



Release Notes for Cisco Intrusion Prevention System 5.1(8)E3

Revised: July 9, 2012

Contents

- [Signature Engine Updates, page 2](#)
- [IPS 5.1\(8\)E3 File List, page 2](#)
- [Supported Platforms, page 3](#)
- [Supported Servers, page 3](#)
- [ROMMON and TFTP, page 4](#)
- [IPS Management and Event Viewers, page 4](#)
- [New and Changed Information, page 5](#)
- [Cisco Security Intelligence Operations, page 5](#)
- [Before Upgrading to Cisco IPS 5.1\(8\)E3, page 6](#)
- [Upgrading to Cisco IPS 5.1\(8\)E3, page 18](#)
- [After Upgrading to Cisco IPS 5.1\(8\)E3, page 22](#)
- [Restrictions and Limitations, page 31](#)
- [Connecting IPS-4240 to a Cisco 7200 Series Router, page 32](#)
- [Recovering the Password, page 33](#)
- [Caveats, page 33](#)
- [Related Documentation, page 35](#)
- [Obtaining Documentation and Submitting a Service Request, page 36](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2006-2012 Cisco Systems, Inc. All rights reserved.

**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 Software on Cisco.com, page 9](#).

Signature Engine Updates

Cisco introduced signature engine updates to the IPS Version 5.1 train for the first time with the release of 5.1(5)E1. Signature engine updates allow us to deliver new inspection engines more rapidly, which increases the overall security effectiveness of the sensor. We recommend that you treat signature engine updates like signature updates and install them immediately.

As a result of the introduction of signature engine, the IPS signature engine update nomenclature changed from IPS-sig-S2XX-minreq-5.1-4.pkg to IPS-sig-S2XX-req-E1.pkg to reflect the new signature engine requirements (E1).

With each signature engine release, the latest service pack and system image files are repackaged to include the new engine update. To install a signature engine update, your sensor must be running the required IPS version, which is contained in the filename of the signature engine update package. For example, to install the IPS-K9-engine-E1-req-5.1-5.pkg signature engine update, your sensor must be running IPS version 5.1(5) or later.

If you are running an earlier IPS version, such as IPS version 5.1(4), you can upgrade the sensor to 5.1(8)E3 using the service pack files.

For More Information

For detailed information on IPS signature file naming, see [IPS Software Versioning, page 10](#).

IPS 5.1(8)E3 File List

The following files are part of Cisco IPS 5.1(8)E3:

- Readme Files
 - IPS-5.1-8-E3.readme.txt
- IPS 5.1-8-E3 Service Pack Files
 - IPS-K9-5.1-8-E3.pkg
 - IPS-4260-K9-5.1-8-E3.pkg
 - IPS-CS-MGR-4260-K9-5.1-8-E3.zip
 - IPS-CS-MGR-K9-5.1-8-E3.zip
- System Image Files
 - IPS-4215-K9-sys-1.1-a-5.1-8-E3.img
 - IPS-4240-K9-sys-1.1-a-5.1-8-E3.img
 - IPS-4255-K9-sys-1.1-a-5.1-8-E3.img
 - IPS-4260-K9-sys-1.1-a-5.1-8-E3.img
 - IPS-NM_CIDS-K9-sys-1.1-a-5.1-8-E3.img

- IPS-IDSM2-K9-sys-1.1-a-5.1-8-E3.bin.gz
- IPS-SSM_10-K9-sys-1.1-a-5.1-8-E3.img
- IPS-SSM_20-K9-sys-1.1-a-5.1-8-E3.img
- Recovery Images
 - IPS-K9-r-1.1-a-5.1-8-E3.pkg
 - IPS-4260-K9-r-1.1-a-5.1-8-E3.pkg
- ISO Image
 - IPS-K9-cd-1.1-a-5.1-8-E3.iso

For More Information

- For the procedure for obtaining these files on Cisco.com, see [Obtaining Software on Cisco.com, page 9](#).
- For the procedure for installing service pack files, see [Upgrading to 5.1\(8\)E3, page 20](#).
- For the procedure for installing system image files, refer [Installing System Images](#).
- For the procedure for installing recovery image files, refer to [Recovering the Application Partition](#).
- For the procedure for installing ISO image files, see [Installing the ISO Image File, page 21](#).

Supported Platforms

Cisco IPS 5.1(8)E3 is supported on the following platforms:

- IDS-4210 Series Sensor Appliances
- IDS-4215 Series Sensor Appliances
- IDS-4235 Series Sensor Appliances
- IPS-4240 Series Sensor Appliances
- IDS-4250 Series Sensor Appliances
- IPS-4255 Series Sensor Appliances
- IPS-4260 Series Sensor Appliances
- WS-SVC-IDSM2 series Intrusion Detection System Module (IDSM-2)
- NM-CIDS Intrusion Detection System Network Module
- ASA-SSM-AIP-10 series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP-SSM)
- ASA-SSM-AIP-20 series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP-SSM)

Supported Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8

- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- VMS - Apache Server (Tomcat)
- VMS - Apache Server (JRun)


Note

The sensor cannot download software updates from Cisco.com. You must download the software update from Cisco.com to your FTP server, and then configure the sensor to download them from your FTP server.

ROMMON and TFTP

ROMMON uses TFTP to download an image and launch it. TFTP does not address network issues such as latency or error recovery. It does implement a limited packet integrity check so that packets arriving in sequence with the correct integrity value have an extremely low probability of error. But TFTP does not offer pipelining so the total transfer time is equal to the number of packets to be transferred times the network average RTT. Because of this limitation, we recommend that the TFTP server be located on the same LAN segment as the sensor. Any network with an RTT less than a 100 milliseconds should provide reliable delivery of the image. Be aware that some TFTP servers limit the maximum file size that can be transferred to ~32 MB.

For More Information

- For the procedure for downloading IPS software from Cisco.com, see [Obtaining Software on Cisco.com, page 9](#).
- For the procedure for configuring automatic updates, refer to [Configuring Automatic Upgrades](#).

IPS Management and Event Viewers

Use IDM, ASDM, or the CLI to configure 5.1(8)E3 sensors.


