CHAPTER 12

Obtaining Software

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

Caution The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/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 IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see Obtaining Cisco IPS Software, page 12-1.

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.

Note You must be logged in to Cisco.com to download software.

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

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.

IPS Software Versioning

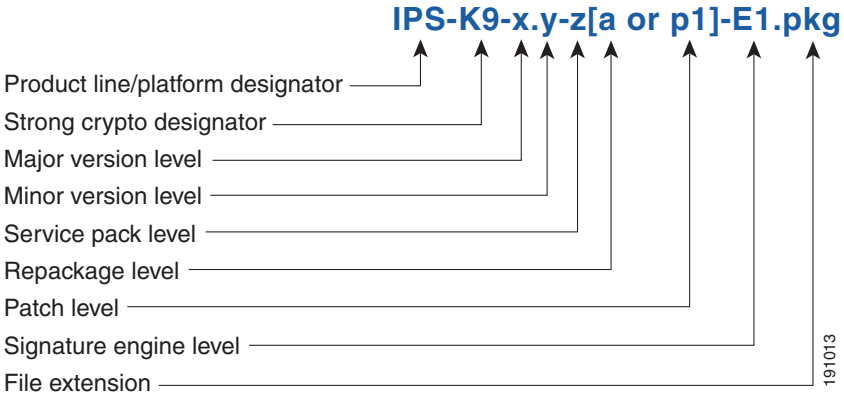
When you download IPS software images from Cisco.com, you should understand the versioning scheme so that you know which files are base files, which are cumulative, and which are incremental.

This section describes the various IPS software files, gives software release examples, and contains the following topics:

Major and Minor Updates, Service Packs, and Patch Releases

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



Major Update

Contains new functionality or an architectural change in the product. For example, the IPS 5.0 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 5.0(1) requires 4.*x*. With each major update there are corresponding system and recovery packages.

Note The 5.0(1) major update is only used to upgrade 4.*x* sensors to 5.0(1). If you are reinstalling 5.0(1) on a sensor that already has 5.0(1) installed, use the system image or recovery procedures rather than the major update.

Minor Update

Incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 5.0 is 5.1(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 Packs

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

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.

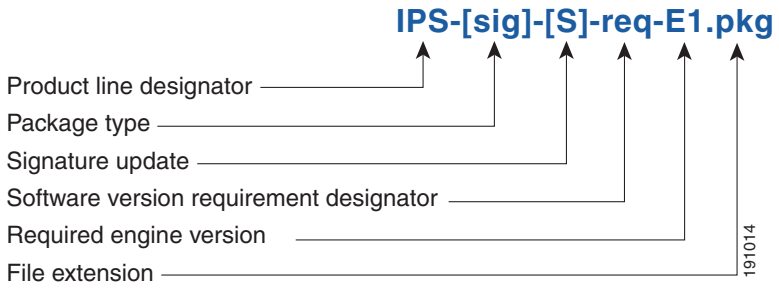
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 5.0(1p1) requires 5.0(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 5.0(1p1) to 5.0(1p2) without first uninstalling 5.0(1p1).

Signature/Virus Updates and Signature Engine Updates

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

Figure 12-2 IPS Software File Name for Signature/Virus Updates,



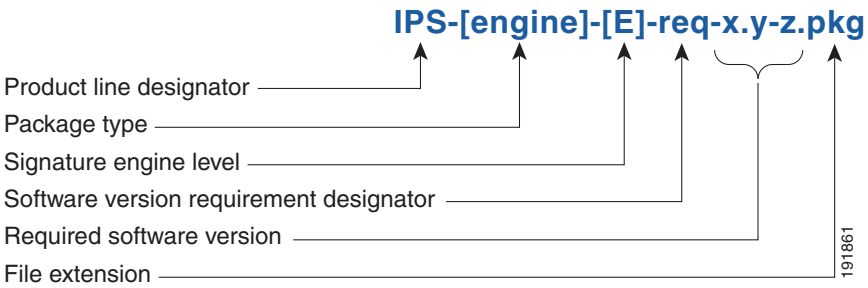
Signature/Virus Updates

Executable 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.

A virus component for the signature updates is packaged with the signature update. Virus updates are generated by Trend Microsystems for use by the Cisco Intrusion Containment System (Cisco ICS). Once created for use by Cisco ICS, they are later be incorporated into standard Cisco signature updates.

