



Release Notes for Cisco Intrusion Prevention System 6.1(1)E1

April 21, 2008

Revised: October 8, 2009

Contents

- [IPS 6.1\(1\)E1 File List, page 2](#)
- [Supported Platforms, page 2](#)
- [Supported Servers, page 3](#)
- [ROMMON and TFTP, page 3](#)
- [IPS Management and Event Viewers, page 4](#)
- [Receiving Cisco IPS Active Update Bulletins, page 4](#)
- [Cisco Security Center, page 5](#)
- [New and Changed Information, page 5](#)
- [Before Upgrading to Cisco IPS 6.1\(1\)E1, page 7](#)
- [Upgrading to Cisco IPS 6.1\(1\)E1, page 15](#)
- [After Upgrading to Cisco IPS 6.1\(1\)E1, page 17](#)
- [Installing Cisco IME, page 25](#)
- [Restrictions and Limitations, page 26](#)
- [Caveats, page 27](#)
- [Related Documentation, page 28](#)
- [Obtaining Documentation and Submitting a Service Request, page 29](#)



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

© 2006-2009 Cisco Systems, Inc. All rights reserved.

**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.

IPS 6.1(1)E1 File List

The following files are part of Cisco IPS 6.1(1)E1:

- Readme File
 - IPS-6.1-1-E1.readme.txt
- Minor Version Upgrade Files
 - IPS-K9-6.1-1-E1.pkg
 - IPS-AIM-K9-6.1-1-E1.pkg
- System Image Files
 - IPS-4240-K9-sys-1.1-a-6.1-1-E1.img
 - IPS-4255-K9-sys-1.1-a-6.1-1-E1.img
 - IPS-4260-K9-sys-1.1-a-6.1-1-E1.img
 - IPS-4270-K9-sys-1.1-a-6.1-1-E1.img
 - WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1-E1.bin.gz
 - IPS-SSM_10-K9-sys-1.1-a-6.1-1-E1.img
 - IPS-SSM_20-K9-sys-1.1-a-6.1-1-E1.img
 - IPS-SSM_40-K9-sys-1.1-a-6.1-1-E1.img
 - IPS-AIM-K9-sys-1.1-a-6.1-1-E1.img
- Recovery Image Files
 - IPS-K9-r-1.1-a-6.1-1-E1.pkg
 - IPS-AIM-K9-r-1.1-a-6.1-1-E1.pkg

For More Information

For the procedure for obtaining these files on Cisco.com, see [Obtaining Software on Cisco.com](#), page 9.

Supported Platforms

**Note**

All IPS platforms allow ten concurrent log in sessions.

Cisco IPS 6.1(1)E1 is supported on the following platforms:

- IPS-4240 Series Sensor Appliances
- IPS-4255 Series Sensor Appliances
- IPS-4260 Series Sensor Appliances

- IPS 4270-20 Series Sensor Appliances
- WS-SVC-IDSM2 series Intrusion Detection System Module (IDSM-2)
- ASA-SSM-AIP-10 series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP-SSM-10)
- ASA-SSM-AIP-20 series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP-SSM-20)
- ASA-SSM-AIP-40 series Cisco ASA Advanced Inspection and Prevention Security Service Modules (AIP-SSM-40)
- Intrusion Prevention System Advanced Integration Module (AIM-IPS)

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)

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.

Some TFTP servers limit the maximum file size that can be transferred to ~32 MB. Therefore, we recommend the following TFTP servers:

- For Windows:
Tftpd32 version 2.0, available at:
<http://tftpd32.jounin.net/>
- For UNIX:
Tftp-hpa series, available at:
<http://www.kernel.org/pub/software/network/tftp/>

For More Information

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

IPS Management and Event Viewers

Use the following tools for configuring Cisco IPS 6.1(1) E1 sensors:

- Cisco IDM 6.1
- Cisco IME 6.1
- IPS CLI 6.1
- ASDM 5.2 and above
- CSM 3.2

Use the following tools for monitoring Cisco IPS 6.1(1)E1 sensors:

- Cisco IME 6.1
- MARS 4.2 and 4.3(1)
- CWSIMS v3.3.1.v3.4 mad v3.4.1
- CIC Security Monitor 3.6

**Note**

Viewers that are already configured to monitor the Cisco IPS 6.0 sensors may need to be configured to accept a new SSL certificate for the Cisco IPS 6.1(1)E1 sensors.

Receiving Cisco IPS Active Update Bulletins

You can subscribe to Cisco IPS Active Update Bulletins on Cisco.com to receive e-mails when signature updates and service pack updates occur.

