Obtaining Software

This chapter provides information on obtaining Cisco IPS software for the sensor. It contains the following sections:

⚠

Caution The BIOS on Cisco IPS sensors is specific to Cisco 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 Cisco IPS sensors voids the warranty.

Obtaining Cisco IPS 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 as needed. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

✎

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 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 the Readme to install the update.

> **Note**   Major and minor updates, service packs, recovery files, signature and signature engine updates are the same for all sensors. System image files are unique per platform.

For More Information

- For the procedure for obtaining and installing the license key, see Obtaining a License Key From Cisco.com, page 12-10.

- For an explanation of the IPS file versioning scheme, see IPS Software Versioning, page 12-3.

- For the procedure for obtaining and installing the license key, see Obtaining a License Key From Cisco.com, page 12-10.

IPS Software Versioning

When you download IPS software images from Cisco.com, you should understand the versioning scheme so that 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 6.0 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 6.0(1) requires 5.*x*. With each major update there are corresponding system and recovery packages.

Note   The 6.0(1) major update is only used to upgrade 5.*x* sensors to 6.0(1) If you are reinstalling 6.0(1) on a sensor that already has 6.0(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 6.0 is 6.1(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 used for the release of defect fixes with no new enhancements. Service packs contain all service pack fixes since the last base version (minor or major) and the new 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 6.0(3) is released, and E3 is the latest engine level, the service pack is released as 6.0(3)E3.

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.
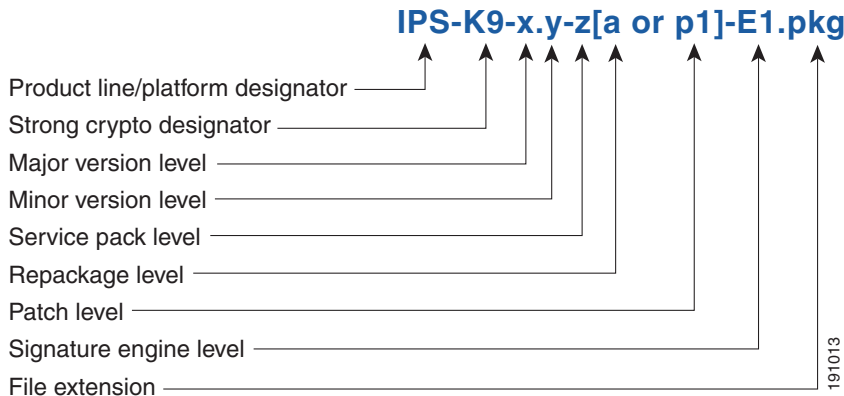
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 6.0(1p1) requires 6.0(1).

Note   Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 6.0(1p1) to 6.0(1p2) without first uninstalling 6.0(1p1).

Figure 12-1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 12-1   *IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases*

IPS-K9-x.y-z[a or p1]-E1.pkg

Product line/platform designator

Strong crypto designator

Major version level

Minor version level

Service pack level

Repackage level

Patch level

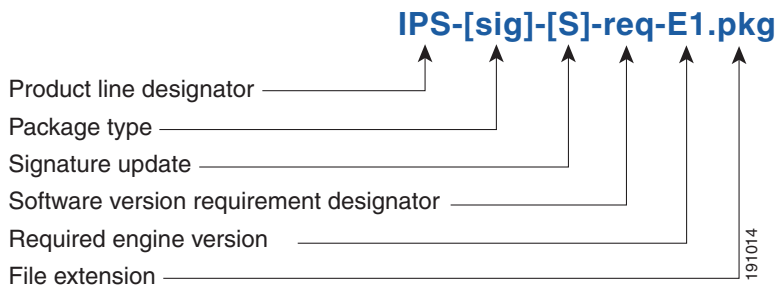Signature engine level

File extension

191013

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 12-2 illustrates what each part of the IPS software file represents for signature updates.

