassis):

- The sensor requires 50 seconds from the time that AC power is applied before the power state can be updated and stored. This means that any changes to the power state within the first 50 seconds of applying AC power will not be observed if AC power is removed within that time.
- The sensor requires 10 seconds from the time it is placed into standby mode before the power state can be updated and stored. This means any changes to the power state within the first 10 seconds of entering standby mode (including the standby mode itself) will not be observed if AC power is removed within that time.

For More Information

For information on the AC power supplies in the IPS 4300 series sensors, refer to Installing the IPS 4345 and IPS 4360.

The IDM and JRE 1.7

In IPS versions 7.1(1)E4 through 7.1(5)E4, the IDM fails to connect to the sensor due to a failure during the initial handshake, because the web server is not RFC 5746-compliant. Try the following workaround.

Problem Cannot launch the IDM, when the IDM is running under JRE 1.7 with IPS 7.1(1)E4 through 7.1(5)E4.

Solution Use JRE 1.6 or enable the SSL 2.0-compatible ClientHello format in the Java settings under Control Panel.

The ASA 5500-X IPS SSP and Memory Usage

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

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

Table 1 lists the Yellow Threshold and the Red Threshold health values.

Table 1 ASA 5500-X IPS SSP Memory Usage Values

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

For More Information

For the procedure for configuring sensor health metrics, for the IDM refer to Configuring Sensor Health, for the IME refer to Configuring Sensor Health, and for the CLI refer to Configuring Health Status Information.

The Sensor and Jumbo Packet Frame Size

For IPS standalone appliances with 1 G and 10 G fixed or add-on interfaces, the maximum jumbo frame size is 9216 bytes. For integrated IPS sensors, such as the ASA 5500-X and ASA 5585-X series, refer to the following URL for information:

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/interface_start.html#wp1328869

Note A jumbo frame is an Ethernet packet that is larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS).

The ASA IPS Modules and Jumbo Packets

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

Obtaining Software

You can find major and minor updates, service packs, signature and signature engine updates, system and recovery files, firmware upgrades, and Readmes on the Download Software site on Cisco.com. Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com in a release train format, a new release every three months. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

You must have an account with cryptographic access before you can download software. You set this account up the first time you download IPS software from the Download Software site.

Note You must be logged in to Cisco.com to download software. You must have an active IPS maintenance contract and a Cisco.com password to download software. You must have a sensor license to apply signature updates.

Downloading Cisco IPS Software

To download software on Cisco.com, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 From the Support drop-down menu, choose **Download Software**.

Step 3 Under Select a Software Product Category, choose **Security Software**.

Step 4 Choose **Intrusion Prevention System (IPS)**.

Step 5 Enter your username and password.

Step 6 In the Download Software window, choose **IPS Appliances > Cisco Intrusion Prevention System** and then click the version you want to download.

Note You must have an IPS subscription service license to download software.

Step 7 Click the type of software file you need. The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.

Step 8 Click the file you want to download. The file details appear.

Step 9 Verify that it is the correct file, and click **Download**.

Step 10 Click **Agree** to accept the software download rules. The File Download dialog box appears. The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.

a. Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.

b. Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again.

Step 11 Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme or the Release Notes to install the update.

Upgrading to IPS 7.1(3)E4

This section describes how to upgrade the IPS 4270-20 and the ASA 5585-X IPS SSP series, and contains the following topics:

- Upgrade Notes and Caveats, page 9
- Upgrading the Sensor, page 10

Upgrade Notes and Caveats

Pay attention to the following upgrade notes and caveats when upgrading to IPS 7.1(3)E4:

- If you are upgrading the IPS 4270-20 and you have a license for 6.0.*x* and earlier, you receive the following error message:

  ```
  Currently installed License is not valid in 7.1(3). Install a license that is
  applicable for IPS versions 6.1 and above.
  ```

  You must get a new license before upgrading your IPS 4270-20.
- Anomaly detection has been disabled by default. If you did not configure the operation mode manually before the upgrade, it defaults to inactive after you upgrade to IPS 7.1(3)E4. If you configured the operation mode to detect, learn, or inactive, the tuned value is preserved after the upgrade.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- You must have a valid maintenance contract per sensor to download software upgrades from Cisco.com.
- For the ASA 5585-X IPS SSP series, you must be running IPS 7.1(1)E4 or later to upgrade to IPS 7.1(3)E4. For the IPS 4270-20, you must be running IPS 6.0(6) or later.
- This service pack automatically reboots the sensor to apply the changes. During reboot, inline network traffic is disrupted.
- You cannot uninstall 7.1(3)E4. To revert to a previous version, you must reimage the sensor using the appropriate system image file

For More Information

- For the procedure to download software from Cisco.com, see Obtaining Software, page 7.
- For the procedure for using the **upgrade** command to upgrade the sensor, see Upgrading the Sensor, page 10.
- For the procedure for using ROMMON to restore the IPS 4270-20 system image, see Installing the IPS 4270-20 System Image, page 12.
- For the procedure for installing the ASA 5500-X IPS SSP system image, see Installing the ASA 5500-X IPS SSP System Image, page 18.
- For the procedure for installing the ASA 5585-X IPS SSP system image, see Installing the ASA 5585-X IPS SSP System Image, page 19.

Upgrading the Sensor

Use the **upgrade** *source-url* command to apply service pack, signature update, engine update, minor version, major version, or recovery partition file upgrades.

The following options apply:

- *source-url*—Specifies the location of the source file to be copied:
  - ftp:—Source 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 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.

Upgrading the Sensor

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the sensor.

```
sensor(config)# upgrade url/IPS-SSP_10-K9-7.1-3-E4.pkg
```

The URL points to where the update file is located, for example, to retrieve the update using FTP, enter the following:

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-SSP_10-K9-7.1-3-E4.pkg
```

Step 5 Enter the password when prompted.

```
Enter password: ********
```

Step 6 Enter **yes** to complete the upgrade.

Note Major updates, minor updates, and service packs may force a restart of the IPS processes or even force a reboot of the sensor to complete installation.

Note The operating system is reimaged and all files that have been placed on the sensor through the service account are removed.

Step 7 Verify your new sensor version.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(3)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S605.0              2011-10-25
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS10
Serial Number:          123456789AB
No license present
Sensor up-time is 11 days.
Using 4395M out of 5839M bytes of available memory (75% usage)
system is using 26.2M out of 160.0M bytes of available disk space (16% usage)
application-data is using 69.6M out of 171.6M bytes of available disk space (43%
 usage)
boot is using 57.3M out of 70.5M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600   Running
AnalysisEngine     S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600   Running
CollaborationApp   S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600   Running
CLI                S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600

Upgrade History:

  IPS-K9-7.1-3-E4   00:30:07 UTC Wed Nov 16 2011

Recovery Partition Version 1.1 - 7.1(3)E4
```

```
Host Certificate Valid from: 16-Nov-2011 to 16-Nov-2013
sensor#
```

For More Information

For a list of the specific IPS upgrade filenames, see IPS File List, page 2.

Reimaging the Sensor

This section describes how to reimage the sensor using the system image, and contains the following topics:

- Installing the IPS 4270-20 System Image, page 12
- Installing the IPS 4345 and IPS 4360 System Image, page 15
- Installing the ASA 5500-X IPS SSP System Image, page 18
- Installing the ASA 5585-X IPS SSP System Image, page 19

Installing the IPS 4270-20 System Image

You can install the IPS 4270-20 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4270-20 system image, follow these steps:

Step 1 Download the IPS 4270-20 system image file to the tftp root directory of a TFTP server that is accessible from your IPS 4270-20.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4270-20.