To receive bulletins about updates, follow these steps:

-
- Step 1** Log in to [Cisco.com](#).
 - Step 2** Under Quick Links on the right side of the window, click **Security Center**.
 - Step 3** Scroll down and under Products and Service Updates, choose **Cisco IPS Active Update Bulletins**.
 - Step 4** Click one of the Cisco IPS Active Update Bulletins.
 - Step 5** Under In this Issue, click **Subscription Information**.
 - Step 6** Under Subscription Information, click **subscribe now**.
 - Step 7** Fill out the required information, as follows:
 - a. Would you like to receive IDS Active Update Bulletin? Select **Yes** or **No** from the drop-down list.
 - b. Enter your first name in the **First Name** field.

- c. Enter your last name in the **Last Name** field.
 - d. Enter the name of your company in the **Company** field.
 - e. Choose your country from the drop-down menu.
 - f. Enter your e-mail address in the **E-mail** field.
- Step 8** Check the check box if you want to receive further information about Cisco products and offerings by e-mail.
- Step 9** Fill in the optional information if desired.
- a. Choose your job function from the drop-down list.
 - b. Choose your job level from the drop-down list.
 - c. Choose your industry or business type from the drop-down list.
 - d. Choose how many people your organization employs worldwide from the drop-down list.
 - e. Choose your company or organization type from the drop-down list.
- Step 10** Click **Submit**.
- You receive e-mail notifications of updates when they occur and instructions on how to obtain them.
-

Cisco Security Center

The Cisco Security Center 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. The Cisco Security Center contains the top ten intelligence reports listed by date, severity, urgency, and whether there is a new signature available to deal with the threat.

The Cisco Security Center contains a Security News section that lists security articles of interest. There are related security tools and links.

You can access the Cisco Security Center at this URL:

<http://tools.cisco.com/MySDN/Intelligence/home.x>

The Cisco Security Center is also a repository of information for individual signatures, including signature ID, type, structure, and description.

You can access the signature search at this URL:

<http://tools.cisco.com/security/center/search.x?search=Signature>

New and Changed Information

Cisco IPS 6.1(1)E1 includes the following new features:

- IPS sensor enhancements
 - Automatic signature updates from Cisco.com
 - Sensor and security health statistics

- Simplified initialization using the **setup** command
- Unauthenticated NTP
- Improved upgrade status information
- Support of inline asymmetric traffic
- Password integrity service
- Cisco Intrusion Prevention System Manager Express (IME)
 - Real-time and historical events monitoring
 - Health-monitoring console
 - Integrated configuration
 - Customizable dashboards
 - Tools (ping, traceroute, whois, DNS lookup)
 - RSS feeds
 - Video help
 - Reporting
- Enhanced IDM
 - Startup wizard
 - Health monitoring improvements
 - Customizable dashboards
 - Improved policy and signature tables
 - User interface performance improvements
- In earlier 6.0 releases, a manual workaround was available to support inline asymmetric traffic. In the IPS 6.1(1)E1 release, you can enable inline asymmetric traffic using the CLI or IDM. If you used the workaround to enable asymmetric traffic, remove the manual setting in the CLI, and reenable asymmetric traffic.



Note If you do not remove the manual entry in the `sensorApp.conf` file, you will receive the following `main.log` warning each time you reboot the sensor: `NormalizerSettings in sensorApp.conf (AsynchMode and AsymmetricFlows) have been removed. Use Service AnalysisEngine - VS - inline-TCP-evasion-protection-mode.`

- The legacy RDEP Event Server, used by IDS versions 4.x to communicate events, is not enabled by default in this release. You can enable RDEP Event Server subscriptions in IDM or IME. We recommend you migrate to SDEE/CIDEE because the RDEP Event Server is not supported in future releases.
- IPS 6.1(1)E1 includes the S329 signature update.

For More Information

- For more information on Inline TCP session tracking mode, refer to [Inline TCP Session Tracking Mode](#).
- For the procedure for enabling inline TCP evasion protection mode, refer to [Adding Virtual Sensors](#).
- For the procedure for enabling RDEP Event Server subscriptions, for the IDM procedure, refer to [Configuring Network Settings](#), and for the IME procedure, refer to [Configuring Network Settings](#).

