



Release Notes for Cisco Intrusion Prevention System 6.1(1)E3

Published: November 1, 2008, OL-19697-01

Revised: August 16, 2011

Contents

- [IPS 6.1\(1\)E3 File List, page 2](#)
- [Supported Platforms, page 3](#)
- [Supported Servers, page 3](#)
- [ROMMON and TFTP, page 3](#)
- [IPS Management and Event Viewers, page 4](#)
- [Cisco Security Intelligence Operations, page 4](#)
- [New and Changed Information, page 5](#)
- [MySDN Decommissioned, page 6](#)
- [Before Upgrading to Cisco IPS 6.1\(1\)E3, page 7](#)
- [Upgrading to Cisco IPS 6.1\(1\) E3, page 15](#)
- [After Upgrading to Cisco IPS6.1\(1\)E3, page 19](#)
- [Installing Cisco IME, page 25](#)
- [Restrictions and Limitations, page 26](#)
- [Recovering the Password, page 27](#)
- [Caveats, page 34](#)
- [Related Documentation, page 37](#)
- [Obtaining Documentation and Submitting a Service Request, page 37](#)



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

© 2006-2010 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)E3 File List

The following files are part of Cisco IPS 6.1(1)E3:

- Readme File
 - IPS-6.1-1-E3.readme.txt
- Minor Version Upgrade File
 - IPS-K9-6.1-1-E3.pkg
 - IPS-AIM-K9-6.1-1-E3.pkg
- System Image Files
 - IPS-4240-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-4255-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-4260-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-4270_20-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-AIM-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-IDSM2-K9-sys-1.1-a-6.1-1-E3.bin.gz
 - IPS-SSM_10-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-SSM_20-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-SSM_40-K9-sys-1.1-a-6.1-1-E3.img
 - IPS-NME-K9-sys-1.1-a-6.1-1-E3.pkg
- Recovery Image Files
 - IPS-K9-r-1.1-a-6.1-1-E3.pkg
 - IPS-AIM-K9-r-1.1-a-6.1-1-E3.pkg
 - IPS-NME-K9-r-1.1-a-6.1-1-E3.pkg
- E3 Engine Update Files
 - IPS-engine-E3-req-6.1-1.pkg

For More Information

For the procedure for obtaining IPS software, see [Obtaining Software on Cisco.com, page 10](#).

Supported Platforms


Note

All IPS platforms allow ten concurrent log in sessions.

Cisco IPS6.1(1)E3 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
- Intrusion Detection System Module (IDSM2) for Catalyst 6500 series
- 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)
- Intrusion Prevention System Network Module (NME 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:

- CMS - Apache Server (Tomcat)
- CMS - 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 [After Upgrading to Cisco IPS 6.1\(1\)E3](#), page 19.
- 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)E3 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)E3 sensors:

- Cisco IME 6.1
- MARS 4.2 and 4.3(1)
- CSM 4.0



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)E3 sensors.

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>

New and Changed Information

Cisco IPS 6.1(1)E3 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 reenables 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 `ServiceAnalysisEngine - 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.
- The S365 signature update is a built in to the E3 signature engine update. You cannot download S365 separately. The E3 signature engine update includes the following:

- 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 **I4-protocol** UDP. The purpose of this parameter is to check if UDP total length falls within a specific range.

For More Information

- For detailed information about Inline TCP Session Tracking mode, refer to [Inline TCP Session Tracking Mode](#) and [Adding, Editing, and Deleting Virtual Sensors](#).
- For detailed information about the Atomic engines, refer to [Atomic Engine](#).

MySDN Decommissioned

Because MySDN has been decommissioned, the URL in older versions of IDM and IME is no longer functional. If you are using IPS 6.0 or later, we recommend that you upgrade your version of IDM and IME.