Figure 12-2   *IPS Software File Name for Signature Updates*

IPS-[sig]-[S]-req-E1.pkg

Product line designator

Package type

Signature update

Software version requirement designator

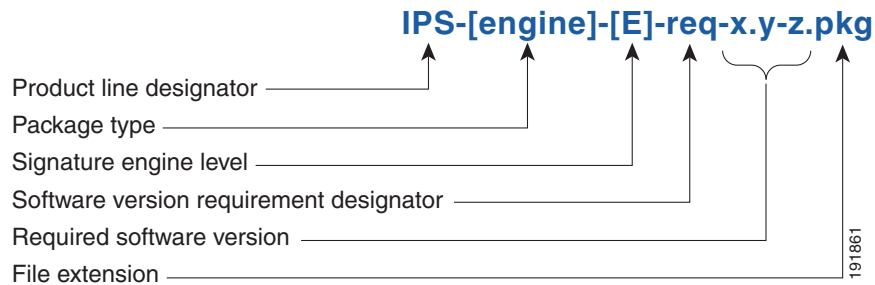Required engine version

File extension

191014

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 12-3 illustrates what each part of the IPS software file represents for signature engine updates.

Figure 12-3   IPS Software File Name for Signature Engine Updates

IPS-[engine]-[E]-req-x.y-z.pkg

Product line designator

Package type

Signature engine level

Software version requirement designator

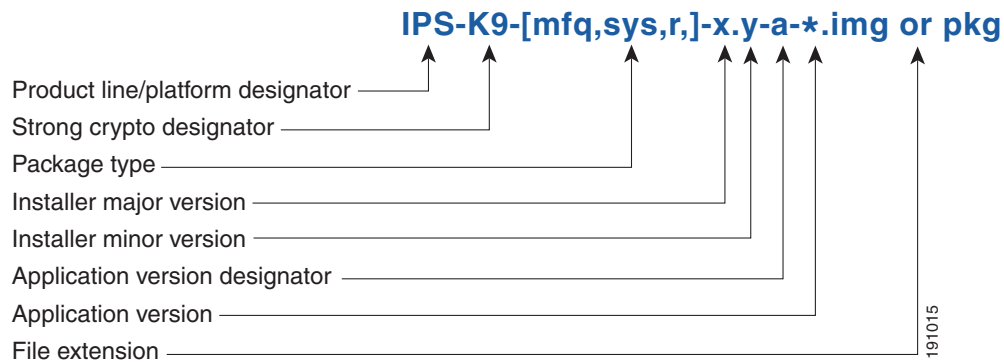Required software version

File extension

191861

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 12-4 illustrates what each part of the IPS software file represents for recovery and system image files.

Figure 12-4   IPS Software File Name for Recovery and System Image Files

IPS-K9-[mfq,sys,r,]-x.y-a-*.img or pkg

Product line/platform designator

Strong crypto designator

Package type

Installer major version

Installer minor version

Application version designator

Application version

File extension

191015

Software Release Examples

Table 12-1 lists platform-independent Cisco IPS 6.*x* software release examples. Refer to the Readmes that accompany the software files for detailed instructions on how to install the files.

Table 12-1   Platform-Independent Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update[1]	Weekly	sig	S353	IPS-sig-S353-req-E3.pkg
Signature engine update[2]	As needed	engine	E3	IPS-engine-E3-req-6.2-1.pkg
Service packs[3]	Semi-annually or as needed	—	6.1(3)	IPS-K9-6.2-3-E3.pkg
Minor version update[4]	Annually	—	6.1(1)	IPS-K9-6.2-1-E3.pkg **Note** IPS-AIM-K9-6.1-1-E3.pkg is the minor version update for AIM-IPS. IPS-NME-K-9-6.1-1-E3.pkg is the minor version update for NME-IPS.
Major version update[5]	Annually	—	6.0(1)	IPS-K9-6.0-1-E3.pkg
Patch release[6]	As needed	patch	6.0(1p1)	IPS-K9-patch-6.2-1pl-E3.pkg
Recovery package[7]	Annually or as needed	r	1.1-6.1(1)	IPS-K9-r-1.1-a-6.2-1-E3.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 6.0(1), but the recovery partition image will be r 1.2.

Table 12-2 describes platform-dependent software release examples.

Table 12-2   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-6.2-1-E3.img
Maintenance partition image[2]	Annually	mp	IDSM-2	c6svc-mp.2-1-2.bin.gz

Table 12-2   Platform-Dependent Release Examples (continued)

Release	Target Frequency	Identifier	Supported Platform	Example Filename
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 IDSM-2 maintenance partition. The file is installed from but does not affect the IDSM-2 application partition.

