CHAPTER **20**

Obtaining Software

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

IPS 7.2(*x*) File List

The currently supported IPS 7.2(*x*) versions are 7.2(1)E4 and 7.2(2)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 an explanation of the IPS file versioning scheme, see IPS Software Versioning, page 20-2.

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 7.2 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 7.2(1) requires 5.1(6) and later. With each major update there are corresponding system and recovery packages.

Note The 7.2(1) major update is used to upgrade 5.1(6) and later sensors to 7.2(1) If you are reinstalling 7.2(1) on a sensor that already has 7.2(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 7.2 is 7.3. 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 7.2(3) is released, and E4 is the latest engine level, the service pack is released as 7.2(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.
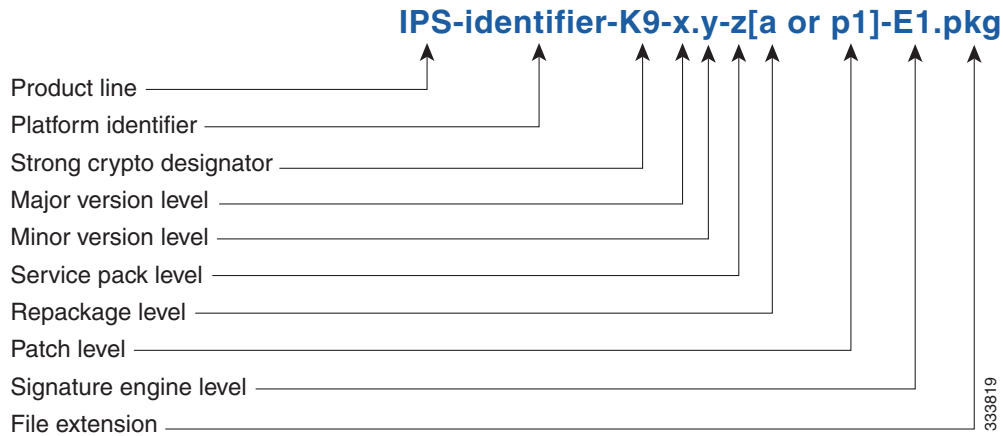
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 7.2(1p1) requires 7.2(1).

Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 7.2(1p1) to 7.2(1p2) without first uninstalling 7.2(1p1).

Figure 20-1 illustrates what each part of the IPS software file represents for major and minor updates, service packs, and patch releases.

Figure 20-1   IPS Software File Name for Major and Minor Updates, Service Packs, and Patch Releases
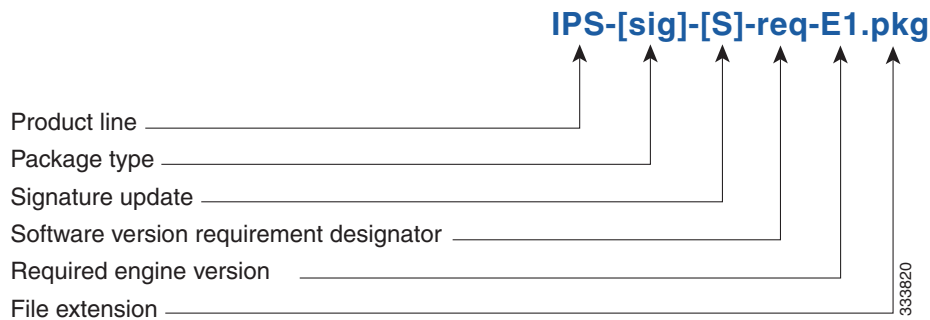
IPS-identifier-K9-x.y-z[a or p1]-E1.pkg

Product line
Platform identifier
Strong crypto designator
Major version level
Minor version level
Service pack level
Repackage level
Patch level
Signature engine level
File extension

333819

Signature Update and Signature Engine 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.

The signature engine update is contained in the signature updates.

Figure 20-2 illustrates what each part of the IPS software file represents for signature updates and signature engine updates.