You can upgrade to the following versions to get the functioning MySDN URL:

- IDM 7.0.3
- IME 7.0.3

- IPS 7.0(4), which contains IDM 7.0.4

If you are using version IPS 5.x, you must look up signature information manually at this URL:

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

For More Information

For detailed information on MySDN, for IDM refer to [MySDN](#), and for IME refer to [MySDN](#).

Before Upgrading to Cisco IPS 6.1(1)E3

This section describes the actions you should take before upgrading to Cisco IPS 6.1(1) E3. It contains the following topics:

- [Perform These Tasks, page 7](#)
- [Backing Up and Restoring the Configuration File Using a Remote Server, page 8](#)
- [Obtaining Software on Cisco.com, page 10](#)
- [IPS Software Versioning, page 11](#)
- [Software Release Examples, page 14](#)

Perform These Tasks

Before you upgrade your sensors to Cisco IPS 6.1(1) E3, 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.



Note

To apply the E3 engine update, you must have version 6.1(1)E2 installed on your sensor. If you need to upgrade your system, consider installing the 6.1(1)E3 minor update, which eliminates the need for the E3 engine update because the E3 functionality is built in to the minor update.

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 21](#).
- For the procedure for creating a backup copy of your configuration, see [Backing Up and Restoring the Configuration File Using a Remote Server, page 8](#).
- 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](#).

Backing Up 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 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.

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

Downloading IPS Software

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

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



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

- Step 7** Click the type of software file you need. The available files appear in a list in the right side of the window. You can sort by file name, file size, memory, and release date. And you can access the Release Notes and other product documentation.
- Step 8** Click the file you want to download. The file details appear.
- Step 9** Verify that it is the correct file, and click **Download**.
- Step 10** Click **Agree** to accept the software download rules. The first time you download a file from Cisco.com, you must fill in the Encryption Software Export Distribution Authorization form before you can download the software.
 - Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.
 - Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again. The File Download dialog box appears.
- Step 11** Open the file or save it to your computer.
- Step 12** Follow the instructions in the Readme to install the update.



Note Major and minor updates, service packs, recovery files, signature and signature engine updates are the same for all sensors. System image files are unique per platform.

IPS Software Versioning

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

Major Update

A major update contains new functionality or an architectural change in the product. For example, the Cisco IPS 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

A minor update is 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 Pack

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

Patch Release

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

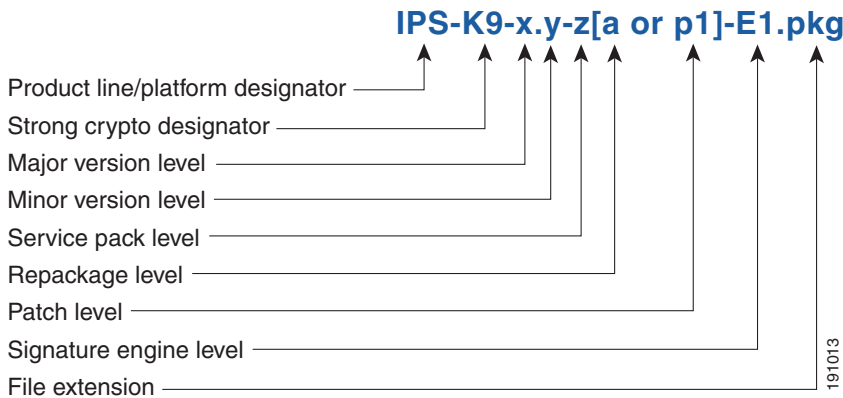
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 5.0(1p1) requires 5.0(1).



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).