Table 12-3 describes the platform identifiers used in platform-specific names.

Table 12-3   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	SSC_5 SSM_10 SSM_20 SSM_40

For More Information

For instructions on how to access these files on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Upgrading Cisco IPS Software to 6.2

Observe the following when upgrading your sensor:

- The minimum required version for upgrading to 6.2 is 5.0(1) or later, which is available as a download from Cisco.com.

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

- Use IPS-AIM-K9-6.2-1-E3.pkg to upgrade AIM-IPS and IPS-NME-K9-6.2-1-E3 to upgrade NME-IPS. For all other supported sensors, use the IPS-K9-6.2-1-E3.pkg upgrade file.

- If you configured Auto Update for your sensor, copy the Cisco IPS 6.2(1)E3 update files to the directory on the server that your sensor polls for updates. If you install an update on your sensor and the sensor is unusable after it reboots, you must reimage your sensor.

- 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 6.2(1)E3 upgrade file (IPS-K9-6.2-1-E3.pkg), the AIM-IPS upgrade file (IPS-AIM-K9-6.2-1-E3.pkg), and the NME-IPS upgrade file (IPS-NME-K9-6.2-1-E3) on the automatic update server so that AIM-IPS and NME-IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the 6.2(1)E3 upgrade file (IPS-K9-6.2-1-E3.pkg) on the server, AIM-IPS and NME-IPS will download and try to install the wrong file.

You can reimage your sensor in the following ways:

- For all sensors, use the **recover** command.
- For IPS-4240, IPS-4255, IPS-4260, and IPS 4270-20, use the ROMMON to restore the system image.
- For AIM-IPS and NME-IPS, use the bootloader.
- For IDSM-2, reimage the application partition from the maintenance partition.

> **Note**   You cannot upgrade the IDSM (WS-X6381) to IPS 6.*x*. You must replace your IDSM (WS-X6381) with IDSM-2 (WS-SVC-IDSM2-K9), which supports version 6.2(1)E3.

- For AIP-SSM and AIP-SSC, 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 procedure for accessing downloads on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.
- For the procedure for using the **upgrade** command to upgrade the sensor, see Upgrading the Sensor, page 13-2.
- For the procedure for configuring automatic upgrades on the sensor, see Configuring Automatic Upgrades, page 13-6.
- For the procedure for using the **recover** command, see Recovering the Application Partition, page 13-11.
- For the procedures for using ROMMON to restore the system image, see Installing the IPS-4240 and IPS-4255 System Images, page 13-14, Installing the IPS-4260 System Image, page 13-17, and Installing the IPS 4270-20 System Image, page 13-19.
- For the procedure for restoring the AIM-IPS system image, see Installing the AIM-IPS System Image, page 13-22.
- For the procedure for using the **hw-module module 1 recover configure/boot** command to reimage AIP-SSM and AIP-SSC-5, see Installing the AIP-SSM and AIP-SSC-5 System Image, page 13-25.
- For the procedure for reimaging the IDSM-2 application partition from the maintenance partition, see Installing the IDSM-2 System Image, page 13-27.
- For the procedure for restoring the NME-IPS system image, see Installing the NME-IPS System Image, page 13-39.

Accessing IPS Documentation

You can find IPS documentation at this URL:

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

Or to access IPS documentation from Cisco.com, follow these steps:

Step 1   Log in to Cisco.com.

Step 2   Click **Support**.

Step 3   Under Support at the bottom of the page, click **Documentation**.

Step 4   Choose **Products > Security > Intrusion Prevention System (IPS) > IPS Appliances > Cisco IPS 4200 Series Sensors**. The Cisco IPS 4200 Series Sensors page appears. All of the most up-to-date IPS documentation is on this page.

> **Note**   Although you will see references to other IPS documentation sites on Cisco.com, this is the site with the most complete and up-to-date IPS documentation.

Step 5   Click one of the following categories to access Cisco IPS documentation:

- **Download Software**—Takes you to the Download Software site.

