



Release Notes for Cisco Intrusion Prevention System 6.0(4)E2

Published: June 19, 2008

Revised: August 16, 2011, OL-20146-01

Contents

- [IPS 6.0\(4\)E2 File List, page 2](#)
- [Supported Platforms, page 2](#)
- [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 5](#)
- [Before Upgrading to Cisco IPS 6.0\(4\)E2, page 6](#)
- [Upgrading to Cisco IPS 6.0\(4\)E2, page 15](#)
- [After Upgrading to Cisco IPS 6.0\(4\)E2, page 16](#)
- [Restrictions and Limitations, page 23](#)
- [Recovering the Password, page 24](#)
- [Caveats, page 31](#)
- [Related Documentation, page 34](#)
- [Obtaining Documentation and Submitting a Service Request, page 35](#)



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

© 2006-2011 Cisco Systems, Inc. All rights reserved.

**Caution**

The BIOS on Cisco IDS/IPS sensors is specific to Cisco IDS/IPS sensors and must only be upgraded under instructions from Cisco with BIOS files obtained from the Cisco website. Installing a non-Cisco or third-party BIOS on Cisco IDS/IPS sensors voids the warranty. For more information on how to obtain instructions and BIOS files from the Cisco website, see [Obtaining Software on Cisco.com, page 9](#).

IPS 6.0(4)E2 File List

The following files are part of Cisco IPS 6.0(4)E2:

- IPS 6.0-4-E2 Engine Update Files
 - IPS-engine-E2-req-6.0-4.pkg
 - IPS-CS-MGR-engine-E2-req-6.0-4.zip
- Readme Files
 - IPS-engine-E2.readme.txt

For More Information

- For the procedure for obtaining these files on Cisco.com, see [Obtaining Software on Cisco.com, page 9](#).
- For the procedure for installing signature engine upgrade files, see [Upgrading to Cisco IPS 6.0\(4\)E2, page 15](#).

Supported Platforms

**Note**

The number of concurrent CLI sessions is limited based on the platform. The IDS 4215 and NM CIDS are limited to three concurrent CLI sessions. All other platforms allow ten concurrent sessions.

Cisco IPS 6.0(4)E2 is supported on the following platforms:

- IDS 4215 Series Sensor Appliances
- IDS 4235 Series Sensor Appliances
- IPS 4240 Series Sensor Appliances
- IDS 4250 Series Sensor Appliances
- IPS 4255 Series Sensor Appliances
- IPS 4260 Series Sensor Appliances
- IPS 4270-20 Series Sensor Appliances
- WS-SVC-IDSM2 series Intrusion Detection System Module (IDSM2)
- Intrusion Detection System Network Module (NM CIDS)
- 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:

- CMS - Apache Server (Tomcat)
- CMS - Apache Server (JRun)



Note

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

ROMMON and TFTP

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

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, refer to [Configuring Automatic Upgrades](#).

IPS Management and Event Viewers

Use the following tools for configuring IPS 6.0(4)E2 and E2 sensors:

- IDM 6.0
- IPS CLI 6.0
- ASDM 5.2
- CSM 3.1

Use the following tools for monitoring 6.0(4)E2 sensors:

- MARS 4.2 and 4.3(1)
- IEV 5.2
- CSM 4.0

**Note**

Viewers that are already configured to monitor the 5.x sensors may need to be configured to accept a new SSL certificate for the 6.0(4)E2 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 6.0(4)E2 includes the following new features:

- The S339 signature update is built in to the E2 engine update. You cannot download S399 separately.
- The E2 engine update contains the following new and changed engines:
 - P2P engine—The existing Peer-to-Peer signatures have been organized in to a dedicated, optimized engine that lets the sensor monitor all 65, 536 ports in both the TPC and UDP protocols for peer-to-peer traffic. The P2P engine is enabled by default and because of the implementation style of this engine, you cannot create custom P2P signatures.
 - Fixed Depth All Ports Inspection engine—A series of new engines similar to the String TCP engine has been developed to provide a more optimized approach to monitoring all ports. The fixed inspection engines—Fixed TPC, Fixed UDP, and Fixed ICMP—provide monitoring for all ports (TCP and UDP) by default. They inspect traffic in a stream mode per AaBb tuple to a maximum of 250 bytes in both directions, that is, 250 bytes to service and 250 bytes from service. The service ports option describes the ports for which you do not want to generate alerts. Inspection still occurs, but alerts are suppressed for these ports defined per signature.
 - Service Generic engine—This engine has been enhanced to support TCP stream processing, which lets the Cisco signature team provide increased, higher fidelity support for protocol analysis signatures when a dedicated engine does not already exist.
 - Meta engine—The Meta engine now uses an OR operator and nesting, which allows complex AND/OR combination to be used in the Meta signature logic.

For More Information

For more information on the new signature engines, refer to [Signature Engines](#).

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 information on MySDN (formerly known as NSDB) in IDM, refer to [Configuring Signatures](#).

Before Upgrading to Cisco IPS 6.0(4)E2

This section describes the actions you should take before upgrading to Cisco IPS 6.0(4)E2. It contains the following topics:

- [Perform These Tasks, page 6](#)
- [Backing Up and Restoring the Configuration File Using a Remote Server, page 6](#)
- [Obtaining Software on Cisco.com, page 9](#)
- [IPS Software Versioning, page 10](#)
- [Software Release Examples, page 13](#)

Perform These Tasks

Before you upgrade your sensors to Cisco IPS 6.0(4)E2, make sure you perform the following tasks:

- To apply the E2 engine update, you must have version 6.0(4)E1 installed on your sensor.
- 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 Cisco service contracts, see [Service Programs for IPS Products, page 19](#).
- For the procedure for creating a backup copy of your configuration, see [Backing Up and Restoring the Configuration File Using a Remote Server, page 6](#).
- For the procedure for displaying version information, refer to [Displaying Version Information](#).
- 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 CLI procedure for adding TLS trusted hosts, refer to [Adding TLS Trusted Hosts](#). For the IDM procedure, refer to [Adding Trusted Hosts](#).
- For the CLI procedure for adding remote hosts to the SSH known hosts list, refer to [Adding Hosts to the SSH Known Hosts List](#). For the IDM procedure, refer to [Defining Known Host Keys](#).

Obtaining Software on Cisco.com

You can find major and minor updates, service packs, signature and signature engine updates, system and recovery files, firmware upgrades, and readmes on the Download Software site on Cisco.com.



Note You must be logged in to Cisco.com to download software.

Signature updates are posted to Cisco.com approximately every week, more often if needed. Service packs are posted to Cisco.com as needed. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.



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

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

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



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

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

- Fill out the form and click **Submit**. The Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy appears.
- Read the policy and click **I Accept**. The Encryption Software Export/Distribution Form appears.

If you previously filled out the Encryption Software Export Distribution Authorization form, and read and accepted the Cisco Systems Inc. Encryption Software Usage Handling and Distribution Policy, these forms are not displayed again. The File Download dialog box appears.

- Step 11** Open the file or save it to your computer.

Step 12 Follow the instructions in the Readme to install the update.



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

For More Information

- For the procedure for obtaining and installing the license, see [Licensing the Sensor, page 18](#).
- For an explanation of the IPS file versioning scheme, see [IPS Software Versioning, page 10](#).

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 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 Packs

Service packs are 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.

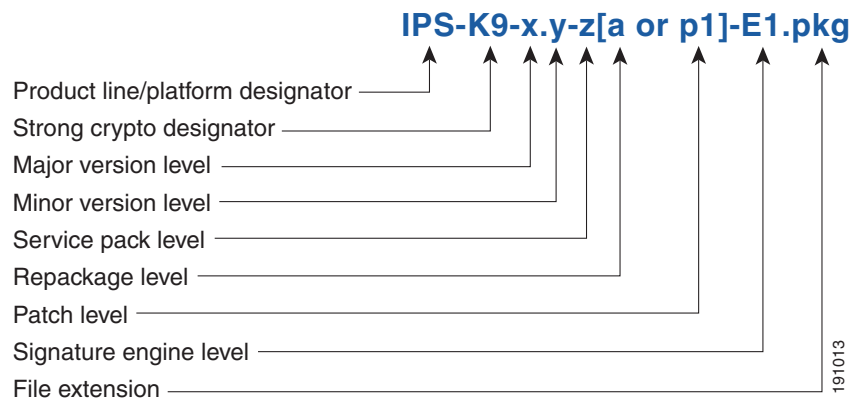
Before you can install a patch release, the most recent major or minor update, or service pack must be installed. For example, patch release 5.0(1p1) requires 5.0(1).