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*

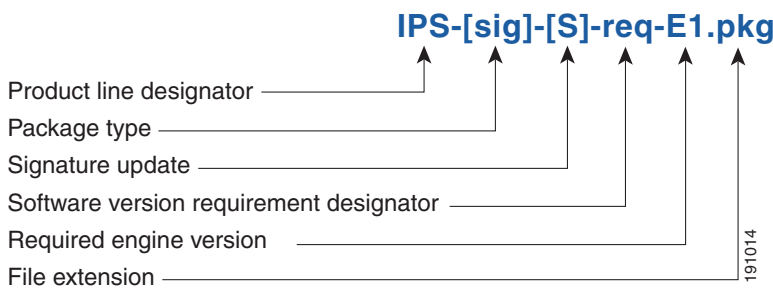


Signature Update

A signature update is a package file containing a set of rules designed to recognize malicious network activities. Signature updates are released independently from other software updates. Each time a major or minor update is released, you can install signature updates on the new version and the next oldest version for a period of at least six months. Signature updates are dependent on a required signature engine version. Because of this, a *req* designator lists the signature engine required to support a particular signature update.

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

Figure 2 *IPS Software File Name for Signature Updates*

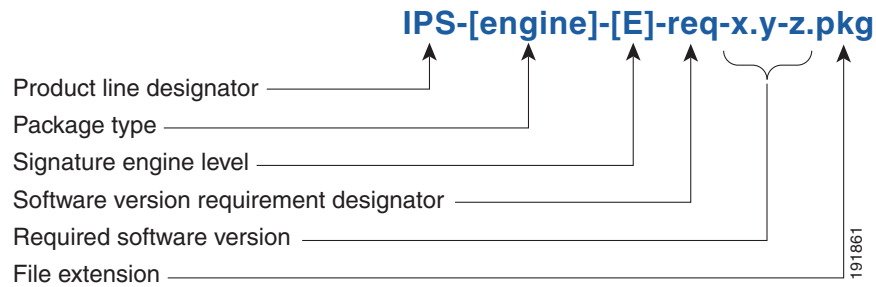


Signature Engine Update

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

Figure 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*



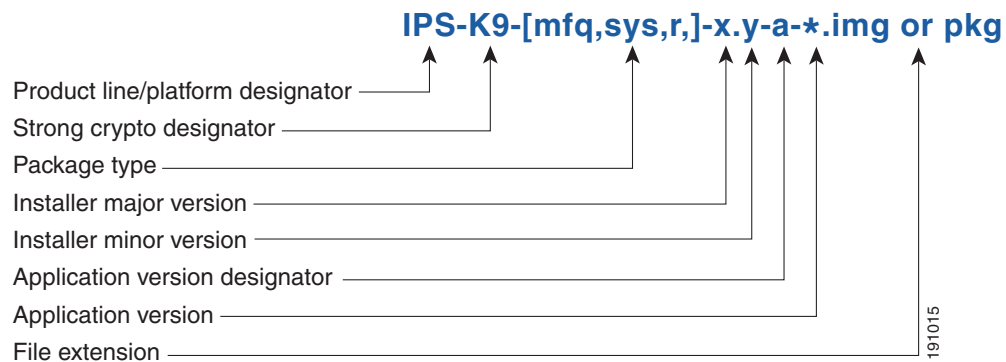
Recovery and System Image Files

Recovery and system image files contain separate versions for the installer and the underlying application. The installer version contains a major and minor version field. The major version is incremented by one of any major changes to the image installer, for example, switching from .tar to rpm or changing kernels. The minor version can be incremented by any one of the following:

- Minor change to the installer, for example, a user prompt added.
- Repackages require the installer minor version to be incremented by one if the image file must be repackaged to address a defect or problem with the installer.

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

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



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 Note IPS-AIM-K9-6.1-1-E3.pkg is the minor version update for the AIM IPS. IPS-NME-K-9-6.1-1-E3 .pkg is the minor version update for the NME IPS.
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-6.0-1pl-E1.pkg
Recovery package ⁷	Annually or as needed	r	1.1-6.0(1)	IPS-K9-r-1.1-a-6.0-1-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-E3.img
Maintenance partition image ²	Annually	mp	IDS M2	c6svc-mp.2-1-2.bin.gz

Table 2 Platform-Dependent Release Examples (continued)

