



Release Notes for Cisco Intrusion Prevention System 5.0

May 4, 2005

Contents

- [Before Upgrading to Cisco IPS 5.0, page 1](#)
- [Upgrading to Cisco IPS 5.0, page 7](#)
- [After Upgrading to Cisco IPS 5.0, page 13](#)
- [Restrictions and Limitations, page 20](#)
- [IPS Management and Event Viewers, page 21](#)
- [New and Changed Information, page 21](#)
- [Password Recovery, page 24](#)
- [Caveats, page 25](#)
- [Related Documentation, page 25](#)
- [Obtaining Documentation and Submitting a Service Request, page 26](#)

Before Upgrading to Cisco IPS 5.0

Before you upgrade your sensors to Cisco IPS 5.0, you need to make sure you have performed the following tasks:

- Created a backup copy of your configuration. For the procedure, see [Copying and Restoring the Configuration File Using a Remote Server, page 2](#).
- Saved the output of the **show version** command.



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

If you need to downgrade, you will need to know what version you had, and you can then apply the configuration you saved when you backed up your configuration. For the procedure, refer to [Displaying Version Information](#). For the procedure for downgrading your sensor, refer to [Downgrading the Sensor](#).



Note You cannot use the **downgrade** command to downgrade from 5.0(1) to 4.x.

- Upgraded the IDS-4210 memory to 512 MB.
For the procedure, see [Upgrading the IDS-4210 Memory, page 3](#).
- Upgraded the IDS-4215 BIOS to the most recent version.
For the procedure, see [Upgrading the IDS-4215 BIOS, page 5](#).

This section contains the following topics:

- [Copying and Restoring the Configuration File Using a Remote Server, page 2](#)
- [Upgrading the IDS-4210 Memory, page 3](#)
- [Upgrading the IDS-4215 BIOS, page 5](#)

Copying and Restoring the Configuration File Using a Remote Server

Use the **copy** [**/erase**] *source-url destination-url keywords* command to copy the configuration file to a remote server. You can then restore the current configuration from the remote server. You are prompted to back up the current configuration first.



Note

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

The following options apply:

- **/erase**—Erases the destination file before copying.
This keyword only applies to the current-config; the backup-config is always overwritten. If this keyword is specified for destination current-config, the source configuration is applied to the system default configuration. If it is not specified for the destination current-config, the source configuration is merged with the current-config.
- *source-url*—The location of the source file to be copied. It can be a URL or keyword.
- *destination-url*—The location of the destination file to be copied. It can be a URL or a keyword.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- **ftp**:—Source or destination URL for an FTP network server. The syntax for this prefix is:
ftp://[username@] location]/relativeDirectory]/filename
ftp://[username@]location]//absoluteDirectory]/filename
- **scp**:—Source or destination URL for the SCP network server. The syntax for this prefix is:
scp://[username@] location]/relativeDirectory]/filename
scp://[username@] location]//absoluteDirectory]/filename

- **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 FTP or SCP protocol, you are prompted for a password.

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

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



Caution

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

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

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

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

```
sensor# copy current-config ftp://qa_user@10.89.146.1//tftpboot/update/qmaster89.cfg
Password: *****
```

Step 3 To restore the configuration file that you copied to the remote server:

```
sensor# copy ftp://qa_user@10.89.146.1//tftpboot/update/qmaster89.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 4 Press **Enter** to copy the configuration file or type **no** to stop.

Upgrading the IDS-4210 Memory

IDS-4210, IDS-4210-K9, and IDS-4210-NFR must have 512 MB of RAM to support Cisco IPS 5.0. If you are upgrading an existing IDS-4210, IDS-4210-K9, or IDS-4210-NFR to 5.0, you must insert one additional 256-MB DIMM (part number IDS-4210-MEM-U) to upgrade the memory to the required 512 MB minimum.



Note

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



Caution

Read the safety warnings in *Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor* and follow proper safety procedures when performing these steps.

To upgrade the memory, follow these steps:

Step 1 Log in to the CLI.

Step 2 Prepare the appliance to be powered off:

```
sensor# reset powerdown
```

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



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

Step 3 Power off the appliance.

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

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

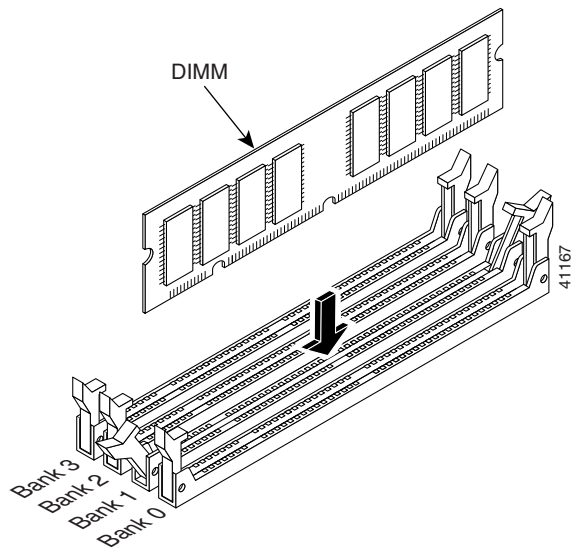
For more information, refer to [Working in an ESD Environment](#).

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

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



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



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

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



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

Step 10 Replace the chassis cover and reconnect the power.

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



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

Upgrading the IDS-4215 BIOS

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/>

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

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

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

For the procedure for locating software on Cisco.com, see [Obtaining Software on Cisco.com, page 8](#).



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

Step 2 Boot IDS-4215.

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

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

The console display resembles the following:

```
CISCO SYSTEMS IDS-4215
Embedded BIOS Version 5.1.3 05/12/03 10:18:14.84
```

```

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

```

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

```
rommon> interface port_number
```

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



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

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

```
rommon> address ip_address
```



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

Step 6 Specify the TFTP server IP address:

```
rommon> server ip_address
```

Step 7 Specify the gateway IP address:

```
rommon> gateway ip_address
```

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

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

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

```
rommon> file filename
```

Example:

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



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

Step 10 Download and run the update utility:

```
rommon> tftp
```

- Step 11** Type `y` at the upgrade prompt and the update is executed.
IDS-4215 reboots when the update is complete.

**Caution**

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

Upgrading to Cisco IPS 5.0

This section provides information on upgrading to IPS 5.0. It contains the following topics:

- [Upgrading from 4.x to 5.0, page 7](#)
- [Installing the 5.0\(2\) Service Pack, page 8](#)
- [Obtaining Software on Cisco.com, page 8](#)
- [IPS Software Versioning, page 9](#)
- [Upgrading to 5.0, page 12](#)

Upgrading from 4.x to 5.0

The following caveats apply to upgrading from 4.x to 5.0:

- If you have 4.0 installed on your sensor, you must upgrade to 4.1, then upgrade to 5.0.

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

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

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

- In 4.x, custom signature IDs start at 20000. Any custom signatures that you have created in 4.x are converted to the 5.0 custom signature range, which begins at 60000.
- In 4.x, there is a parameter that lets you enable and disable signatures. In 5.0, there is a similar parameter, but there is also a parameter that lets you retire and unretire signatures. When you upgrade to 5.0, some signatures will be marked as enabled; however, they may also have been retired in 5.0 and therefore the enabled setting is ignored. You must manually unretire the signature to ensure that it is enabled. For the CLI procedure, refer to [Configuring the Status of Signatures](#). For the IDM procedure, refer to [Configuring Signatures](#).
- In 5.0, you receive messages indicating that you need to install a license. The sensor functions properly without a license, but you need a license to install signature updates. For the procedure, see [Licensing the Sensor, page 15](#).

- Upgrading from 4.1 to 5.0 preserves the sensor’s configuration. The upgrade may stop if it comes across a value that it cannot translate. If this occurs, the resulting error message provides enough information to adjust the parameter to an acceptable value. After editing the configuration, try the upgrade again.
- After you upgrade to 5.0, you cannot downgrade. If you want to return to the previous version, you must reimage (refer to [Upgrading, Downgrading, and Installing System Images](#)) and then copy the backup configuration to the reimaged sensor. For the procedure, see [Copying and Restoring the Configuration File Using a Remote Server, page 2](#).
- IDS MC cannot manage sensors that have been upgraded to 5.0 until the IDS MC 2.1 release.
- The 5.0(1) major upgrade installs a new OS on the sensor.
- The 5.0(1) major upgrade upgrades both the application partition and the recovery partitions.
- The 5.0(1) major upgrade when applied to NM-CIDS upgrades the bootloader to 1.0.17-1.

Installing the 5.0(2) Service Pack

When you install the 5.0(2) service pack, ASA-SSM is rebooted after the upgrade. The 5.0(2) service pack modifies the `biphysarea` argument passed to the Linux kernel for ASA-SSM. When IPS is started at the end of the package install, it detects that the kernel arguments have changed, and triggers a reboot so that Linux can use the new argument. A downgrade from 5.02 to 5.01 also triggers a reboot on ASA-SSM for the same reason.

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 in a release train format, a new release every three months. Major and minor updates are also posted periodically. Check Cisco.com regularly for the latest IPS software.

You must have an account with cryptographic access before you can download software. You set this account up the first time you download IPS software from the Download Software site.



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 sensor license to apply signature updates.

Downloading Cisco 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 File Download dialog box appears. 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.
- Step 11** Open the file or save it to your computer.
- Step 12** Follow the instructions in the Readme or the Release Notes to install the update.

IPS Software Versioning

This section describes IPS software naming conventions and provides examples. It contains the following topics:

- [IPS Software Image Naming Conventions, page 9](#)
- [5.0 Software Release Examples, page 11](#)

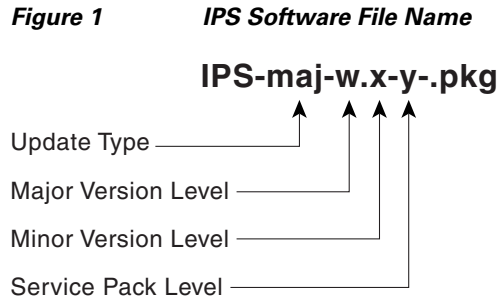
IPS Software Image Naming Conventions

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.

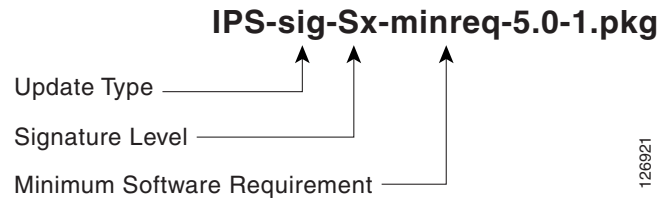


Note You can determine which software version is installed on your sensor by using the **show version** command.

Figure 1 illustrates what each part of the IPS software file represents:



- IDS-K9-sp-5.0-2-.pkg—Service Pack Update
- IDS-K9-min-5.1-1-.pkg—Minor Version Update
- IDS-K9-maj-5.0-1-.pkg—Major Version Update



126921

A major version upgrade contains new functionality or an architectural change in the product. For example, the IPS 5.0 base version release includes everything since the previous major release (the minor version features, service pack fixes, and signature updates) plus any new changes. Major upgrade 5.0(1) requires 4.1.



Note

The 5.0(1) major upgrade is only used to upgrade 4.1 sensors to 5.0(1). If you are reinstalling 5.0(1) on a sensor that already has 5.0(1) installed, use the system image or recovery procedures rather than the major upgrade.

