Release Notes for Cisco Intrusion Prevention System 7.0(7)E4

Published: January 31, 2012, OL-25390-01

Revised: October 28, 2013

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Caution The BIOS on Cisco IPS sensors is specific to IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on IPS sensors voids the warranty.

IPS File List

Note All IPS platforms allow ten concurrent CLI sessions.

Note The AIM IPS and the NME IPS do not support the IPv6 features, because the router in which they are installed does not send them IPv6 data. IPv6 inspection may work on the IDSM2, but we do not officially support it. There is no support for IPv6 on the management (command and control) interface.

The following files are part of Cisco IPS 7.0(7)E4:

- Readme
  - IPS-7_0-7-E4_readme.txt
- Minor Version Upgrade Files
  - IPS-K9-7.0-7-E4.pkg
  - IPS-AIM-K9-7.0-7-E4.pkg
  - IPS-NME-K9-7.0-7-E4.pkg
- System Image Files
  - IPS-4240-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-4255-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-4260-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-4270_20-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-IDSM2-K9-sys-1.1-a-7.0-7-E4.bin.gz
  - IPS-SSM_10-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-SSM_20-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-SSM_40-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-AIM-K9-sys-1.1-a-7.0-7-E4.img
  - IPS-NME-K9-sys-1.1-a-7.0-7-E4.img
- Recovery Image Files
  - IPS-K9-r-1.1-a-7.0-7-E4.pkg
  - IPS-AIM-K9-r-1.1-a-7.0-7-E4.pkg
  - IPS-NME-K9-r-1.1-a-7.0-7-E4.pkg

For More Information

For the procedure for obtaining these files on Cisco.com, see Obtaining Software on Cisco.com, page 9.

Supported Platforms

Cisco IPS 7.0(7)E4 is supported on the following platforms:

- IPS 4240 Series Sensor Appliances
- IPS 4255 Series Sensor Appliances
- IPS 4260 Series Sensor Appliances
- IPS 4270-20 Series Sensor Appliances
- IDSM2 Series Intrusion Detection System Modules (IDSM2)
- ASA-SSM-AIP-10 Series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP SSM-10)
- ASA-SSM-AIP-20 Series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP SSM-20)
- ASA-SSM-AIP-40 Series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP SSM-40)
- Intrusion Prevention System Advanced Integration Modules (AIM IPS)
- Intrusion Prevention System Network Modules (NME IPS)

Cisco IPS 7.0(7)E4 is not supported on the following platforms:

- ASA 5500 series adaptive security appliances with AIP SSC-5

  Note The AIP SSC-5 is currently only supported in Cisco IPS 6.2.

- ASA 5585-X adaptive security appliances with IPS SSP

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.

For More Information

- For the procedure for downloading IPS software updates from Cisco.com, see Obtaining Software on Cisco.com, page 9.
- For the procedure for configuring automatic updates, for the CLI refer to Configuring Automatic Updates, for the IDM refer to Configuring Automatic Update, and for the IME refer to Configuring Automatic Update.

IPS Management and Event Viewers

Use the following tools for configuring Cisco IPS 7.0(7)E4 sensors:

- Cisco IDM 7.1.1

  IDM 7.1.1 is included within the IPS 7.0(7)E4 files.
- 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.

  IDM 7.1.3 is included within IME 7.2.1.
- IPS CLI 7.0.7
- ASDM 5.2 and later

Use the following tools for monitoring Cisco IPS 7.0(7)E4 sensors:

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

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 7.0(7)E4 sensors.

New and Changed Information

Cisco IPS 7.0(7)E4 contains the following new and changed information:

- Signature update S615
- IDM 7.1.1
- Serviceability enhancements
  - New **show inspection-load command**—When you execute the **show inspection-load command**, it shows a timestamp and the current inspection load. When executed with the **history** option, the **show inspection-load history** command shows a histogram of the inspection load over the past 60 minutes and over the past 72 hours.

Use this command to determine the load on the sensor instead of the CPU Usage information from the **show statistics host** command. The inspection load is a more accurate representation of the processing level of the sensor.

The Processing Load category in the **show statistics virtual-sensor** output has been renamed to Inspection Load Percentage and shows the same value seen in the **show inspection load** command.

The calculation of the inspection load has also been enhanced to provide a more accurate calculation of the sensor load at lower traffic levels.

- New **erase license-key** command—You can now delete an installed license from a sensor without restarting the sensor or logging into the sensor using the service account.
- Detail information added to **show statistics global-correlation** command—The output now includes any failures that have been detected.
- TCP Normalizer signature warning—You receive the following warning if you disable a default-enabled TCP Normalizer signature or remove a default-enabled modify packet inline, deny packet inline, or deny connection inline action:

```
Use caution when disabling, retiring, or changing the event action settings of a
<Sig ID> TCP Normalizer signature for a sensor operating in IPS mode. The TCP
Normalizer signature default values are essential for proper operation of the
sensor.
If the sensor is seeing duplicate packets, consider assigning the traffic to
multiple virtual sensors. If you are having problems with asymmetric or
out-of-order TCP packets, consider changing the normalizer mode from strict
evasion protection to asymmetric mode protection. Contact Cisco TAC if you require
further assistance.
```

- Reboot sensor warning—When a user reboots the sensor, a message with a timestamp is logged so that the time of the reboot can be tracked.
- Asymmetric protection mode warning—Make sure anomaly detection is configured to inactive if the sensor is monitoring asymmetric traffic. Using asymmetric mode protection with anomaly detection enabled causes excessive resource usage and possible false positives for anomaly detection signatures.