Release	Target Frequency	Identifier	Supported Platform	Example Filename
Bootloader	As needed	bl	AIM IPS NME IPS	pse_aim_x.y.z.bin pse_nm_x.y.z.bin (where x, y, z is the release number)
Mini-kernel	As needed	mini-kernel	AIM IPS NME IPS	pse_mini_kernel_1.1.10.64.bz2

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

Table 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	IDSM2
IPS network module	AIM NME
AIP SSM	SSM_10 SSM_20 SSM_40

Upgrading to Cisco IPS 6.1(1) E3

This section provides information on upgrading to Cisco IPS 6.1(1) E3, and contains the following topics:

- [E3 Signature Engine Upgrade Notes and Caveats, page 16](#)
- [Upgrading to the E3 Signature Engine, page 16](#)
- [IPS 6.1\(1\)E3 Upgrade Notes and Caveats, page 17](#)
- [Upgrading to IPS 6.1\(1\)E3, page 18](#)

E3 Signature Engine Upgrade Notes and Caveats

The following upgrade notes and caveats apply to upgrading to 6.1(1)E3:

- Do not use the IPS-K9-6.1-1-E3.pkg, IPS-NME-K9-6.1-1-E3.pkg, or IPS-AIM-K9-6.1-1-E3.pkg to upgrade an existing 6.1(1)E1 or 6.1(1)E2 sensor to E3. You must use the E3 engine upgrade file IPS-engine-E3-req-6.1-1.pkg.
- Installing the E3 engine update only replaces the sensing software portion of the sensor. IPS inspection is halted and the sensor is placed in bypass mode according to your bypass mode configuration. If bypass mode is configured to auto or on, traffic is bypassed without inspection. If bypass mode is set to off, traffic is not passed during the update.
- The sensor configuration settings are maintained, but we strongly advise you to save a copy of the current configuration of your sensor to an FTP server before you install the E3 engine upgrade.
- Your sensor must show version 6.1(1)E2 for you to upgrade to E3. If you have an earlier version, you can install the minor version upgrade file, IPS-K9-6.1-1-E3.pkg or IPS-AIM-K9-6.1-1-E3.pkg, or IPS-NME-K9-6.1-1-E3.pkg.

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](#).

Upgrading to the E3 Signature Engine



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 with the E3 signature engine, follow these steps:

Step 1 Download the appropriate file (for example, IPS-engine-E3-req-6.1-1.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-engine-E3-req-6.1-1.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-engine-E3-req-6.1-1.pkg
```

Step 5 Enter the password when prompted.

Enter password: *****

Step 6 Enter **yes** to complete the upgrade.



Note Installing the E3 engine update does not require the sensor to reboot except for the AIM IPS. For the duration of the update and subsequent software initialization, IPS inspection is halted and data bypassed according to the bypass configuration of the sensor.



Note In some rare instances, the E3 engine upgrade causes the CLI to hang during the install, and attempts to log in to the sensor CLI fail. Rebooting the sensor restores functionality.

For More Information

For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privileges, see [Obtaining Software on Cisco.com, page 10](#).

IPS 6.1(1)E3 Upgrade Notes and Caveats

- If you are using automatic upgrade with the AIM IPS, NME IPS, and other IPS appliances or modules, make sure you put both the minor version upgrade file, IPS-K9-6.1-1-E3.pkg, the AIM IPS upgrade file, IPS-AIM-K9-6.1-1-E3.pkg, and the NME IPS upgrade file, IPS-NME-K9-6.1-1-E3.pkg, on the automatic update server so that the AIM IPS and NME IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the minor version upgrade file, IPS-K9-6.1-1-E2.pkg, on the automatic update server, the AIM IPS and NME IPS will download and try to install it, which is the incorrect file for the AIM IPS and NME IPS.
- To install the IPS-K9-6.1-1-E3.pkg, IPS-AIM-K9-6.1-1-E3.pkg, or IPS-NME-K9-6.1-1-E3.pkg minor upgrade file, you must be running IPS version 5.0(1) or later on your sensor. Use IPS-AIM-K9-6.1-1-E2.pkg to upgrade the AIM IPS only. Use IPS-NME-K9-6.1-1-E3.pkg to upgrade the NME IPS only. Use IPS-K9-6.1-1-E2.pkg for all other supported sensors.
- When you upgrade the AIM IPS and NME IPS using manual upgrade, you must disable heartbeat reset on the router before installing the upgrade. You can reenale heartbeat reset after you complete the upgrade. If you do not disable heartbeat reset, the upgrade can fail and leave the AIM IPS and NME IPS in an unknown state, which can require a system reimage to recover.

For More Information

- For the procedures for reimaging all sensors, refer to [Installing System Images](#).
- 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 the procedure for disabling heartbeat reset, for the AIMIPS refer to [Enabling and Disabling Heartbeat Reset](#), and for the NME IPS refer to [Enabling and Disabling Heartbeat Reset](#).

Upgrading to IPS 6.1(1)E3


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 to IPS 6.1(1)E3, follow these steps:

Step 1 Download the appropriate file (for example, IPS-K9-6.1-1-E3.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-E3.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-E3.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 information on obtaining a service contract, see [Service Programs for IPS Products, page 21](#).
- For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privileges, see [Obtaining Software on Cisco.com, page 10](#).

After Upgrading to Cisco IPS6.1(1)E3

This section provides information about what to do after you install Cisco IPS 6.1(1) E3. It contains the following topics:

- [Comparing Configurations, page 19](#)
- [Importing a New SSL Certificate, page 19](#)
- [Logging In to IDM, page 19](#)
- [Licensing the Sensor, page 20](#)

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)E3 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)E3 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) E3 caveats, see [Caveats, page 34](#).

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. A Security Alert dialog box appears.

```
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`).

- 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, and then 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, and then the IDM on *ip_address* dialog box appears.
- Step 5** To create a shortcut for IDM, click **Yes**. The Cisco IDM Launcher dialog box appears.



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.

- Step 6** To authenticate IDM, enter your username and password, and click **OK**. 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 Both the default username and password are **cisco**. You were prompted to change the password during sensor initialization.



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 21](#)
- [Service Programs for IPS Products, page 21](#)
- [Obtaining and Installing the License Key, page 22](#)

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
- IDSM2

When you purchase an ASA 5500 series adaptive security appliance product that does not contain IPS, you must purchase a SMARTnet contract.



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

When you purchase an ASA 5500 series adaptive security appliance product that ships with the AIP SSM installed, or if you purchase it to add to your ASA 5500 series adaptive security appliance product, you must purchase the Cisco Services for IPS service contract.



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 22](#)
- [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.

Installing the License Key

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)E3

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-E3 15:36:05 UTC Thu Apr 24 2008

Recovery Partition Version 1.1 - 6.1(1)E3

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) E3 software and the products that run 6.1(1) E3:

- You must reboot the AIM IPS and NME IPS when you apply the E3 engine update and it takes a very long time to install because of the limited CPU in these modules. Update times as long as 40 minutes have been recorded. During the update time, the module is in bypass mode, passing traffic without inspection.
- The AIM IPS and NME IPS do not support virtualization.
- When you reload the router, the AIM IPS and NME IPS also reload. To ensure that there is no loss of data on the module, 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, the AIM IPS, or NME IPS at the same time.
- When the AIM IPS and NME IPS are used with an IOS firewall, make sure SYN flood prevention is done by the IOS firewall.

The AIM IPS, and NME IPS, and the IOS firewall complement abilities of each other to create security zones in the network and inspect traffic in those zones. Because the modules 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. The 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 the 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 in to 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 IDSM2s 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](#).