Step 2 Boot the IPS 4270-20.

```
Booting system, please wait...
Cisco Systems ROMMON Version (1.0(12)10) #7: Thu Jun 21 13:50:04 CDT 2007

ft_id_update: Invalid ID-PROM Controller Type (0x5df)

ft_id_update: Defaulting to Controller Type (0x5c2)
```

Note The controller type errors are a known issue and can be disregarded.

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
```

```
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set

ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

The variables have the following definitions:

- Address—Specifies the local IP address of the IPS 4270-20.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the IPS 4270-20.
- Port—Specifies the Ethernet interface used for IPS 4270-20 management.
- VLAN—Specifies the VLAN ID number (leave as untagged).
- Image—Specifies the system image file/path name.
- Config—Unused by these platforms.

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, assign an IP address for the local port on the IPS 4270-20.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4270-20.

Step 6 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 7 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

UNIX Example

```
rommon> IMAGE=/system_images/IPS-4270_20-K9-sys-1.1-a-7.1-3-E4.img
```

Note The path is relative to the UNIX TFTP server default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=\system_images\IPS-4270_20-K9-sys-1.1-a-7.1-3-E4.img
```

Step 10 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 11 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4270-20 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4270-20. Be sure to use the IPS 4270-20 image.

For More Information

- For the procedure for locating software, see Obtaining Software, page 7.
- For a list of supported TFTP servers, see Supported Servers, page 3.
- For a list of the specific IPS software files, see IPS File List, page 2.
- For the procedure for initializing the sensor with the **setup** command, see Initializing the Sensor, page 29.

Installing the IPS 4345 and IPS 4360 System Image

You can install the IPS 4345 and IPS 4360 system image by using the ROMMON on the appliance to TFTP the system image on to the compact flash device.

Note This procedure is for IPS 4345, but is also applicable to IPS 4360. The system image for IPS 4360 has "4360" in the filename.

To install the IPS 4345 and IPS 4360 system image, follow these steps:

Step 1 Download the IPS 4345 system image file to the tftp root directory of a TFTP server that is accessible from your IPS 4345.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4345.

Step 2 Boot the IPS 4345.

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90

Low Memory: 631 KB
High Memory: 2048 MB
PCI Device Table.
Bus  Dev  Func  VendID  DevID  Class              Irq
00   00   00    8086    2578   Host Bridge
00   01   00    8086    2579   PCI-to-PCI Bridge
00   03   00    8086    257B   PCI-to-PCI Bridge
00   1C   00    8086    25AE   PCI-to-PCI Bridge
00   1D   00    8086    25A9   Serial Bus         11
00   1D   01    8086    25AA   Serial Bus         10
00   1D   04    8086    25AB   System
00   1D   05    8086    25AC   IRQ Controller
00   1D   07    8086    25AD   Serial Bus         9
00   1E   00    8086    244E   PCI-to-PCI Bridge
00   1F   00    8086    25A1   ISA Bridge
00   1F   02    8086    25A3   IDE Controller     11
00   1F   03    8086    25A4   Serial Bus         5
00   1F   05    8086    25A6   Audio              5
02   01   00    8086    1075   Ethernet           11
03   01   00    177D    0003   Encrypt/Decrypt    9
03   02   00    8086    1079   Ethernet           9
03   02   01    8086    1079   Ethernet           9
03   03   00    8086    1079   Ethernet           9
03   03   01    8086    1079   Ethernet           9
04   02   00    8086    1209   Ethernet           11
04   03   00    8086    1209   Ethernet           5

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004

Platform IPS-4345-K9
Management0/0
```

```
MAC Address: 0000.c0ff.ee01
```

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon> set

ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
      PORT=Management0/0
      VLAN=untagged
      IMAGE=
      CONFIG=
```

The variables have the following definitions:

- Address—Local IP address of the IPS 4345.
- Server—TFTP server IP address where the application image is stored.
- Gateway—Gateway IP address used by the IPS 4345.
- Port—Ethernet interface used for the IPS 4345 management.
- VLAN—VLAN ID number (leave as untagged).
- Image—System image file/path name.
- Config—Unused by these platforms.

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, change the interface used for the TFTP download.

Note The default interface used for TFTP downloads is Management 0/0, which corresponds to the MGMT interface of the IPS 4345.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the IPS 4345.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the IPS 4345.

Step 7 Assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 8 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path file_name
```

Caution Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX Example

```
rommon> IMAGE=system_images IPS-4345-K9-sys-1.1-a-7.1-3-E4.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=system_images IPS-4345-K9-sys-1.1-a-7.1-3-E4.img
```

Step 11 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 12 Download and install the system image.

```
rommon> tftp
```

Caution To avoid corrupting the system image, do not remove power from the IPS 4345 while the system image is being installed.

Note If the network settings are correct, the system downloads and boots the specified image on the IPS 4345. Be sure to use the IPS 4345 image.

For More Information

- For the procedure for locating software, see Obtaining Software, page 7.
- For a list of supported TFTP servers, see Supported Servers, page 3.
- For a list of the specific IPS software files, see IPS File List, page 2.
- For the procedure for initializing the sensor with the **setup** command, see Initializing the Sensor, page 29.

Installing the ASA 5500-X IPS SSP System Image

Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

To install the system image on the ASA 5500-X IPS SSP, follow these steps:

Step 1 Download the IPS system image file corresponding to your ASA platform to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of the adaptive security appliance.

Step 2 Log in to the adaptive security appliance.

Step 3 Enter enable mode.

```
asa> enable
```

Step 4 Copy the IPS image to the disk0 flash of the adaptive security appliance.

```
asa# copy tftp://192.0.2.0/directory/IPS-5545-K9-sys-1.1-a-7.1-3-E4.aip disk0:
```

Step 5 Image the ASA 5500-X IPS SSP.

```
asa# sw-module module ips recover configure image
disk0:/IPS-SSP_5545-K9-sys-1.1-a-7.1-3-E4.aip
```

Step 6 Execute the recovery. This transfers the image from the TFTP server to the ASA 5500-X IPS SSP and restarts it.

```
asa# sw-module module ips recover boot
```

Step 7 Periodically check the recovery until it is complete.

```
asa# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 Cisco ASA 5545 Appliance with 8 GE ports, 1  ASA5545            ABC1234D56E
```

```
  1 IPS 5545 Intrusion Protection System         IPS5545            ABC1234D56E

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---  --------------------------------- ------------ ------------ -------------
0    503d.e59c.6dc1 to 503d.e59c.6dca  1.0                       8.6.1
ips  503d.e59c.6dcb to 503d.e59c.6dcb  N/A          N/A          7.1(3)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.1(3)E4

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

asa#
```

Note The Status field in the output indicates the operational status of the ASA 5500-X IPS SSP. An ASA 5500-X IPS SSP operating normally shows a status of "Up." While the adaptive security appliance transfers an application image to the ASA 5500-X IPS SSP, the Status field in the output reads "Recover." When the adaptive security appliance completes the image transfer and restarts the ASA 5500-X IPS SSP, the newly transferred image is running.

Note To debug any errors that may happen in the recovery process, use the **debug module-boot** command to enable debugging of the system reimaging process.

Step 8 Session to the ASA 5500-X IPS SSP and initialize it with the **setup** command.

For More Information

- For the procedure for locating software, see Obtaining Software, page 7.
- For a list of supported TFTP servers, see Supported Servers, page 3.
- For a list of the specific IPS software files, see IPS File List, page 2.
- For the procedure for initializing the sensor with the **setup** command, see Initializing the Sensor, page 29.

Installing the ASA 5585-X IPS SSP System Image

This section describes how to install the ASA 5585-X IPS SSP system image using the **hw-module** command or ROMMON, and contains the following topics:

- Using the hw-module Command, page 20
- Using ROMMON, page 22

Using the hw-module Command

To install the system image, transfer the software image from a TFTP server to the ASA 5585-X IPS SSP using the adaptive security appliance CLI. The adaptive security appliance can communicate with the ROMMON application of the ASA 5585-X IPS SSP to transfer the image.

Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

Note This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

To install the ASA 5585-X IPS SSP software image, follow these steps:

Step 1 Download the ASA 5585-X IPS SSP system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your adaptive security appliance.

Step 2 Log in to the adaptive security appliance.

Step 3 Enter enable mode.

```
asa# enable
```

Step 4 Configure the recovery settings for the ASA 5585-X IPS SSP.

```
asa (enable)# hw-module module 1 recover configure
```

Note If you make an error in the recovery configuration, use the **hw-module module 1 recover stop** command to stop the system reimaging and then you can correct the configuration.

Step 5 Specify the TFTP URL for the software image.

```
Image URL [tftp://0.0.0.0/]:
```

Example

```
Image URL [tftp://0.0.0.0/]: tftp://192.0.2.0/IPS-SSP_40-K9-sys-1.1-a-7.1-3-E4.img
```

Step 6 Specify the command and control interface of the ASA 5585-X IPS SSP.

Note The port IP address is the management IP address of the ASA 5585-X IPS SSP.

```
Port IP Address [0.0.0.0]:
```

Example

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

Step 7 Leave the VLAN ID at 0.

```
VLAN ID [0]:
```

Step 8 Specify the default gateway of the ASA 5585-X IPS SSP.

```
Gateway IP Address [0.0.0.0]:
```

Example

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

Step 9 Execute the recovery. This transfers the software image from the TFTP server to the ASA 5585-X IPS SSP and restarts it.

```
asa# hw-module module 1 recover boot
```

Step 10 Periodically check the recovery until it is complete.

Note The status reads `Recovery` during recovery and reads `Up` when installation is complete.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS40
Hardware version:   1.0
Serial Number:      JAF1350ABSL
Firmware version:   2.0(1)3
Software version:   7.1(3)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(3)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       192.0.2.0
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       10.89.148.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa#
```

Note The Status field in the output indicates the operational status of the ASA 5585-X IPS SSP. An ASA 5585-X IPS SSP operating normally shows a status of "Up." While the adaptive security appliance transfers the software image to the ASA 5585-X IPS SSP, the Status field in the output reads "Recover." When the adaptive security appliance completes the software image transfer and restarts the ASA 5585-X IPS SSP, the newly transferred image is running.

Note To debug any errors that may happen during this process, use the **debug module-boot** command to enable debugging of the software installation process.

Step 11 Session to the ASA 5585-X IPS SSP.

Step 12 Enter **cisco** three times and your new password twice.

Step 13 Initialize the ASA 5585-X IPS SSP with the **setup** command.

For More Information

- For the procedure for locating software, see Obtaining Software, page 7.
- For a list of supported TFTP servers, see Supported Servers, page 3.
- For a list of the specific IPS software files, see IPS File List, page 2.
- For the procedure for initializing the sensor with the **setup** command, see Initializing the Sensor, page 29.

Using ROMMON

You can install the ASA 5585-X IPS SSP system image by using the ROMMON on the adaptive security appliance to TFTP the system image onto the ASA 5585-X IPS SSP.

To install the ASA 5585-X IPS SSP system image, follow these steps:

Step 1 Download the ASA 5585-X IPS SSP system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.

Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your adaptive security appliance.

Step 2 Boot the ASA 5585-X IPS SSP.

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 0.0(2)10 11:16:38 04/15/10
Com KbdBuf SMM UsbHid Msg0 Prompt Pmrt Cache1 LowM ExtM HugeM Cache2 Flg Siz0 Amrt PMM
PnpDsp Smbios Lpt0 Npx1 Apm Lp1 Acpi Typ Dbg Enb Mp MemReduce MemSync1 CallRoms MemSync2
DriveInit


Total memory : 12 GB
Total number of CPU cores : 8
Com Lp1 Admgr2 Brd10 Plx2 OEM0=7EFF5C74
Cisco Systems ROMMON Version (1.0(12)10) #0: Thu Apr  8 00:12:33 CDT 2010

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is UP
MAC Address: 5475.d029.7fa9
```

Step 3 Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

Note You have ten seconds to press **Break** or **Esc**.

```
Use BREAK or ESC to interrupt boot.
```

```
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

Step 4 Check the current network settings.

```
rommon #0> set
ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

The variables have the following definitions:

- Address—Specifies the local IP address of the ASA 5585-X IPS SSP.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the ASA 5585-X IPS SSP.
- Port—Specifies the ethernet interface used for the ASA 5585-X IPS SSP management.
- VLAN—Specifies the VLAN ID number (leave as untagged).
- Image—Specifies the system image file/path name.
- Config—Specifies the unused by these platforms.

Note Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

Step 5 If necessary, change the interface used for the TFTP download.

Note The default interface used for TFTP downloads is Management 0/0, which corresponds to the management interface of the ASA 5585-X IPS SSP.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the ASA 5585-X IPS SSP.

```
rommon> ADDRESS=ip_address
```

Note Use the same IP address that is assigned to the ASA 5585-X IPS SSP.

Step 7 If necessary, assign the TFTP server IP address.

```
rommon> SERVER=ip_address
```

Step 8 If necessary, assign the gateway IP address.

```
rommon> GATEWAY=ip_address
```

Step 9 Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands.

```
rommon> ping server_ip_address
rommon> ping server
```

Step 10 If necessary define the path and filename on the TFTP file server from which you are downloading the image.

```
rommon> IMAGE=path/file_name
```

Caution Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX Example

```
rommon> IMAGE=/system_images/IPS-SSP_10-K9-sys-1.1-a-7.1-3-E4.img
```

Note The path is relative to the default tftpboot directory of the UNIX TFTP server. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows Example

```
rommon> IMAGE=\system_images\IPS-SSP_10-K9-sys-1.1-a-7.1-3-E4.img
```

Step 11 Enter **set** and press **Enter** to verify the network settings.

Note You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must enter this information each time you want to boot an image from ROMMON.

Step 12 Download and install the system image.

```
rommon> tftp
```

Note If the network settings are correct, the system downloads and boots the specified image on the ASA 5585-X IPS SSP. Be sure to use the ASA 5585-X IPS SSP image.

Caution To avoid corrupting the system image, do not remove power from the ASA 5585-X IPS SSP while the system image is being installed.

For More Information

- For the procedure for locating software, see Obtaining Software, page 7.
- For a list of supported TFTP servers, see Supported Servers, page 3.

- For a list of the specific IPS software files, see IPS File List, page 2.
- For the procedure for initializing the sensor with the **setup** command, see Initializing the Sensor, page 29.

Licensing the Sensor

You can install the license key through the CLI, IDM, or IME. This section describes how to obtain and install the license key, and contains the following topics:

- Using the IDM or IME, page 25
- Using the CLI, page 26
- Obtaining a New License for the IPS 4270-20, page 28
- Licensing the ASA 5500-X IPS SSP, page 29

Using the IDM or IME

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

To obtain and install the license key, follow these steps:

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

Step 2 For the IDM choose **Configuration > Sensor Management > Licensing**. For the IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**.

Step 3 The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.

Step 4 Obtain a license key by doing one of the following:

- Click the **Cisco.com** radio button to obtain the license from Cisco.com. The IDM or the IME contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 5.
- Click the **License File** radio button to use a license file. To use this option, you must apply for a license key at this URL: www.cisco.com/go/license. The license key is sent to you in e-mail and you save it to a drive that the IDM or the IME can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.

Step 5 Click **Update License**, and in the Licensing dialog box, click **Yes** to continue. The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.

Step 6 Click **OK**.

Step 7 Log in to Cisco.com.

Step 8 Go to www.cisco.com/go/license.

Step 9 Fill in the required fields. Your license key will be sent to the e-mail address you specified.