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



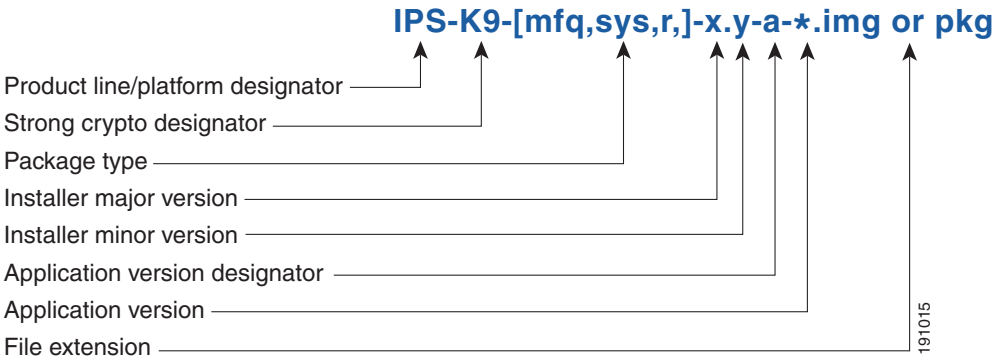
Signature Engine Updates

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

Recovery, Manufacturing, and System Images

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

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



Recovery and system images contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field.

Installer Major Version

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.

Installer Minor Version

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.

IPS 5.1 Software Release Examples

Table 12-1 lists platform-independent IDS 5.1(5)E1 software release examples. Refer to the Readmes that accompany the software files for detailed instructions on how to install the files. For instructions on how to access these files on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.

Table 12-1 Platform-Independent Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update[1]	Weekly	sig	S700	IPS-sig-S700-req-E1.pkg
Signature engine update[2]	As needed	engine	E1	IPS-engine-E1-req-5.1-3.pkg
Service packs[3]	Semi-annually or as needed	—	5.1(3)	IPS-K9-5.1-3-E1.pkg
Minor version update[4]	Annually	—	5.1(1)	IPS-K9-5.1-1-E1.pkg
Major version update[5]	Annually	—	5.0(1)	IPS-K9-6.0-1-E1.pkg
Patch release[6]	As needed	patch	5.0(1p1)	IPS-K9-patch-5.1-1pl-E1.pkg
Recovery package[7]	Annually or as needed	r	1.1-5.0(1)	IPS-K9-r-1.1-a-5.1-1-E1.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 5.0(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-5.1-1-E1.img
Maintenance partition image[2]	Annually	mp	IDSM-2	c5svc-mp.2-1-2.bin.gz
Bootloader	As needed	bl	NM-CIDS AIM-IPS NME-IPS	servicesengine-boot-1.0-4.bin

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.

Note IDS-4235 and IDS-4250 do not use platform-specific image files.

Table 12-3 Platform Identifiers

Sensor	Identifier
IDS-4215	IDS-4215-
IPS-4240	IPS-4240-
IPS-4255	IPS-4255-
IPS-4260	IPS-4260-
IDS module for Catalyst 6K	WS-SVC-IDSM2-
IDS network module	IPS-NM-CIDS-
AIP-SSM	IPS-SSM-

Upgrading Cisco IPS Software to 5.*x*

Note You cannot upgrade the IDSM (WS-X6381) to Cisco IDS 5.*x*. You must replace your IDSM (WS-X6381) with IDSM-2 (WS-SVC-IDSM2-K9), which supports version 5.*x*.

Pay attention to the following when upgrading to IPS 5.x:

- The minimum required version for upgrading to 5.1 is 5.0. The minimum required version for upgrading to 5.0 is 4.1(1). The upgrades from Cisco 5.0 to 5.1 and Cisco 4.1 to 5.0 are available as a downloads from Cisco.com. For the procedure for accessing Downloads on Cisco.com, see Obtaining Cisco IPS Software, page 12-1.
- After downloading the 5.1 upgrade file, refer to the accompanying Readme for the procedure for installing the 5.1 upgrade file using the **upgrade** command. Fro more information, see Upgrading the Sensor, page 13-2.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- If you configured Auto Update for your sensor, copy the 5.1 upgrade file to the directory on the server that your sensor polls for updates. See Configuring Automatic Upgrades, page 13-6.
- If you install an upgrade on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. Upgrading a sensor from any Cisco IDS version before 4.1 also requires you to use the **recover** command or the recovery/upgrade CD.