Before Upgrading to Cisco IPS 6.1(1)E1

This section describes the actions you should take before upgrading to Cisco IPS 6.1(1)E1. It contains the following topics:

- [Perform These Tasks, page 7](#)
- [Copying and Restoring the Configuration File Using a Remote Server, page 7](#)
- [Obtaining Software on Cisco.com, page 9](#)
- [IPS Software Versioning, page 10](#)

Perform These Tasks

Before you upgrade your sensors to Cisco IPS 6.1(1)E1, make sure you perform the following tasks:

- Make sure you have a valid Cisco Service for IPS service contract per sensor so that you can apply software upgrades.
- Created a backup copy of your configuration.
- Saved the output of the **show version** command.

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

For More Information

- For more information on how to obtain a valid Cisco Service for IPS service contract, see [Service Programs for IPS Products, page 20](#).
- For the procedure for creating a backup copy of your configuration, see [Copying and Restoring the Configuration File Using a Remote Server, page 7](#).
- For the procedure for finding your Cisco IPS software version, for the CLI refer to [Displaying Version Information](#), for IDM refer to [IDM Home Window](#), and for IME refer to [Sensor Information Gadget](#).
- For the procedure for downgrading signature updates on your sensor, refer to [Upgrading, Downgrading, and Installing System Images](#).

Copying and Restoring the Configuration File Using a Remote Server

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.



Note

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

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.

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.

The following keywords are used to designate the file location on the sensor:

- **current-config**—The current running configuration. The configuration becomes persistent as the commands are entered.
- **backup-config**—The storage location for the configuration backup.



Caution

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

To back up and restore your current configuration, follow these steps:

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

Step 2 To back up the current configuration to the remote server.

```
sensor# copy scp://user@10.1.1.1//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** so the sensor does not replace the existing configuration.

For More Information

For the procedure for adding trusted hosts, for the CLI refer to [Adding TLS Trusted Hosts](#), for IDM refer to [Adding Trusted Hosts](#), and for IME refer to [Adding 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.



Note 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

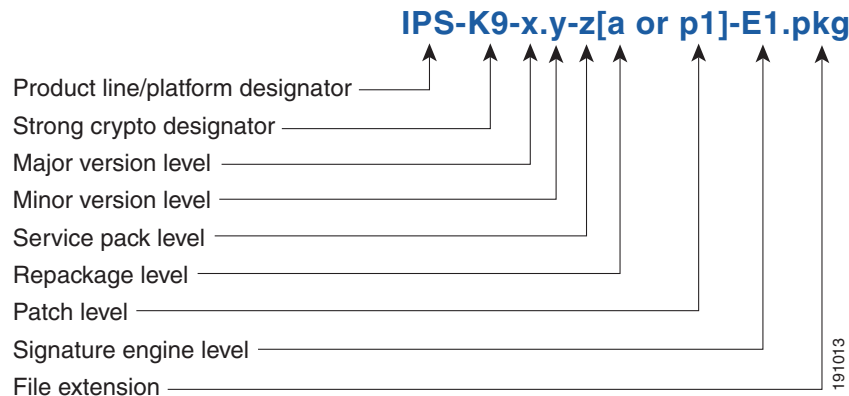
This section describes the various IPS software files, and contains the following sections:

- [Major and Minor Updates, Service Packs, and Patch Releases, page 11](#)
- [Signature/Virus Updates and Signature Engine Updates, page 12](#)
- [Recovery and System Image Filenames, page 13](#)
- [6.x Software Release Examples, page 14](#)

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 Cisco IPS 6.0 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 6.0(1) requires 5.x. With each major update there are corresponding system and recovery packages.



Note The 6.0(1) major update is only used to upgrade 5.x sensors to 6.0(1). If you are reinstalling 6.0(1) on a sensor that already has 6.0(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 6.0 is 6.1(1). Minor updates are released for minor enhancements to the product. Minor updates contain all previous minor features (except deprecated features), service pack fixes, signature updates since the last major version, and the new minor features being released. You can install the minor updates on the previous major or minor version (and often even on earlier versions). The minimum supported version needed to upgrade to the newest minor version is listed in the Readme that accompanies the minor update. With each minor update there are corresponding system and recovery packages.

Service Packs

Cumulative following a base version release (minor or major). Service packs are used for the release of defect fixes with no new enhancements. Service packs contain all service pack fixes since the last base version (minor or major) and the new defect fixes being released. Service packs require the minor version. The minimum supported version needed to upgrade to the newest service pack is listed in the Readme that accompanies the service pack. Service packs also include the latest engine update. For example, if service pack 6.0(3) is released, and E3 is the latest engine level, the service pack is released as 6.0(3)E3.

Patch Release

Used to address defects that are identified in the upgrade binaries after a software release. Rather than waiting until the next major or minor update, or service pack to address these defects, a patch can be posted. Patches include all prior patch releases within the associated service pack level. The patches roll into the next official major or minor update, or service pack.

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

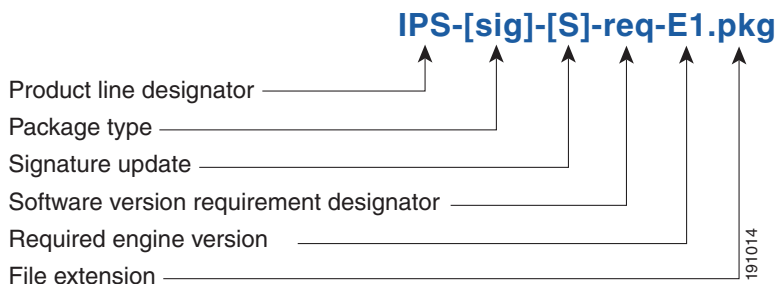


Note Upgrading to a newer patch does not require you to uninstall the old patch. For example, you can upgrade from patch 5.0(1p1) to 5.0(1p2) without first uninstalling 5.0(1p1).

Signature/Virus Updates and Signature Engine Updates

Figure 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,



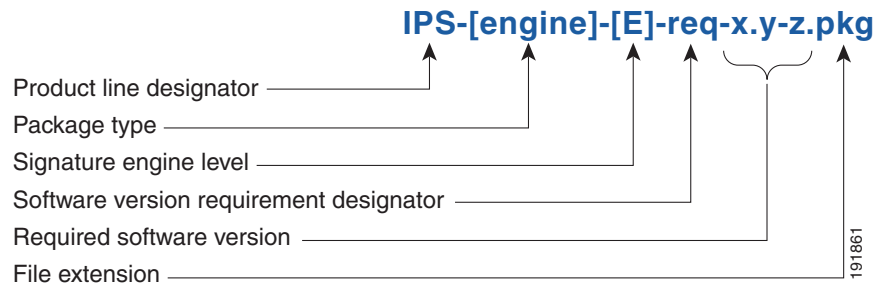
Signature/Virus Updates

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



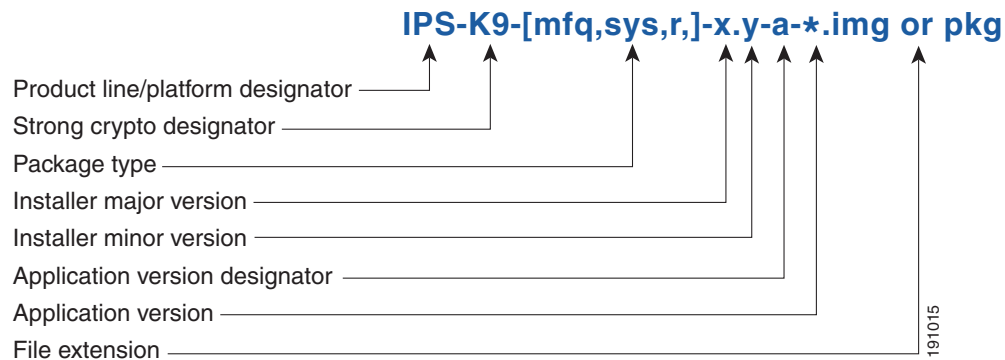
Signature Engine Updates

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 and System Image Filenames

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.

6.x Software Release Examples

Table 1 lists platform-independent Cisco IPS 6.x 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-6.1-3.pkg
Service packs ³	Semi-annually or as needed	—	6.1(3)	IPS-K9-6.1-3-E1.pkg
Minor version update ⁴	Annually	—	6.1(1)	IPS-K9-6.1-1-E1.pkg
Major version update ⁵	Annually	—	6.0(1)	IPS-K9-6.0-1-E1.pkg
Patch release ⁶	As needed	patch	6.0(1p1)	IPS-K9-patch-6.0-1p1-E1.pkg
Recovery package ⁷	Annually or as needed	r	1.1-6.0(1)	IPS-K9-r-1.1-a-6.1-1-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 6.0(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-6.1-1-E1.img
Maintenance partition image ²	Annually	mp	IDSM-2	c6svc-mp.2-1-2.bin.gz
Bootloader	As needed	bl	AIM-IPS	pse_aim_x.y.z.bin (where x, y, z is the release number)
Mini-kernel	As needed	mini-kernel	AIM-IPS	pse_mini_kernel_1.1.10.64.bz2

- The system image includes the combined recovery and application image used to reimagine 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.

Table 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	IDS2M2
IPS network module	AIM
AIP-SSM	SSM_10 SSM_20 SSM_40

Upgrading to Cisco IPS 6.1(1)E1

This section provides information on upgrading to Cisco IPS 6.1(1)E1, and contains the following topics:

- [Upgrade Notes and Caveats, page 15](#)
- [Upgrading to IPS 6.1\(1\)E1, page 16](#)

Upgrade Notes and Caveats

The following upgrade notes and caveats apply to upgrading to 6.1(1)E1:

- The minimum required version for upgrading to 6.1(1)E1 is 5.0(1) or later, which is available as a download from Cisco.com.
- Use the IPS-AIM-K9-6.1-1-E1.pkg upgrade file to upgrade AIM-IPS. For all other supported sensors, use the IPS-K9-6.1-1-E1.pkg upgrade file.
- If you configured Auto Update for your sensor, copy the Cisco IPS 6.1(1)E1 update to the directory on the server that your sensor polls for updates. If you install an update on your sensor and the sensor is unusable after it reboots, you must reimage your sensor.
- For AIP-SSM, reimage from the adaptive security appliance using the **hw-module module 1 recover configure/boot** command.
- When you install the system image for your sensor, all accounts are removed and the default account and password are reset to **cisco**.
- You must have a valid Cisco Service for IPS Maintenance contract per sensor to receive and use software upgrades from Cisco.com.
- When you upgrade AIM-IPS, you must disable heartbeat reset on the router before installing an upgrade. You can reenble heartbeat reset after you complete the upgrade. If you do not disable heartbeat reset, the upgrade can fail and leave AIM-IPS in an unknown state, which may require a system reimage to recover.

- If you are using automatic upgrade with AIM-IPS and other IPS appliances or modules, make sure you put both the 6.1(1) upgrade file, IPS-K9-6.1-1-E1.pkg, and the AIM-IPS upgrade file, IPS-AIM-K9-6.1-1-E1.pkg, on the automatic update server so that AIM-IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the 6.1(1) upgrade file, IPS-K9-6.1-1-E1.pkg, on the automatic update server, AIM-IPS will download and try to install it, which is the incorrect file for AIM-IPS.

For More Information

- For the procedure for using the **show version** command in the CLI, refer to [Displaying Version Information](#). To view version information in IDM, refer to [System Information](#), and in IME refer to [System Information](#).
- For the procedure for disabling heart beat reset, refer to [Enabling and Disabling Heartbeat Reset](#).
- For the procedure for configuring automatic update, for the CLI refer to [Configuring Automatic Upgrades](#), for IDM refer to [Configuring Automatic Update](#), and for IME refer to [Configuring Automatic Update](#).
- For more information on reimaging the sensor, refer to [Upgrading, Downgrading, and Installing System Images](#).

Upgrading to IPS 6.1(1)E1



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.

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file (for example, IPS-K9-6.1-1-E1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

Step 2 Log in to the CLI using an account with administrator privileges.

Step 3 Enter configuration mode.