Recovering the Password

For most IPS platforms, you can now recover the password on the sensor rather than using the service account or reimaging the sensor. This section describes how to recover the password for the various IPS platforms. It contains the following topics:

- [Understanding Password Recovery](#), page 28
- [Recovering the Appliance Password](#), page 28
- [Recovering the IDSM2 Password](#), page 30
- [Recovering the AIP SSM Password](#), page 30
- [Recovering the AIM IPS Password](#), page 31
- [Recovering the NME IPS Password](#), page 32
- [Disabling Password Recovery](#), page 32
- [Verifying the State of Password Recovery](#), page 33
- [Troubleshooting Password Recovery](#), page 34

Understanding Password Recovery

Password recovery implementations vary according to IPS platform requirements. Password recovery is implemented only for the cisco administrative account and is enabled by default. The IPS administrator can then recover user passwords for other accounts using the CLI. The cisco user password reverts to **cisco** and must be changed after the next login.


Note

Administrators may need to disable the password recovery feature for security reasons.

Table 4 lists the password recovery methods according to platform.

Table 4 Password Recovery Methods According to Platform

Platform	Description	Recovery Method
4200 series sensors	Stand-alone IPS appliances	GRUB prompt or ROMMON
AIP SSM	ASA 5500 series adaptive security appliance modules	ASA CLI command
IDSM2	Switch IPS module	Password recovery image file
AIM IPS	Router IPS modules	Bootloader command

For More Information

For more information on when and how to disable password recovery, see [Disabling Password Recovery, page 32](#).

Recovering the Appliance Password

This section describes the two ways to recover the password for appliances. It contains the following topics:

- [Using the GRUB Menu, page 28](#)
- [Using ROMMON, page 29](#)

Using the GRUB Menu

For 4200 series appliances, the password recovery is found in the GRUB menu, which appears during bootup. When the GRUB menu appears, press any key to pause the boot process.


Note

You must have a terminal server or direct serial connection to the appliance to use the GRUB menu to recover the password.

To recover the password on appliances, follow these steps:

Step 1 Reboot the appliance.

The following menu appears:

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
-----
```

```

0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
-----

```

Use the ^ and v keys to select which entry is highlighted.
 Press enter to boot the selected OS, 'e' to edit the
 Commands before booting, or 'c' for a command-line.

Highlighted entry is 0:

Step 2 Press any key to pause the boot process.

Step 3 Choose **2: Cisco IPS Clear Password (cisco)**.

The password is reset to **cisco**. You can change the password the next time you log in to the CLI.

For More Information

For more information on connecting an appliance to a terminal server, refer to [Connecting an Appliance to a Terminal Server](#).

Using ROMMON

For the IPS 4240 and IPS 4255 you can use the ROMMON to recover the password. To access the ROMMON CLI, reboot the sensor from a terminal server or direct connection and interrupt the boot process.

To recover the password using the ROMMON CLI, follow these steps:

Step 1 Reboot the appliance.

Step 2 To interrupt the boot process, press **ESC** or **Control-R** (terminal server) or send a **BREAK** command (direct connection).

The boot code either pauses for 10 seconds or displays something similar to one of the following:

- Evaluating boot options
- Use BREAK or ESC to interrupt boot

Step 3 Enter the following commands to reset the password:

```

confreg 0x7
boot

```

Sample ROMMON session:

```

Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155

```

```
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

Recovering the IDSM2 Password

To recover the password for the IDSM2, you must install a special password recovery image file. This installation only resets the password, all other configuration remains intact. The password recovery image is version-dependent and can be found on the Cisco Download Software site. For IPS 6.x, download WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz. For IPS 7.x, download WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz.

FTP is the only supported protocol for image installations, so make sure you put the password recovery image file on an FTP server that is accessible to the switch. You must have administrative access to the Cisco 6500 series switch to recover the password on the IDSM2.

During the password recovery image installation, the following message appears:

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

This message is in error. Installing the password recovery image does not remove any configuration, it only resets the login account.

