# Upgrading, Downgrading, and Installing System Images

Table Of Contents


Upgrading, Downgrading, and Installing System Images

Overview

Upgrading the Sensor

Overview

Upgrade Command and Options

Using the Upgrade Command

Upgrading the Recovery Partition

Configuring Automatic Upgrades

Overview

UNIX-Style Directory Listings

Auto-upgrade Command and Options

Using the auto-upgrade Command

Downgrading the Sensor

Recovering the Application Partition

Overview

Using the Recover Command

Installing System Images

Overview

Installing the IDS-4215 System Image

Upgrading the IDS-4215 BIOS and ROMMON

Installing the IPS-4240 and IPS-4255 System Image

Using the Recovery/Upgrade CD

Installing the NM-CIDS System Image

Overview

Installing the NM-CIDS System Image

Upgrading the Bootloader

Installing the IDSM-2 System Image

Installing the System Image

Configuring the Maintenance Partition

Upgrading the Maintenance Partition

Installing the AIP-SSM System Image



Download this chapter

Upgrading, Downgrading, and Installing System Images

[+] Feedback


## Upgrading, Downgrading, and Installing System Images

This chapter describes how to upgrade, downgrade, and install system images. It contains the following sections:


- Overview
- Upgrading the Sensor
- Configuring Automatic Upgrades
- Downgrading the Sensor
- Recovering the Application Partition
- Installing System Images


### Overview

You can upgrade and downgrade the software on the sensor. Upgrading applies a service pack, signature update, minor version, major version, or recovery partition file. Downgrading removes the last applied upgrade from the sensor.


**GoSecure, Inc.**
**Exhibit 2009**
**CrowdStrike v. GoSecure**
**IPR2025-00068**

Ex. 2009-001

**Caution** You cannot use the **downgrade** command to go from 5.0 to 4.x. To revert to 4.x, you must reimage the sensor. You can use the **downgrade** command for releases after 5.0(1).

You can recover the application partition image on your sensor if it becomes unusable. Using the **recover** command lets you retain your host settings while other settings revert to the factory defaults.

To install a new system image on the sensor, use the recovery /upgrade CD, ROMMON, the bootloader/helper file, or the maintenance partition depending on which platform you have.

When you install a new system image on your sensor, all accounts are removed and the default cisco account is reset to use the default password "cisco." After installing the system image, you must initialize the sensor again. For the procedure, see Initializing the Sensor.

After you reimage and initialize your sensor, upgrade your sensor with the most recent service pack, signature update, minor version, major version, and recovery partition file. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

### Upgrading the Sensor

This section explains how to use the **upgrade** command to upgrade the software on the sensor. It contains the following topics:

- Overview
- Upgrade Command and Options
- Using the Upgrade Command
- Upgrading the Recovery Partition

### Overview

You can upgrade the sensor with the following files, all of which have the extension .pkg:

- Signature updates, for example, IPS-sig-S150-minreq-5.0-1.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

Upgrading the sensor 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.

The following options apply:

- **default**— Sets the value back to the system default setting.
- **directory**— Directory where upgrade files are located on the file server.

A leading `/' indicates an absolute path.

- **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. For the procedure, see Adding Hosts to the Known Hosts List.

- **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**—Configure the days of the week and times of day that automatic upgrades will be performed.

**days-of-week**—Days of the week on which auto-upgrades will be 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 day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.

– **periodic-schedule**—Configure 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.

### Using the Upgrade Command

To upgrade the sensor, follow these steps:

---

**Step 1** Download the major update file (IPS-K9-maj-6.0-1-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 Cisco IPS Software.

---

**Note** You must log in to Cisco.com using an account with cryptographic privileges to download the file. Do not change the file name. You must preserve the original file name for the sensor to accept the update. For the procedure for obtaining an account with cryptographic privileges, refer to *Release Notes for Cisco Intrusion Prevention System 5.0*.

---

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

**Step 3** Enter configuration mode:

```
sensor# configure terminal
```

**Step 4** Upgrade the sensor:

```
sensor# configure terminal

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

**Step 5** Enter the password when prompted:

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

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

**Step 6** 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 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: AIP-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#
```

---

### Upgrading the Recovery Partition

Use the **upgrade** command to upgrade the recovery partition with the most recent version so that it is ready if you need to recover the application partition on your sensor.