- Network participation enhancements
  - In the case of SensorApp failure, the generated core.txt file will be sent with the network participation update.
  - Data gathered for the **show health** command has been added to the network participation upload.

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.

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

MySDN Decommissioned

Because MySDN has been decommissioned, the URL in older versions of the IDM and the IME is no longer functional. If you are using IPS 6.0 or later, we recommend that you upgrade your version of the IDM and the IME.

You can upgrade to the following versions to get the functioning MySDN URL:

- IME 7.2.1
- IPS 7.0(7), which contains IDM 7.1.1

If you are using version IPS 5.x, you must look up signature information manually at this URL:

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

For More Information

For information on MySDN, for the IDM refer to Understanding MySDN, and for the IME refer to MySDN.

Before Upgrading to Cisco IPS 7.0(7)E4

This section describes the actions you should take before upgrading to Cisco IPS 7.0(7)E4. It contains the following topics:

Perform These Tasks

Before you upgrade your sensors to IPS 7.0(7)E4, make sure you perform the following tasks:

- Check to make sure you have a valid Cisco Service for IPS service contract per sensor so that you can apply software upgrades.
- Created a backup copy of your configuration.
- Saved the output of the **show version** command.

If you need to downgrade a signature update, you will know what version you had, and you can then apply the configuration you saved when you backed up your configuration.

For More Information

- For more information on how to obtain a valid Cisco Service for IPS service contract, see Service Programs for IPS Products, page 21.
- For the procedure for creating a backup copy of your configuration, see Backing Up and Restoring the Configuration File Using a Remote Server, page 7.

- For the procedure for finding your Cisco IPS software version, for the CLI refer to Displaying Version Information, for the IDM refer to IDM Home Window, and for the IME refer to Sensor Information Gadget.
- For the procedure for downgrading signature updates on your sensor, refer to Upgrading, Downgrading, and Installing System Images.

Backing Up and Restoring the Configuration File Using a Remote Server

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

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

The following options apply:

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

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

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

- ftp:—Source 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.

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

Backing Up the Current Configuration to a Remote Server

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

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

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

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

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

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

Restoring the Current Configuration From a Backup File

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

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

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

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

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

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

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

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

For More Information

For the procedure for adding trusted hosts, for the CLI refer to Adding TLS Trusted Hosts, for the IDM refer to Configuring Trusted Hosts, and for the IME refer to Adding Trusted Hosts.

Obtaining Software on Cisco.com

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 following a train schedule. 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 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 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.

- Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.
- 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. The File Download dialog box appears.

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

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

IPS Software Versioning

When you download IPS software images from Cisco.com, you should understand the versioning scheme so you know which files are base files, which are cumulative, and which are incremental.

Major Update

A major update contains new functionality or an architectural change in the product. For example, the Cisco IPS 7.0 base version includes everything (except deprecated features) since the previous major release (the minor update features, service pack fixes, and signature updates) plus any new changes. Major update 7.0(1) requires 5.1(6) and later. With each major update there are corresponding system and recovery packages.

Note The 7.0(1) major update is used to upgrade 5.1(6) and later sensors to 7.0(1) If you are reinstalling 7.0(1) on a sensor that already has 7.0(1) installed, use the system image or recovery procedures rather than the major update.

Minor Update

A minor update is incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 7.0 is 7.1. Minor updates are released for minor enhancements to the product. Minor updates contain all previous minor features (except deprecated features), service pack fixes, signature updates since the last major version, and the new minor features being released. You can install the minor updates on the previous major or minor version (and often even on earlier versions). The minimum supported version needed to upgrade to the newest minor version is listed in the Readme that accompanies the minor update. With each minor update there are corresponding system and recovery packages.

Service Pack

A service pack is cumulative following a base version release (minor or major). Service packs are released in a train release format with several new features per train. Service packs contain all service pack fixes since the last base version (minor or major) and the new features and defect fixes being released. Service packs require the minor version. The minimum supported version needed to upgrade to the newest service pack is listed in the Readme that accompanies the service pack. Service packs also include the latest engine update. For example, if service pack 7.0(7) is released, and E4 is the latest engine level, the service pack is released as 7.0(7)E4.

