Obtaining Software

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

IPS 7.3 File List

The currently supported IPS 7.3(*x*) version is 7.3(1)E4.

For a list of the specific IPS filenames and the IPS versions that each sensor supports, refer to the Release Notes for your IPS version found at this URL:

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

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 in a release train format, a new release every three months. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

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

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

Downloading Cisco IPS Software

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

Step 1 Log in to Cisco.com.

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

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

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

Step 5 Enter your username and password.

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

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

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

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

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

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

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

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

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

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

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

For More Information

- For the procedure for obtaining and installing the license key, see Obtaining a License Key From Cisco.com, page C-8.
- For an explanation of the IPS file versioning scheme, see IPS Software Versioning, page C-3.

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. This section describes the various IPS software files.

Major Update

A major update contains new functionality or an architectural change in the product. For example, the Cisco IPS 7.3 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 7.3(1) requires 5.1(6) and later. With each major update there are corresponding system and recovery packages.

Note The 7.3(1) major update is used to upgrade 5.1(6) and later sensors to 7.3(1) If you are reinstalling 7.3(1) on a sensor that already has 7.3(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 7.3 is 7.4. 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 packs 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 7.3(3) is released, and E4 is the latest engine level, the service pack is released as 7.3(3)E4.

Patch Release

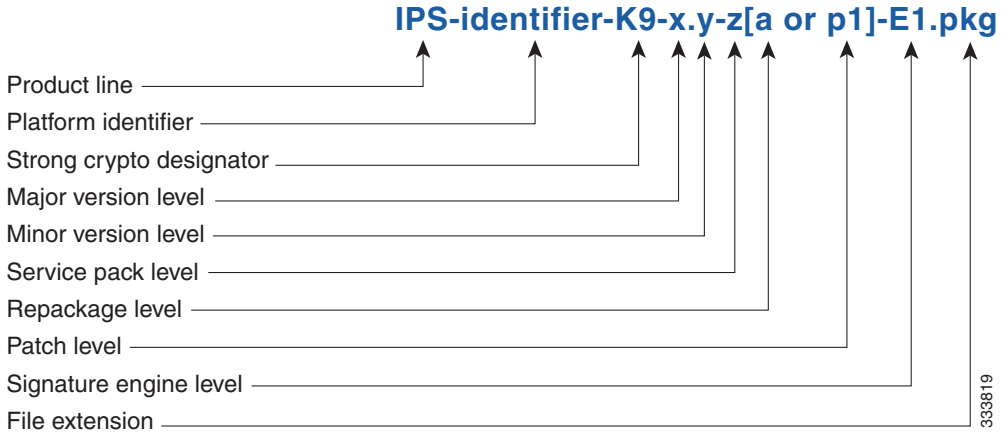
A patch release is used to address defects that are identified in the upgrade binaries after a software release. Rather than waiting until the next major or minor update, or service pack to address these defects, a patch can be posted. Patches include all prior patch releases within the associated service 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 7.3(1p1) requires 7.3(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 7.3(1p1) to 7.3(1p2) without first uninstalling 7.3(1p1).

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

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

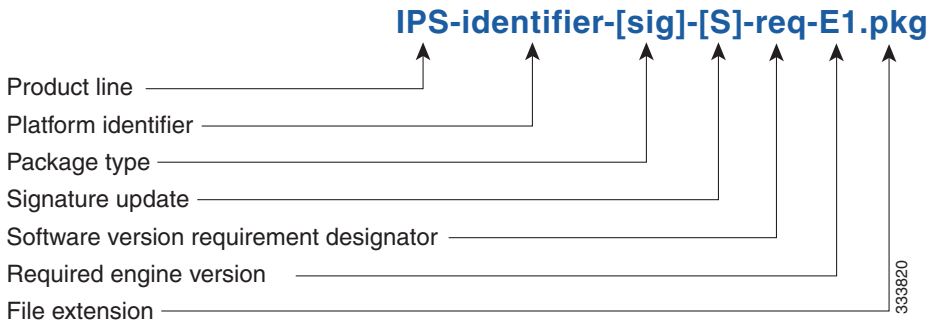


Signature Update

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. Signature updates also contain the latest threat profile updates. If there is a new threat profile, it will be installed along with the signature update.