Caution You must have the correct IPS device serial number and product identifier (PID) because the license key only functions on the device with that number.

Step 10 Save the license key to a hard-disk drive or a network drive that the client running the IDM or the IME can access.

Step 11 Log in to the IDM or the IME.

Step 12 For the IDM choose **Configuration > Sensor Management > Licensing**. For the IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**.

Step 13 Under Update License, click the **License File** radio button.

Step 14 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 15 Browse to the license file and click **Open**.

Step 16 Click **Update License**.

Using the CLI

Note You cannot install an older license key over a newer license key.

Use the **copy** *source-url license_file_name* **license-key** command to copy the license key to your sensor.

The following options apply:

- *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.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.

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

- ftp:—Source 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 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.

Installing the License Key

To install the license key, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 Apply for the license key at this URL: www.cisco.com/go/license.

Note In addition to a valid Cisco.com username and password, you must also have a Cisco Services for IPS service contract before you can apply for a license key.

Step 3 Fill in the required fields. Your Cisco IPS Signature Subscription Service license key will be sent by email to the e-mail address you specified.

Note You must have the correct IPS device serial number and product identifier (PID) because the license key only functions on the device with that number.

Step 4 Save the license key to a system that has a Web server, FTP server, or SCP server.

Step 5 Log in to the CLI using an account with administrator privileges.

Step 6 Copy the license key to the sensor.

```
sensor# copy scp://user@192.168.1.2/24://tftpboot/dev.lic license-key
Password: *******
```

Step 7 Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(3)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S605.0              2011-10-25
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS10
Serial Number:          123456789AB
No license present
Sensor up-time is 12 days.
Using 4395M out of 5839M bytes of available memory (75% usage)
```

```
system is using 26.2M out of 160.0M bytes of available disk space (16% usage)
application-data is using 69.6M out of 171.6M bytes of available disk space (43% usage)
boot is using 57.3M out of 70.5M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


MainApp            S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600   Running
AnalysisEngine     S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600   Running
CollaborationApp   S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600   Running
CLI                S-2011_NOV_16_00_20_7_1_3_46   (Release)   2011-11-16T00:23:0
6-0600

Upgrade History:

  IPS-K9-7.1-3-E4   00:30:07 UTC Wed Nov 16 2011

Recovery Partition Version 1.1 - 7.1(3)E4

Host Certificate Valid from: 16-Nov-2011 to 16-Nov-2013
sensor#
```

Obtaining a New License for the IPS 4270-20

If your IPS 4270-20 has a license that was generated for IPS 6.0.*x* versions or earlier, you need to get a new license. To obtain a new license for your IPS 4270-20, follow these steps:

Step 1 Log in to Cisco.com.

Step 2 Go to www.cisco.com/go/license.

Step 3 Under Licenses Not Requiring a PAK, click **Demo and Evaluation licenses**.

Step 4 Under Security Products/Cisco Services for IPS service license (Version 6.1 and later), click **All IPS Hardware Platforms**.

Step 5 Fill in the required fields. Your license key will be sent to the email address you specified.

Caution You must have the correct IPS device serial number and product identifier (PID) because the license key only functions on the device with that number.

Step 6 Save the license key to a hard-disk drive or a network drive that the client running the IDM or the IME can access.

Step 7 Log in to the IDM or the IME.

Step 8 For the IDM choose **Configuration > Sensor Management > Licensing**. For the IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**.

Step 9 Under Update License, click the **License File** radio button.

Step 10 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 11 Browse to the license file and click **Open**.

Step 12 Click **Update License**.

Licensing the ASA 5500-X IPS SSP

For the ASA 5500-X series adaptive security appliances with the IPS SSP, the ASA requires the IPS Module license. To view your current ASA licenses, in ASDM choose **Home > Device Dashboard > Device Information > Device License**. For more information about ASA licenses, refer to the licensing chapter in the configuration guide. After you obtain the ASA IPS Module license, you can obtain and install the IPS license key.

For More Information

- For more information about getting started using the ASA 5500-X IPS SSP, refer to the *Cisco IPS Module on the ASA Quick Start Guide*.
- For the procedures for obtaining and installing the IPS License key, see Licensing the Sensor, page 25.

Initializing the Sensor

This section describes how to initialize the sensor using the **setup** command, and contains the following sections:

- Understanding Initialization, page 29
- Simplified Setup Mode, page 30
- System Configuration Dialog, page 30
- Basic Sensor Setup, page 32
- Advanced Setup for the IPS 4270-20, IPS 4345, and IPS 4360, page 35
- Advanced Setup for the ASA 5500-X IPS SSP, page 40
- Advanced Setup for the ASA 5585-X IPS SSP, page 44
- Verifying Initialization, page 47

Understanding Initialization

Note You must be administrator to use the **setup** command.

After you install the sensor on your network, you must use the **setup** command to initialize it so that you can communicate with it over the network. You cannot use the IDM or the IME to configure the sensor until you initialize the sensor using the **setup** command.

With the **setup** command, you configure basic sensor settings, including the hostname, IP interfaces, access control lists, global correlation servers, and time settings. You can continue using advanced setup in the CLI to enable Telnet, configure the web server, and assign and enable virtual sensors and interfaces, or you can use the Startup Wizard in the IDM or the IME. After you configure the sensor with the **setup** command, you can change the network settings in the IDM or the IME.

Caution You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

Simplified Setup Mode

The sensor automatically calls the **setup** command when you connect to the sensor using a console cable and the sensor basic network settings have not yet been configured. The sensor does not call automatic setup under the following conditions:

- When initialization has already been successfully completed.
- If you have recovered or downgraded the sensor.
- If you have set the host configuration to default after successfully configuring the sensor using automatic setup.

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the default values last set.

System Configuration Dialog

When you enter the **setup** command, an interactive dialog called the System Configuration Dialog appears on the system console screen. The System Configuration Dialog guides you through the configuration process. The values shown in brackets next to each prompt are the current values.

You must go through the entire System Configuration Dialog until you come to the option that you want to change. To accept default settings for items that you do not want to change, press **Enter**.

To return to the EXEC prompt without making changes and without going through the entire System Configuration Dialog, press **Ctrl-C**. The System Configuration Dialog also provides help text for each prompt. To access the help text, enter `?` at a prompt.

When you complete your changes, the System Configuration Dialog shows you the configuration that you created during the setup session. It also asks you if you want to use this configuration. If you enter `yes`, the configuration is saved. If you enter `no`, the configuration is not saved and the process begins again. There is no default for this prompt; you must enter either `yes` or `no`.

You can configure daylight savings time either in recurring mode or date mode. If you choose recurring mode, the start and end days are based on week, day, month, and time. If you choose date mode, the start and end days are based on month, day, year, and time. Choosing disable turns off daylight savings time.

Note You only need to set the date and time in the System Configuration Dialog if the system is an appliance and is NOT using NTP.

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

Example 1 shows a sample System Configuration Dialog.

Example 1 Example System Configuration Dialog

```
    --- Basic 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 time: Wed Nov 11 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.168.1.2/24,192.168.1.1]:
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Global Correlation?[no]:
  DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Global Correlation?[no]:
  HTTP proxy server IP address[128.107.241.169]:
  HTTP proxy server Port number[8080]:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances. We do not collect the data content of traffic
or other sensitive business or personal information. All data is aggregated and sent via
secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared
with Cisco will be anonymous and treated as strictly confidential.
```

```
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
  * Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs. promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
  * Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

Basic Sensor Setup

To perform basic sensor setup using the **setup** command, follow these steps:

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

Note Both the default username and password are **cisco**.

Step 2 The first time you log in to the sensor you are prompted to change the default password. Passwords must be at least eight characters long and be strong, that is, not be a dictionary word. After you change the password, basic setup begins.