Patch Release

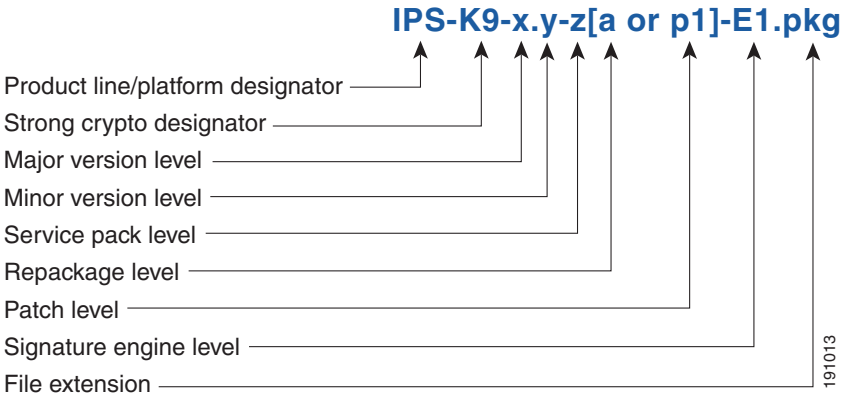
A patch release is used to address defects that are identified in the upgrade binaries after a software release. Rather than waiting until the next major or minor update, or service pack to address these defects, a patch can be posted. Patches include all prior patch releases within the associated service pack level. The patches roll into the next official major or minor update, or service pack.

Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 7.0(1p1) requires 7.0(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 7.0(1p1) to 7.0(1p2) without first uninstalling 7.0(1p1).

Figure 1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 1 IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases

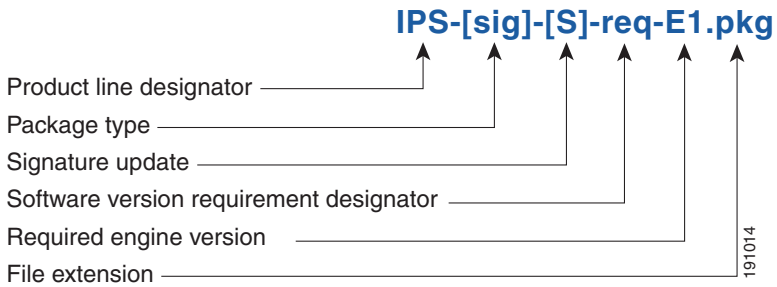


Signature Update

A signature update is a package file containing a set of rules designed to recognize malicious network activities. Signature updates are released independently from other software updates. Each time a major or minor update is released, you can install signature updates on the new version and the next oldest version for a period of at least six months. Signature updates are dependent on a required signature engine version. Because of this, a *req* designator lists the signature engine required to support a particular signature update.

Figure 2 illustrates what each part of the IPS software file represents for signature updates.

Figure 2 IPS Software File Name for Signature Updates

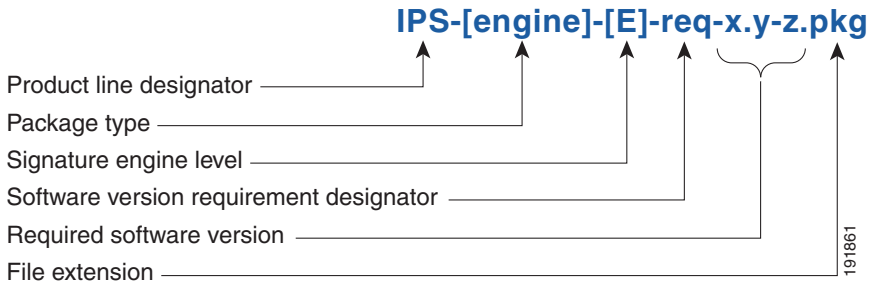


Signature Engine Update

A signature engine update is an executable file containing binary code to support new signature updates. Signature engine files require a specific service pack, which is also identified by the *req* designator.

Figure 3 illustrates what each part of the IPS software file represents for signature engine updates.

Figure 3 IPS Software File Name for Signature Engine Updates



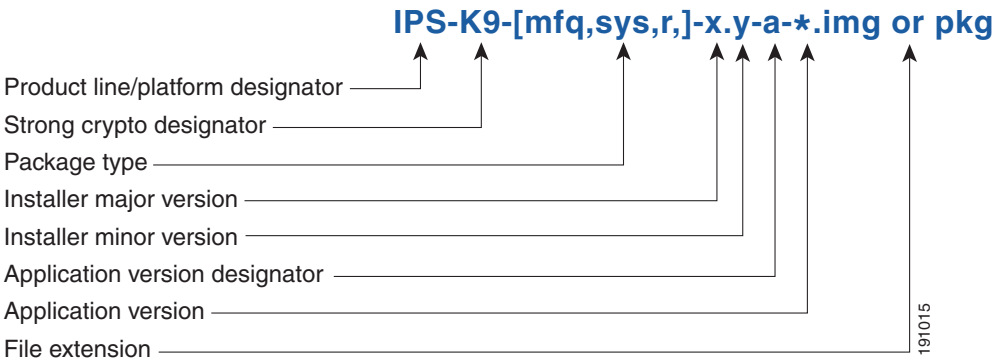
Recovery and System Image Files

Recovery and system image files contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field. The major version is incremented by one of any major changes to the image installer, for example, switching from .tar to rpm or changing kernels. The minor version can be incremented by any one of the following:

- Minor change to the installer, for example, a user prompt added.
- Repackages require the installer minor version to be incremented by one if the image file must be repackaged to address a defect or problem with the installer.