A minor version upgrade is incremental to the major version. Minor version upgrades are also base versions for service packs. The first minor version upgrade for 5.0 is 5.1(1). Minor version upgrades are released for minor enhancements to the product. Minor version upgrades contain all previous minor features, service pack fixes, and signature updates since the last major version, and the new minor features being released. The minor upgrade requires the major version.

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.

Signature updates are cumulative and increment by one with each new release (for example, S145, S146, S147). Signature updates include every signature since the initial signature release (S1) in addition to the new signatures being released. Signature updates require the minimum version listed in the filename.

To install the most recent signature update, you must have the most recent minor version. Service packs are dependent on the most recent minor version, which is dependent on the most recent major version.

**Note**

For a table listing the types of files with examples of filenames and corresponding software releases, see [5.0 Software Release Examples, page 11](#).

In addition there are system image files for the IDS-4215, IPS-4240, IPS-4255, NM-CIDS, IDSM-2, ASA-SSM-10, and ASA-SSM-20, recovery partition files for all sensors, and a maintenance partition file for the IDSM-2:

- System image files (IDS-4215, IPS-4240, IPS-4255 NM-CIDS, IDSM-2, ASA-SSM-10, and ASA-SSM-20)—Full IPS application and recovery image used for reimaging an entire sensor.
- Recovery partition image file—A recovery partition image file is a partition on the sensor that contains a full IPS application image to be used for recovery.
- Maintenance partition image file (IDSM-2 only)—A maintenance partition image file is used to reimage the maintenance partition of the IDSM-2. Maintenance partition files are released when new major or minor versions of the maintenance partition are released. Maintenance partition image files are not released for service packs to the maintenance partition. A service pack may be released to address defects identified in existing maintenance partition images, but new maintenance partition images are not produced for subsequently released service packs.

**Note**

The maintenance partition image file does not contain a signature designator.

5.0 Software Release Examples

[Table 1](#) lists platform-independent IDS 5.x software release examples. Refer to the readmes that accompany the software files for detailed instructions on how to install the files. For instructions on how to access these files on Cisco.com, see [Obtaining Software on Cisco.com, page 8](#).

Table 1 Platform-Independent Release Examples

| Release | Target Frequency | Identifier | Supported Platform | Example File Name |
|-------------------------------|----------------------------|------------|--------------------|------------------------------|
| Signature update ¹ | Weekly | sig | All | IPS-sig-S70-minreq-5.0-1.pkg |
| Service pack ² | Semi-annually or as needed | sp | All | IPS-K9-sp-5.0-2.pkg |
| Minor version ³ | Annually | min | All | IPS-K9-min-5.1-1.pkg |
| Major version ⁴ | Annually | maj | All | IPS-K9-maj-5.0-1.pkg |
| Patch release ⁵ | As needed | patch | All | IPS-K9-patch-5.0-1pl.pkg |
| Recovery package ⁶ | Annually or as needed | r | All | IPS-K9-r-1.1-a-5.0-1.pkg |

1. Signature updates include the latest cumulative IPS signatures.
2. Service packs include defect fixes.
3. Minor versions include new features and/or functionality (for example, signature engines).
4. Major versions include new functionality or new architecture.
5. Patch releases are for interim fixes.
6. The r 1.1 can be revised to r 1.2 if it is necessary to release a new recovery package that contains the same underlying application image. If there are defect fixes for the installer, for example, the underlying application version may still be 5.0(1), but the recovery partition image will be r 1.2.

Table 2 describes platform-dependent release examples.

Table 2 Platform-Dependent Release Examples

| Release | Target Frequency | Identifier | Supported Platform | Example File Name |
|--|-----------------------|------------|------------------------------------|---------------------------------|
| System image ¹ | Annually | sys | All | IPS-4240-K9-sys-1.1-a-5.0-1.img |
| Maintenance partition image ² | Annually | mp | IDS-2 only | c6svc-mp.2-1-2.bin.gz |
| Recovery and upgrade CD | Annually or as needed | cd | All appliances with a CD-ROM drive | — |

1. The system image includes the combined recovery and application image used to reimagine an entire sensor.
2. The maintenance partition image includes the full image for the maintenance partition. The file is platform specific. If you have to recover the IDS-2 from the maintenance partition, the application partition reflects the applicable 5.0 version after the recovery operation has been completed.

Upgrading to 5.0

To upgrade the sensor, follow these steps:

Step 1 Download the major update file (IPS-K9-maj-5.0-1-pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

For the procedure for locating software on Cisco.com, see [Obtaining Software on Cisco.com, page 8](#).

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

Step 3 Upgrade the sensor:

```
sensor# configure terminal
sensor(config)# upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg

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

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



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

Step 5 Verify your new sensor version:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: ASA-SSM-20
Serial Number: 021
No license present
Sensor up-time is 5 days.
Using 490110976 out of 1984704512 bytes of available memory (24% usage)
```

```

system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 37.7M out of 166.6M bytes of available disk space (24 usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)

```

```

MainApp          2005_Mar_04_14.23  (Release)  2005-03-04T14:35:11-0600  Running
AnalysisEngine  2005_Mar_04_14.23  (Release)  2005-03-04T14:35:11-0600  Running
CLI              2005_Mar_04_14.23  (Release)  2005-03-04T14:35:11-0600

```

Upgrade History:

```

IDS-K9-maj-5.0-1-  14:16:00 UTC Thu Mar 04 2004

```

Recovery Partition Version 1.1 - 5.0(1)S149

sensor#

After Upgrading to Cisco IPS 5.0

This section provides information about what to do after you install IPS 5.0. It contains the following topics:

- [Comparing Configurations, page 13](#)
- [SSL Certificate, page 13](#)
- [Increasing the Memory Size of the Java Plug-In, page 14](#)
- [Licensing the Sensor, page 15](#)

Comparing Configurations

Compare your backed up and saved 4.x configuration with the output of the **show configuration** command after upgrading to 5.0 to verify that all the configuration has been properly converted.

IPS 5.0 has some new configuration parameters. The 4.x configuration has to be converted to the 5.0 commands.



Caution

If the configuration is not properly converted, see [Caveats, page 25](#) or check Cisco.com for any upgrade issues that have been found. Contact the TAC if no DDTs refers to your situation.

SSL Certificate

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

For the CLI procedure, refer to [Configuring TLS](#). For the IDM procedure, refer to [Adding Trusted Hosts](#).

Increasing the Memory Size of the Java Plug-In

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

You must change the memory settings of Java Plug-in before using IDM. The mandatory minimum memory size is 256 MB.

This section contains the following topics:

- [Java Plug-In on Windows, page 14](#)
- [Java Plug-In on Linux and Solaris, page 14](#)

Java Plug-In on Windows

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

-
- Step 1** Close all instances of Internet Explorer or Netscape.
- Step 2** Click **Start > Settings > Control Panel**.
- Step 3** If you have Java Plug-in 1.4.2 installed:
- a. Click Java Plug-in.
The Java Plug-in Control Panel appears.
 - b. Click the **Advanced** tab.
 - c. Type `-xmx256m` in the Java RunTime Parameters field.
 - d. Click **Apply** and exit the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
- a. Click Java.
The Java Control Panel appears.
 - b. Click the **Java** tab.
 - c. Click **View** under Java Applet Runtime Settings.
The Java Runtime Settings Panel appears.
 - d. Type `-xmx256m` in the Java Runtime Parameters field and then click **OK**.
 - e. Click **OK** and exit the Java Control Panel.
-

Java Plug-In on Linux and Solaris

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

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



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



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

- Step 3** If you have Java Plug-in 1.4.2 installed:
- Click the **Advanced** tab.
 - Type `-Xmx256m` in the Java RunTime Parameters field.
 - Click **Apply** and close the Java Control Panel.
- Step 4** If you have Java Plug-in 1.5 installed:
- Click the **Java** tab.
 - Click **View** under Java Applet Runtime Settings.
 - Type `-Xmx256m` in the Java Runtime Parameters field and then click **OK**.
 - Click **OK** and exit the Java Control Panel.

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:

- [Obtaining a License Key from Cisco.com, page 15](#)
- [Installing the License, page 16](#)

Obtaining a License Key from Cisco.com

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



Note You can install the first few signature updates for 5.0 without a license. This gives you time to get your sensor licensed. If you are unable to get your sensor licensed because of confusion with your contract, you can obtain a 60-day trial license that supports signature updates that require licensing.

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

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

Whenever you start IDM, a dialog box informs you of your license status—whether you have a trial, invalid, or expired license key. With no license key, an invalid license key, or an expired license key, you can continue to use IDM but you cannot download signature updates.

When you enter the CLI, you receive the following message if there is no license installed:

```
***LICENSE NOTICE***  
There is no license key installed on the system.  
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
```

You will continue to see this message until you install a license. Go to <http://www.cisco.com/go/license> and click **IPS Signature Subscription Service** to apply for a license.


Installing the License

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

- [Using IDM, page 17](#)
- [Using the CLI, page 18](#)

Using IDM

To install the sensor license, follow these steps:

-
- Step 1** Click **Configuration > Licensing**.
The Licensing panel appears.
- Step 2** Choose the method to deliver the license:
- Select **Cisco Connection Online** 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 3](#).
 - Select **License File** to use a license file.
To use this option, you must apply for a license at www.cisco.com/go/license.
The license is sent to you in e-mail and you save it to a drive that is accessible by IDM. This option is useful if your computer does not have access to Cisco.com.
Go to [Step 6](#).
- Step 3** Click **Update License**.
The Licensing dialog box appears.
- Step 4** Click **Yes** to continue.
The Status dialog box informs you that the sensor is trying to connect to Cisco.com.
The Information dialog box confirms that the license 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 Cisco IPS Signature Subscription Service license key will be sent by e-mail to the e-mail address you specified.
- Step 8** Save the license file to a hard-disk drive or a network drive that is accessible by the client running IDM.
- Step 9** Log in to IDM or ASDM.
- Step 10** Click **Configuration > Licensing**.
- Step 11** Under Update License, select **Update From: License File**.
- Step 12** 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 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 file to your sensor. The following options apply:

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



Note

You cannot install an older license key over a newer license key.

The exact format of the source and destination URLs varies according to the file. Here are the valid types:

- **ftp:**—Source or destination URL for an FTP network server. The syntax for this prefix is:
ftp:[//[username@] location]/relativeDirectory]/filename
ftp:[//[username@]location]//absoluteDirectory]/filename
- **scp:**—Source or destination URL for the SCP network server. The syntax for this prefix is:
scp:[//[username@] location]/relativeDirectory]/filename
scp:[//[username@] location]//absoluteDirectory]/filename
- **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 FTP or SCP, you are prompted for a password.



Note

If you use SCP, the remote host must be on the SSH known hosts list. For the CLI procedure, refer to [Adding Hosts to the Known Hosts List](#). For the IDM procedure, refer to [Defining Known Host Keys](#).



Note

If you use HTTPS, the remote host must be a TLS trusted host. For the CLI procedure, refer to [Adding TLS Trusted Hosts](#). For the IDM procedure, refer to “[Adding TLS Trusted Hosts](#)”.

To install the license key, follow these steps:

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

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 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23% usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)
```

```
MainApp          2005_Feb_18_03.00  (Release)  2005-02-18T03:13:47-0600  Running
AnalysisEngine   2005_Feb_15_03.00  (QATest)   2005-02-15T12:59:35-0600  Running
CLI              2005_Feb_18_03.00  (Release)  2005-02-18T03:13:47-0600
```

