

# Upgrade the Image and Signature IDS 4.1 to IPS 5.0 and Later(AIP-SSM, NM-IDS, IDSM-2) Configuration Example

Document ID: 88954

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Configure

#### Upgrade the Sensor

- Overview

- Upgrade Command and Options

- Use the Upgrade Command

#### Configuring Automatic Upgrades

- Automatic Upgrades

- Use the auto-upgrade Command

#### Re-image the Sensor

#### Related Information

---

## Introduction

This document describes how to upgrade the image and signature for Cisco Intrusion Detection Sensor (IDS) software from version 4.1 to Cisco Intrusion Prevention System (IPS) 5.0 and later.

**Note:** From software version 5.x and later, Cisco IPS replaces Cisco IDS which is applicable until version 4.1.

**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.

Refer to the Installing the AIP-SSM System Image section of Upgrading, Downgrading, and Installing System Images for the procedure.

Refer to Password Recovery Procedure for the Cisco IDS Sensor and IDS Services Modules (IDSM-1, IDSM-2) in order to learn more about how to recover the Cisco Secure IDS (formerly NetRanger) appliance and the modules for versions 3.x and 4.x.

**Note:** Refer to the Upgrading Cisco IPS Software from 5.1 to 6.x section of Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0 for more information about the procedure to upgrade the IPS 5.1 to version 6.x.

## Prerequisites

### Requirements

The minimum required software version you need in order to upgrade to 5.0 is 4.1(1).

## Components Used

The information in this document is based on the Cisco 4200 Series IDS hardware that runs software version 4.1 (to be upgraded to version 5.0).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Configure

In this section, you are presented with the information to configure the features described in this document.

The upgrade from Cisco 4.1 to 5.0 is available as a download from Cisco.com. Refer to Obtaining Cisco IPS Software for the procedure you use to access IPS Software downloads on Cisco.com.

You can use any of the methods listed here in order to perform the upgrade:

- After you download the 5.0 upgrade file, refer to the Readme for the procedure on how to install the 5.0 upgrade file using the **upgrade** command. See the Use the Upgrade Command section of this document for more information.
- If you configured Auto Update for your Sensor, copy the 5.0 upgrade file to the directory on the server that your Sensor polls for updates. See the Use the auto-upgrade Command section of this document for more information.
- If you install an upgrade on your Sensor and the Sensor is unusable after it reboots, you must reimage your Sensor. An upgrade of a Sensor from any Cisco IDS version earlier than 4.1 also requires you to use the **recover** command or the recovery/upgrade CD. See the Re-image the Sensor section of this document for more information.

## Upgrade the Sensor

These sections explain how to use the **upgrade** command to upgrade the software on the Sensor:

- Overview
- Upgrade Command and Options
- Use the Upgrade Command

### Overview

You can upgrade the Sensor with these files, all of which have the extension .pkg:

- Signature updates, for example, IPS-sig-S150-minreq-5.0-1.pkg
- Signature engine updates, for example, IPS-engine-E2-req-6.0-1.pkg
- Major updates, for example, IPS-K9-maj-6.0-1-pkg
- Minor updates, for example, IPS-K9-min-5.1-1.pkg
- Service pack updates, for example, IPS-K9-sp-5.0-2.pkg
- Recovery partition updates, for example, IPS-K9-r-1.1-a-5.0-1.pkg
- Patch releases, for example, IPS-K9-patch-6.0-1p1-E1.pkg

- Recovery partition updates, for example, IPS-K9-r-1.1-a-6.0-1.pkg

A Sensor upgrade changes the software version of the Sensor.

## Upgrade Command and Options

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades.

These options apply:

- **default** Sets the value back to the system default setting.
- **directory** Directory where upgrade files are located on the file server.
- **file-copy-protocol** File copy protocol used to download files from the file server. The valid values are **ftp** or **scp**.

**Note:** If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the Sensor can communicate with it through SSH. Refer to Adding Hosts to the Known Hosts List for the procedure.

- **ip-address** IP address of the file server.
- **password** User password for authentication on the file server.
- **schedule-option** Schedules when automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.

- ◆ **calendar-schedule** Configures the days of the week and times of day that automatic upgrades are performed.

- ◇ **days-of-week** Days of the week on which auto-upgrades are performed. You can select multiple days. Sunday through Saturday are the valid values.