Figure 4 illustrates what each part of the IPS software file represents for recovery and system image files.

Figure 4 IPS Software File Name for Recovery and System Image Files



Software Release Examples

Table 1 lists platform-independent Cisco IPS software release examples.

Table 1 Platform-Independent Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update[1]	Weekly	sig	S369	IPS-sig-S369-req-E4.pkg
Signature engine update[2]	As needed	engine	E4	IPS-engine-E4-req-7.0-1.pkg
Service packs[3]	Semi-annually or as needed	—	7.0(6)	IPS-K9-7.0-7-E4.pkg
Minor version update[4]	Annually	—	7.1(1)	IPS-K9-7.1-1-E4.pkg **Note** IPS-AIM-K9-7.1-1-E4.pkg is the minor version update for the AIM IPS. IPS-NME-K-9-7.1-1-E4.pkg is the minor version update for the NME IPS.
Major version update[5]	Annually	—	7.0(1)	IPS-K9-7.0-1-E4.pkg
Patch release[6]	As needed	patch	7.0(1p1)	IPS-K9-patch-7.0-1pl-E4.pkg
Recovery package[7]	Annually or as needed	r	1.1-7.0(1)	IPS-K9-r-1.1-a-7.0-1-E4.pkg

1. Signature updates include the latest cumulative IPS signatures.
2. Signature engine updates add new engines or engine parameters that are used by new signatures in later signature updates.
3. Service packs include defect fixes.
4. Minor versions include new minor version features and/or minor version functionality.
5. Major versions include new major version functionality or new architecture.
6. Patch releases are for interim fixes.

7. The r 1.1 can be revised to r 1.2 if it is necessary to release a new recovery package that contains the same underlying application image. If there are defect fixes for the installer, for example, the underlying application version may still be 7.0(6), but the recovery partition image will be r 1.2.

Table 2 describes platform-dependent software release examples.

Table 2 Platform-Dependent Release Examples

Release	Target Frequency	Identifier	Supported Platform	Example Filename
System image[1]	Annually	sys	Separate file for each sensor platform	IPS-4240-K9-sys-1.1-a-7.0-1-E4.img
Maintenance partition image[2]	Annually	mp	IDSM2	c6svc-mp.2-1-2.bin.gz
Bootloader	As needed	bl	AIM IPS NME IPS	pse_aim_x.y.z.bin pse_nm_x.y.z.bin (where x, y, z is the release number)
Mini-kernel	As needed	mini-kernel	AIM IPS NME IPS	pse_mini_kernel_1.1.10.64.bz2

1. The system image includes the combined recovery and application image used to reimage an entire sensor.
2. The maintenance partition image includes the full image for the IDSM2 maintenance partition. The file is installed from but does not affect the IDSM2 application partition.

Table 3 describes the platform identifiers used in platform-specific names.

Table 3 Platform Identifiers

Sensor Family	Identifier
IPS 4240 series	4240
IPS 4255 series	4255
IPS 4260 series	4260
IPS 4270-20 series	4270_20
IDS module for Catalyst 6K	IDSM2
IPS network module	AIM NME
Adaptive security appliance modules	SSM_10 SSM_20 SSM_40

Upgrading to Cisco IPS

This section provides information on upgrading to Cisco IPS 7.0(7)E4, and contains the following topics:

Upgrade Notes and Caveats

The following upgrade notes and caveats apply to upgrading your sensor to IPS 7.0(7)E4:

- This service pack contains the S615 signature level.
- You cannot uninstall IPS 7.0(7)E4. To revert to your previous version, you must reimage the sensor using the system image file, which causes all configuration settings to be lost.
- You must have a valid Cisco Service for IPS Maintenance contract per sensor to receive and use software upgrades from Cisco.com.
- The minimum required version for upgrading to 7.0(7)E4 is 5.1(6)E3 or later.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- For supported sensors, use the IPS-K9-7.0-7-E4.pkg upgrade file. Use the following specific files for these platforms:
  - For the AIM IPS, use IPS-AIM-K9-7.0-7-E4.pkg.
  - For the NME IPS, use IPS-NME-K9-7.0-7-E4.pkg.
- Using automatic update:
  - If you are using automatic update with a mixture of AIM IPS, NME IPS, and other IPS appliances or modules, make sure you put both the 7.0(7)E4 upgrade file (IPS-K9-7.0-7-E4.pkg), the AIM IPS upgrade file (IPS-AIM-K9-7.0-7-E4.pkg), and the NME IPS upgrade file (IPS-NME-K9-7.0-7-E4.pkg) on the automatic update server so that the AIM IPS and NME IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the 7.0(7)E4 upgrade file (IPS-K9-7.0-7-E4.pkg) on the server, the AIM IPS and NME IPS will download and try to install the wrong file.
  - When you upgrade the AIM IPS or NME IPS using automatic update, you must disable heartbeat reset on the router before placing the upgrade file on your automatic update server. After the AIM IPS and NME IPS have been automatically updated, you can reenable heartbeat reset. If you do not disable heartbeat reset, the update can fail and leave the AIM IPS and NME IPS in an unknown state, which can require a system reimage to recover.
  - If you are using automatic update from an FTP or SCP server with a mixture of platforms that are supported by IPS 7.0(7)E4 as well as platforms that are not supported by IPS 7.0(7)E4, we recommend that you create a separate automatic update directory for the IPS 7.0(7)E4 files. Modify the automatic update configuration for sensors supporting IPS 7.0(7)E4 to point to the new directory. Placing the IPS 7.0(7)E4 files in the automatic update directory for those sensors not supporting IPS 7.0(7)E4 results in those sensors constantly downloading the update and generating errors during the attempted update.