Figure 20-2   IPS Software File Name for Signature Updates and Signature Engine Updates

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

Product line
Package type
Signature update
Software version requirement designator
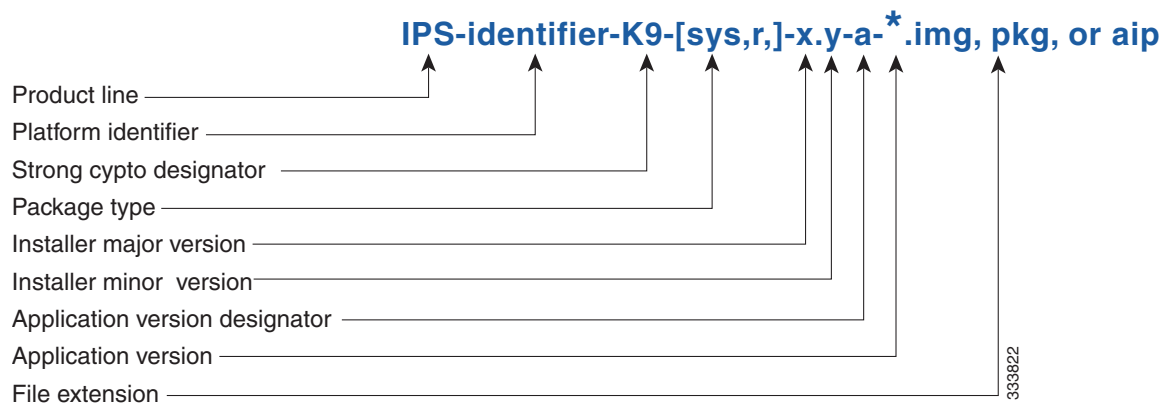Required engine version
File extension

333820

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 20-3 illustrates what each part of the IPS software file represents for recovery and system image filenames.

Figure 20-3   IPS Software File Name for Recovery and System Image Files

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

Product line
Platform identifier
Strong cypto designator
Package type
Installer major version
Installer minor version
Application version designator
Application version
File extension

333822

IPS Software Release Examples

Table 20-1 lists Cisco IPS software release examples.

Table 20-1   Cisco IPS Software Release Examples

Release	Target Frequency	Identifier	Example Version	Example Filename
Signature update and signature engine update[1]	Weekly	sig	S552 E4	IPS-sig-S552-req-E4.pkg
Service packs[2]	Every three months	—	7.2(2)	IPS-*identifier*-K9-7.2-2-E4.pkg
Minor version update[3]	Annually	—	7.2(1)	IPS-*identifier*-K9-7.2-1-E4.pkg
Major version update[4]	Annually	—	8.0(1)	IPS-*identifier*-K9-8.0-1-E4.pkg
Patch release[5]	As needed	patch	7.2(1p1)	IPS-*identifier*-K9-patch-7.2-1pl-E4.pkg
Recovery package[6]	Annually or as needed	r	1.1-7.2(1)	IPS-*identifier*-K9-r-1.1-a-7.2-1-E4.pkg
System image[7]	Annually	sys	Separate file per sensor platform	IPS-*identifier*-K9-sys-1.1-a-7.2-2-E4.img IPS-*identifier*-K9-sys-1.1-a-7.2-2-E4.aip

1. Signature updates include the latest cumulative IPS signatures. Signature engine updates add new engines or engine parameters that are used by new signatures in later signature updates.

2. Service packs include new features and defect fixes.

3. Minor versions include new minor version features and/or minor version functionality.

4. Major versions include new major version functionality or new architecture.

5. Patch releases are for interim fixes.

6. 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.

7. The system image includes the combined recovery and application image used to reimage an entire sensor.

Table 20-2 describes the platform identifiers used in platform-specific names.

Table 20-2   Platform Identifiers

Sensor Family	Identifier
ASA 5500-X series	SSP_5512 SSP_5515 SSP_5525 SSP_5545 SSP_5555
ASA 5585-X series	SSP_10 SSP_20 SSP_40 SSP_60
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 20-1.

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