Note

You cannot use IDS MC 2.0 to configure 5.1(8)E3 sensors. Support for 5.1(8)E3 sensors is being added to IDS MC 2.1

Use the following tools for monitoring 5.1(8)E3 sensors:

- Security Monitor 2.0.1
- CTR 2.1
- IEV 5.2
- Protego PN-MARS 3.3.3

**Note**

If you are using these tools to monitor 5.1(8)E3 sensors, add the sensors to the configuration as if they were 4.1 sensors. You cannot view the new fields in 5.1(8)E3 alerts in these alarm viewers until they have been upgraded to accommodate the new fields in 5.1(8)E3. Security Monitor 2.1 is being upgraded to display the fields in 5.1(8)E3 alerts.

**Note**

Viewers that are already configured to monitor the 4.x sensors may need to be configured to accept a new SSL certificate for the 5.1(8)E3 sensors.

For More Information

For the procedure for configuring a new SSL certificate, for the CLI, refer to [Configuring TLS](#), and for IDM, refer to [Adding Trusted Hosts](#).

New and Changed Information

Cisco IPS 5.1(8)E3 includes the E3 signature engine update and the S365 signature update. The S365 signature update is a built in to the E3 engine update. You cannot download S365 separately.

- Signature date and type

The signature date represents the date at which the signature was first created. The date is stored in the format YYYYMMDD. The signature type represents the category in which a specific signature falls. Signatures are broadly classified as vulnerability, exploit, anomaly, component, or other. The default is other.

- Duplicate packet detector statistics

Duplicate packet statistics are now added to the TCP Normalizer Stage Statistics section of the **show statistics virtual sensor** command output. Large numbers of duplicate packets being reported by the Normalizer can aid in the detection of sensor deployment and configuration problems. Duplicate packets are often seen in situations where a single virtual sensor is monitoring two or more networks, and is seeing a TCP connection crossing two or more of these networks. In this situation you can reconfigure the sensor to monitor each network using a different virtual sensor. If both networks must be monitored by a single virtual sensor, configure the virtual sensor with the **inline-TCP-session-tracking-mode** parameter set to either **interface-and-vlan** or **vlan-only**.

- UDP length parameter in Atomic engines

A new parameter to match a specific UDP length was added. This engine parameter is added in the Atomic IP Advanced and Atomic IP engine for **l4-protocol** UDP. The purpose of this parameter is to check if UDP total length falls within a specific range.

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>

Before Upgrading to Cisco IPS 5.1(8)E3

This section describes what to do before upgrading your sensor, and contains the following topics:

- [Perform These Tasks, page 6](#)
- [Copying and Restoring the Configuration File Using a Remote Server, page 7](#)
- [Obtaining Software on Cisco.com, page 9](#)
- [IPS Software Versioning, page 10](#)
- [Upgrading the IDS-4210 Memory, page 15](#)
- [Upgrading the IDS-4215 BIOS, page 17](#)

Perform These Tasks

Before you upgrade your sensors to Cisco IPS 5.1(8)E3, make sure you have performed the following tasks:

- Created a backup copy of your configuration.
- Saved the output of the **show version** command.

If you need to downgrade a service pack or signature update, you will know what versions you had, and you can then apply the configuration you saved when you backed up your configuration.



Note You cannot use the **downgrade** command to downgrade from 5.1(8)E3 to 5.0. You can only downgrade from new service packs and signature upgrades to the previous version of service pack or signature upgrade.

- Upgraded the IDS-4210 memory to 512 MB.
- Upgraded the IDS-4215 BIOS to the most recent version.

For More Information

- For the procedure for making a backup copy of your configuration, see [Copying and Restoring the Configuration File Using a Remote Server, page 7](#).
- For the procedure for viewing version information, refer to [Displaying Version Information](#).
- For the procedure for downgrading your sensor, refer to [Downgrading the Sensor](#).

- For the procedure for upgrading the IDS-4210 memory, see [Upgrading the IDS-4210 Memory, page 15](#).
- For the procedure for upgrading the IDS-4215 BIOS, see [Upgrading the IDS-4215 BIOS, page 17](#).

Copying and Restoring the Configuration File Using a Remote Server



Note

We recommend copying the current configuration file to a remote server before upgrading.

Use the **copy** [/erase] *source_url destination_url keyword* command to copy the configuration file to a remote server. You can then restore the current configuration from the remote server. You are prompted to back up the current configuration first.

Options

The following options apply:

- **/erase**—Erases the destination file before copying.
This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.
- *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.
- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.
- **backup-config**—The storage location for the configuration backup.

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 also 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 HTTP and HTTPS prompt for a password if a username is required to access the website. If you use HTTPS protocol, the remote host must be a TLS trusted host.



Caution Copying a configuration file from another sensor may result in errors if the sensing interfaces and virtual sensors are not configured the same.

Backing Up the Current Configuration to a Remote Server

To back up your current configuration to a remote server, follow these steps:

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

Step 2 Back up the current configuration to the remote server.

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: *****
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg          100% |*****| 36124          00:00
```

Restoring the Current Configuration From a Backup File

To restore your current configuration from a backup file, follow these steps:

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

Step 2 Back up the current configuration to the remote server.

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: *****
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

Step 3 Enter **yes** to copy the current configuration to a backup configuration.

```
cfg          100% |*****| 36124          00:00
```

```
Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

Step 4 Enter **no** to retain the currently configured hostname, IP address, subnet mask, management interface, and access list. We recommend you retain this information to preserve access to your sensor after the rest of the configuration has been restored.

For More Information

- For the procedure for adding remote hosts to the SSH known hosts list, refer to [Adding Hosts to the Known Hosts List](#).
- For the procedure for making a remote host a TLS trusted host, refer to [Adding TLS Trusted Hosts](#).