- Using manual update:
  - If you want to manually update your sensor, copy the IPS 7.0(7)E4 update files to the directory on the server that your sensor polls for updates.
  - When you upgrade the AIM IPS or NME IPS using manual upgrade, you must disable heartbeat reset on the router before installing the upgrade. You can reenable heartbeat reset after you complete the upgrade. If you do not disable heartbeat reset, the upgrade can fail and leave the AIM IPS or NME IPS in an unknown state, which can require a system reimage to recover.
- Global correlation health status defaults to red and changes to green after a successful global correlation update. Successful global correlation updates require a DNS server or an HTTP proxy server. Because DNS and HTTP proxy server configuration features are beginning with IPS 7.0(1)E3, they are unconfigured after an upgrade from 6.*x* to 7.0(1)E3 or higher. As a result, global correlation health and overall sensor health status are red until you configure a DNS or HTTP proxy server on the sensor. If the sensor is deployed in an environment where a DNS or HTTP proxy server is not available, you can address the red global correlation health and overall sensor health status by disabling global correlation and configuring sensor health status not to include global correlation health status.
- If you install an update on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. You can reimage your sensor in the following ways:
  - For all sensors, use the **recover** command.
  - For the IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20, use the ROMMON to restore the system image.
  - For the AIM IPS and NME IPS, use the bootloader.
  - For the IDSM2, reimage the application partition from the maintenance partition.
  - For the AIP SSM, reimage from the adaptive security appliance using the **hw-module module 1 recover configure/boot** command.

Caution When you install the system image for your sensor, all accounts are removed and the default account and password are reset to **cisco**.

For More Information

For the procedures for reimaging sensors, refer to Upgrading, Downgrading, and Installing System Images.

Upgrading to IPS 7.0(7)E4

Caution You must log in to Cisco.com using an account with cryptographic privileges to download software. The first time you download software on Cisco.com, you receive instructions for setting up an account with cryptographic privileges.

Caution Do not change the filename. You must preserve the original filename for the sensor to accept the update.

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file (for example, IPS-K9-7.0-7-E4.pkg) 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-K9-7.0-7-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-K9-7.0-7-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 Version your new sensor version:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(7)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S615.0                  2012-01-03
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS-4260-K9
Serial Number:          AZBW5470014
No license present
Sensor up-time is 5 days.
Using 1887371264 out of 4100345856 bytes of available memory (46% usage) system is using
18.2M out of 38.5M bytes of available disk space (47% usage) application-data is using
48.0M out of 166.8M bytes of available disk space (30% usage) boot is using 46.1M out of
69.5M bytes of available disk space (70% usage) application-log is using 494.0M out of
513.0M bytes of available disk space (96% usage)


MainApp            B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
AnalysisEngine     B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
```

```
CollaborationApp    B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)    2012-01-16T04:53:24-0600
Running
CLI              B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600

Upgrade History:

  IPS-K9-7.0-7-E4   05:05:07 UTC Mon Jan 16 2012

Recovery Partition Version 1.1 - 7.0(7)E4

Host Certificate Valid from: 17-Jan-2012 to 17-Jan-2014

sensor#
```

For More Information

- For the procedure for locating software on Cisco.com, see Obtaining Software on Cisco.com, page 9.
- For the procedure for enabling and disabling heartbeat reset on the AIM IPS and the NME IPS, refer to Enabling and Disabling Heartbeat Reset.
- For the procedure for reimaging sensors, refer to Upgrading, Downgrading, and Installing System Images.
- For the procedure for configuring automatic updates, for the CLI refer to Configuring Automatic Updates, for the IDM refer to Configuring Automatic Update, and for the IME refer to Configuring Automatic Update.
- For the procedure for disabling global correlation, for the CLI refer to Configuring Global Correlation Inspection and Reputation Filtering, for the IDM refer to Configuring Global Correlation Inspection and Reputation Filtering, and for the IME refer to Configuring Global Correlation Inspection and Reputation Filtering.
- For the procedure for omitting global correlation from the overall sensor health status, for the CLI refer to Configuring Health Status Information, for the IDM refer to Configuring Sensor Health, and for the IME refer to Configuring Sensor Health.

After Upgrading to Cisco IPS 7.0(7)E4

This section provides information about what to do after you install IPS 7.0(7)E4. It contains the following topics:

Comparing Configurations

Compare your backed up and saved previous IPS configuration with the output of the **show configuration** command after upgrading to 7.0(7)E4 to verify that all the configuration has been properly converted.

Caution If the configuration is not properly converted, check the caveats for IPS 7.0(7)E4 or check Cisco.com for any upgrade issues that have been found. Contact the TAC if no DDTS refers to your situation.

For More Information

For a list of the caveats associated with this release, see Caveats, page 37.

Importing a New SSL Certificate

If necessary import the new SSL certificate for the upgraded sensor in to each tool being used to monitor the sensor.

For More Information

For the procedures for configuring TLS/SSL, for the CLI refer to Configuring TLS, for the IDM refer to Configuring Trusted Hosts, and for the IME refer to Configuring Trusted Hosts.

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://10.1.9.201:1040).

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. 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. The IDM on *ip_address* dialog box appears. 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 5 To authenticate the IDM, enter your username and password, and click **OK**. The IDM begins to load. If you change panes from Home to Configuration or Monitoring before the IDM has complete 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 Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization.

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, is it not necessary for this window to remain open.

Installing and Uninstalling the Sensor License

This section describes how to obtain a license key, how to license the sensor using the CLI, the IDM, or the IME, and how to remove the license. It contains the following topics:

Understanding the License

Although the sensor functions without the license key, you must have a license key to obtain signature updates and use the global correlation features. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract—Contact your reseller, Cisco service or product sales to purchase a contract.
- Your IPS device serial number—To find the IPS device serial number in the IDM or the IME, for the IDM choose **Configuration > Sensor Management > Licensing**, and for the IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**, or in the CLI use the **show version** command.
- Valid Cisco.com username and password

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to http://www.cisco.com/go/license and click **IPS Signature Subscription Service** to apply for a license key.

You can view the status of the license key in these places:

- IDM Home window Licensing section on the Health tab
- IDM Licensing pane (**Configuration > Licensing**)
- IME Home page in the Device Details section on the Licensing tab
- License Notice at CLI login

Whenever you start the IDM, the IME, or the CLI, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use the IDM, the IME, and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key to the computer that the IDM or the IME is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

When you purchase an ASA 5500 series adaptive security appliance product that does not contain IPS, you must purchase a SMARTnet contract.

Note SMARTnet provides operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

When you purchase an ASA 5500 series adaptive security appliance product that ships with the AIP SSM installed, or if you purchase it to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract.

Note Cisco Services for IPS provides IPS signature updates, operating system updates, access to Cisco.com, access to TAC, and hardware replacement NBD on site.

For example, if you purchase an ASA-5510 and then later want to add IPS and purchase an ASA-SSM-AIP-10-K9, you must now purchase the Cisco Services for IPS service contract. After you have the Cisco Services for IPS service contract, you must also have your product serial number to apply for the license key.

Caution If you ever send your product for RMA, the serial number changes. You must then get a new license key for the new serial number.

Obtaining and Installing the License Key

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

- Using the IDM or the IME, page 22
- Using the CLI, page 23

Using the IDM or the 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**. 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 3 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 4.
- 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 4 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 5 Click **OK**.

Step 6 Go to www.cisco.com/go/license. 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 because the license key only functions on the device with that number.

Step 7 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 8 Log in to the IDM or the IME.

Step 9 For the IDM choose **Configuration > Sensor Management > Licensing**. For the IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**.

Step 10 Under Update License, click the **License File** radio button.

Step 11 In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 12 Browse to the license file and click **Open**.

Step 13 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 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 2 Fill in the required fields. Your Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.

Note You must have the correct IPS device serial number because the license key only functions on the device with that number.

Step 3 Save the license key to a system that has a Web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor.

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

Step 6 Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(7)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S615.0                  2012-01-03
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS-4260-K9
Serial Number:          AZBW5470014
```

```
No license present
Sensor up-time is 5 days.
Using 1887371264 out of 4100345856 bytes of available memory (46% usage) system is using
18.2M out of 38.5M bytes of available disk space (47% usage) application-data is using
48.0M out of 166.8M bytes of available disk space (30% usage) boot is using 46.1M out of
69.5M bytes of available disk space (70% usage) application-log is using 494.0M out of
513.0M bytes of available disk space (96% usage)


MainApp            B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
AnalysisEngine     B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
CollaborationApp   B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
CLI              B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600

Upgrade History:

  IPS-K9-7.0-7-E4   05:05:07 UTC Mon Jan 16 2012

Recovery Partition Version 1.1 - 7.0(7)E4

Host Certificate Valid from: 17-Jan-2012 to 17-Jan-2014

sensor#
```

Uninstalling the License Key

Use the **erase license-key** command to uninstall the license key on your sensor. This allows you to delete an installed license key from a sensor without restarting the sensor or logging into the sensor using the service account.