Upgrade History:

```
IDS-K9-maj-5.0-1- 14:16:00 UTC Thu Mar 04 2004
```

Recovery Partition Version 1.1 - 5.0(1)S149

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#
```

Restrictions and Limitations

The following restrictions and limitations apply to Cisco IPS 5.0 software and the products that run 5.0:

- An IPS appliance can support both promiscuous and inline monitoring at the same time; however you cannot configure promiscuous monitoring and inline monitoring on the same physical interface of the sensor. You must configure each physical interface in either promiscuous or inline mode. Because inline monitoring requires the use of two sensing interfaces, the sensor must contain at least three physical sensing interfaces to perform both promiscuous and inline monitoring. The exception to this is ASA-SSM. ASA-SSM can support both promiscuous and inline monitoring on its single physical back plane interface inside the ASA. The configuration on the main ASA can be used to designate which packets/connections should be monitored by ASA-SSM as either promiscuous or inline.
- IDSM-2 only supports inline mode for Catalyst Software 8.4.4(1) with Supervisor Engine 1a, Supervisor Engine 2, Supervisor Engine 32, and Supervisor Engine 720. Inline support for Cisco IOS will be added at a later date.
- IDSM-2 only supports EtherChanneling load balancing for Cisco IOS Software 12.2(18)SXE with Supervisor Engine 720 in promiscuous mode only. EtherChanneling load balancing for Catalyst software will be added at a later date.
- You can configure only one IDSM-2 for inline monitoring between two VLANs. Configuring more than one IDSM-2 in inline mode between the same two VLANs can cause a packet loop in the switch. If you need to use more than one IDSM-2 in inline mode in the switch, you must configure each IDSM-2 for inline monitoring for a unique set of two VLANs.
- NM-CIDS does not run in inline mode.
- IDM does not support any non-English characters, such as the German umlaut or any other special language characters. If you enter such characters as a part of an object name through IDM, they are turned into something unrecognizable and you cannot delete or edit the resulting object through IDM or the CLI.

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

- You can only install eight IDSM-2s per switch chassis.
- Do not confuse Cisco IOS IDS (a software-based intrusion-detection application that runs in the Cisco IOS) with the IPS that runs on the NM-CIDS. The NM-CIDS runs Cisco IPS 5.0. Because performance can be reduced and duplicate alarms can be generated, we recommend that you do not run Cisco IOS IDS and Cisco IPS 5.0 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-CDIDS.
- IDS Event Viewer (IEV) is no longer supported.
- The HTML-based IDM has been replaced with a Java applet.
- You cannot use IDS MC 2.0 to configure 5.0 sensors. Support for 5.0 sensors is being added to IDS MC 2.1.

IPS Management and Event Viewers

Use IDM or the CLI for configuring 5.0 sensors.



Note

You cannot use IDS MC 2.0 to configure 5.0 sensors. Support for 5.0 sensors is being added to IDS MC 2.1

Use the following tools for monitoring 5.0 sensors:

- Security Monitor 2.0.1
- CTR 2.1
- IEV 4.x



Note

Although IEV is no longer supported, you can use it to monitor 5.0 sensors. However, the new 5.0 features will not be reported by IEV.

- Protego PN-MARS 3.3.3



Note

If you are using these tools to monitor 5.0 sensors, add the sensors to the configuration as if they were 4.1 sensors. You cannot view the new fields in 5.0 alerts in these alarm viewers until they have been upgraded to accommodate the new fields in 5.0. Security Monitor 2.1 is being upgraded to display the fields in 5.0 alerts.



Note

Viewers that are already configured to monitor the 4.x sensors may need to be configured to accept a new SSL certificate for the 5.0 sensors.

New and Changed Information

This section contains the following topics:

- [New Features, page 22](#)
- [Changed Features, page 22](#)
- [Cisco Security Center, page 23](#)
- [Active Update Notifications, page 23](#)
- [IPS 5.0 Files, page 24](#)

New Features

This release has the following new features:

- Inline intrusion prevention functionality.
- Advanced intrusion prevention:
 - New packet drop actions to stop attacks that augments TCP reset and ACL modification.
 - Hybrid detection and prevention capabilities that allow a single sensor to operate simultaneously as an IDS sensor and an IPS sensor.
 - Broad platform coverage with IPS 5.0 capabilities delivered on both the Cisco 4200 series appliances and the Catalyst 6500 series module.
- Application inspection technologies that allow enforcement of policy decisions based on content detected at the application layer.
- Detection and prevention of covert channel tunneling through Port 80.
- RFC-compliance checking for HTTP methods.
- Filtering of traffic based on malicious select MIME types, such as jpeg extensions.
- Control of permitted traffic through user-defined policies.
- VoIP engine to ensure protocol compliance of H225 call setup messages.

This engine also delivers protection against attacks to voice gateways through advanced buffer overflow and URL overflow mitigation.
- Support for the inspection and mitigation of threats in MPLS environments.
- Support for advanced traffic normalization algorithms, such as fragmentation and TCP session normalization.
- Ability to identify attacks in IPv6 environments through the inspection of IPv4 traffic being tunneled in IPv6.
- New monitoring using SNMP.
- IDM now a Java applet rather than HTML.
- New IPS device manager, ASDM.
- Added filtering features that let you filter specific actions and filter by port.