Obtaining Software on Cisco.com

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

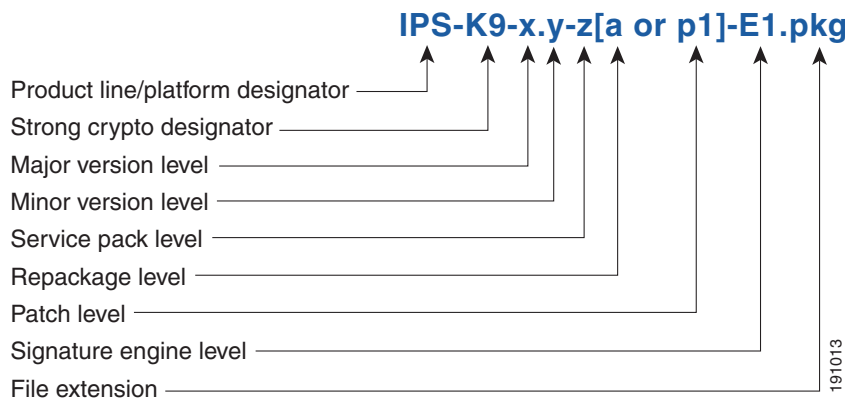
This section describes the various IPS software files, and contains the following sections:

- [Major and Minor Updates, Service Packs, and Patch Releases, page 10](#)
- [Signature/Virus Updates and Signature Engine Updates, page 12](#)
- [Recovery, Manufacturing, and System Images, page 13](#)
- [5.1 Software Release Examples, page 13](#)

Major and Minor Updates, Service Packs, and Patch Releases

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

Figure 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).

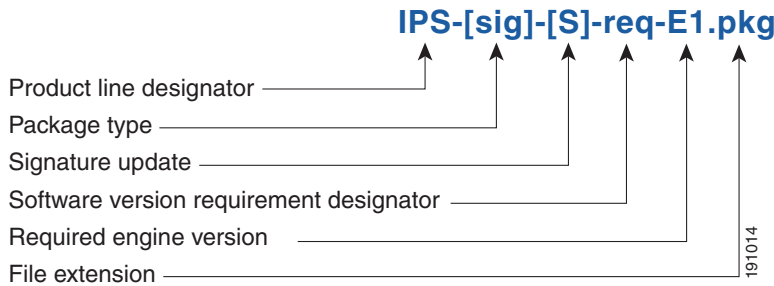
For More Information

For a table listing the types of files with examples of filenames and corresponding software releases, see [5.1 Software Release Examples, page 13](#).

Signature/Virus Updates and Signature Engine Updates

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

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



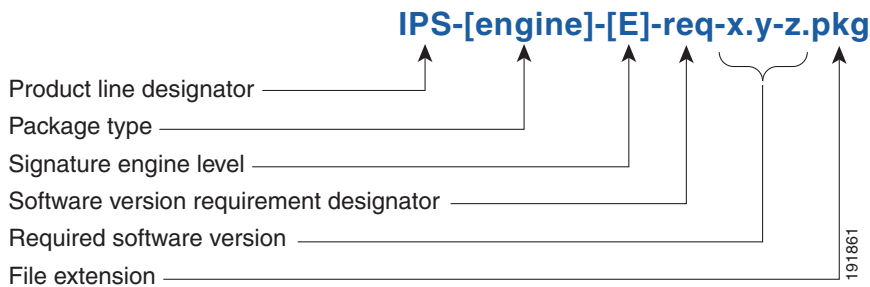
Signature/Virus Updates

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

Figure 3 IPS Software File Name for Signature Engine Updates



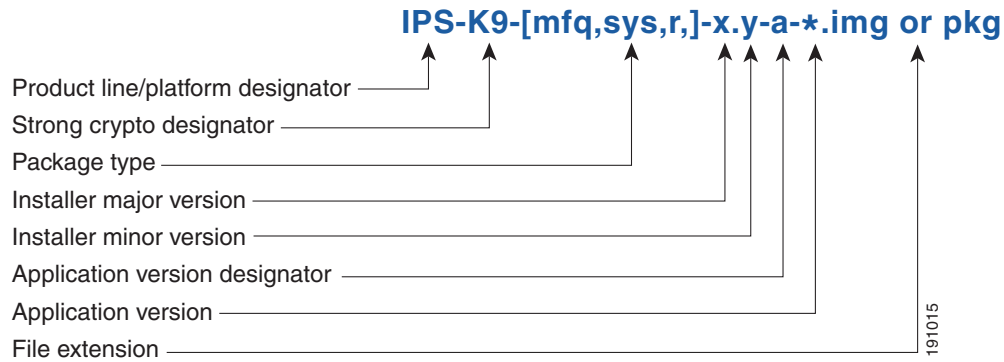
Signature Engine Updates

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

Figure 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.

5.1 Software Release Examples

Table 1 lists platform-independent IDS 5.1 software release examples. Refer to the Readmes that accompany the software files for detailed instructions on how to install the files.

Table 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 update ⁴	Annually	—	5.1(1)	IPS-K9-5.1-1-E1.pkg
Major update ⁵	Annually	—	5.0(1)	IPS-K9-6.0-1-E1.pkg

Table 1 Platform-Independent Release Examples (Continued)

Release	Target Frequency	Identifier	Example Version	Example Filename
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

- 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.
- Patch releases are for interim fixes.
- 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 2 describes platform-dependent software release examples.

Table 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	servicesengine-boot-1.0-4.bin

- The system image includes the combined recovery and application image used to reimage an entire sensor.
- 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 3 describes the platform identifiers used in platform-specific names.



Note

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

Table 3 Platform Identifiers

Sensor	Identifier
IDS-4215	IDS-4215-
IPS-4240	IPS-4240-
IPS-4255	IPS-4255-
IPS-4260	IPS-4260-

Table 3 Platform Identifiers (Continued)

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

For More Information

For instructions on how to access these files on Cisco.com, see [Obtaining Software on Cisco.com](#), page 9.

Upgrading the IDS-4210 Memory

IDS-4210, IDS-4210-K9, and IDS-4210-NFR must have 512 MB of RAM to support Cisco IPS 5.x. If you are upgrading an existing IDS-4210, IDS-4210-K9, or IDS-4210-NFR to 5.x, you must insert one additional 256-MB DIMM (part number IDS-4210-MEM-U) to upgrade the memory to the required 512 MB minimum.

**Note**

Do not install an unsupported DIMM. Doing so nullifies the warranty.

**Caution**

Follow proper safety procedures when performing these steps by reading the safety warnings in [Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor](#).