Step 3 Enter the **setup** command. The System Configuration Dialog is displayed.

Step 4 Specify the hostname. The hostname is a case-sensitive character string up to 64 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

Step 5 Specify the IP interface. The IP interface is in the form of IP Address/Netmask,Gateway: *X.X.X.X/nn*,*Y.Y.Y.Y*, where *X.X.X.X* specifies the sensor IP address as a 32-bit address written as 4 octets separated by periods, *nn* specifies the number of bits in the netmask, and *Y.Y.Y.Y* specifies the default gateway as a 32-bit address written as 4 octets separated by periods.

Step 6 Enter **yes** to modify the network access list:

a. If you want to delete an entry, enter the number of the entry and press **Enter**, or press **Enter** to get to the Permit line.

b. Enter the IP address and netmask of the network you want to add to the access list.

Note For example, 10.0.0.0/8 permits all IP addresses on the 10.0.0.0 network (10.0.0.0-10.255.255.255) and 10.1.1.0/24 permits only the IP addresses on the 10.1.1.0 subnet (10.1.1.0-10.1.1.255). If you want to permit access to a single IP address than the entire network, use a 32-bit netmask. For example, 10.1.1.1/32 permits just the 10.1.1.1 address.

c. Repeat Step b until you have added all networks that you want to add to the access list, and then press **Enter** at a blank permit line to go to the next step.

Step 7 You must configure a DNS server or an HTTP proxy server for global correlation to operate:

a. Enter **yes** to add a DNS server, and then enter the DNS server IP address.

b. Enter **yes** to add an HTTP proxy server, and then enter the HTTP proxy server IP address and port number.

Caution You must have a valid sensor license for global correlation features to function. You can still configure and display statistics for the global correlation features, but the global correlation databases are cleared and no updates are attempted. Once you install a valid license, the global correlation features are reactivated.

Step 8 Enter **yes** to modify the system clock settings:

a. Enter **yes** to modify summertime settings.

Note Summertime is also known as DST. If your location does not use Summertime, go to Step m.

b. Enter **yes** to choose the USA summertime defaults, or enter **no** and choose recurring, date, or disable to specify how you want to configure summertime settings. The default is recurring.

c. If you chose recurring, specify the month you want to start summertime settings. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is march.

d. Specify the week you want to start summertime settings. Valid entries are first, second, third, fourth, fifth, and last. The default is second.

e. Specify the day you want to start summertime settings. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

f. Specify the time you want to start summertime settings. The default is 02:00:00.

Note The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2:00 a.m. on the second Sunday in March, and a stop time of 2:00 a.m. on the first Sunday in November. The default summertime offset is 60 minutes.

g. Specify the month you want summertime settings to end. Valid entries are january, february, march, april, may, june, july, august, september, october, november, and december. The default is november.

h. Specify the week you want the summertime settings to end. Valid entries are first, second, third, fourth, fifth, and last. The default is first.

i. Specify the day you want the summertime settings to end. Valid entries are sunday, monday, tuesday, wednesday, thursday, friday, and saturday. The default is sunday.

j. Specify the time you want summertime settings to end. The default is 02:00:00.

k. Specify the DST zone. The zone name is a character string up to 24 characters long in the pattern [A-Za-z0-9()+:,_/-]+$.

l. Specify the summertime offset. Specify the summertime offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 60.

m. Enter **yes** to modify the system time zone.

n. Specify the standard time zone name. The zone name is a character string up to 24 characters long.

o. Specify the standard time zone offset. Specify the standard time zone offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian). The default is 0.

p. Enter **yes** if you want to use NTP. To use authenticated NTP, you need the NTP server IP address, the NTP key ID, and the NTP key value. If you do not have those at this time, you can configure NTP later. Otherwise, you can choose unauthenticated NTP.

Step 9 Enter **off**, **partial**, or **full** to participate in the SensorBase Network Participation:

- Off—No data is contributed to the SensorBase Network.
- Partial—Data is contributed to the SensorBase Network, but data considered potentially sensitive is filtered out and never sent.
- Full—All data is contributed to the SensorBase Network except the attacker/victim IP addresses that you exclude.

The SensorBase Network Participation disclaimer appears. It explains what is involved in participating in the SensorBase Network.

Step 10 Enter **yes** to participate in the SensorBase Network.

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24, 192.168.1.1
host-name sensor
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option enabled
ntp-keys 1 md5-key 8675309
ntp-servers 10.10.1.2 key-id 1
exit
service global-correlation
```

```
    network-participation full
    exit


    [0] Go to the command prompt without saving this config.
    [1] Return to setup without saving this config.
    [2] Save this configuration and exit setup.
    [3] Continue to Advanced setup.
```

Step 11 Enter **2** to save the configuration (or **3** to continue with advanced setup using the CLI).

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 12 If you changed the time setting, enter **yes** to reboot the sensor.

Advanced Setup for the IPS 4270-20, IPS 4345, and IPS 4360

Note Adding new subinterfaces is a two-step process. You first organize the interfaces when you edit the virtual sensor configuration. You then choose which interfaces and subinterfaces are assigned to which virtual sensors.

To continue with advanced setup for the appliance, follow these steps:

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

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration and to see the current interface configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Promiscuous:
   GigabitEthernet0/0
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
```

```
  Signature Definitions: sig0

 Virtual Sensor: vs1
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs2
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 7 Enter **1** to edit the interface configuration.

Note The following options let you create and delete interfaces. You assign the interfaces to virtual sensors in the virtual sensor configuration. If you are using promiscuous mode for your interfaces and are not subdividing them by VLAN, no additional configuration is necessary.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 8 Enter **2** to add inline VLAN pairs and display the list of available interfaces.

Caution The new VLAN pair is not automatically added to a virtual sensor.

```
Available Interfaces
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Step 9 Enter **1** to add an inline VLAN pair to GigabitEthernet 0/0, for example.

```
Inline Vlan Pairs for GigabitEthernet0/0
   None
```

Step 10 Enter a subinterface number and description.

```
Subinterface Number:
Description[Created via setup by user asmith]:
```

Step 11 Enter numbers for VLAN 1 and 2.

```
Vlan1[]: 200
Vlan2[]: 300
```

Step 12 Press **Enter** to return to the available interfaces menu.

Note Entering a carriage return at a prompt without a value returns you to the previous menu.

```
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

Note At this point, you can configure another interface, for example, GigabitEthernet 0/1, for inline VLAN pair.

Step 13 Press **Enter** to return to the top-level interface editing menu.

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 14 Enter **4** to add an inline interface pair and see these options.

```
Available Interfaces
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3
```

Step 15 Enter the pair name, description, and which interfaces you want to pair.

```
Pair name: newPair
Description[Created via setup by user asmith:
Interface1[]: GigabitEthernet0/1
Interface2[]: GigabitEthernet0/2
Pair name:
```

Step 16 Press **Enter** to return to the top-level interface editing menu.

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

Step 17 Press **Enter** to return to the top-level editing menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 18 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 19 Enter **2** to modify the virtual sensor configuration, vs0.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/3
   [2] GigabitEthernet0/0
  Inline Vlan Pair:
   [3] GigabitEthernet0/0:1 (Vlans: 200, 300)
  Inline Interface Pair:
   [4] newPair (GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 20 Enter **3** to add inline VLAN pair GigabitEthernet0/0:1.

Step 21 Enter **4** to add inline interface pair NewPair.

Step 22 Press **Enter** to return to the top-level virtual sensor menu.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
   GigabitEthernet0/0:1 (Vlans: 200, 300)
  Inline Interface Pair:
   newPair (GigabitEthernet0/1, GigabitEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option: GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

Step 23 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 24 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 25 Enter **yes** to disable automatic threat prevention on all virtual sensors.

Step 26 Press **Enter** to exit the interface and virtual sensor configuration.