**Note** Recovery partition images are generated for major and minor software releases and only in rare situations for service packs or signature updates.

**Note** To upgrade the recovery partition the sensor must already be running version 5.0(1) or later.

To upgrade the recovery partition on your sensor, follow these steps:

**Step 1** Download the recovery partition image file (IPS-K9-r-1.1-a-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 Cisco IPS Software.

**Caution** Some browsers add an extension to the filename. The filename of the saved file must match what is displayed on the download page or you cannot use it to upgrade the recovery partition.

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

**Step 3** Enter configuration mode:

```
sensor# configure terminal
```

**Step 4** Upgrade the recovery partition:

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-5.0-1.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-5.0-1.pkg
```

**Step 5** Type the server password.

The upgrade process begins.

**Note** This procedure only reimages the recovery partition. The application partition is not modified by this upgrade. To reimage the application partition after the recovery partition, use the **recover application-partition** command. For the procedure, see Using the Recover Command.

### Configuring Automatic Upgrades

This section describes how to configure the sensor to automatically look for upgrades in the upgrade directory. It contains the following topics:

- Overview
- UNIX-Style Directory Listings
- Auto-upgrade Command and Options
- Using the auto-upgrade Command

#### Overview

You can configure the sensor to look for new upgrade files in your upgrade directory automatically.

You must download the software upgrade from Cisco.com and copy it to the upgrade directory before the sensor can poll for automatic upgrades. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

#### UNIX-Style Directory Listings

To configure automatic update using an FTP server, the FTP server must provide directory listing responses in UNIX style. MS-DOS style directory listing is not supported by the sensor automatic update feature.

**Note** If the server supplies MS-DOS style directory listings, the sensor cannot parse the directory listing and does not know that there is a new update available.

To change Microsoft IIS to use UNIX-style directory listings, follow these steps:

**Step 1** **Choose Start > Program Files > Administrative Tools**.

**Step 2** Click the **Home Directory** tab.

**Step 3** Click the **UNIX directory listings style** radio button.

---

### Auto-upgrade Command and Options

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

The following options apply:

- **default**— Sets the value back to the system default setting.
- **directory**— Directory where upgrade files are located on the file server.

A leading `/' indicates an absolute path.

- **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. For the procedure, see Adding Hosts to the Known Hosts List.

---

- **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**—Configure the days of the week and times of day that automatic upgrades will be performed.

**days-of-week**—Days of the week on which auto-upgrades will be 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 day at which auto-upgrades will begin. You can select multiple times. The valid value is *hh:mm[:ss]*.

– **periodic-schedule**—Configure 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.

### Using the auto-upgrade Command

To schedule automatic upgrades, follow these steps:

---

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

**Step 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
```

**Step 3** Specify the scheduling:

**a.** For calendar scheduling, which starts upgrades at specific times on specific day:

```
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
```

**b.** 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
```

**Step 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
```

**Step 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
```

**Step 6** Specify the username for authentication on the file server:

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

**Step 7** Specify the password of the user:

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

Enter password[]: ******

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

**Step 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. For the procedure, see Adding Hosts to the Known Hosts List.

---

**Step 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)#
```

**Step 10** Exit auto upgrade submode:

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

sensor(config-hos)# exit

Apply Changes:?[yes]:
```

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

---

### Downgrading the Sensor

Use the **downgrade** command to remove the last applied upgrade from the sensor.

---

**Caution** You cannot use the **downgrade** command to go from 5.0 to 4.x. To revert to 4.x, you must reimage the sensor. You can use the **downgrade** command for releases after 5.0(1).

---

To remove the last applied upgrade from the sensor, follow these steps:

---

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

**Step 2** Enter global configuration mode:

```
sensor# configure terminal
```

**Step 3** Downgrade the sensor:

```
sensor(config)# downgrade

Warning: Executing this command will reboot the system and downgrade to
IPS-K9-sp.5.0-2.pkg. Configuration changes made since the last upgrade will be lost and
the system may be rebooted.

