



CHAPTER 20

Obtaining Software

This chapter describes how to obtain and install the latest Cisco IPS software, and contains the following topics:

- [Obtaining Cisco IPS Software, page 20-1](#)
- [IPS Software Versioning, page 20-3](#)
- [Software Release Examples, page 20-6](#)
- [Upgrading Cisco IPS Software to 7.0, page 20-8](#)
- [Accessing IPS Documentation, page 20-9](#)
- [Cisco Security Intelligence Operations, page 20-10](#)

Obtaining Cisco IPS Software

You can download the latest Cisco IPS software from Cisco.com. You must have an account with cryptographic access before you can download software and you must be logged into Cisco.com to access the software download site. You can sign up for IPS Alert Bulletins to receive information on the latest software releases.



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.

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

Downloading IPS Software

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

-
- Step 1** Log in to Cisco.com.
 - Step 2** From the Support drop-down menu, choose **Download Software**.
 - Step 3** Under Select a Software Product Category, choose **Security Software**.
 - Step 4** Choose **Intrusion Prevention System (IPS)**.
 - Step 5** Enter your username and password.
 - Step 6** In the Download Software window, choose **IPS Appliances > Cisco Intrusion Prevention System** and then click the version you want to download.



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

- Step 7** Click the type of software file you need. The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.
- Step 8** Click the file you want to download. The file details appear.
- Step 9** Verify that it is the correct file, and click **Download**.
- Step 10** Click **Agree** to accept the software download rules. The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.
 - Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.
 - Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again. The File Download dialog box appears.
- Step 11** Open the file or save it to your computer.
- Step 12** Follow the instructions in 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 [Configuring Licensing, page 16-12](#).
- For an explanation of the IPS file versioning scheme, see [IPS Software Versioning, page 20-3](#).

IPS Software Versioning

**Note**

The software version installed on your sensor is listed in the Sensor Information gadget in the Home pane of the IDM.

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 7.0 base version includes everything (except deprecated features) since the previous major release (the minor update features, service pack fixes, and signature updates) plus any new changes. Major update 7.0(1) requires 5.1(6) and later. With each major update there are corresponding system and recovery packages.

**Note**

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

Minor Update

A minor update is incremental to the major version. Minor updates are also base versions for service packs. The first minor update for 7.0 is 7.1(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 7.0(3) is released, and E3 is the latest engine level, the service pack is released as 7.0(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 7.0(1p1) requires 7.0(1).