```
The following configuration was entered.
```

```
service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option disabled
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 342
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user asmith
vlan1 200
vlan2 300
exit
exit
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
exit
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 GigabitEthernet0/1
interface2 GigabitEthernet0/2
exit
exit
service analysis-engine
virtual-sensor newVs
description Created via setup by user cisco
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/0
exit
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 1
logical-interface newPair
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit
```

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 27 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 28 Reboot the appliance.

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

Step 29 Enter **yes** to continue the reboot.

Step 30 Apply the most recent service pack and signature update. You are now ready to configure your appliance for intrusion prevention.

Advanced Setup for the ASA 5500-X IPS SSP

To continue with advanced setup for the ASA 5500-X IPS SSP, follow these steps:

Step 1 Session in to the IPS using an account with administrator privileges.

```
asa# session ips
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel 0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
```

```
Option:
```

Step 7 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5500-X IPS SSP. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5500-X IPS SSP than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 8 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 9 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

Step 10 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel 0/0
Add Interface:
```

Step 11 Enter **1** to add PortChannel 0/0 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign PortChannel 0/0. We recommend that you assign PortChannel 0/0 to vs0, but you can assign it to another virtual sensor if you want to.

Step 12 Press **Enter** to return to the main virtual sensor menu.

Step 13 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 14 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
```

```
Option[2]:
```

Step 15 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 16 Enter **2** to create a signature-definition configuration file.

Step 17 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 18 Enter **1** to use the existing event-action-rules configuration, rules0.

Note If PortChannel 0/0 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 19 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 20 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 21 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name asa-ips
telnet-option disabled
access-list 10.0.0.0/8
```

```
access-list 64.0.0.0/8
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 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 22 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 23 Reboot the ASA 5500-X IPS SSP.

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

Step 24 Enter **yes** to continue the reboot.

Step 25 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
asa-ips# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 26 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5500-X IPS SSP with a web browser.

Step 27 Apply the most recent service pack and signature update. You are now ready to configure the ASA 5500-X IPS SSP for intrusion prevention.

Advanced Setup for the ASA 5585-X IPS SSP

To continue with advanced setup for the ASA 5585-X IPS SSP, follow these steps:

Step 1 Session in to the ASA 5585-X IPS SSP using an account with administrator privileges.

```
asa# session 1
```

Step 2 Enter the **setup** command. The System Configuration Dialog is displayed. Press **Enter** or the spacebar to skip to the menu to access advanced setup.

Step 3 Enter **3** to access advanced setup.

Step 4 Specify the Telnet server status. You can disable or enable Telnet services. The default is disabled.

Step 5 Specify the web server port. The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note The web server is configured to use TLS/SSL encryption by default. Setting the port to 80 does not disable the encryption.

Step 6 Enter **yes** to modify the interface and virtual sensor configuration.

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 7 Enter **1** to edit the interface configuration.

Note You do not need to configure interfaces on the ASA 5585-X IPS SSP. You should ignore the modify interface default VLAN setting. The separation of traffic across virtual sensors is configured differently for the ASA 5585-X IPS SSP than for other sensors.

```
  [1] Modify interface default-vlan.
Option:
```

Step 8 Press **Enter** to return to the top-level interface and virtual sensor configuration menu.

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

Step 9 Enter **2** to edit the virtual sensor configuration.

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
```

```
  [3] Create new virtual sensor.
Option:
```

Step 10 Enter **2** to modify the virtual sensor vs0 configuration.

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel0/0
Add Interface:
```

Step 11 Enter **1** to add PortChannel 0/0 to virtual sensor vs0.

Note Multiple virtual sensors are supported. The adaptive security appliance can direct packets to specific virtual sensors or can send packets to be monitored by a default virtual sensor. The default virtual sensor is the virtual sensor to which you assign PortChannel 0/0. We recommend that you assign PortChannel 0/0 to vs0, but you can assign it to another virtual sensor if you want to.

Step 12 Press **Enter** to return to the main virtual sensor menu.

Step 13 Enter **3** to create a virtual sensor.

```
Name[]:
```

Step 14 Enter a name and description for your virtual sensor.

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

Step 15 Enter **1** to use the existing anomaly-detection configuration, ad0.

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

Step 16 Enter **2** to create a signature-definition configuration file.

Step 17 Enter the signature-definition configuration name, **newSig**.

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

Step 18 Enter **1** to use the existing event action rules configuration, rules0.

Note If PortChannel 0/0 has not been assigned to vs0, you are prompted to assign it to the new virtual sensor.

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

Step 19 Press **Enter** to exit the interface and virtual sensor configuration menu.

```
Modify default threat prevention settings?[no]:
```

Step 20 Enter **yes** if you want to modify the default threat prevention settings.

Note The sensor comes with a built-in override to add the deny packet event action to high risk rating alerts. If you do not want this protection, disable automatic threat prevention.

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

Step 21 Enter **yes** to disable automatic threat prevention on all virtual sensors.

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
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 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
```

```
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

Step 22 Enter **2** to save the configuration.

```
Enter your selection[2]: 2
Configuration Saved.
```

Step 23 Reboot the ASA 5585-X IPS SSP.

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

Step 24 Enter **yes** to continue the reboot.

Step 25 After reboot, log in to the sensor, and display the self-signed X.509 certificate (needed by TLS).

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 26 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when using HTTPS to connect to this ASA 5585-X IPS SSP with a web browser.

Step 27 Apply the most recent service pack and signature update. You are now ready to configure your ASA 5585-X IPS SSP for intrusion prevention.

Verifying Initialization

Note The following **show configuration** output is an example of what your configuration may look like. It will not match exactly because of the optional setup choices.

To verify that you initialized your sensor, follow these steps:

Step 1 Log in to the sensor.

Step 2 View your configuration.

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Tue Nov 01 10:40:39 2011
! ------------------------------
! Version 7.1(3)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S581.0   2011-07-11
```

```
! ------------------------------
service interface
exit
! ------------------------------
service authentication
permit-packet-logging true
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
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
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset -360
standard-time-zone-name GMT-06:00
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
exit
exit
signatures 2004 0
alert-frequency
summary-mode fire-all
exit
exit
status
enabled true
exit
exit
exit
! ------------------------------
service ssh-known-hosts
rsa1-keys 10.89.146.1
length 1024
exponent 35
modulus 12783094292288326767015615132168773328115097561020607196221632570955980 2
69998149478748431202060218539250569954487820368372742332963486465122675278103455
02382074147081976580477367448761372704018006749147530115354456086472735887860780
```

```
209232035656491654023918931928054450310003049389864127423289403797 11869015427
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 analysis-engine
exit
sensor#
```

Note You can also use the **more current-config** command to view your configuration.

Step 3 Display the self-signed X.509 certificate (needed by TLS).

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

Step 4 Write down the certificate fingerprints. You need the fingerprints to check the authenticity of the certificate when connecting to this sensor with a web browser.

Logging In to the IDM

The IDM is a web-based, Java Web Start application that enables you to configure and manage your sensor. The web server for the IDM resides on the sensor. You can access it through Internet Explorer or Firefox web browsers.

Note The IDM is already installed on the sensor.

To log in to the IDM, follow these steps:

Step 1 Open a web browser and enter the sensor IP address. A Security Alert dialog box appears.

```
https://sensor_ip_address
```

Note The default IP address is 192.168.1.2/24,192.168.1.1, which you change to reflect your network environment when you initialize the sensor. When you change the web server port, you must specify the port in the URL address of your browser when you connect to the IDM in the format https://*sensor_ip_address:port* (for example, https://192.0.2.1:1040).

Step 2 Click **Yes** to accept the security certificate. The Cisco IPS Device Manager Version window appears.