Continue with downgrade?:
```

**Step 4** Type yes to continue with the downgrade.

**Step 5** If there is no recently applied service pack or signature update, the **downgrade** command is not available:

```
sensor(config)# downgrade

No downgrade available.

sensor(config)#
```

### Recovering the Application Partition

This section explains how to recover the application partition, and contains the following topics:

- Overview
- Using the Recover Command

#### Overview

You can recover the application partition image for the appliance if it becomes unusable. Some network configuration information is retained when you use this method, which lets you have network access after the recovery is performed.

Use the **recover application-partition** command to boot to the recovery partition, which automatically recovers the application partition on your appliance.

**Note** If you have upgraded your recovery partition to the most recent version before you recover the application partition image, you can install the most up-to-date software image. For the procedure for upgrading the recovery partition to the most recent version, see Upgrading the Recovery Partition.

Because you can execute the **recover application-partition** command through a Telnet or SSH connection, we recommend using this command to recover sensors that are installed at remote locations.

**Note** If the appliance supports it, you can also use the recovery/upgrade CD to reinstall both the recovery and application partitions. For the procedure, see Using the Recovery/Upgrade CD.

**Note** When you reconnect to the sensor after recovery, you must log in with the default username and password `cisco`.

#### Using the Recover Command

To recover the application partition image, follow these steps:

**Step 1** Download the recovery partition image file (IPS-K9-r-1.1-a-5.0-2.pkg) to the tftp root directory of a TFTP server that is accessible from your sensor.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Note** Make sure you can access the TFTP server location from the network connected to your sensor's Ethernet port.

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

**Step 3** Enter configuration mode:

```
sensor# configure terminal
```

**Step 4** Recover the application partition image:

```
sensor(config)# recover application-partition

Warning: Executing this command will stop all applications and re-image the node to
version 5.0(0.27)S91(0.27). All configuration changes except for network settings will be
```

```
reset to default.

Continue with recovery? []:
```

**Step 5** Type **yes** to continue.

Shutdown begins immediately after you execute the **recover** command. Shutdown can take a while, and you will still have access to the CLI, but access will be terminated without warning.

The application partition is reimaged using the image stored on the recovery partition. You must now initialize the appliance with the **setup** command. For the procedure, see Initializing the Sensor.

**Note** The IP address, netmask, access lists, time zone, and offset are saved and applied to the reimaged application partition. If you executed the **recover application-partition** command remotely, you can SSH to the sensor with the default username and password (cisco/cisco) and then initialize the sensor again with the **setup** command. You cannot use Telnet until you initialize the sensor because Telnet is disabled by default.

If you cannot access the CLI to execute the **recover application-partition** command, you can reboot the sensor and select the option from the boot menu during the bootup process. This lets you boot to the recovery partition and reimage the application partition. Executing the **recovery** command in this way requires console or keyboard and monitor access to the sensor, which is possible on the appliances and NM-CIDS, but not on the IDSM-2 or AIP-SSM.

### Installing System Images

This section contains the procedures for installing system images on the appliances and modules. It contains the following topics:

- Overview
- Installing the IDS-4215 System Image
- Upgrading the IDS-4215 BIOS and ROMMON
- Installing the IPS-4240 and IPS-4255 System Image
- Using the Recovery/Upgrade CD
- Installing the NM-CIDS System Image
- Installing the IDSM-2 System Image
- Installing the AIP-SSM System Image

#### Overview

**Caution** All user configuration settings are lost when you install the system image. Before trying to recover the sensor by installing the system image, try to recover by using the **recover application-partition** command or by selecting the recovery partition during sensor bootup. For the procedure, see Recovering the Application Partition.

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. Be aware that some TFTP servers limit the maximum file size that can be transferred to ~32 MB.

#### Installing the IDS-4215 System Image

You can install the IDS-4215 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

**Caution** Before installing the system image, you must first upgrade the IDS-4215 BIOS to version 5.1.7 and the ROMMON to version 1.4 using the upgrade utility file IDS-4215-bios-5.1.7-rom-1.4.bin. For the procedure, see Upgrading the IDS-4215 BIOS and ROMMON.

To install the IDS-4215 system image, follow these steps:

**Step 1** Download the IDS-4215 system image file (IPS-4215-K9-sys-1.1-a-5.0-1.img) to the tftp root directory of a TFTP server that is accessible from your IDS-4215.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

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

**Step 2** Boot IDS-4215.

**Step 3** Press **Ctrl-R** at the following prompt while the system is booting:

```
Evaluating Run Options...
```

**Note** You have five seconds to press **Ctrl-R**.

The console display resembles the following:

```
CISCO SYSTEMS IDS-4215

Embedded BIOS Version 5.1.7 02/23/04 15:50:39.31

Compiled by dnshep

Evaluating Run Options ...