```
sensor# configure terminal
```

Step 4 Upgrade the sensor.

```
sensor(config)# upgrade url/IPS-K9-6.1-1-E1.pkg
```

The URL points to where the update file is located, for example, to retrieve the update using FTP, enter the following:

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-K9-6.1-1-E1.pkg
```

Step 5 Enter the password when prompted.

```
Enter password: *****
```

Step 6 Enter **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.



Note The operating system is reimaged and all files that have been placed on the sensor through the service account are removed.

For More Information

- For more information on obtaining service contracts, see [Service Programs for IPS Products, page 20](#).
- For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privileges, see [Obtaining Software on Cisco.com, page 9](#).

After Upgrading to Cisco IPS 6.1(1)E1

This section provides information about what to do after you install Cisco IPS 6.1(1)E1. It contains the following topics:

- [Comparing Configurations, page 17](#)
- [Importing a New SSL Certificate, page 18](#)
- [Logging In to IDM, page 18](#)
- [Licensing the Sensor, page 19](#)

Comparing Configurations

Compare your backed up and saved 6.0 configuration with the output of the **show configuration** command after upgrading to 6.1(1)E1 to verify that all the configuration has been properly converted.



Caution

If the configuration is not properly converted, check the caveats for Cisco IPS 6.1(1)E1 or check Cisco.com for any upgrade issues that have been found. Contact the TAC if no DDTS refers to your situation.

For More Information

- For the procedure for showing the output of the **show configuration** command, refer to [Displaying the Current Configuration](#).
- For a list of IPS 6.1(1)E1 caveats, see [Caveats, page 27](#).

Importing a New 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 procedure for configuring TLS/SSL, for the CLI refer to [Configuring TLS](#), for IDM refer to [Configuring Trusted Hosts](#), and for IME refer to [Configuring Trusted Hosts](#).