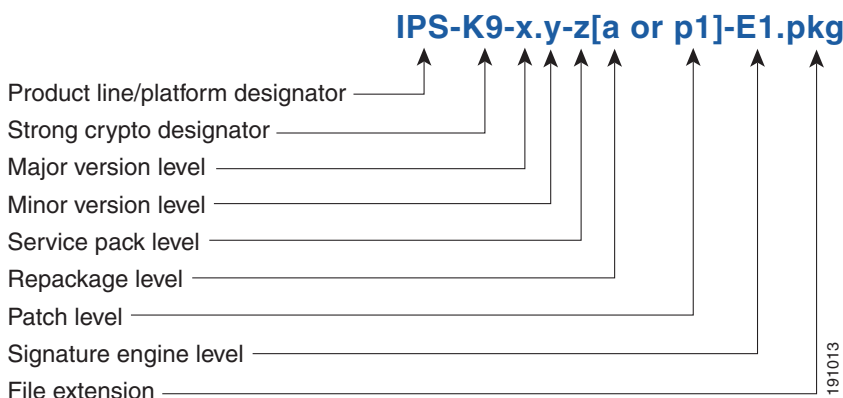


Note

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

Figure 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

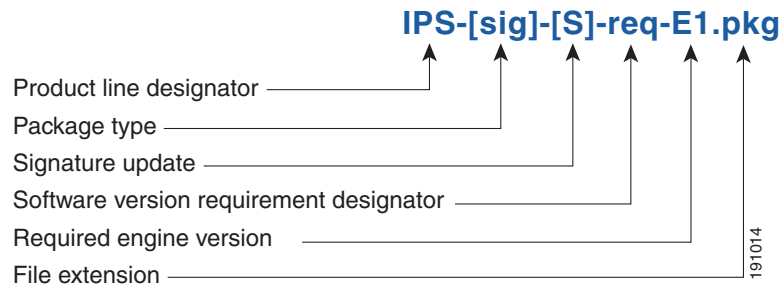


Signature Update

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

Figure 20-2 IPS Software File Name for Signature Updates

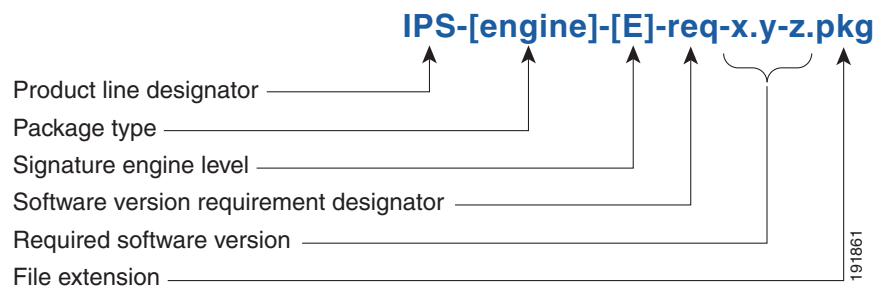


Signature Engine Update

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 20-3 illustrates what each part of the IPS software file represents for signature engine updates.

Figure 20-3 IPS Software File Name for Signature Engine Updates



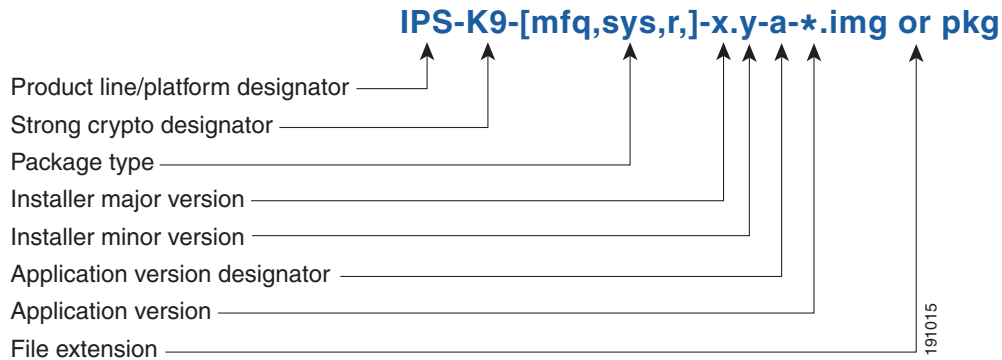
Recovery and System Image

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 20-4 illustrates what each part of the IPS software file represents for recovery and system image files.

Figure 20-4 IPS Software File Name for Recovery and System Image Files



Software Release Examples

Table 20-1 lists platform-independent Cisco IPS 7.x software release examples. Refer to the Readmes that accompany the software files for detailed instructions on how to install the files.

Table 20-1 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-7.0-1.pkg |
| Service packs ³ | Semi-annually or as needed | — | 7.1(3) | IPS-K9-7.1-3-E3.pkg |
| Minor version update ⁴ | Annually | — | 7.1(1) | IPS-K9-7.1-1-E3.pkg Note IPS-AIM-K9-7.1-1-E3.pkg is the minor version update for the AIM IPS. IPS-NME-K-9-7.1-1-E3.pkg is the minor version update for the NME IPS. |
| Major version update ⁵ | Annually | — | 7.0(1) | IPS-K9-7.0-1-E3.pkg |
| Patch release ⁶ | As needed | patch | 7.0(1p1) | IPS-K9-patch-7.0-1pl-E3.pkg |
| Recovery package ⁷ | Annually or as needed | r | 1.1-7.0(1) | IPS-K9-r-1.1-a-7.0-1-E3.pkg |

- 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.
- Service packs include defect fixes.
- Minor versions include new minor version features and/or minor version functionality.
- 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 20-2 describes platform-dependent software release examples.