- ◇ **no** Removes an entry or selection setting.

- ◇ **times-of-day** Times of the day at which auto-upgrades begin. You can select multiple times. The valid value is hh:mm[:ss].

- ◆ **periodic-schedule** Configures the time that the first automatic upgrade should occur, and how long to wait between automatic upgrades.

- ◇ **interval** The number of hours to wait between automatic upgrades. Valid values are 0 to 8760.

- ◇ **start-time** The time of day to start the first automatic upgrade. The valid value is hh:mm[:ss].

- **user-name** Username for authentication on the file server.

For the IDM procedure for upgrading the sensor, refer to Updating the Sensor.

## Use the Upgrade Command

You receive SNMP errors if you do not have the **read-only-community** and **read-write-community** parameters configured before upgrading to IPS 6.0. If you are using SNMP **set** and/or **get** features, you must configure the **read-only-community** and **read-write-community** parameters before you upgrade to IPS 6.0. In IPS 5.x, the **read-only-community** was set to public by default, and the **read-write-community** was set to private by default. In IPS 6.0 these two options do not have default values. If you did not use SNMP **gets** and **sets** with IPS 5.x, for example, **enable-set-get** was set to false, then there is no problem to upgrade to IPS 6.0. If you used SNMP **gets** and **sets** with IPS 5.x, for example, **enable-set-get** was set to true, you must configure the **read-only-community** and **read-write-community** parameters to specific values or

the IPS 6.0 upgrade fails.

You receive this error message:

```
Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true,
but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
continue with null values in these fields.
```

**Note:** IPS 6.0 denies high risk events by default. This is a change from IPS 5.x. In order to change the default, create an event action override for the deny packet inline action and configure it to be disabled.

Complete these steps in order to upgrade the Sensor:

1. Download the major update file (IPS-K9-maj-5.0-1-S149.rpm.pkg ) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your Sensor.

Refer to Obtaining Cisco IPS Software for the procedure on how to locate software on Cisco.com.

**Note:** You must log in to Cisco.com using an account with cryptographic privileges in order to download the file. Do not change the file name. You must preserve the original file name for the Sensor to accept the update.

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

2. Log in to the CLI using an account with administrator privileges.
3. Enter configuration mode:

```
sensor#configure terminal
```

4. Upgrade the sensor:

```
sensor(config)#upgrade scp://<username>@<server IP>//upgrade/<file name>
```

**Example:**

**Note:** This command is on two lines due to spatial reasons.

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

**Note:** Refer to Supported FTP and HTTP/HTTPS Servers for a list of supported FTP and HTTP/HTTPS servers. Refer to Adding Hosts to the SSH Known Hosts List for more information on how to add the SCP server to the SSH known hosts list.

5. Enter the password when prompted:

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

6. Type **yes** to complete the upgrade.

**Note:** Major updates, minor updates, and service packs might force a restart of the IPS processes or even force a reboot of the Sensor to complete the installation. So, there is an interruption of service for at least two minutes. However, signature updates do not require a reboot after the update is done. Refer to Download Signature Updates ( registered customers only) for the latest updates.

7. 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#

**Note:** For IPS 5.x, you receive a message that states the upgrade is of unknown type. You can ignore this message.

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

Refer to Updating the Sensor for more information on the IDM procedure for upgrading the sensor.

## Configuring Automatic Upgrades

### Automatic Upgrades

You can configure the sensor to look for new upgrade files in your upgrade directory automatically. For example, several sensors can point to the same remote FTP server directory with different update schedules, such as every 24 hours, or Monday, Wednesday, and Friday at 11:00 pm.

You specify this information in order to schedule automatic upgrades:

- Server IP address
- Path of the directory on the file server where the sensor checks for upgrade files
- File copy protocol (SCP or FTP)
- Username and password
- Upgrade schedule

You must download the software upgrade from Cisco.com and copy it to the upgrade directory before the sensor can poll for automatic upgrades.

**Note:** If you use automatic upgrade with AIM-IPS and other IPS appliances or modules, make sure you put both the 6.0(1) upgrade file, IPS-K9-6.0-1-E1.pkg, and the AIM-IPS upgrade file, IPS-AIM-K9-6.0-4-E1.pkg, on the automatic update server so that AIM-IPS can correctly detect which file needs to be automatically downloaded and installed. If you only put the 6.0(1) upgrade file, IPS-K9-6.0-1-E1.pkg, on the automatic update server, AIM-IPS downloads and tries to install it, which is the incorrect file for AIM-IPS.