To upgrade the memory, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

Wait for the power down message before continuing with Step 3.

**Note**

You can also power down the sensor from IDM or ASDM.

Step 3 Power off the appliance.

Step 4 Remove the power cord and other cables from the appliance.

Step 5 Place the appliance in an ESD-controlled environment.

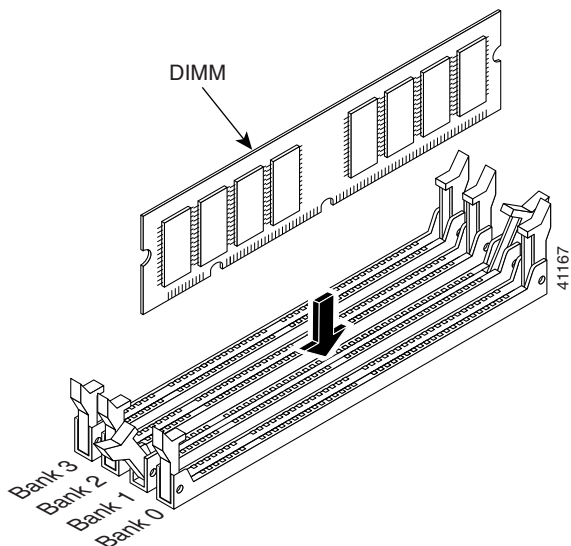
Step 6 Remove the chassis cover by unscrewing the screw on the front of the cover and sliding the cover straight back.

Step 7 Locate the DIMM sockets and select an empty DIMM socket next to the existing DIMM.



Note

The existing DIMM is installed in socket 0. The angled position of the DIMM sockets make installing an additional DIMM in socket 1 difficult if a DIMM occupies socket 0. Therefore, you should first remove the existing DIMM from socket 0, place the new DIMM in socket 1, and then replace the existing DIMM in socket 0.



Step 8 Locate the ejector tabs on either side of the DIMM socket. Press down and out on tabs to open the slot in the socket.

Step 9 Install the new DIMM, by positioning the DIMM into the socket and pressing it into place.



Note

Do not force the DIMM into the socket. Alignment keys on the DIMM ensure that it only fits in the socket one way. If you need additional leverage, you can gently press down on the DIMM with your thumbs while pulling up on the ejector tabs.

Step 10 Replace the chassis cover and reconnect the power.

Step 11 Power on the sensor and make sure the new memory total is correct.



Note

If the memory total does not reflect the added DIMMs, repeat Steps 1 through 4 to ensure the DIMMs are seated correctly in the socket.

For More Information

For more information about ESD-controlled environments, refer to [Working in an ESD Environment](#).

Upgrading the IDS-4215 BIOS

The BIOS/ROMMON upgrade utility (IDS-4215-bios-5.1.7-rom-1.4.bin) upgrades the BIOS of IDS-4215 to version 5.1.7 and the ROMMON to version 1.4.

To upgrade the BIOS and ROMMON on IDS-4215, follow these steps:

- Step 1** Download the BIOS ROMMON upgrade utility (IDS-4215-bios-5.1.7-rom-1.4.bin) to the TFTP root directory of a TFTP server that is accessible from IDS-4215.



Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of IDS-4215.

- Step 2** Boot IDS-4215.

While rebooting, IDS-4215 runs the BIOS POST. After the completion of POST, the console displays the message: `Evaluating Run Options ...` for about 5 seconds.

- Step 3** Press **Ctrl-R** while this message is displayed to display the ROMMON menu.

The console display resembles the following:

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.3 05/12/03 10:18:14.84
Compiled by ciscouser
Evaluating Run Options ...
Cisco ROMMON (1.2) #0: Mon May 12 10:21:46 MDT 2003
Platform IDS-4215
0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:11)
Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01
Use ? for help.
rommon>
```

- Step 4** If necessary, change the port number used for the TFTP download:

```
rommon> interface port_number
```

The port in use is listed just before the rommon prompt. Port 1 (default port) is being used as indicated by the text, `Using 1: i82557 @ PCI(bus:0 dev:14 irq:11), MAC: 0000.c0ff.ee01`.



Note Ports 0 (monitoring port) and 1 (command and control port) are labeled on the back of the chassis.

- Step 5** Specify an IP address for the local port on IDS-4215:

```
rommon> address ip_address
```



Note Use the same IP address that is assigned to IDS-4215.

- Step 6** Specify the TFTP server IP address:

```
rommon> server ip_address
```

- Step 7** Specify the gateway IP address:

```
rommon> gateway ip_address
```

Step 8 Verify that you have access to the TFTP server by pinging it from the local Ethernet port:

```
rommon> ping server_ip_address
rommon> ping server
```

Step 9 Specify the filename on the TFTP file server from which you are downloading the image:

```
rommon> file filename
```

Example:

```
rommon> file IDS-4215-bios-5.1.7-rom-1.4.bin
```



Note The syntax of the file location depends on the type of TFTP server used. Contact your system or network administrator for the appropriate syntax if the above format does not work.

Step 10 Download and run the update utility:

```
rommon> tftp
```

Step 11 Type **y** at the upgrade prompt and the update is executed.

IDS-4215 reboots when the update is complete.



Caution

Do not remove power to IDS-4215 during the update process, otherwise the upgrade can get corrupted. If this occurs, IDS-4215 will be unusable and require an RMA.

For More Information

For the procedure for locating software on Cisco.com, see [Obtaining Software on Cisco.com, page 9](#)

Upgrading to Cisco IPS 5.1(8)E3

This section provides information on upgrading to IPS 5.1(8)E3. It contains the following topics:

- [Upgrade Notes and Caveats, page 18](#)
- [Upgrading to 5.1\(8\)E3, page 20](#)
- [Installing the ISO Image File, page 21](#)

Upgrade Notes and Caveats

The following caveats apply to upgrading to 5.1(8)E3:

- The sensor must show version 5.0(1) or later before you can apply this service pack.
- Installing 5.1(8)E3 completely reimages the sensor. Sensor configuration settings are maintained, but all data written to the Event Store and any unsupported customizations are lost.
- We strongly advise you to save a copy of the current configuration settings of the sensor to an FTP server before you upgrade.

- You cannot uninstall the 5.1(8)E3 service pack. You must reimage the sensor using a system image file. All configuration settings are lost.
- Auto Update does not recognize the IPS-4260 package file (IPS-4260-K9-5.1-8-E3.pkg).

If Auto Update is configured on the IPS-4260, it does not install the 4260 files because it does not recognize them. Use the CLI or IDM to install the 5.1(8)E3 service pack.



Note IPS version 5.1(x) does not recognize platform-specific major, minor, or service pack file names.

- If you have 4.0 installed on your sensor, you must upgrade to 4.1, then upgrade to 5.0, then upgrade to 5.1(8)E3.

If you try to upgrade a 4.0 sensor to 5.0, you receive an error that Analysis Engine is not running rather than an error that the sensor cannot be upgraded from 4.0 to 5.0:

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-maj-5.0-1-S148.rpm.pkg
Password: *****
Warning: Executing this command will apply a major version upgrade to the application
partition. The system may be rebooted to complete the upgrade.
Continue with upgrade? : yes
Error: AnalysisEngine is not running. Please reset box and attempt upgrade again.
```

If you receive this error, you must upgrade from 4.0 to 4.1 and then to 5.0. Or you can use the recovery CD (if your sensor has a CD-ROM) or the system image file to reimage directly to version 5.1(8)E3. You can reimage a 4.0 sensor to 5.0 because the reimage process does not check to see what version was previously installed.

- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- In 4.x, custom signature IDs start at 20000. Any custom signatures that you have created in 4.x are converted to the 5.x custom signature range, which begins at 60000.
- In 4.x, there is a parameter that lets you enable and disable signatures. In 5.x, there is a similar parameter, but there is also a parameter that lets you retire and unretire signatures. When you upgrade to 5.x, some signatures will be marked as enabled; however, they may also have been retired in 5.x and therefore the enabled setting is ignored. You must manually unretire the signature to ensure that it is enabled.
- In 5.1(8)E3, you will receive messages indicating the you need to install a license. The sensor functions properly without a license, but you will need a license to install signature updates.
- Upgrading from 4.1 to 5.x preserves the configuration of the sensor. The upgrade may stop if it comes across a value that it cannot translate. If this occurs, the resulting error message provides enough information to adjust the parameter to an acceptable value. After editing the configuration, try the upgrade again.
- After you upgrade from 4.x to 5.0, you cannot downgrade. If you want to return to the previous version, you must reimage and then copy the backup configuration to the reimaged sensor. You cannot downgrade from 5.1(8)E3 to 5.0.
- IDS MC cannot manage sensors that have been upgraded to 5.x until the IDS MC 2.1 release.

For More Information

- For the procedure for changing the status of signatures, refer to [Configuring the Status of Signatures](#).
- For the procedure for obtaining and installing the license, see [Licensing the Sensor, page 26](#).

- For the procedure for reimaging sensor, refer to [Upgrading, Downgrading, and Installing System Images](#).
- For the procedure for copying the backup configuration to a reimaged sensor, see [Copying and Restoring the Configuration File Using a Remote Server](#), page 7.

Upgrading to 5.1(8)E3

To upgrade the sensor, follow these steps:

- Step 1** Download the upgrade file (IPS-K9-5.1-8-E3.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.



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.



Note If you use HTTPS, the remote host must be a TLS trusted host.



Caution You must log in to Cisco.com using an account with cryptographic privileges to download software. The first time you download software on Cisco.com, you receive instructions for setting up an account with cryptographic privileges.



Caution Do not change the filename. You must preserve the original filename for the sensor to accept the update.

- Step 2** Log in to the CLI using an account with Administrator privileges.

- Step 3** Upgrade the sensor:

```
sensor# configure terminal
sensor(config)# upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-5.1-8-E3.pkg

Enter password: *****
Re-enter password: *****
```

- Step 4** Type **yes** to complete the upgrade.



Note Major updates, minor updates, and service packs may force a restart of the IPS processes or even force a reboot of the sensor to complete installation.

- Step 5** Verify your new sensor version:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.1(8)E3

Host:
  Realm Keys          key1.0
```

```

Signature Definition:
  Signature Update      S278.0                2007-03-28
  Virus Update         V1.2                2005-11-24
OS Version:           2.4.26-IDS-smp-bigphys
Platform:             IDS-4210
Serial Number:       8R2D501
No license present
Sensor up-time is 12 days.
Using 500482048 out of 510238720 bytes of available memory (98% usage)
system is using 17.4M out of 29.0M bytes of available disk space (60% usage)
application-data is using 36.8M out of 174.7M bytes of available disk space (22%
usage)
boot is using 35.3M out of 75.9M bytes of available disk space (49% usage)
application-log is using 532.6M out of 2.8G bytes of available disk space (20% u
sage)

```

```

MainApp      2007_FEB_02_15_58  (Release)  2007-02-02T16:04:00-0600  Running
AnalysisEngine  2007_FEB_02_15_58  (Release)  2007-02-02T16:04:00-0600  Running
CLI          2007_FEB_02_15_58  (Release)  2007-02-02T16:04:00-0600

```

Upgrade History:

```

IPS-K9-sp-5.1-8-E3  15:58:00 UTC Fri Feb 02 2007

```

Recovery Partition Version 1.1 - 5.1(8)E3

sensor#

For More Information

- For the procedure for adding remote hosts to the SSH known hosts list, refer to [Adding Hosts to the Known Hosts List](#).
- For the procedure for making a remote host a TLS trusted host, refer to [Adding TLS Trusted Hosts](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Software on Cisco.com](#), page 9.

Installing the ISO Image File



Note

You must create a recovery CD on a Linux system to install the ISO image for IDS-4235 and IDS-4250.

The Recovery ISO Image is for IDS-4235 and IDS-4250 sensors only.

To create the recovery CD for the ISO image for IDS-4235 and IDS-4250, follow these steps:

Step 1 Insert a blank CD-R media in to the CD-R recorder of the burn host.

Step 2 Enter the following command:

```

host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-6.0-5-E2.iso
host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-6.0-5-E3.iso
host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-6.0-4-E2.iso
host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-6.0-4a-E1.iso
host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-6.0-2-E1.iso

```

```
host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-6.0-3-E1.iso
host# cdrecord -v speed=6 dev=0,0 IPS-K9-cd-1.1-a-5.1-8-E3.iso
```

Step 3 Follow the command line arguments for cdrecord.



Note The command line arguments are self-explanatory. For more information, refer to the cdrecord man page.

Step 4 Follow the instructions for using a recovery CD to install the ISO image on IDS-4235 and IDS-4250.

For More Information

For the procedure for using a recovery CD to install images, refer to [Using the Recovery/Upgrade CD](#).

After Upgrading to Cisco IPS 5.1(8)E3

This section provides information about what to do after you install IPS 5.1(8)E3. It contains the following topics:

- [Comparing Configurations, page 22](#)
- [SSL Certificate, page 23](#)
- [Increasing the Memory Size of the Java Plug-In, page 23](#)
- [Logging In to IDM, page 24](#)
- [Licensing the Sensor, page 26](#)

Comparing Configurations

Compare your backed up and saved 5.0 configuration with the output of the **show configuration** command after upgrading to 5.1(8)E3 to verify that all the configuration has been properly converted.



Note

If you are converting from IPS 4.x, the 4.x configuration has to be converted to the 5.1(8)E3 commands, because IPS 5.1(8)E3 has some new configuration parameters.



Caution

If the configuration is not properly converted, see [Caveats, page 33](#), or check Cisco.com for any upgrade issues that have been found. Contact the TAC if no DDTS refers to your situation.

SSL Certificate

If necessary import the new SSL certificate for the upgraded sensor in to each tool being used to monitor the sensor.

For More Information

For the CLI procedure, refer to [Configuring TLS](#), or for the IDM procedure, refer to [Configuring Certificates](#).

Increasing the Memory Size of the Java Plug-In

To correctly run IDM, your browser must have Java Plug-in 1.4.2 or 1.5 installed. By default the Java Plug-in allocates 64 MB of memory to IDM. IDM can run out of memory while in use, which can cause IDM to freeze or display blank screens. Running out of memory can also occur when you click **Refresh**. An `OutOfMemoryError` message appears in the Java console whenever this occurs. You must change the memory settings of Java Plug-in before using IDM. The mandatory minimum memory size is 256 MB.



Note

We recommend that you use Sun Microsystems Java. Using any other version of Java could cause problems with IDM.

This section contains the following topics:

- [Java Plug-In on Windows, page 23](#)
- [Java Plug-In on Linux and Solaris, page 24](#)

Java Plug-In on Windows

To change the settings of Java Plug-in on Windows for Java Plug-in 1.4.2 and 1.5, follow these steps:

-
- Step 1** Close all instances of Internet Explorer or Netscape.
- Step 2** Choose **Start > Settings > Control Panel**.
- Step 3** If you have Java Plug-in 1.4.2 installed:
- a. Choose **Java Plug-in**. The Java Plug-in Control Panel appears.
 - b. Click the **Advanced** tab.
 - c. In the Java RunTime Parameters field, enter **-xms256m**.
 - d. Click **Apply** and exit the Java Control Panel.

- Step 4** If you have Java Plug-in 1.5 installed:
- a. Choose **Java**. The Java Control Panel appears.
 - b. Click the **Java** tab.
 - c. Click **View** under Java Applet Runtime Settings. The Java Runtime Settings window appears.
 - d. In the Java Runtime Parameters field, enter `-Xms256m`, and then click **OK**.
 - e. Click **OK** and exit the Java Control Panel.
-

Java Plug-In on Linux and Solaris

To change the settings of Java Plug-in 1.4.2 or 1.5 on Linux and Solaris, follow these steps:

- Step 1** Close all instances of Netscape or Mozilla.
- Step 2** Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.



Note In the Java 2 SDK, this file is located at <SDK installation directory>/jre/bin/ControlPanel. For example if your Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel.



Note In a Java 2 Runtime Environment installation, the file is located at <JRE installation directory>/bin/ControlPanel.

- Step 3** If you have Java Plug-in 1.4.2 installed:
- a. Click the **Advanced** tab.
 - b. In the Java RunTime Parameters field, enter `-Xms256m`.
 - c. Click **Apply** and close the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
- a. Click the **Java** tab.
 - b. Click **View** under Java Applet Runtime Settings.
 - c. In the Java Runtime Parameters field, enter `-Xms256m`, and then click **OK**.
 - d. Click **OK** and exit the Java Control Panel.
-

Logging In to IDM

IDM is a web-based, Java Web Start application that enables you to configure and manage your sensor. The web server for IDM resides on the sensor. You can access it through Internet Explorer or Firefox web browsers.

To log in to IDM, follow these steps:

Step 1 Open a web browser and enter the sensor IP address:

https://*sensor_ip_address*



Note IDM is already installed on the sensor.



Note The default IP address is 192.168.1.2/24,192.168.1.1, which you change to reflect your network environment when you initialize the sensor. When you change the web server port, you must specify the port in the URL address of your browser when you connect to IDM in the format **https://sensor_ip_address:port** (for example, **https://10.1.9.201:1040**).

A Security Alert dialog box appears.

Step 2 Click **Yes** to accept the security certificate.

The Cisco IPS Device Manager Version window appears.

Step 3 To launch IDM, click **Run IDM**.

The JAVA loading message box appears.

The Warning - Security dialog box appears.

Step 4 To verify the security certificate, check the Always trust content from this publisher check box, and click **Yes**.

The JAVA Web Start progress dialog box appears.

The IDM on *ip_address* dialog box appears.

Step 5 To create a shortcut for IDM, click **Yes**.



Note You must have JRE 1.5 (JAVA 5) installed to create shortcuts for IDM. If you have JRE 1.6 (JAVA 6) installed, the shortcut is created automatically.

The Cisco IDM Launcher dialog box appears.

Step 6 To authenticate IDM, enter your username and password, and click **OK**.



Note Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization.

IDM begins to load.

If you change panes from Home to Configuration or Monitoring before IDM has complete initialization, a Status dialog box appears with the following message:

Please wait while IDM is loading the current configuration from the sensor.

The main window of IDM appears.



Note If you created a shortcut, you can launch IDM by double-clicking the IDM shortcut icon. You can also close the The Cisco IPS Device Manager Version window. After you launch IDM, is it not necessary for this window to remain open.

For More Information