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*

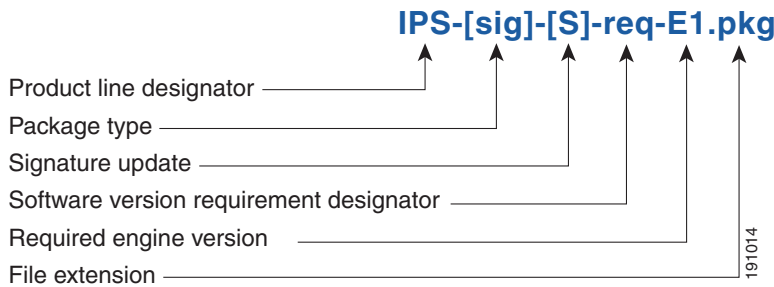


Signature Update

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/virus updates.

Figure 2 *IPS Software File Name for Signature Updates*

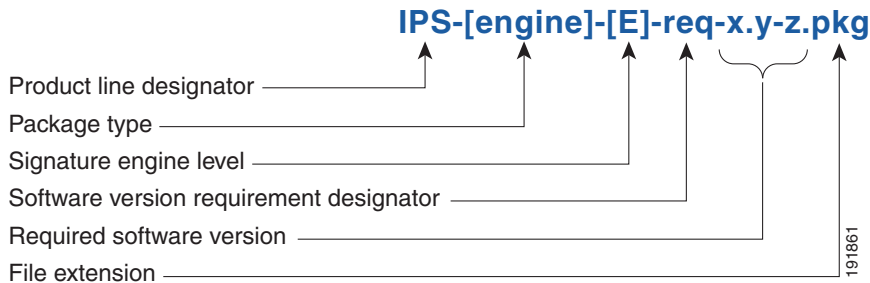


Signature Engine Update

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*



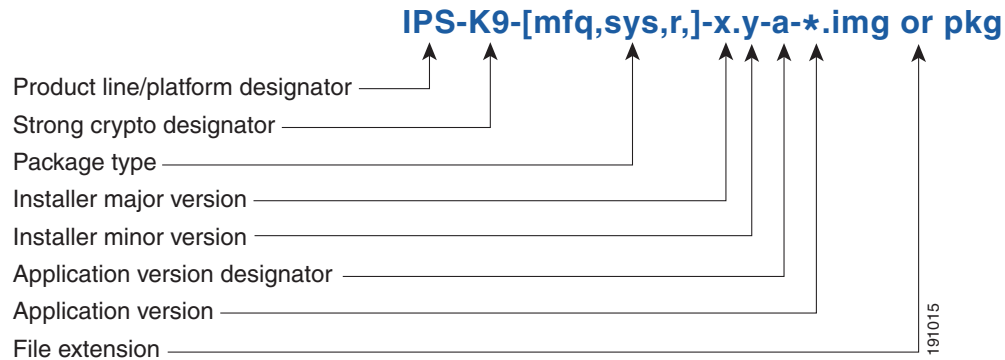
Recovery and System Image Filenames

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 filenames.

Figure 4 IPS Software File Name for Recovery and System Image Filenames



Software Release Examples

Table 1 lists platform-independent IDS 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-6.0-1-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-6.0-1-E1.img |
| Maintenance partition image ² | Annually | mp | IDSM2 | c6svc-mp.2-1-2.bin.gz |
| Bootloader | As needed | bl | NM CIDS AIM IPS | servicesengine-boot-1.0-4.bin 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 |

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.