Step 3 To launch the IDM, click **Run IDM**. The JAVA loading message box appears, and then the Warning - Security dialog box appears.

Step 4 To verify the security certificate, check the Always trust content from this publisher check box, and click **Yes**. The JAVA Web Start progress dialog box appears, and then the IDM on *ip_address* dialog box appears.

Step 5 To create a shortcut for the IDM, click **Yes**. The Cisco IDM Launcher dialog box appears.

Note You must have JRE 1.5 (JAVA 5) installed to create shortcuts for the IDM. If you have JRE 1.6 (JAVA 6) installed, the shortcut is created automatically.

Step 6 To authenticate the IDM, enter your username and password, and click **OK**. Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization. The IDM begins to load. If you change panes from Home to Configuration or Monitoring before the IDM has completed initialization, a Status dialog box appears with the following message:

```
Please wait while IDM is loading the current configuration from the sensor.
```

The main window of the IDM appears.

Note If you created a shortcut, you can launch the IDM by double-clicking the IDM shortcut icon. You can also close the The Cisco IPS Device Manager Version window. After you launch the IDM, it is not necessary for this window to remain open.

Installing or Upgrading the IME

This section describes how to install and upgrade the IME, and how to migrate data from IEV or a previous version of IME.

Cisco IEV, Cisco IOS IPS, and CSM

If you have a version of Cisco IPS Event Viewer installed, the Install wizard prompts you to remove it before installing the IME.

The IME event monitoring is also supported in IOS-IPS versions that support the Cisco IPS 5.x/6.x signature format. We recommend IOS-IPS 12.4(15)T4 if you intend to use the IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

Caution Do not install the IME on top of existing installations of CSM. You must uninstall CSM before installing the IME.

Installation Notes and Caveats

Note If you are using Windows 7 or Windows Server 2008, and an IME version earlier than 7.1.1, uninstall IME before upgrading it. Otherwise, just upgrade from your current IME version.

Observe the following when installing or upgrading the IME:

- You can install the IME over all versions of the IME but not over IEV. All alert database and user settings are preserved.
- The IME detects previous versions of IEV and prompts you to manually remove the older version before installing the IME or to install the IME on another system. The installation program then stops.
- Make sure you close any open instances of the IME before upgrading to a new version of the IME.
- Disable any anti-virus or host-based intrusion detection software before beginning the installation, and close any open applications. The installer spawns a command shell application that may trigger your host-based detection software, which causes the installation to fail.
- You must be administrator to install the IME.
- The IME coexists with other instances of the MySQL database. If you have a MySQL database installed on your system, you do NOT have to uninstall it before installing the IME.

Installing or Upgrading the IME

To install the IME, follow these steps:

Step 1 From the Download Software site on Cisco.com, download the IME executable file to your computer, or start the IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file. IME-7.2.1.exe is an example of what the IME executable file might look like.

Step 2 Double-click the executable file. The Cisco IPS Manager Express - InstallShield Wizard appears. You receive a warning if you have a previous version of Cisco IPS Event Viewer installed. Acknowledge the warning, and exit installation. Remove the older version of IEV, and then continue the IME installation

Step 3 Click **Next** to start the IME installation.

Step 4 Accept the license agreement and click **Next**.

Step 5 Click **Next** to choose the destination folder, click **Install** to install the IME, and then click **Finish** to exit the wizard. The Cisco IME and Cisco IME Demo icons are now on your desktop.

Note The first time you start the IME, you are prompted to set up a password.

Migrating IEV Data

To migrate IEV 5.*x* events to the IME, you must exit the installation and manually export the old events by using the IEV 5.*x* export function to move the data to local files. After installing the IME, you can import these files to the new IME system.

Note The IME does not support import and migration functions for IEV 4.*x*.

To export event data from IEV 5.*x* to a local file:

Step 1 From IEV 5.*x*, choose **File > Database Administration > Export Database Tables**.

Step 2 Enter the file name and select the table(s).

Step 3 Click **OK**. The events in the selected table(s) are exported to the specified local file.

Importing IEV Event Data In to IME

To import event data in to the IME, follow these steps:

Step 1 From the IME, choose **File > Import**.

Step 2 Select the file exported from IEV 5.*x* and click **Open**. The contents of the selected file are imported in to the IME.

For More Information

For more information about the IME, refer to *Cisco Intrusion Prevention System Manager Express Installation Guide for IPS 7.1*.

Enabling Anomaly Detection

The following section explains how to enable anomaly detection through the IDM, IME, and the CLI. It contains the following topics:

- Enabling Anomaly Detection Using the IDM or IME, page 52
- Enabling Anomaly Detection Using the CLI, page 53

Enabling Anomaly Detection Using the IDM or IME

To enable anomaly detection, follow these steps:

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

Step 2 Choose **Configuration > Policies > IPS Policies**.

Step 3 Select the virtual sensor for which you want to turn on anomaly detection, and then click **Edit**.

Step 4 Under Anomaly Detection, choose an anomaly detection policy from the Anomaly Detection Policy drop-down list. Unless you want to use the default ad0, you must have already added a anomaly detection policy by choosing **Configuration > Policies > Anomaly Detections > Add**.

Step 5 Choose Detect as the anomaly detection mode from the AD Operational Mode drop-down list. The default is Inactive.

Tip To discard your changes and close the Edit Virtual Sensor dialog box, click **Cancel**.

Step 6 Click **OK**.

Tip To discard your changes, click **Reset**.

Step 7 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For more detailed information about anomaly detection, refer to Configuring Anomaly Detection.

Enabling Anomaly Detection Using the CLI

To enable 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 enable.

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

Step 4 Enable anomaly detection operational mode.

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode detect
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 detailed information about anomaly detection, refer to Configuring Anomaly Detection.

Disabling Anomaly Detection

The following section explains how to disable anomaly detection through the IDM, IME, or the CLI. It contains the following topics:

- Disabling Anomaly Detection Using the IDM or IME, page 54
- Disabling Anomaly Detection Using the CLI, page 54

Disabling Anomaly Detection Using the IDM or IME

To disable anomaly detection, follow these steps:

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

Step 2 Choose **Configuration > Policies > IPS Policies.**

Step 3 Select the virtual sensor for which you want to turn off anomaly detection, and then click **Edit**.

Step 4 Under Anomaly Detection, from the AD Operational Mode drop-down list, choose Inactive as the anomaly detection mode.

Tip To discard your changes and close the Edit Virtual Sensor dialog box, click **Cancel**.

Step 5 Click **OK**.

Tip To discard your changes, click **Reset**.

Step 6 Click **Apply** to apply your changes and save the revised configuration.

For More Information

For more detailed information about anomaly detection, refer to Configuring Anomaly Detection.

Disabling Anomaly Detection Using the CLI

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 detailed information about anomaly detection, refer to Configuring Anomaly Detection.

Cisco Security Intelligence Operations

The Cisco Security Intelligence Operations site on Cisco.com provides intelligence reports about current vulnerabilities and security threats. It also has reports on other security topics that help you protect your network and deploy your security systems to reduce organizational risk.

You should be aware of the most recent security threats so that you can most effectively secure and manage your network. Cisco Security Intelligence Operations contains the top ten intelligence reports listed by date, severity, urgency, and whether there is a new signature available to deal with the threat.

Cisco Security Intelligence Operations contains a Security News section that lists security articles of interest. There are related security tools and links.

You can access Cisco Security Intelligence Operations at this URL:

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations is also a repository of information for individual signatures, including signature ID, type, structure, and description.