Refer to Updating the Sensor Automatically for more information on the IDM procedure for upgrading the sensor automatically

## Use the auto-upgrade Command

See the Upgrade Command and Options section of this document for the **auto-update** commands.

Complete these steps in order to schedule automatic upgrades:

1. Log in to the CLI using an account with administrator privileges.
2. Configure the Sensor to automatically look for new upgrades in your upgrade directory.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#auto-upgrade-option enabled
```

3. Specify the scheduling:

- ◆ For calendar scheduling, which starts upgrades at specific times on specific days:

```
sensor(config-hos-ena)#schedule-option calendar-schedule
sensor(config-hos-ena-cal)#days-of-week sunday
sensor(config-hos-ena-cal)#times-of-day 12:00:00
```

- ◆ For periodic scheduling, which starts upgrades at specific periodic intervals:

```
sensor(config-hos-ena)#schedule-option periodic-schedule
sensor(config-hos-ena-per)#interval 24
sensor(config-hos-ena-per)#start-time 13:00:00
```

4. Specify the IP address of the file server:

```
sensor(config-hos-ena-per)#exit
sensor(config-hos-ena)#ip-address 10.1.1.1
```

5. Specify the directory where the upgrade files are located on the file server:

```
sensor(config-hos-ena)#directory /tftpboot/update/5.0_dummy_updates
```

6. Specify the username for authentication on the file server:

```
sensor(config-hos-ena)#user-name tester
```

7. Specify the password of the user:

```
sensor(config-hos-ena)#password
```

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

8. Specify the file server protocol:

```
sensor(config-hos-ena)#file-copy-protocol ftp
```

**Note:** If you use SCP, you must use the **ssh host-key** command to add the server to the SSH known hosts list so the Sensor can communicate with it through SSH. Refer to Adding Hosts to the Known Hosts List for the procedure.

9. Verify the settings:

```
sensor(config-hos-ena)#show settings

enabled

-----

schedule-option

-----

periodic-schedule

-----

start-time: 13:00:00

interval: 24 hours

-----

-----

ip-address: 10.1.1.1

directory: /tftpboot/update/5.0_dummy_updates

user-name: tester

password: <hidden>

file-copy-protocol: ftp default: scp

-----
```

```
sensor(config-hos-ena)#
```

10. Exit auto-upgrade submode:

```
sensor(config-hos-ena)#exit
sensor(config-hos)#exit
```

```
Apply Changes:?[yes]:
```

11. Press **Enter** to apply the changes or type **no** to discard them.

## Re-image the Sensor

You can reimage your Sensor in these ways:

- For IDS appliances with a CD-ROM drive, use the recovery/upgrade CD.

Refer to the Using the Recovery/Upgrade CD section of Upgrading, Downgrading, and Installing System Images for the procedure.

- For all Sensors, use the **recover** command.

Refer to the Recovering the Application Partition section of Upgrading, Downgrading, and Installing System Images for the procedure.

- For the IDS–4215, IPS–4240, and IPS 4255, use ROMMON to restore the system image.

Refer to the Installing the IDS–4215 System Image and Installing the IPS–4240 and IPS–4255 System Image sections of Upgrading, Downgrading, and Installing System Images for the procedures.

- For NM–CIDS, use the bootloader.

Refer to the Installing the NM–CIDS System Image section of Upgrading, Downgrading, and Installing System Images for the procedure.

- For IDSM–2, reimage the application partition from the maintenance partition.

Refer to the Installing the IDSM–2 System Image section of the Upgrading, Downgrading, and Installing System Images for the procedure.

- For AIP–SSM, reimage from the ASA using the **hw–module module 1 recover [configure | boot]** command.

Refer to the Installing the AIP–SSM System Image section of Upgrading, Downgrading, and Installing System Images for the procedure.

---

## Related Information

- [Cisco Intrusion Prevention System Support Page](#)
- [Upgrading, Downgrading, and Installing System Images for IPS 6.0](#)
- [Cisco Catalyst 6500 Series Intrusion Detection System \(IDSM–2\) Module Support Page](#)
- [Password Recovery Procedure for the Cisco IDS Sensor and IDS Services Modules 1, IDSM–2\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 12, 2009

Document ID: 88954

---