> **Note**   You must be logged into Cisco.com to access the software download site.

- **Release and General Information**—Contains documentation roadmaps and release notes.
- **Reference Guides**—Contains command references and technical references.
- **Design**—Contains design guide and design tech notes.
- **Install and Upgrade**—Contains hardware installation and regulatory guides.
- **Configure**—Contains configuration guides for IPS CLI, IDM, and IME.
- **Troubleshoot and Alerts**—Contains TAC tech notes and field notices.

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

Obtaining a License Key From Cisco.com

This section describes how to obtain a license key from Cisco.com and how to install it using the CLI, IDM, or IME. It contains the following topics:

- Understanding Licensing, page 12-10
- Service Programs for IPS Products, page 12-11
- Obtaining and Installing the License Key Using IDM or IME, page 12-12

Understanding Licensing

Although the sensor functions without the license key, you must have a license key to obtain signature updates. 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 IDM or IME, for IDM choose **Configuration > Sensor Management > Licensing**, and for 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 IDM, 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 IDM, 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 IDM or 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
- IDSM-2
- 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 AIP-SSM or AIP-SSC-5 installed, or if you purchase them 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 purchased an ASA-5510 and then later wanted to add IPS and purchased 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 will change. You must then get a new license key for the new serial number.

Obtaining and Installing the License Key Using 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 IDM or IME using an account with administrator privileges.

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

  IDM or 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 IDM or 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.

Step 7   Fill in the required fields.

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

Your license key will be sent to the e-mail address you specified.

Step 8   Save the license key to a hard-disk drive or a network drive that the client running IDM or IME can access.

Step 9   Log in to IDM or IME.

Step 10   For IDM choose **Configuration > Sensor Management > Licensing**. For IME choose **Configuration >** *sensor_name* **> Sensor Management > Licensing**.

Step 11   Under Update License, click the **License File** radio button.

Step 12   In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.

Step 13   Browse to the license file and click **Open**.

Step 14   Click **Update License**.

For More Information

For more information about obtaining a Cisco Services for IPS service contract, see Service Programs for IPS Products, page 12-11.

Obtaining and Installing the License Key Using the CLI

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.

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

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

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

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

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

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

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

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

  > **Note** If you use FTP or SCP protocol, you are prompted for a password. If you use SCP protocol, you must add the remote host to the SSH known hosts list.

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

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

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

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

  > **Note** If you use HTTPS protocol, 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.

![Note icon]

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

Your Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.

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@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

Step 6   Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.2(1)E3

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S391.0                    2008-04-16
    Virus Update        V1.2                      2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               ASA-SSM-20
Serial Number:          P300000220
Sensor up-time is 3 days.
Using 1031888896 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 52.4M out of 166.6M bytes of available disk space (33% usage)
boot is using 37.8M out of 68.5M bytes of available disk space (58% usage)


MainApp          N-2007_JUN_19_16_45   (Release)   2007-06-19T17:10:20-0500   Running
AnalysisEngine   N-2007_JUN_19_16_45   (Release)   2007-06-19T17:10:20-0500   Running
CLI              N-2007_JUN_19_16_45   (Release)   2007-06-19T17:10:20-0500


Upgrade History:

  IPS-K9-6.2-1-E3 15:36:05 UTC Thu Apr 24 2008

Recovery Partition Version 1.1 - 6.2(1)E3

Host Certificate Valid from: 25-Apr-2008 to 26-Apr-2010

sensor#
```

Step 7   Copy your license key from a sensor to a server to keep a backup copy of the license.

```
sensor# copy license-key scp://user@10.89.147.3://tftpboot/dev.lic
Password: *******
sensor#
```

For More Information

- For the procedure for adding a remote host to the SSH known hosts list, for IDM refer to Defining Known Hosts Keys, for IME refer to Defining Known Host Keys, and for the CLI refer to Adding Hosts to the SSH Known Hosts List.

- For the procedure for adding a remote host to the trusted hosts list, for IDM refer to Adding Trusted Hosts, for IME refer to Adding Trusted Hosts, and for the CLI refer to Adding TLS Trusted Hosts.

- For more information about obtaining a Cisco Services for IPS service contract, see Service Programs for IPS Products, page 12-11.