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 6.1 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 1.4.2 or 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 6.1 window. After you launch IDM, is it not necessary for this window to remain open.

Licensing the Sensor

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

- [Understanding the License, page 19](#)
- [Service Programs for IPS Products, page 20](#)
- [Obtaining and Installing the License Key, page 21](#)

Understanding the License

Although the sensor functions without the license key, you must have a license key to obtain signature updates. To obtain a license key, you must have the following:

- Cisco Service for IPS service contract
Contact your reseller, Cisco service or product sales to purchase a contract.
- Your IPS device serial number
To find the IPS device serial number in IDM or IME, for IDM choose **Configuration > Sensor Management > Licensing**, and for IME choose **Configuration > sensor_name > Sensor Management > Licensing**, or in the CLI use the **show version** command.
- Valid Cisco.com username and password

Trial license keys are also available. If you cannot get your sensor licensed because of problems with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

You can obtain a license key from the Cisco.com licensing server, which is then delivered to the sensor. Or, you can update the license key from a license key provided in a local file. Go to <http://www.cisco.com/go/license> and click **IPS Signature Subscription Service** to apply for a license key.

You can view the status of the license key in these places:

- IDM Home window Licensing section on the Health tab
- IDM Licensing pane (Configuration > Licensing)
- IME Home page in the Device Details section on the Licensing tab
- License Notice at CLI login

Whenever you start IDM, IME, or the CLI, you are informed of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use IDM, IME, and the CLI, but you cannot download signature updates.

If you already have a valid license on the sensor, you can click **Download** on the License pane to download a copy of your license key to the computer that IDM or IME is running on and save it to a local file. You can then replace a lost or corrupted license, or reinstall your license after you have reimaged the sensor.

Service Programs for IPS Products

You must have a Cisco Services for IPS service contract for any IPS product so that you can download a license key and obtain the latest IPS signature updates. If you have a direct relationship with Cisco Systems, contact your account manager or service account manager to purchase the Cisco Services for IPS service contract. If you do not have a direct relationship with Cisco Systems, you can purchase the service account from a one-tier or two-tier partner.

When you purchase the following IPS products you must also purchase a Cisco Services for IPS service contract:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS 4270-20
- AIM-IPS
- IDSM-2

For ASA 5500 series adaptive security appliance products, if you purchased one of the following ASA 5500 series adaptive security appliance 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 5500 series adaptive security appliance products that ships with the AIP-SSM installed or if you purchased AIP-SSM to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract:

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA5520-AIP40-K9
- ASA5540-AIP40-K9
- ASA-SSM-AIP-10-K9=
- ASA-SSM-AIP-20-K9=
- ASA-SSM-AIP-40-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.

Obtaining and Installing the License Key

You can install the license key through the CLI, IDM, or IME. This section describes how to obtain and install the license key, and contains the following topics:

- [Using IDM or IME, page 21](#)
- [Using the CLI, page 23](#)


Using IDM or IME



Note

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

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

-
- Step 1** Log in to IDM or IME using an account with administrator privileges.
- Step 2** For IDM choose **Configuration > Sensor Management > Licensing**. For IME choose **Configuration > *sensor_name* > Sensor Management > 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:
- Click the **Cisco.com** radio button to obtain the license from Cisco.com.
IDM or IME contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.
 - Click the **License File** radio button to use a license file.
To use this option, you must apply for a license key at www.cisco.com/go/license.
The license key is sent to you in e-mail and you save it to a drive that IDM or IME can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.
- Step 4** Click **Update License**, and in the Licensing dialog box, click **Yes** to continue.
The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.
- Step 5** Click **OK**.
- Step 6** Go to www.cisco.com/go/license.
- Step 7** 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 8** Save the license key to a hard-disk drive or a network drive that the client running IDM or IME can access.
- Step 9** Log in to IDM or IME.
- Step 10** For IDM choose **Configuration > Sensor Management > Licensing**. For IME choose **Configuration > *sensor_name* > Sensor Management > Licensing**.
- Step 11** Under Update License, click the **License File** radio button.
- Step 12** In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file.
- Step 13** Browse to the license file and click **Open**.
- Step 14** Click **Update License**.
-

Using the CLI

Use the **copy source-url license_file_name license-key** command to copy the license key to your sensor. The following options apply:

- *source-url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination-url*—The location of the destination file to be copied. It can be a URL or a keyword.
- **license-key**—The subscription license file.
- *license_file_name*—The name of the license file you receive.