Note

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

Table 3 Platform Identifiers

| Sensor Family | Identifier |
|----------------------------|----------------------------|
| IDS 4215 series | 4215 |
| IPS 4240 series | 4240 |
| IPS 4255 series | 4255 |
| IPS 4260 series | 4260 |
| IPS 4270-20 series | 4270_20 |
| IDS module for Catalyst 6K | IDSM2 |
| IDS network module | NM_CIDS |
| IPS network module | AIM |
| AIP SSM | SSM_10 SSM_20 SSM_40 |

For More Information

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

Upgrading to Cisco IPS 6.0(4)E2


Caution

You must have a valid Cisco Service for IPS Maintenance contract per sensor to receive and use software upgrades from Cisco.com.

To upgrade the sensor, follow these steps:

Step 1

Download the signature engine update file (IPS-engine-E2-req-6.0-4.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.


Caution

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


Caution

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

Step 2

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

Step 3

Determine the sensor version:

```
sensor# show version
```

Step 4

Enter configuration mode:

```
sensor# configure terminal
```

Step 5

Upgrade the sensor with the signature engine update:

```
sensor(config)# upgrade scp://tester@10.1.1.1//upgrade/IPS-engine-E2-req-6.0-4.pkg
```

Step 6

Enter the password when prompted:

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

Step 7

Enter **yes** to complete the upgrade.


Note

The sensor reboots after installing the signature engine.

Step 8

Verify your new sensor version:

```
sensor# show version
```

```
Application Partition:
```

```
Cisco Intrusion Prevention System, Version 6.0(4)E2
```

```
Host:
```

```
  Realm Keys          key1.0
```

```
Signature Definition:
```

```
  Signature Update    S291.0          2007-06-18
```

```
  Virus Update        V1.2           2005-11-24
```

```
OS Version:
```

```
2.4.30-IDS-smp-bigphys
```

```
Platform:
```

```
ASA-SSM-20
```

```
Serial Number:
```

```
P300000220
```

```
No license present
```

```
Sensor up-time is 13 days.
Using 1039052800 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 49.9M out of 166.6M bytes of available disk space (32% 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-K9-6.0-4-E.2 15:31:13 UTC Mon Sep 10 2007
```

Recovery Partition Version 1.1 - 6.0(4)E2

sensor#

For More Information

- For more information on Cisco service contracts, see [Service Programs for IPS Products, page 19](#).
- 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 6.0(4)E2

This section provides information about what to do after you install IPS 6.0(4)E2. It contains the following topics:

- [Comparing Configurations, page 16](#)
- [SSL Certificate, page 17](#)
- [Logging In to IDM, page 17](#)
- [Licensing the Sensor, page 18](#)

Comparing Configurations

Compare your backed up and saved 6.0(4)E1 configuration with the output of the **show configuration** command after upgrading to 6.0(4)E2 to verify that all the configuration has been properly converted.



Caution

If the configuration is not properly converted, check the list of caveats, 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 list of IPS 6.0(4)E2 caveats, see [Caveats, page 31](#).

SSL Certificate

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

For More Information

For the CLI procedure for importing a new SSL certificate, refer to [Configuring TLS](#). For the IDM procedure, refer to [Configuring Certificates](#).

Logging In to IDM

IDM is a web-based, Java 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 address is `https://10.1.9.201`, 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 6.0 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. The 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 6.0 window. After you launch IDM, is it not necessary for this window to remain open.

For More Information

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

Licensing the Sensor

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

- [Understanding the License, page 18](#)
- [Service Programs for IPS Products, page 19](#)
- [Obtaining and Installing the License Key, page 20](#)

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, choose **Configuration > 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 on the Licensing pane in IDM. Whenever you start IDM, 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 but you cannot download signature updates.

When you enter the CLI, you are informed of your license status. For example, you receive the following message if there is no license installed:

```
***LICENSE NOTICE***
There is no license key installed on the system.
The system will continue to operate with the currently installed
signature set. A valid license must be obtained in order to apply
signature updates. Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
```

You will continue to see this message until you install a license key.