To uninstall the license key, follow these steps:

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

Step 2 Uninstall the license key on the sensor.

```
sensor# erase license-key
Warning: Executing this command will remove the license key installed on the sensor.

You must have a valid license key installed on the sensor to apply the Signature Updates
and use the Global Correlation features.

Continue? []: yes
sensor#
```

Step 3 Verify the sensor key has been uninstalled.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(7)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S615.0                  2012-01-03
OS Version:             2.4.30-IDS-smp-bigphys
```

```
Platform:               IPS-4260-K9
Serial Number:          AZBW5470014
No license present
Sensor up-time is 5 days.
Using 1887371264 out of 4100345856 bytes of available memory (46% usage) system is using
18.2M out of 38.5M bytes of available disk space (47% usage) application-data is using
48.0M out of 166.8M bytes of available disk space (30% usage) boot is using 46.1M out of
69.5M bytes of available disk space (70% usage) application-log is using 494.0M out of
513.0M bytes of available disk space (96% usage)


MainApp            B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
AnalysisEngine     B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
CollaborationApp   B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600
Running
CLI              B-2012_JAN_16_04_50_7_0_7 (Ipsbuild)   2012-01-16T04:53:24-0600

Upgrade History:

  IPS-K9-7.0-7-E4   05:05:07 UTC Mon Jan 16 2012

Recovery Partition Version 1.1 - 7.0(7)E4

Host Certificate Valid from: 17-Jan-2012 to 17-Jan-2014
```

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 7.0(7)E4 software and the products that run it:

- 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.
- 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.
- The AIM IPS and the NME IPS do not support the IPv6 features, because the router in which they are installed does not send them IPv6 data. IPv6 inspection is also not supported on the IDSM2. The switch is able to send IPv6 packets to the IDSM2, but this has not been tested and is not officially supported. There is no support for IPv6 on the management (command and control) interface. With ASA 8.2.1, the AIP SSM supports IPv6 features.
- VACLs on Catalyst switches do not have IPv6 support. The most common method for copying traffic to a sensor configured in promiscuous mode is to use VACL capture. If you want to have IPv6 support, you can use SPAN ports.
- 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.
- The AIM IPS and the NME IPS do not support virtualization.
- When you reload the router, the AIM IPS and the NME IPS also reload. To ensure that there is no loss of data on the AIM IPS or the NME IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.
- Do not deploy IOS IPS and the and the NME IPS at the same time.
- When the AIM IPS and the NME IPS are used with an IOS firewall, make sure SYN flood prevention is done by the IOS firewall.

  The AIM IPS, the NME IPS, and the IOS firewall complement abilities of each other to create security zones in the network and inspect traffic in those zones. Because the AIM IPS, the NME IPS, and the IOS firewall operate independently, sometimes they are unaware of the activities of the other. In this situation, the IOS firewall is the best defense against a SYN flood attack.
- Cisco access routers only support one IDS/IPS per router.
- On IPS sensors with multiple processors (for example, the IPS 4260 and IPS 4270-20), packets may be captured out of order in the IP logs and by the **packet** command. Because the packets are not processed using a single processor, the packets can become out of sync when received from multiple processors.
- An IPS appliance can support both promiscuous and inline monitoring at the same time; however you must configure each physical interface in either promiscuous or inline mode. The sensor must contain at least two physical sensing interfaces to perform both promiscuous and inline monitoring. The exceptions to this are the AIP SSM-10, AIP SSM-20, and AIP SSM-40. The AIP SSM can support both promiscuous and inline monitoring on its single physical back plane interface inside

the adaptive security appliance. The configuration on the main adaptive security appliance can be used to designate which packets/connections should be monitored by the AIP SSM as either promiscuous or inline.

- 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 the IDM, they are turned into something unrecognizable and you will not be able to delete or edit the resulting object through the IDM or the CLI.

  This is true for any string that is used by CLI as an identifier, for example, names of time periods, inspect maps, server and URL lists, and interfaces.
- You can only install eight IDSM2s per switch chassis.
- 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.
- The IDM and the 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 detailed information on RADIUS authentication, for the IDM refer to Configuring Authentication and Users, and for the CLI refer to Configuring User Parameters.
- For the procedure for using the **unlock** command to unlock a locked user account, refer to Unlocking Locked Accounts.
- For more information on interoperability between modules, refer to Interoperability With Other IPS Modules.
- For more information about IPv6, switches, and lack of VACL capture, see IPv6, Switches, and Lack of VACL Capture.

Recovering the Password

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

Understanding Password Recovery

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

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

Table 4 lists the password recovery methods according to platform.

Table 4 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4200 series sensors	Standalone IPS appliances	GRUB prompt or ROMMON
AIP SSM	ASA 5500 series adaptive security appliance module	ASA CLI command
IDSM2	Switch IPS module	Password recovery image file
AIM IPS NME IPS	Router IPS modules	Bootloader command

For More Information

For more information on when and how to disable password recovery, see Disabling Password Recovery, page 35.

Recovering the Appliance Password

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

Using the GRUB Menu

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

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

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance. The following menu appears:

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

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

    Highlighted entry is 0:
```

Step 2 Press any key to pause the boot process.

Step 3 Choose **`2: Cisco IPS Clear Password (cisco)`**. The password is reset to **cisco**. You can change the password the next time you log into the CLI.

For More Information

For more information on connecting an appliance to a terminal server, refer to Connecting an Appliance to a Terminal Server.

Using ROMMON

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

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

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

Step 1 Reboot the appliance.