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 www.cisco.com/go/license.


Note

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

Step 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 by e-mail to the e-mail address you specified.

Step 3 Save the license key to a system that has a web server, FTP server, or SCP server.

Step 4 Log in to the CLI using an account with administrator privileges.

Step 5 Copy the license key to the sensor.

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *****
```

Step 6 Verify the sensor is licensed.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.1(1)E1

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S391.0          2008-04-16
  Virus Update        V1.2             2005-11-24
OS Version:          2.4.30-IDS-smp-bigphys
Platform:            ASA-SSM-20
Serial Number:       P300000220
Sensor up-time is 3 days.
Using 1031888896 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 52.4M out of 166.6M bytes of available disk space (33% usage)
boot is using 37.8M out of 68.5M bytes of available disk space (58% usage)

MainApp              N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
AnalysisEngine       N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
CLI                  N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500

Upgrade History:

  IPS-K9-6.1-1-E1   15:36:05 UTC Thu Apr 24 2008

Recovery Partition Version 1.1 - 6.1(1)E1

Host Certificate Valid from: 25-Apr-2008 to 26-Apr-2010

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#
```

Installing Cisco IME

If you have a version of Cisco IPS Event Viewer installed, the Install wizard prompts you to remove it before installing IME.

IME event monitoring is also supported in IOS-IPS versions that support the Cisco IPS 5.x/6.x signature format. We recommend IOS-IPS 12.4(15)T4 if you intend to use IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.



Caution

Do not install IME on top of existing installations of CSM or IEV. You must uninstall these applications before installing IME.



Caution

Disable any anti-virus or host-based intrusion detection software before beginning the installation, and close any open applications. The installer spawns a command shell application that may trigger your host-based detection software, which causes the installation to fail.



Note

You must be administrator to install IME.

To install IME, follow these steps:

-
- Step 1** Download the IME executable file to your computer, or start IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file.
IME-6.1.0.32.exe is an example of what the IME executable file might look like.
 - Step 2** Double-click the executable file.
The Cisco IPS Manager Express - InstallShield Wizard appears.
 - Step 3** You receive a warning if you have a previous version of Cisco IPS Event Viewer installed. Acknowledge the warning, and exit installation. Remove the older version of IEV, and then continue IME installation.
 - Step 4** Double-click the executable file.
The Cisco IPS Manager Express - InstallShield Wizard appears.
 - Step 5** Click **Next** to start IME installation.
 - Step 6** Accept the license agreement and click **Next**.
 - Step 7** Click **Next** to choose the destination folder, click **Install** to install IME, and then click **Finish** to exit the wizard.

The Cisco IME and Cisco IME Demo icons are now on your desktop.

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IPS 6.1(1)E1 software and the products that run 6.1(1)E1:

- AIM-IPS does not support virtualization.
- When you reload the router, AIM-IPS also reloads. To ensure that there is no loss of data on AIM-IPS, make sure you shut down the module using the **shutdown** command before you use the **reload** command to reboot the router.
- Do not deploy IOS IPS and AIM-IPS at the same time.
- When AIM-IPS is used with an IOS firewall, make sure SYN flood prevention is done by the IOS firewall.

AIM-IPS and the IOS firewall complement abilities of each other to create security zones in the network and inspect traffic in those zones. Because AIM-IPS and the IOS firewall operate independently, sometimes they are unaware of the activities of the other. In this situation, the IOS firewall is the best defense against a SYN flood attack.

- Cisco access routers only support one IDS/IPS per router.
- 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. The sensor must contain at least two physical sensing interfaces to perform both promiscuous and inline monitoring. The exceptions to this are AIP-SSM-10, AIP-SSM-20, and AIP-SSM-40. AIP-SSM can support both promiscuous and inline monitoring on its single physical back plane interface inside the adaptive security appliance. The configuration on the main adaptive security appliance can be used to designate which packets/connections should be monitored by AIP-SSM as either promiscuous or inline.
- When deploying an IPS sensor monitoring two sides of a network device that does TCP sequence number randomization, we recommend using a virtual sensor for each side of the device.
- 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.
- 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.
- IDM and IME launch MySDN from the last browser window you opened, which is the default setting for Windows. To change this default behavior, in Internet Explorer, choose **Tools > Internet Options**, and then click the **Advanced** tab. Scroll down and uncheck the **Reuse windows for launching shortcuts** check box.

For More Information

For more information on interoperability between modules, refer to [Interoperability With Other IPS Modules](#).