You can reimage your sensor in the following ways:

- For IDS appliances with a CD-ROM drive, use the recovery/upgrade CD.

  For the procedure, see Using the Recovery/Upgrade CD, page 13-22.
- For all sensors, use the **recover** command.

  For the procedure, see Recovering the Application Partition, page 13-9.
- For the IDS-4215, IPS-4240, IPS 4255, and IPS-4260 use the ROMMON to restore the system image.

  For the procedures, see Installing the IDS-4215 System Image, page 13-14, Installing the IPS-4240 and IPS-4255 System Image, page 13-17, and Installing the IPS-4260 System Image, page 13-20.
- For NM-CIDS, use the bootloader.

  For the procedure, see Installing the NM-CIDS System Image, page 13-23.
- For IDSM-2, reimage the application partition from the maintenance partition.

  For the procedure, see Installing the IDSM-2 System Image, page 13-25.
- For AIP-SSM, reimage from ASA using the **hw-module module 1 recover configure/boot** command.

  For the procedure, see Installing the AIP-SSM System Image, page 13-36.

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

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 or IDM. It contains the following topics:

Overview

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. For more information, see Service Programs for IPS Products, page 12-9.

- Your IPS device serial number

  To find the IPS device serial number in IDM, click **Configuration > Licensing**, or in the CLI use the **show version** command.

- Valid Cisco.com username and password

Note You can install the first few signature updates for 5.*x* without a license. This gives you time to get your sensor licensed. If you are unable to get your sensor licensed because of confusion with your contract, you can obtain a 60-day trail 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. For the procedure, see Obtaining and Installing the License, page 12-11.

Whenever you start IDM, a dialog box informs you 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 but you cannot download signature updates.

When you enter the CLI, you receive the following message if there is no license installed:

```
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
```

You will continue to see this message until you have installed a license.

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:

- IDS-4215
- IPS-4240
- IPS-4255
- IDSM-2
- NM-CIDS

For ASA products, if you purchased one of the following ASA products that do not contain IPS, you must purchase a SMARTnet contract:

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8
- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9

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

If you purchased one of the following ASA products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA product, you must purchase the Cisco Services for IPS service contract:

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9

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. For the procedure, see Obtaining and Installing the License, page 12-11.

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

This section describes how to obtain and install the license using IDM or the CLI. It contains the following topics:

Using IDM

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. For more information, see Service Programs for IPS Products, page 12-9.

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

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

Step 2 Choose **Configuration > Licensing**. The Licensing pane appears. Information about the current license state is displayed. If you have already installed your license, you can click **Download** to update it if needed.

Step 3 Choose the method to deliver the license:

a. Select **Cisco Connection Online** to obtain the license from Cisco.com.

IDM 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.

b. Select **License File** to use a license file.

To use this option, you must apply for a license at www.cisco.com/go/license.

The license is sent to you in e-mail and you save it to a drive that is accessible by IDM. This option is useful if your computer does not have access to Cisco.com.

Go to Step 7.

Step 4 Click **Update License**. The Licensing dialog box appears.

Step 5 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 has been updated.

Step 6 Click **OK**.

Step 7 Go to www.cisco.com/go/license.

Step 8 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 Cisco IPS Signature Subscription Service license key is sent by e-mail to the e-mail address you specified.

Step 9 Save the license file to a hard-disk drive or a network drive that is accessible by the client running IDM.

Step 10 Log in to IDM.

Step 11 Choose **Configuration > Licensing**.

Step 12 Under Update License, choose **Update From: License File**.

Step 13 In the **Local File Path** field, specify the path to the license file or click **Browse Local** to browse to the file. The Select License File Path dialog box appears.

Step 14 Browse to the license file and click **Open**.

Step 15 Click **Update License**.

Using the CLI

Use the **copy** *source_url license_file_name* **license-key** command to copy the license file 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
- 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 FTP or SCP, you are prompted for a password.

Note If you use SCP, the remote host must be on the SSH known hosts list. For the procedure, see Defining Known Host Keys, page 2-10.

Note If you use HTTPS, the remote host must be a TLS trusted host. For the procedure, see Adding Trusted Hosts, page 2-15.

To install the license key, follow these steps:

Step 1 Apply for the license key at 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. For more information, see Service Programs for IPS Products, page 12-9.

Step 2 Fill in the required fields.

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 is 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 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_15_03.00   (QATest)    2005-02-15T12:59:35-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600
```

```
Upgrade History:

    IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149


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#
```

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

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.