For More Information

- For more information on Cisco service contracts, see [Service Programs for IPS Products, page 19](#).
- For the procedure for obtaining and installing the license key, see [Obtaining and Installing the License Key, page 20](#).

Service Programs for IPS Products

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

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

- IDS 4215
- IDS 4235
- IDS 4250
- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- IDSM2
- NM CIDS
- AIM IPS

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 on-site hardware replacement next business day.

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 send your product for RMA, the serial number will change. You must then get a new license key for the new serial number.

For More Information

For the procedure for obtaining and installing the license key, see [Obtaining and Installing the License Key, page 20](#).

Obtaining and Installing the License Key

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

- [Using IDM, page 20](#)
- [Using the CLI, page 21](#)

Using IDM

**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 using an account with administrator privileges.
- Step 2** Choose **Configuration > Licensing**. The Licensing pane displays the status of the current license. If you have already installed your license, you can click **Download** to save it if needed.
- Step 3** Obtain a license key by doing one of the following:
 - Check the **Cisco Connection Online** check box to obtain the license from Cisco.com. IDM contacts the license server on Cisco.com and sends the server the serial number to obtain the license key. This is the default method. Go to Step 4.
 - Check the **License File** check box to use a license file. To use this option, you must apply for a license key at this URL: www.cisco.com/go/license. The license key is sent to you in e-mail and you save it to a drive that IDM can access. This option is useful if your computer cannot access Cisco.com. Go to Step 7.
- Step 4** Click **Update License**. The Licensing dialog box appears.

- Step 5** Click **Yes** to continue. The Status dialog box informs you that the sensor is trying to connect to Cisco.com. An Information dialog box confirms that the license key has been updated.
- Step 6** Click **OK**.
- Step 7** Go to www.cisco.com/go/license.
- Step 8** Fill in the required fields. Your license key will be sent to the e-mail address you specified.



Caution You must have the correct IPS device serial number because the license key only functions on the device with that number.

- Step 9** Save the license key to a hard-disk drive or a network drive that the client running IDM can access.
- Step 10** Log in to IDM.
- Step 11** Choose **Configuration > Licensing**.
- Step 12** Under Update License, check the **Update From: License File** check box.
- Step 13** In the Local File Path field, specify the path to the license file or click **Browse Local** to browse to the file. The Select License File Path dialog box appears.
- Step 14** Browse to the license file and click **Open**.
- Step 15** Click **Update License**.

For More Information

For more information on Cisco service contracts, see [Service Programs for IPS Products, page 19](#).

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 must to the SSH known hosts list.

- http:—Source URL for the web server. The syntax for this prefix is:
http:[[/[username@]location]/directory]/filename
- https:—Source URL for the web server. The syntax for this prefix is:
https:[[/[username@]location]/directory]/filename



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

To install the license key, follow these steps:

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



Note 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 6.0(4)E2

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S317.0   2008-02-13
  Virus Update        V1.2     2005-11-24
OS Version:          2.4.30-IDS-smp-bigphys
Platform:            IPS-4255-K9
Serial Number:       ABC1234DEFG
Licensed, expires:   30-Dec-2008 UTC
Sensor up-time is 45 min.
Using 1885913088 out of 3974135808 bytes of available memory (47% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
```

```
application-data is using 43.5M out of 166.8M bytes of available disk space (28% usage)
boot is using 38.5M out of 68.6M bytes of available disk space (59% usage)
```

```
MainApp          N-2008_FEB_15_16_16  (Release)  2008-02-15T17:08:23-0600  Running
AnalysisEngine  N-2008_FEB_15_16_16  (Release)  2008-02-15T17:08:23-0600  Running
CLI             N-2008_FEB_15_16_16  (Release)  2008-02-15T17:08:23-0600
```