- For more information about security and IDM, refer to [IDM and Certificates](#).
- For the procedure for initializing the sensor, refer to [Initializing the Sensor](#).

Licensing the Sensor

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

- [Understanding the License, page 26](#)
- [Service Programs for IPS Products, page 27](#)
- [Obtaining and Installing the License Key, page 28](#)

Understanding the License

Although the sensor functions without the license, you must have a license to obtain signature updates. To obtain a license, you must have a Cisco Service for IPS service contract. Contact your reseller, Cisco service or product sales to purchase a contract.



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 trial license that supports signature updates that require licensing.

You can view the status of the IPS subscription license key on the Licensing panel in IDM. You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the sensor license key from a license key provided in a local file.

You must know your IPS device serial number to obtain a license key. You can find the IPS device serial number in by clicking **Configuration > Licensing**, or through the CLI by using the **show version** command.

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 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. Go to <http://www.cisco.com/go/license> and click **IPS Signature Subscription Service** to apply for a license.

For More Information

- For more information on Cisco service contracts, see [Service Programs for IPS Products](#), page 27.
- For the procedure for obtaining and installing the License key, see [Obtaining and Installing the License Key](#), page 28.

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.



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.

For More Information

For the procedure for obtaining and installing the License key, see [Obtaining and Installing the License Key, page 28](#).

Obtaining and Installing the License Key

You can install the license key through the CLI or IDM. This section contains the following topics:

- [Using IDM, page 28](#)
- [Using the CLI, page 29](#)

Using IDM

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

-
- Step 1** Log in to IDM using an account with administrator privileges.
- Step 2** Choose **Configuration > 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:
- Check the **Cisco Connection Online** check box 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.
 - Check the **License File** check box 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 can access. This option is useful if your computer cannot access 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 key 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 license key will be sent to the e-mail address you specified.

- Step 9** Save the license key to a hard-disk drive or a network drive that the client running IDM can access.
- Step 10** Log in to IDM.
- Step 11** Choose **Configuration > Licensing**.
- Step 12** Under Update License, check the **Update From: License File** check box.
- 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



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.

To install the license key, follow these steps:

Step 1 Apply for the license key at this URL: www.cisco.com/go/license.



Note You must have a Cisco Services for IPS service contract before you can apply for a license key.

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 will be sent 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.



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.

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 5.1(8)E3

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: ABC1234DEFG
Licensed, expires: 19-Dec-2008 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)  2008-02-18T03:13:47-0600  Running
AnalysisEngine  2005_Feb_15_03.00  (Release)  2008-02-15T12:59:35-0600  Running
CLI              2005_Feb_18_03.00  (Release)  2008-02-18T03:13:47-0600
```

```
Upgrade History:
```

```
IDS-K9-min-5.1-8-E3 14:16:00 UTC Thu Mar 04 2008
```

```
Recovery Partition Version 1.1 - 5.1(8)E3
```

```
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 remote hosts to the SSH known hosts list, refer to [Adding Hosts to the Known Hosts List](#).
- For the procedure for making a remote host a TLS trusted host, refer to [Adding TLS Trusted Hosts](#).
- For more information on Cisco service contracts, see [Service Programs for IPS Products, page 27](#).

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IPS 5.1(8)E3 software and the products that run 5.1(8)E3:

- An IPS appliance can support both promiscuous and inline monitoring at the same time; however you must configure each physical interface in either promiscuous or inline mode. Because inline monitoring requires the use of two sensing interfaces, the sensor must contain at least three physical sensing interfaces to perform both promiscuous and inline monitoring. The exceptions to this are AIP-SSM-10 and AIP-SSM-20. AIP-SSM can support both promiscuous and inline monitoring on its single physical back plane interface inside the ASA. The configuration on the main ASA can be used to designate which packets/connections should be monitored by AIP-SSM as either promiscuous or inline.
- You can configure only one IDSM-2 for inline monitoring between two VLANs. Configuring more than one IDSM-2 in inline mode between the same two VLANs can cause a packet loop in the switch. If you need to use more than one IDSM-2 in inline mode in the switch, you must configure each IDSM-2 for inline monitoring for a unique set of two VLANs.
- NM-CIDS does not run in inline mode.
- We do not support deploying an IPS sensor monitoring two sides of a network device that does TCP sequence number randomization.

The PIX and ASA Firewalls and other security devices support a feature known as TCP Sequence Randomization. The initial TCP packets for a connection have their initial Sequence Numbers randomized as they flow through the firewall. A sensor monitoring the side of the firewall where the TCP client is located as well as monitoring the side of the firewall where the TCP server is located sees the same TCP session twice, but with different sequence numbers. If the sensor is monitoring in promiscuous mode, this can confuse the TCP Reassembly software and the sensor may not be able to properly track the TCP Session and may not be able to send alerts for any attacks within the TCP connection. If the sensor is monitoring in inline mode (inline interface pair, or inline VLAN pair), it sees the TCP packets with the randomized sequence numbers as being out of order when compared to the original sequence numbers. When this happens the inline sensor drops/denies the TCP packets with the randomized sequence numbers and prevent the TCP connection from continuing.

- After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.