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

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

Step 3 Enter the following commands to reset the password.

```
confreg 0x7
boot
```

Sample ROMMON session:

```
Booting system, please wait...
CISCO SYSTEMS
```

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

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

```
confreg 0
```

Recovering the IDSM2 Password

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

FTP is the only supported protocol for image installations, so make sure you put the password recovery image file on an FTP server that is accessible to the switch. You must have administrative access to the Cisco 6500 series switch to recover the password on the IDSM2.

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

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

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

Once you have downloaded the password recovery image file, follow the instructions to install the system image file but substitute the password recovery image file for the system image file. The IDSM2 should reboot into the primary partition after installing the recovery image file. If it does not, enter the following command from the switch:

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

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

For More Information

- For the procedures for reimaging IDSM2, refer to Installing the IDSM2 System Image.
- For more information on downloading Cisco IPS software, see Obtaining Software on Cisco.com, page 9.

Recovering the AIP SSM Password

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

Note To reset the password, you must have ASA 7.2.2 or later.

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

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

Resetting the Password Using the CLI

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

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

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

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

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

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

Step 2 Reset the password for module 1.

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

Step 3 Press **Enter** to confirm.

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

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

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

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

Mod SSM Application Name           Status           SSM Application Version
```

```
--- ------------------------------ ---------------- --------------------------
  1 IPS                            Up               7.0(7)E4

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

Step 5 Session to the AIP SSM.

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

Step 6 Enter the default username (**cisco**) and password (**cisco**) at the login prompt.

```
login: cisco
Password: cisco

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

Step 7 Enter your new password twice.

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

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

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

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

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

Using the ASDM

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

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

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

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

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

Recovering the AIM IPS Password

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

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

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

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

Step 4 Session in to the AIM IPS.

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

Example:

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

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

Step 6 Reset the AIM IPS from the router console:

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

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

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

Step 9 Clear the password.

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

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

Recovering the NME IPS Password

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

To recover the password for NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

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

Step 4 Session in to the NME IPS.

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

Example

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

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

Step 6 Reset the NME IPS from the router console.

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

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

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

Step 9 Clear the password.

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

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

Disabling Password Recovery

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

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

Disabling Password Recovery Using the CLI

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

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

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

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

Step 4 Disable password recovery.

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

Disabling Password Recovery Using the IDM

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

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

Step 2 Choose **Configuration > Sensor Setup > Network**. The Network pane appears.

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

For More Information

- If you are not certain about whether password recovery is enabled or disabled, see Verifying the State of Password Recovery, page 36.
- For more information on reimaging sensors, refer to Upgrading, Downgrading, and Installing System Images.

Verifying the State of Password Recovery

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

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

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

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

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

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

```
sensor(config-hos)#
```

Troubleshooting Password Recovery

To troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If password recovery is attempted, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as the AIM IPS and NME IPS bootloader, ROMMON, and the maintenance partition for the IDSM2, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.
- To check the state of password recovery, use the **show settings | include password** command.
- When performing password recovery on the IDSM2, you see the following message: `Upgrading will wipe out the contents on the storage media`. You can ignore this message. Only the password is reset when you use the specified password recovery image.

For More Information

- For more information on reimaging sensors, refer to Upgrading, Downgrading, and Installing System Images.
- For the procedure for disabling password recovery, see Disabling Password Recovery, page 35.
- For the procedure for verifying the state of password recovery, see Verifying the State of Password Recovery, page 36.

Caveats

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

Resolved Caveats

The following known issues were recently found and resolved in the 7.0(7)E4 release:

- CSCte74540—AIP-SSM deny-connection on GRE packet causes GRE tunnel to be denied
- CSCtq95375—Radius module should handle multiple cisco-av-pair responses
- CSCtr19702—CLI/IME connection to IPS going down due to CT issue for FlexLM license
- CSCtr83959—Copy from file to current-config fails if auto-upgrade user is in file
- CSCts08725—IDCONF does not escape double quotes in signature names
- CSCts21378—Normalizer signature 1330.12 drops legit reset packet and keeps tracking

- CSCts26332—SSH TCP port forwarding is enabled - MIPS platform
- CSCts98784—IPS SSP collaborationApp core
- CSCtu45014—Deny-attacker-inline not working for ipv6 traffic - 7.1-3 service pack
- CSCtu74892—Summary alerts for IPv6 alerts are getting assigned negative score

Relevant Unresolved Caveats

The following known issue exists in the 7.0(7)E4 release:

- CSCtx03253—Signature Updates are happening, after removing the license from Sensor

Related Documentation

For more information on Cisco IPS, refer to the following documentation found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

- *Documentation Roadmap for Cisco Intrusion Prevention System*
- *Release Notes for Cisco Intrusion Prevention System*
- *Cisco Intrusion Prevention System Device Manager Configuration Guide*
- *Cisco Intrusion Prevention System Manager Express Configuration Guide*
- *Cisco Intrusion Prevention System Command Reference*
- *Cisco Intrusion Prevention System Sensor CLI Configuration Guide*
- *Cisco Intrusion Prevention System Appliance and Module Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*

Obtaining Documentation 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.