```
Upgrade History:
```

```
IPS-K9-6.0-4-E2 17:45:18 UTC Tue May 06 2008
```

```
Recovery Partition Version 1.1 - 6.0(4)E2
```

```
sensor#
```

Step 7 Copy your license key from a sensor to a server to keep a backup copy of the license:

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

For More Information

- For the CLI procedure for adding hosts to the known hosts list, refer to [Adding Hosts to the SSH Known Hosts List](#). For the IDM procedure, refer to [Defining Known Host Keys](#).
- For the CLI procedure for adding TLS trusted hosts, refer to [Adding TLS Trusted Hosts](#). For the IDM procedure, refer to [Adding Trusted Hosts](#).
- For more information on Cisco service contracts, see [Service Programs for IPS Products, page 19](#).

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IPS 6.0(4)E2 software and the products that run 6.0(4)E2:

- Do not confuse Cisco IOS IDS or Cisco IPS (a software-based intrusion-detection/prevention application that runs in the Cisco IOS) with the IPS that runs on the NM CIDS. The NM CIDS runs Cisco IPS 6.0(4)E2. Because performance can be reduced and duplicate alarms can be generated, we recommend that you do not run Cisco IOS IDS and Cisco IPS 6.0(4)E2 simultaneously.
- Only one NM CIDS is supported per Cisco 2600, 2811, 2821 2851, 3825, 3845, and 3700 series router.
- Jumbo frames are not supported on the NM CIDS.
- The NM CIDS does not run in inline mode.
- The AIM IPS, IDS 4215, and NM CIDS do not support virtualization.
- When you reload the router, the AIM IPS also reloads. To ensure that there is no loss of data on the 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 the AIM IPS at the same time.
- When the AIM IPS is used with an IOS firewall, make sure SYN flood prevention is done by the IOS firewall.

The AIM IPS and the IOS firewall complement each other's abilities to create security zones in the network and inspect traffic in those zones. Because the AIM IPS and the IOS firewall operate independently, sometimes they are unaware of the other's activities. 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. If you are using the IDS 4125, which does not support virtualization, configure vs0 to track TCP sessions by VLAN and interface.
- 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.
- The HTML-based IDM has been replaced with a Java applet.
- 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.

For More Information

For more information about which modules Cisco routers support, 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 25](#)
- [Recovering the Appliance Password, page 25](#)
- [Recovering the IDSM2 Password, page 27](#)
- [Recovering the NM CIDS Password, page 28](#)
- [Recovering the AIP SSM Password, page 28](#)
- [Recovering the AIM IPS Password, page 29](#)
- [Disabling Password Recovery, page 29](#)

- [Verifying the State of Password Recovery, page 30](#)
- [Troubleshooting Password Recovery, page 31](#)

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 |
| NM CIDS 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 29](#).

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 25](#)
- [Using ROMMON, page 26](#)

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 about setting up 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 9](#).

Recovering the NM CIDS Password

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


Note

There is no minimum IOS release requirement for password recovery on the NM CIDS.


Note

Recovering the password for the NM CIDS requires a new bootloader image.

To recover the password for the NM CIDS, follow these steps:

Step 1 Session in to the NM CIDS:

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

Step 2 Press **Control-shift-6** followed by **x** to navigate to the router CLI.

Step 3 Reset NM-CIDS from the router console:

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

Step 4 Press **Enter** to return to the router console.

Step 5 When prompted for boot options, enter ******* quickly. You are now in the bootloader.

Step 6 Clear the password:

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

Step 7 Restart the NM CIDS:

```
ServicesEngine boot-loader# boot disk
```


Caution

Do not use the **reboot** command to start the NM CIDS. This causes the password recovery action to be ignored. Make sure you use the **boot disk** command.

For More Information

For the procedure for installing a new bootloader image, refer to [Upgrading the NM CIDS Bootloader](#).

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.

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 30](#).
- For the procedures for 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 NM CIDS bootloader, ROMMON, and the maintenance partition for the 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 for the NM CIDS, do not use the **reboot** command to restart the NM CIDS. This causes the recovery action to be ignored. Use the **boot disk** command.
- When performing password recovery on the 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 information on reimaging the sensor, refer to [Upgrading, Downgrading, and Installing System Images](#).
- For more information on when and how to disable password recovery, see [Disabling Password Recovery, page 29](#).
- For the procedure to verify the state of password recovery, see [Verifying the State of Password Recovery, page 30](#).

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

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

- [Resolved Caveats, page 31](#)
- [Known Caveats, page 33](#)

Resolved Caveats

The following known issues have been resolved in Cisco IPS 6.0(4)E2:

- CSCsi23979—4250-x1 locks up with 1 gig 256 byte ixia traffic
- CSCsl76809—Calendar allows schedule in to current slice causing infinite loop
- CSCsj17459—low-end sensor out of memory during sigupdate
- CSCsi87943—traffic conditions can stimulate small memory leak in inspector SNMP
- CSCsj30225—SNMP gets result in mainApp memory leak

- CSCsl04892—sensorApp failure after show stat vi clear
- CSCsl06936—inline-vlan-pair delays passing traffic after reboot
- CSCsl30784—inline-vlan-pair and bypass off down/notconnect after sig update
- CSCsl44621—Analysis Engine aborts when AD files are copied via destination url
- CSCsj70541—Inline int pair not working after reboot when vlan group assigned
- CSCsk43437—upgrade results in /tmp partition full
- CSCsl22365—MAC Address incorrect on SSM backplane
- CSCsm39409—System locks up under heavy traffic stress (Inline mode)
- CSCsj53782—Entire sensor hangs while toggling bypass mode
- CSCsj69905—AxBx insertion rate limiting may corrupt database
- CSCsi17548—Tcp Syn Cookies do not appear to work +
- CSCsh31034—SensorApp may abort when file copy attempt failed (libhoard + fork)
- CSCsi40687—Defaulting Sig0 causes sensorApp to stop repsonding
- CSCsj72253—TCP Session Tracking Mode does not separate vlan properly
- CSCsj49640—SensorApp unable to allocate memory during packet processing
- CSCse24364—4FE - interfaces not reporting Missed Packet Percentage
- CSCsg24632—String.TCP sigs may fire out of order +
- CSCsh50516—IPS Fails to remove blocking if the blocked host is in PIX's name list
- CSCsh50205—IPS 5.1(4) 4215 imaged as CF based system because of HD failure
- CSCsh75673—valid NTP key values stored as -1
- CSCsi48979—Sig 2152:0 false alarms after tunings or restore defaults
- CSCsi98677—erase current-config hangs sensor CLI
- CSCsi45463—6.0(2) TCP SYN Flood Cookies not functioning on XL platform
- CSCsi58602—IPS evasion using Unicode encoding for HTTP-based attacks +
- CSCsi84527—Accounts can be created with invalid usernames
- CSCsj95950—ASA/SSM False Data Plane Failover Occuring
- CSCsk14712—Full Database does not leave enough memory for Sig Update and some conf
- CSCsj74455—service pack install should preserve sensorApp.conf
- CSCsk21795—add log to main.log for mainApp shutdown
- CSCsg86162—MSRPC and SMB engine not handling Fragmentation correctly
- CSCsi75856—Some Database statistics always remain 0
- CSCsj41582—IPS 5.1(5)E1 UDP-string engine does not distinguish direction
- CSCsj29570—IpDual Database insertion rate limiting code merged out of nubra
- CSCsl39701—add globalSummary protection to alarm DB creation
- CSCsk72811—Sig 1315 causes peformance hit in promise
- CSCsk09897—IPS: sends ACK with destination mac of orignal packet, breaks MS NLB
- CSCsk11222—show tech contains garbage chars due to new safenet files
- CSCsg45642—Make CDP drop a configurable option.

- CSCsi22195—Refactor normalizer processTcpOptions unit
- CSCsi52422—POSFP feature does not work with SSM