- IDM does not support any non-English characters, such as the German umlaut or any other special language characters. If you enter such characters as a part of an object name through IDM, they are turned into something unrecognizable and you will not be able to delete or edit the resulting object through IDM or the CLI.

This is true for any string that is used by CLI as an identifier, for example, names of time periods, inspect maps, server and URL lists, and interfaces.

- You can only install eight IDSM-2s per switch chassis.
- Do not confuse Cisco IOS IDS (a software-based intrusion-detection application that runs in the Cisco IOS) with the IPS that runs on the NM-CIDS. The NM-CIDS runs Cisco IPS 5.1(8)E3. Because performance can be reduced and duplicate alarms can be generated, we recommend that you do not run Cisco IOS IDS and Cisco IPS 5.1(8)E3 simultaneously.
- Only one NM-CIDS is supported per Cisco 2600, 2811, 2821 2851, 3825, 3845, and 3700 series router.
- Jumbo frames are not supported on the NM-CIDS.
- The HTML-based IDM has been replaced with a Java applet.
- You cannot use IDS MC 2.0 to configure 5.1(8)E3 sensors. Support for 5.1(8)E3 sensors is being added to IDS MC 2.1.
- When SensorApp is reconfigured there is a short period when SensorApp is unable to respond to any queries. Wait a few minutes after reconfiguration is complete before querying SensorApp for additional information.

Connecting IPS-4240 to a Cisco 7200 Series Router

When an IPS-4240 is connected directly to a 7200 series router and both the IPS-4240 and the router interfaces are hard-coded to speed 100 with duplex Full, the connection does not work. If you set IPS-4240 to speed Auto and duplex Auto, it connects to the router but only at speed 100 and duplex Half.

To connect correctly at speed 100 and duplex Full, set the interfaces of both IPS-4240 and the router to speed Auto and duplex Auto. Also, if either interface is hard-coded, you must make the connection using a crossover cable.

Recovering the Password

The following password recovery options exist:

- If another Administrator account exists, the other Administrator can change the password.
- If a Service account exists, you can log in to the service account and switch to user root using the command **su - root**. Use the **password** command to change the CLI Administrator account's password. For example, if the Administrator username is "adminu," the command is **password adminu**. You are prompted to enter the new password twice.
- You can reimage the sensor using either the recovery partition or a system image file.

For More Information

- For the procedure for creating the service account, refer to [Creating the Service Account](#).
- For the procedures for reimaging the sensor, refer to [Upgrading, Downgrading, and Installing System Images](#).

Caveats

This section lists the resolved and known issues, and contains the following topics:

- [Bug Toolkit, page 33](#)
- [Resolved Caveats, page 34](#)
- [Known Caveats, page 34](#)

Bug Toolkit

For the most complete and up-to-date list of caveats, use the Bug Toolkit to refer to the caveat release note. You can use the Bug Toolkit to search for known bugs based on software version, feature set, and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable. It also lets you save the results of a search in Bug Groups, and also create persistent Alert Agents that can feed those groups with new defect alerts.



Note

You must be logged in to Cisco.com to access the Bug Toolkit.

If you are a registered Cisco.com user, you can view the Bug Toolkit at this URL:

<http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs>

To become a registered cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Resolved Caveats

The following known issues have been resolved in IPS 5.1(8)E3:

- CSCso09813—Missing victim context data in sig 5081
- CSCsq82903—Exact Match Offset Unintended behavior
- CSCsr04917—Signature 5565-4 Alerting twice
- CSCso31980—Fixed Engine "specify-service-ports" has a misleading guiName
- CSCsq94419—False Positive on 11022-1, 7202-0, and 11018.1
- CSCsq74297—SMB Advanced has infinite loop
- CSCsj18246—Event variables not tagged with the smallest locality
- CSCsr23555—IPS: zeroWindowProbe packets cause sequence number miscalculation
- CSCsm90428—String-tcp alert contains incorrect data in 'from target' context
- CSCso28141—Wrong attack context data captured
- CSCsq46856—H225 Engine Consumes Sensor Memory
- CSCsr81621—SensorApp core for 1315_0_ipv6.pcap in Proc6TcpTcb16dumpCurrentStateEv
- CSCso76619—Bad frag/backlog handling causes excess dgram holding & missed 1st frags
- CSCsu05697—Improper calculation for triggering udp-length-mismatch
- CSCsr94117—IOS and sensorApp do not process signatures the same way
- CSCsu36059—AIC HTTP Enforce Accept Content Types always enabled
- CSCsr78743—InspectorAtomicL3L4 needs proper handling of IpHeaderLength param
- CSCsu58580—Fixed-udp signatures perform double inspection
- CSCsu95722—Signature validation in SMB Advanced should emit WARNING
- CSCsu74746—Error message starting SensorApp on backported engine
- CSCso96079—META alarms may have the wrong risk ratings

Known Caveats

The following known issues are found in IPS 5.1(8)E3:

- CSCsg09619—IPS accepts RSA keys with exponent 3 which are vulnerable to forgery
- CSCsg18379—MainApp unexpected behavior due to XML Parsing Error
- CSCsg26929—Interface errors when enabled in cli and ifconfig up
- CSCsg96871—AnalysisEngine InspectorServiceAICWeb::ToServiceInspect abort
- CSCsh45936—Leading Space in the uri-regex in Service-HTTP Works Ambiguously
- CSCsh50760—NAC causes high mainApp usage
- CSCsh89833—Delete event variable referenced by filter or sig from IDM
- CSCsi21029—GRE tunnels blocked by sensorApp inspection defect
- CSCsi43787—Memory leak in mainApp when log event initiated remotely
- CSCsj35723—Sigs not alarming after default service sig sig0

- CSCsj57474—Frag traffic with dot1q headers misses a few sweep and atomic-ip sigs
- CSCsj82458—global-block-timeout allows values outside supported range
- CSCsk53813—upgrade log files are not preserved during an upgrade
- CSCsm44644—Signature 1303 false negative
- CSCsm47102—Signature 1308 does not function
- CSCso40665—Signature id 5732 firing incorrectly
- CSCsq48302—Incorrect format of IPS signatures in CCO XML packages
- CSCsq62966—Sensor at 100% processing level when inline, causing traffic latency
- CSCsu10359—Fragmented traffic may cause false negative

Related Documentation

Refer to the following documentation for more information on IPS 5.1 found at this URL:

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

- *Documentation Roadmap for Cisco Intrusion Prevention System 5.1*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Cisco Intrusion Prevention System Device Manager Configuration Guide for IPS 5.1*
- *Command Reference for Cisco Intrusion Prevention System 5.1*
- *Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 5.1*
- *Cisco Intrusion Prevention System Appliance and Module Installation Guide for IPS 5.1*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright © 2006-2012 Cisco Systems, Inc. All rights reserved.