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

Figure C-2 IPS Software File Name for Signature Updates

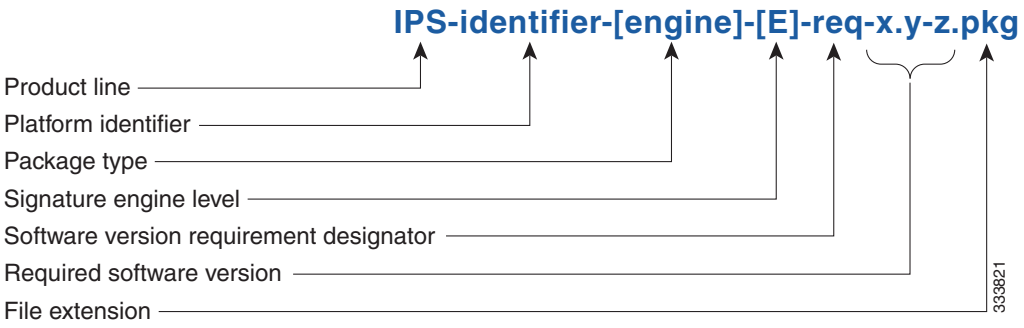


Signature Engine Update

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

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



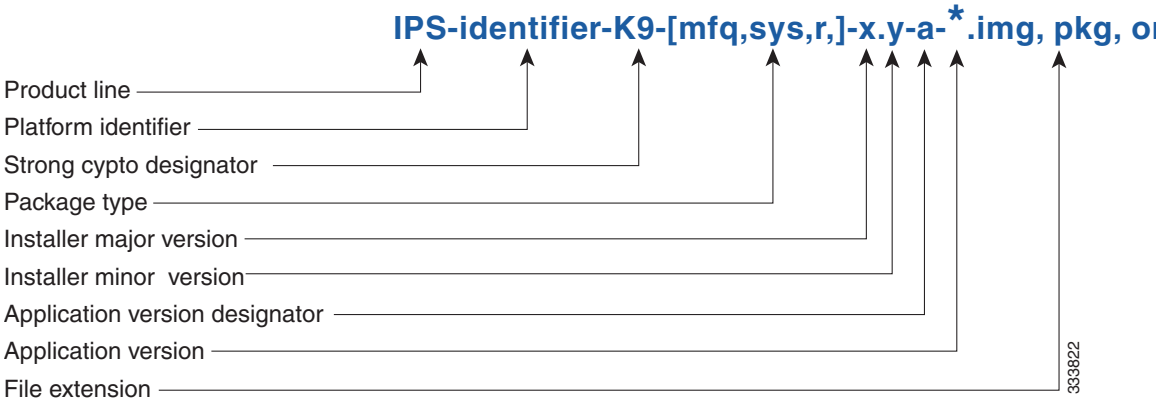
Recovery and System Image Files

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

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



IPS Software Release Examples

Table C-1 lists Cisco IPS software release examples.

Table C-1 Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update[1]	Weekly	sig	S552	IPS-sig-S552-req-E4.pkg
Signature engine update[2]	As needed	engine	E4	IPS-*identifier*-engine-E4-req-7.3-2.pkg
Service packs[3]	Every three months	—	7.3(2)	IPS-*identifier*-K9-7.3-2-E4.pkg
Minor version update[4]	Annually	—	7.3(1)	IPS-*identifier*-K9-7.3-1-E4.pkg
Major version update[5]	Annually	—	8.0(1)	IPS-*identifier*-K9-8.0-1-E4.pkg
Patch release[6]	As needed	patch	7.3(1p1)	IPS-*identifier*-K9-patch-7.3-1pl-E4.pkg
Recovery package[7]	Annually or as needed	r	1.1-7.3(1)	IPS-*identifier*-K9-r-1.1-a-7.3-1-E4.pkg
System image[8]	Annually	sys	Separate file per sensor platform	IPS-*identifier*-K9-sys-1.1-a-7.3-1-E4.img IPS-*identifier*-K9-sys-1.1-a-7.3-1-E4.img

1. Signature updates include the latest cumulative IPS signatures and threat profiles.
2. Signature engine updates add new engines or engine parameters that are used by new signatures in later signature updates.
3. Service packs include new features and 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 7.2(3), but the recovery partition image will be r 1.2.
8. The system image includes the combined recovery and application image used to reimage an entire sensor.

Table C-1 describes the platform identifiers used in platform-specific names.

Table C-2 Platform Identifiers

Sensor Family	Identifier
IPS 4345 series	4345
IPS 4360 series	4360
IPS 4510 series	4510
IPS 4520 series	4520

For More Information

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

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, the IDM, or the IME. It contains the following topics:

Understanding Licensing

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:

- The IDM Home window Licensing section on the Health tab
- The IDM Licensing pane (**Configuration > Licensing**)
- The 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 4345
- IPS 4345-DC
- IPS 4360
- IPS 4510
- IPS 4520

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 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**.

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

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

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

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

Step 6 Click **OK**.

Step 7 Log in to Cisco.com.

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

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

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

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

Step 11 Log in to the IDM or the IME.

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

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

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

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

Step 16 Click **Update License**.

For More Information

For more information about obtaining a Cisco Services for IPS service contract, see Service Programs for IPS Products, page C-9.

Obtaining and Installing the License Key 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 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 Log in to Cisco.com.

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

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

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

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

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

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

Step 6 Copy the license key to the sensor.

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

Step 7 Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

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


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

Upgrade History:

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

Recovery Partition Version 1.1 - 7.3(1)E4

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

sensor#
```

For More Information

- For the procedure for adding a remote host to the SSH known hosts list, for the IDM refer to Defining Known Hosts Keys, for the 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 the IDM refer to Adding Trusted Hosts, for the 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 C-9.

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 7.3(1)E4

Host:
    Realm Keys               key1.0
Signature Definition:
    Signature Update         S741.0        2013-09-10
    Threat Profile Version   2
OS Version:                  2.6.29.1
Platform:                    IPS-4360
Serial Number:               FGL1702401M
No license present
Sensor up-time is 22:09.
Using 14372M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.6M out of 376.4M bytes of available disk space (24% usage)
boot is using 63.1M out of 70.2M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


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

Upgrade History:

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

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

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

sensor#
```