- CSCsj26086—Disabling one CSAMC-EPI removes all the addresses on the Sensor
- CSCsk50777—Anomaly Detection memory/flash usage not restricted for some platforms
- CSCsi58642—IDM does not handle slash in a user name correctly
- CSCsk33892—Engine String may incorrectly warn of regex compile failure
- CSCsh13463—IDSM-2 promiscuous displaying WARNING: Pulled previous index
- CSCsg04913—install - service account's .bash_profile not carried forward
- CSCsi19316—Add ability to enable/disable CDP forwarding from service account
- CSCse54970—Need to add Safenet support to licensing
- CSCsi72263—Allow inline Asymmetric traffic
- CSCsj80570—Add cidDump to upgrades

Known Caveats

The following known issues are found in Cisco IPS 6.0(4)E2:

- CSCsk30811 Unnecessary webserver error logging causes hard drive failure
- CSCsm71528—sensorApp failure in InspectorServiceRpc after reconfig
- CSCsm60273—AIP-SSM stays in Unresponsive state after ASA5500's bootup
- CSCsj78809—IPS 6.0(3) SigProcessor failure with reinjected frag
- CSCsj21080—Promiscuous 4255 in s/w bypass and no response from show stat vi
- CSCsi42747—Memory leak in mainApp when checking license status
- CSCsg09619—IPS accepts RSA keys with exponent 3 which are vulnerable to forgery
- CSCsi43787—Memory leak in mainApp when log event initiated remotely
- CSCsg96871—AnalysisEngine InspectorServiceAICWeb::ToServiceInspect abort
- CSCsh50760—NAC causes high mainApp usage
- CSCsk53813—upgrade log files are not preserved during an upgrade
- CSCsj82458—global-block-timeout allows values outside supported range
- CSCsd19619—NO statistics on traffic under heavy load
- CSCse40651—Config operation on heavily loaded system may cause unresponsive system
- CSCsm50539—MainApp fails to load
- CSCsi88201—Error message too cryptic for events with bad XML
- CSCsi08842—Under high loss conditions in promiscuous mode memory can be exhausted
- CSCsm24466—XL interface pkt drops from jumbo frames
- CSCsi51727—Error while copying AD files to a destination URL.
- CSCsh89833—Delete event variable referenced by filter or sig from IDM
- CSCsi56908—kernel change to 2.6 will create bug related to jiffies in the drivers
- CSCsm46158—Critical memory condition can cause race condition

- CSCsm46218—Non allocating logging method needed
- CSCsj15446—MainApp - core on invalid platform test
- CSCsi73502—6.0(2)E1: No warning message when removing sensor used by ASA
- CSCsm42382—Link drops temporarily on hardware-bypass ports during cids shutdown
- CSCsl24036—AnalysisEngine failure in MSRPC_TCP Inspector ProcessPacket
- CSCsl75224—cli command no mars-category causes sensor connection closed
- CSCsk44582—Sig upgrade within grace period fails prior to reboot
- CSCsk09025—idsm2 interface Operational Mode: down after reload from switch
- CSCsj75538—Auto Update - not pulling platform specific patch
- CSCsj57474—Some sweep and atomic-ip sigs false neg with dot1q headers
- CSCsi39496—IDCONF changes encrypted values of unchanged data
- CSCsi10476—cidsAlertProtocol missing from SNMP Traps
- CSCsj15835—SensorApp - PAWS alerts with telnet through 2 vs
- CSCsj80889—IP frags subjected to modify-packet-inline have been re-fragmented
- CSCsl66235—Setup errors after defaulting sensor config via IDM
- CSCsm72321—AIP module get stuck in high cpu due to main application loop
- CSCsj14632—IP fragmented attacks with IPv6 or IPv4 header produce false negative
- CSCsk84825—Non-printable character in event XML causes cascading events
- CSCsm62246—Affinity is not working properly on MIPS platforms
- CSCsm70093—x1 platforms not meeting performance requirements
- CSCsl73575—sigID 5801:1 multi-string is producing false negative
- CSCsl69776—AD not generating alert for every worm attacker
- CSCsl85441—XL interface stats out of sync with virtual sensor stats
- CSCsm41026—Sig update cause sensor hang sometime

Related Documentation

Refer to the following documentation for more information on IPS 6.0 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 6.0*
- *Regulatory Compliance and Safety Information for the Cisco Intrusion Detection and Prevention System 4200 Series Appliance Sensor*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 6.0*
- *Command Reference for Cisco Intrusion Prevention System 6.0*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0*
- *Installing Cisco Intrusion Prevention System Appliances and Modules 6.0*
- *Installing and Removing Interface Cards in Cisco IPS-4260 and IPS 4270-20*

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.