Table 20-2 Platform-Dependent Release Examples

| Release | Target Frequency | Identifier | Supported Platform | Example Filename |
|--|------------------|-------------|--|--|
| System image ¹ | Annually | sys | Separate file for each sensor platform | IPS 4240-K9-sys-1.1-a-7.0-1-E3.img |
| Maintenance partition image ² | Annually | mp | IDSM2 | c6svc-mp.2-1-2.bin.gz |
| Bootloader | As needed | bl | AIM IPS NME IPS | pse_aim_x.y.z.bin pse_nm_x.y.z.bin (where x, y, z is the release number) |
| Mini-kernel | As needed | mini-kernel | AIM IPS NME IPS | pse_mini_kernel_1.1.10.64.bz2 |

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

Table 20-3 describes the platform identifiers used in platform-specific names.

Table 20-3 Platform Identifiers

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

For More Information

- For instructions on how to access these files on Cisco.com, see [Obtaining Cisco IPS Software, page 20-1](#).
- For procedures for installing the various software files, see [Chapter 21, “Upgrading, Downgrading, and Installing System Images.”](#)

Upgrading Cisco IPS Software to 7.0

Observe the following when upgrading to IPS 7.0:

- The minimum required version for upgrading to 7.0 is 5.1(6) or later.
- Use IPS-AIM-K9-7.0-1-E3.pkg to upgrade the AIM IPS and IPS-NME-K9-7.0-1-E3 to upgrade the NME IPS. For all other supported sensors, use the IPS-K9-7.0-1-E3.pkg upgrade file.
- If you configured automatic update for your sensor, copy the 7.0(1)E3 update files to the directory on the server that your sensor polls for updates.
- If you are using automatic update with a mixture of the AIM IPS, the NME IPS, and other IPS appliances or modules, make sure you put both the 7.0(1)E3 upgrade file (IPS-K9-7.0-1-E3.pkg), the AIM IPS upgrade file (IPS-AIM-K9-7.0-1-E3.pkg), and the NME IPS upgrade file (IPS-NME-K9-7.0-1-E3) on the automatic update server so that the AIM IPS and the NME IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the 7.0(1)E3 upgrade file (IPS-K9-7.0-1-E3.pkg) on the server, the AIM IPS and the NME IPS will download and try to install the wrong file.
- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- The Cisco.com IP address has been changed in the Auto Update configuration.



Caution

In IPS 7.0(8)E4 the default value of the Cisco server IP address has been changed from 198.133.219.25 to 72.163.4.161 in the Auto Update URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new IP address.

- If you install an update on your sensor and the sensor is unusable after it reboots, you must reimage your sensor. You can reimage your sensor in the following ways:
 - For all sensors, use the **recover** command.
 - For IPS 4240, IPS 4255, IPS 4260, and IPS 4270-20, use the ROMMON to restore the system image.
 - For the AIM IPS and the NME IPS, use the bootloader.
 - For the IDSM2, reimage the application partition from the maintenance partition.
 - For the AIP SSM, reimage from the adaptive security appliance using the **hw-module module 1 recover configure/boot** command.



Caution

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

For More Information

- For the procedure for accessing downloads on Cisco.com, see [Obtaining Cisco IPS Software, page 20-1](#).
- For the procedure for using the **upgrade** command to upgrade the sensor, see [Upgrading the Sensor, page 21-2](#).
- For the procedure for configuring automatic upgrades on the sensor, see [Configuring Automatic Upgrades, page 21-6](#).

- For the procedure for using the **recover** command, see [Recovering the Application Partition, page 21-10](#).
- For the procedures for using ROMMON to restore the system image, see [Installing the IPS 4240 and IPS 4255 System Images, page 21-14](#), [Installing the IPS 4260 System Image, page 21-17](#), and [Installing the IPS 4270-20 System Image, page 21-19](#).
- For the procedure for restoring the AIM IPS system image, see [Installing the AIM IPS System Image, page 21-21](#).
- For the procedure for restoring the NME IPS system image, see [Installing the NME IPS System Image, page 21-39](#).
- For the procedure for reimagining the IDSM2 application partition from the maintenance partition, see [Installing the IDSM2 System Image, page 21-27](#).
- For the procedure for using the **hw-module module 1 recover configure/boot** command to reimage the AIP SSM, see [Installing the AIP SSM System Image, page 21-24](#).

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>