You can search for security alerts and signatures at this URL:

http://tools.cisco.com/security/center/search.x

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IPS 7.1(3)E4 software and the products that run it:

- For RADIUS users, the attempt limit feature is enforced only after the RADIUS user's first successful login to the sensor.
- The IPS 4345 and IPS 4360 do not support hardware bypass. Hardware bypass is currently only supported on the IPS 4270-20.
- The ASA 5512-X IPS SSP and the ASA 5515-X IPS SSP do not support the Regex accelerator card and the String XL engines.
- Use the **show statistics virtual-sensor | include load** command (CLI) or look at the statistics for the virtual sensor at **Configuration > Sensor Monitoring > Support Information > Statistics** (IDM/IME) to determine the load value over a longer period of time. The **show statistics analysis-engine** command (CLI) and the statistics for Analysis Engine show values over a shorter period of time. If you compare the output, the values will appear to be inconsistent due to the different time periods. To get an accurate comparison between them, compare the processing load percentage from the statistics for the virtual sensor and the one-minute averaged value from the statistics for Analysis Engine.
- On the IPS 4270-20, rx/tx flow control is disabled. This is a change from IPS 7.0 where rx/tx flow control is enabled by default.
- TACACS+ authentication is not supported in IPS 7.1(3)E4.
- The CLI timeout feature is applicable only for sessions established through SSH, Telnet, and the console. Service account logins are not affected.
- Anomaly detection does not support IPv6 traffic; only IPv4 traffic is directed to the anomaly detection processor.
- IPv6 does not support the following event actions: Request Block Host, Request Block Connection, or Request Rate Limit.
- Global correlation does not support IPv6.
- There is no support for IPv6 on the management (command and control) interface.
- ICMP signature engines do not support ICMPv6, they are IPv4-specific, for example, the Traffic ICMP signature engine. ICMPv6 is covered by the Atomic IP Advanced signature engine.
- CSM and MARS do not support IPv6.
- When deploying an IPS sensor monitoring two sides of a network device that does TCP sequence number randomization, we recommend using a virtual senor for each side of the device.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- The IDM does not support any non-English characters, such as the German umlaut or any other special language characters. If you enter such characters as a part of an object name through IDM, they are turned into something unrecognizable and you will not be able to delete or edit the resulting object through IDM or the CLI. This is true for any string that is used by the CLI as an identifier, for example, names of time periods, inspect maps, server and URL lists, and interfaces.

- When SensorApp is reconfigured, there is a short period when SensorApp is unable to respond to any queries. Wait a few minutes after reconfiguration is complete before querying SensorApp for additional information.
- 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.
- The IDM and IME launch MySDN from the last browser window you opened, which is the default setting for Windows. To change this default behavior, in Internet Explorer, choose **Tools > Internet Options**, and then click the **Advanced** tab. Scroll down and uncheck the **Reuse windows for launching shortcuts** check box.

For More Information

For the procedure for configuring sensor health metrics, for the IDM refer to Configuring Sensor Health, for the IME refer to Configuring Sensor Health, and for the CLI refer to Configuring Health Status Information.

Caveats

This section lists the resolved and unresolved caveats, and contains the following topics:

- Resolved Caveats, page 57
- Unresolved Caveats, page 58

Resolved Caveats

The following known issues are resolved in the 7.1(3)E4 release:

- CSCtl04402—failure in decode params during web server control transaction
- CSCte50759—sensorApp aborts during signature update
- CSCtq05123—treapi error 606 during string-xl or string-tcp signature configuration
- CSCtg38568—IPS 4270 with 10Gig cards will not pass jumbo frames.
- CSCts70493—show health reports 'Failed Applications Green' when sensorApp has cored
- CSCtn81330—hangup on vi session will use 100% cpu
- CSCti08564—IPS TCP normalizer reorders packets but sends them with OoO timestamps
- CSCtn84402—SensorApp not processing packets when eventstore is locked during query
- CSCti43137—IPS AAA PAM module sends incorrect NAS IP in radius packet
- CSCts40849—sensorApp core in atomic-ip-advanced inspector
- CSCti57119—IPS packet capture creates multiple files that are not removable
- CSCtj86988—mainApp hangs in AuthenticationMgr
- CSCti79423—IPS: IP Reputation Update brings down sensorApp on IDSM-2
- CSCtq71035—Inline interface pair stops packet forwarding after rebooting

- CSCts98784—IPS SSP collaborationApp core
- CSCts40616—IPS SSP sensorApp core due to buffer overflow errors
- CSCtg50681—Sensor Upgrade failure. \"ExecUpgradeSoftware: < > already installed\"
- CSCtg73897—SendAckLimiter: repair ReportInterval issue and improve stats collection
- CSCti70744—IPS sensor unable to copy current-config
- CSCtj04994—IDS: service aaa creates local user accounts with invalid characters
- CSCtj51386—sensor out of storage space due to global-correlation log
- CSCtn11478—IDS - ATOMIC.ARP engine creates phantom duplicate signatures upon edit
- CSCto62559—RADIUS sends an empty calling-station-id for HTTP/HTTPS authentication
- CSCto77871—Sensor health status for missed packets is incorrect
- CSCtq00491—Sensor health for signature updates is incorrect
- CSCtq95375—radius module should handle multiple cisco-av-pair responses
- CSCts21378—normalizer signature 1330.12 drops legit reset packet and keeps tracking
- CSCts58648—Old SMB engine should not be allowed to run
- CSCts70337—IPS SSP crash in sensor app(AlarmDBProcessor::lookupRootNode hashtable)
- CSCsv26568—IPS SNMP InterfaceGroup OID does not show correct Virtual Sensor
- CSCta43555—Network Security Level not functioning
- CSCtf02842—ntp daemon may lose synchronization with server
- CSCtg22175—fast retransmit ACK swaps mac address for multicast traffic
- CSCtg22575—Unexpected Behavior using Exact-Match-Offset In Atomic ip
- CSCto97367—Incorrect behaviour while changing cisco password
- CSCtn56839—IPS interface can be configured as promisc and VLAN-pair at same time
- CSCtj93001—Invalid card type error logged in by sensor for SSP-IPS40
- CSCtj31566—SSH TCP port forwarding is enabled - x86 Only
- CSCsk85023—Need a way to disable weak ciphers for HTTPS access to the sensor.
- CSCsu08529—Enh: IPS Add SNMP support for a subset of Health Statistics
- CSCti49271—inline IPS stops traffic after reset in redundant environment (e1000)
- CSCto51204—authentication attemptLimit leaks file handles and hangs mainApp for x86

Unresolved Caveats

The following issues are unresolved in IPS 7.1(3)E4:

- CSCtt10189—LSI insufficient resource error not throttled in main.log - Spyker
- CSCtt43148—Unable to configure IPS from IDM {Error- Unauthorized component Edit}
- CSCtu85641—Custom sigs- string-xl-icmp/string-icmp engine not working for icmp-type
- CSCts72622—Cleared CLI ID's not being cleaned up
- CSCtu75883—Deny-Attacker-ServicePair InLine does not show denied attackers -IPv6
- CSCtw56890—IDM documentation is missing reference to permit-packet-logging av pair

- CSCtu05099—Visual indication of progress required when editing sig actions
- CSCto77478—telnet/ssh connection to CLI may close during "sh ev al"
- CSCtr46541—3401.0 alert not firing for some packet sizes
- CSCtr75697—sensorApp stopped after extended duration packet display of IPSec pkts
- CSCts72622—Cleared CLI ID's not being cleaned up
- CSCtw45784—TCP Normalizer 1330 sigs fire with replayed traffic
- CSCtt02648—Inconsistent behaviour seen for deny action of sig 1204-0

Related Documentation

For a complete list of the Cisco IPS 7.1 documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/ips/7.1/roadmap/19889_01.html

For a complete list of the Cisco ASA 5500 series documentation and where to find it, refer to the following URL:

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

Obtaining Documentation, Using the Cisco Bug Search Tool, and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.