Caveats

For the most complete and up-to-date list of caveats, use the Bug Navigator Tool to refer to the caveat release notes. The Bug Navigator Tool is found at this URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

This section lists the caveats, and contains the following topics:

- [Resolved Caveats, page 27](#)
- [Known Caveats, page 27](#)

Resolved Caveats

The following known issues have been resolved in the 6.1(1)E1 release:

- CSCso31217—encrypted passwords not decrypted after upgrade
- CSCsm99137—cli error on login attempt to 4240 - Monarchos
- CSCsm10898—the external management interface on the NM-IPS will not autonegotiate
- CSCsk3081—Misconfigured remote application can cause sensor HDD failure
- CSCso65593—6.0(4a) upgrade failure with virus version 1.4 has bad error message
- CSCso56465—mainApp cplane error message needs actual error code
- CSCso21050—Frequent error generation - SigEventList not empty
- CSCsm70361—service external-product-interface config not carried forward on upgrade
- CSCsk84825—Non-printable character in event XML causes cascading events
- CSCsk09025—idsm2 interface Operational Mode: down after reload from switch
- CSCsj75538—Auto Update - not pulling platform specific patch
- CSCsj18246—Event variables not tagged with the smallest locality
- CSCsi10476—cidsAlertProtocol missing from SNMP Traps
- CSCsg21826—CISCO-CIDS-MIB v3.5 does not have denyPacket and blockHost defined
- CSCsj68881—Auto update settings won't save correctly in IDM.
- CSCsi96099—Borealis - IDM/webserver - 2 unknown failed control transactions

Known Caveats

The following known issues are found in Cisco IPS 6.1(1)E1:

- CSCso96079—META alarms may have the wrong risk ratings
- CSCso85697—crazy traffic inline causes failure in updateProtocolState
- CSCso78274—ASA/SSM False Failover
- CSCso74628—Attack mis-counts seen with promiscuous mode (moderate traffic)
- CSCso60709—Flood net Engine Sigs 69xx are not firing in promiscuous mode
- CSCso49304—IPS - Large KB Thresholds represented as negatives
- CSCso45473—Analysis Engine terminated prematurely

- CSCso28141—Wrong attack context data captured
- CSCso20750—modify-packet-inline computing incorrect checksum
- CSCso15103—4260 w/ Rev. 8 or 9 4x1Gb NIC may enter HW bypass on engine update
- CSCso09813—Missing victim context data in sig 5081
- CSCso02370—CPU and Load periodically revert to 0
- CSCsm90428—string-tcp alert contains incorrect data in 'from target' context
- CSCsm72321—AIP module get stuck in high cpu due to mainApp infinite loop
- CSCsm46158—Critical memory condition can cause race condition
- CSCsm24466—Jumbo frames on XL interface can cause dropped packets
- CSCsl69776—AD is not generating an alert for every worm attacker
- CSCsl66235—Setup errors after defaulting sensor config via IDM
- CSCsk53813—upgrade log files are not preserved during an upgrade
- CSCsj83029—CRAZYHAWK:sig 1308_0 not firing on fragroute tcp_chaff TTL attack
- CSCsj82458—global-block-timeout allows values outside supported range
- CSCsj80889—IP frags subjected to modify-packet-inline have been re-fragmented
- CSCsj78809—IPS 6.0(3) SigProcessor failure with reinjected frag
- CSCsj70643—Normalizer signatures not modifying-packet-inline
- CSCsj57474—Frag traffic with dot1q headers misses a few sweep and atomic-ip sigs
- CSCsi73502—6.0(2)E1: No warning message when removing sensor used by ASA
- CSCsi60530—69xx firing but reporting wrong interface
- CSCsh89833—Delete event variable referenced by filter or sig from IDM
- CSCsh50760—NAC causes high mainApp usage
- CSCsh16294—IPSVIRTUALIZATION:Physical Interface info not passed to ASA/SSM Database
- CSCsg96871—AnalysisEngine InspectorServiceAICWeb::ToServiceInspect abort
- CSCsd19619—NO statistics on traffic under heavy load
- CSCso96654—Editing EventActionRules removes all like Sig Actions

Related Documentation

For more information on Cisco IPS 6.1, refer to the following documentation 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 6.1*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 6.1*
- *Installing and Using Cisco Intrusion Prevention System Manager Express 6.1*
- *Cisco Intrusion Prevention System Command Reference 6.1*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.1*

- *Installing Cisco Intrusion Prevention System Appliances and Modules 6.1*
- *Installing and Removing Interface Cards in Cisco IPS-4260 and IPS 4270*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*

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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0908R)

Copyright © 2008-2009 Cisco Systems, Inc. All rights reserved.