Once you have downloaded the password recovery image file, follow the instructions to install the system image file but substitute the password recovery image file for the system image file. The IDSM2 should reboot in to the primary partition after installing the recovery image file. If it does not, enter the following command from the switch:

```
hw-module module module_number reset hdd:1
```



Note

The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

For More Information

- For the procedure for installing system images on the IDSM2, refer to [Installing the IDSM2 System Image](#).
- For more information on downloading Cisco IPS software, see [Obtaining Software on Cisco.com, page 10](#).

Recovering the AIP SSM Password



Note

To recover the password on the AIP SSM, you must have ASA 7.2.3.

Use the **hw-module module slot_number password-reset** command to reset the AIP SSM password to the default **cisco**. The ASA 5500 series adaptive security appliance sets the ROMMON confreg bits to 0x7 and then reboots the sensor. The ROMMON bits cause the GRUB menu to default to option 2 (**reset password**).

If the module in the specified slot has an IPS version that does not support password recovery, the following error message is displayed:

```
ERROR: the module in slot <n> does not support password recovery.
```

Recovering the AIM IPS Password

To recover the password for the AIM IPS, use the **clear password** command. You must have console access to the AIM IPS and administrative access to the router.

To recover the password for the AIM IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

Step 4 Session in to the AIM IPS.

```
router# service-module ids-sensor slot/port session
```

Example

```
router# service-module ids-sensor 0/0 session
```

Step 5 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 6 Reset the AIM IPS from the router console.

```
router# service-module ids-sensor 0/0 reset
```

Step 7 Press **Enter** to return to the router console.

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

```
ServicesEngine boot-loader# clear password
```

The AIM IPS reboots. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Recovering the NME IPS Password

To recover the password for the NME IPS, use the **clear password** command. You must have console access to the NME IPS and administrative access to the router.

To recover the password for the NME IPS, follow these steps:

Step 1 Log in to the router.

Step 2 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 3 Confirm the module slot number in your router.

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

Step 4 Session in to the NME IPS.

```
router# service-module ids-sensor slot/port session
```

Example

```
router# service-module ids-sensor 1/0 session
```

Step 5 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 6 Reset NME-IPS from the router console.

```
router# service-module ids-sensor 1/0 reset
```

Step 7 Press **Enter** to return to the router console.

Step 8 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 9 Clear the password.

```
ServicesEngine boot-loader# clear password
```

The NME IPS reboots. The password is reset to **cisco**. Log in to the CLI with username **cisco** and password **cisco**. You can then change the password.

Disabling Password Recovery



Caution

If you try to recover the password on a sensor on which password recovery is disabled, the process proceeds with no errors or warnings; however, the password is not reset. If you cannot log in to the sensor because you have forgotten the password, and password recovery is set to disabled, you must reimagine your sensor.

Password recovery is enabled by default. You can disable password recovery through the CLI or IDM. To disable password recovery in the CLI, follow these steps:

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

Step 2 Enter global configuration mode.

```
sensor# configure terminal
```

Step 3 Enter host mode.

```
sensor(config)# service host
```

Step 4 Disable password recovery.

```
sensor(config-hos)# password-recovery disallowed
```

To disable password recovery in IDM, follow these steps:

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

Step 2 Choose **Configuration > Sensor Setup > Network**. The Network pane appears.

Step 3 To disable password recovery, uncheck the **Allow Password Recovery** check box.

For More Information

- If you are not certain about whether password recovery is enabled or disabled, see [Verifying the State of Password Recovery, page 33](#).
- For more information on reimaging sensors, refer to [Upgrading, Downgrading, and Installing System Images](#).

Verifying the State of Password Recovery

Use the **show settings | include password** command to verify whether password recovery is enabled.

To verify whether password recovery is enabled, follow these steps:

Step 1 Log in to the CLI.

Step 2 Enter service host submode.