- Added a risk rating feature that you can use for event action overrides that adds additional actions based on the risk of the alert.
- Support of getting PEP information on hardware that supports PEP.
- New IPS module, ASA-SSM-10 and ASA-SSM-20.

Changed Features

This release has the following changed features:

- The NSDB is no longer part of the 5.0 sensor. You can access the NSDB on the Cisco Security Center on Cisco.com. For more information, see [Cisco Security Center, page 23](#).
- The SYSLOG engine is no longer supported. 5.0 sensors no longer support the creation of alerts based on Cisco router syslog messages.

Cisco Security Center

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>

Active Update Notifications

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

To receive bulletins about updates, follow these steps:

-
- Step 1** Log in to Cisco.com.
 - Step 2** Under Quick Links on the right side of the window, click **Security Center**.
 - Step 3** Scroll down and under Products and Service Updates, choose **Cisco IPS Active Update Bulletins**.
 - Step 4** Click one of the Cisco IPS Active Update Bulletins.
 - Step 5** Under In this Issue, click **Subscription Information**.
 - Step 6** Under Subscription Information, click **subscribe now**.
 - Step 7** Fill out the required information, as follows:
 - a. Would you like to receive IDS Active Update Bulletin? Select **Yes** or **No** from the drop-down list.
 - b. Enter your first name in the **First Name** field.
 - c. Enter your last name in the **Last Name** field.
 - d. Enter the name of your company in the **Company** field.
 - e. Choose your country from the drop-down menu.
 - f. Enter your e-mail address in the **E-mail** field.
 - Step 8** Check the check box if you want to receive further information about Cisco products and offerings by e-mail.
 - Step 9** Fill in the optional information if desired.
 - a. Choose your job function from the drop-down list.
 - b. Choose your job level from the drop-down list.

- c. Choose your industry or business type from the drop-down list.
- d. Choose how many people your organization employs worldwide from the drop-down list.
- e. Choose your company or organization type from the drop-down list.

Step 10 Click **Submit**.

You receive e-mail notifications of updates when they occur and instructions on how to obtain them.

IPS 5.0 Files

IPS 5.0 contains the following files:

- IPS-K9-maj-5.0-1-S149.rpm.pkg—Major version file
- IPS-4215-K9-sys-1.1-a-5.0-1.img—System image file for IDS-4215
- IPS-4240-K9-sys-1.1-a-5.0-1.img—System image file for IPS-4240
- IPS-4255-K9-sys-1.1-a-5.0-1.img—System image file for IPS-4255
- IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img—System image file for NM-CIDS
- IPS-SSM-K9-sys-1.1-a-5.0-1.img—System image file for ASA-SSM
- WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz—System image file for IDSM-2
- IPS-K9-r-1.1-a-5.0-1.pkg—Recovery image file
- aesop_bl-1.0.17-1—NM-CIDS bootloader file

Password Recovery

The following password recovery options exist:

- If another Administrator account exists, the other administrator can change the password.
- If a Service account exists, you can log in to the Service account and switch to user root using the command **su - root**. Use the **password** command to change the CLI Administrator account's password. For example, if the Administrator username is "adminu," the command is **password adminu**. You are prompted to enter the new password twice. For more information, refer to [Creating the Service Account](#).

You can reimagine the sensor using either the recovery partition or a system image file. For more information, refer to [Upgrading, Downgrading, and Installing System Images](#).

Caveats

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

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

The following caveats apply to Cisco IPS 5.0:

- CSCeg8403—IDM fails to come up occasionally
- CSCeg77288—IDSM2 - Booting MP drops all sensing traffic
- CSCeg79864—IDSM2 - permanent solution to bypass activation bug (CSCeg80380)
- CSCeg82626—Temporarily unable to login following re-imaging from the RP
- CSCeh00649—Creating custom sig for AIC msg-body fails due to failed validation
- CSCeh03676—IDSM-2 inline failover (not supported) can cause broadcast storm
- CSCeh06948—XL card is not reporting missed packets correctly
- CSCeh10004—IDSM-2: Shutdown problem (state remains as Other)
- CSCeh14385—sig 3340 does not fire
- CSCeh16307—Turning on content-verify for 12637 2 false positives 12673
- CSCeh17616—telnet cli session hangs when large buffer is input
- CSCeh17654—Unable to upgrade from 4.0(1) to 5.0
- CSCeh18687—Alerts from 5.0 sensor do not get to SIMS server
- CSCeh21152—default block time not getting transferred from 4.x to 5.x
- CSCeh21616—4250-TX went into ByPass Auto_On after promiscuous stress test
- CSCsa66098—NAC can lose the current config based on previous errors

Related Documentation

Refer to the following documentation for more information on IPS 5.0 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 5.0*
- *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 5.0*
- *Command Reference for Cisco Intrusion Prevention System 5.0*
- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.0*
- *Installing Cisco Intrusion Prevention System Appliances and Modules 5.0*

Obtaining Documentation and Submitting a Service Request

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

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

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

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

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

Copyright © 2005-2009 Cisco Systems, Inc. All rights reserved.