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

Step 3 Verify the state of password recovery by using the **include** keyword to show settings in a filtered output.

```
sensor(config-hos)# show settings | include password
password-recovery: allowed <defaulted>
sensor(config-hos)#
```

Troubleshooting Password Recovery

To troubleshoot password recovery, pay attention to the following:

- You cannot determine whether password recovery has been disabled in the sensor configuration from the ROMMON prompt, GRUB menu, switch CLI, or router CLI. If password recovery is attempted, it always appears to succeed. If it has been disabled, the password is not reset to **cisco**. The only option is to reimage the sensor.
- You can disable password recovery in the host configuration. For the platforms that use external mechanisms, such as the AIM IPS and NME IPS bootloader, ROMMON, and the maintenance partition for IDSM2, although you can run commands to clear the password, if password recovery is disabled in the IPS, the IPS detects that password recovery is not allowed and rejects the external request.

To check the state of password recovery, use the **show settings | include password** command.

- When performing password recovery on IDSM2, you see the following message: `Upgrading will wipe out the contents on the storage media.` You can ignore this message. Only the password is reset when you use the specified password recovery image.

For More Information

- For more information on reimaging sensors, refer to [Upgrading, Downgrading, and Installing System Images](#).
- For the procedure for disabling password recovery, see [Disabling Password Recovery, page 32](#).
- For the procedure for verifying the state of password recovery, see [Verifying the State of Password Recovery, page 33](#).

Caveats

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

- [Bug Toolkit, page 34](#)
- [Resolved E3 Engine Caveats, page 35](#)
- [Resolved 6.1\(1\) Caveats, page 36](#)
- [IPS 6.1\(1\)E3 Caveats, page 36](#)

Bug Toolkit

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.

To access the Bug Toolkit, use this URL:

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

Resolved E3 Engine Caveats

The following issues have been resolved as a part of incorporating the E3 Engine update:

- CSCsq94367—Multistring appears to be deleted twice
- 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
- CSCsd19619—NO statistics on traffic under heavy load
- CSCsr81621—SensorApp core for 1315_0_ipv6.pcap in Proc6TcpTcb16dumpCurrentStateEv
- CSCsr74304 —Virtual Sensor Stats Have No Service Granularity
- CSCsr84513—Fix aggressive mode transition logic
- CSCsr01778—Database shadow nodes contribute to decreased performance
- CSCso21050—Frequent error generation - SigEventList not empty
- CSCso76619—Bad frag/backlog handling causes excess dgram holding & missed 1st frags
- CSCsr49100—Signature 1102 false positive with E2 engine
- 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
- CSCso45473—Analysis Engine terminated prematurely
- CSCsr78743—InspectorAtomicL3L4 needs proper handling of IpHeaderLength param
- CSCsu42884—Repair HashTree::remove runtime fault
- CSCsu79570—Adjust default tcp-max-queue and BacklogQueue defaults
- CSCsu58580—Fixed-udp signatures perform double inspection
- CSCsu77935—4270 adds latency when under low load
- 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

- CSCsr48923—Sig Update or Tuning causes abort in AtomicL3L4 Inspector ParmData logic
- CSCsv10964—Inline asymmetric mode not denying tcp resends

Resolved 6.1(1) Caveats

The following issues have been resolved in this 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
- CSCsk30811—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

IPS 6.1(1)E3 Caveats

The following issues are found in the Cisco IPS 6.1(1)E3 release:

- CSCsq68594—AIM: 'Regex parse failure' message displayed in main.log
- 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
- CSCso20750—modify-packet-inline computing incorrect checksum
- CSCso15103—4260 w/ 4x1Gb NIC may enter HW bypass on engine update
- CSCso02370—CPU and Load periodically revert to 0
- 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
- CSCsq94450—Incorrect error message when upgrading 6.1(1)E1 using 6.1(1)E2 SP
- CSCsq94419—False Positive on 11022

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 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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

Copyright © 2008-2011 Cisco Systems, Inc. All rights reserved.