Cisco ROMMON (1.4) #3: Mon Feb 23 15:52:45 MST 2004

Platform IDS-4215

Image Download Memory Sizing ..................................................

Available Image Download Space: 510MB

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: 0000.0001.0001

Use ? for help.

rommon>
```

**Step 4** Verify that IDS-4215 is running BIOS version 5.1.7 or later and ROMMON version 1.4 or later.

**Note** If IDS-4215 does not have the correct BIOS and ROMMON versions, you must upgrade the BIOS and ROMMON before reimaging. For the procedure, see Upgrading the IDS-4215 BIOS and ROMMON.

The current versions are shown in the console display information identified in Step 3.

**Step 5** If necessary, change the port used for the TFTP download:

```
rommon> interface port_number
```

The port in use is listed just before the rommon prompt. In the example, port 1 is being used as noted by the text, `Using 1: i82557 @ PCI(bus:0 dev:14 irq:11),` MAC: 0000.0001.0001.

**Note** The default port used for TFTP downloads is port 1, which corresponds with the command and control interface of IDS-4215.

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

**Step 6** 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 7** Specify the TFTP server IP address:

```
rommon> server ip_address
```

**Step 8** Specify the gateway IP address:

```
rommon> gateway ip_address
```

**Step 9** 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 10** Specify the path and filename on the TFTP file server from which you are downloading the image:

rommon> file *path/filename*

UNIX example:

rommon> **file /system_images/IDS-4215-K9-sys-1.1-a-5.0-1.img**

**Note** The path is relative to the UNIX TFTP server's default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the file location.

Windows example:

rommon> **file C:***tftp_directory***IDS-4215-K9-sys-1.1-a-5.0-1.img**

**Step 11** Download and install the system image:

rommon> **tftp**

**Note** IDS-4215 reboots several times during the reimaging process. Do not remove power from IDS-4215 during the update process or the upgrade can become corrupted.

### Upgrading the IDS-4215 BIOS and ROMMON

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 Cisco IPS Software.

**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.

### Installing the IPS-4240 and IPS-4255 System Image

You can install the IPS-4240 and IPS-4255 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

**Note** This procedure is for IPS-4240, but is also applicable to IPS-4255. The system image for IPS-4255 has "4255" in the filename.

To install the IPS-4240 and IPS-4255 system image, follow these steps:

**Step 1** Download the IPS-4240 system image file (IPS-4240-K9-sys-1.1-a-5.0-1.img) to the tftp root directory of a TFTP server that is accessible from your IPS-4240.

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Note** Make sure you can access the TFTP server location from the network connected to your IPS-4240's Ethernet port.

**Step 2** Boot IPS-4240.

The console display resembles the following:

```
Booting system, please wait...

CISCO SYSTEMS

Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90

Low Memory: 631 KB

High Memory: 2048 MB
```

```
PCI Device Table.
Bus Dev Func VendID DevID Class              Irq
00  00  00   8086   2578  Host Bridge
00  01  00   8086   2579  PCI-to-PCI Bridge
00  03  00   8086   257B  PCI-to-PCI Bridge
00  1C  00   8086   25AE  PCI-to-PCI Bridge
00  1D  00   8086   25A9  Serial Bus         11
00  1D  01   8086   25AA  Serial Bus         10
00  1D  04   8086   25AB  System
00  1D  05   8086   25AC  IRQ Controller
00  1D  07   8086   25AD  Serial Bus         9
00  1E  00   8086   244E  PCI-to-PCI Bridge
00  1F  00   8086   25A1  ISA Bridge
00  1F  02   8086   25A3  IDE Controller     11
00  1F  03   8086   25A4  Serial Bus         5
00  1F  05   8086   25A6  Audio              5
02  01  00   8086   1075  Ethernet           11
03  01  00   177D   0003  Encrypt/Decrypt    9
03  02  00   8086   1079  Ethernet           9
03  02  01   8086   1079  Ethernet           9
03  03  00   8086   1079  Ethernet           9
03  03  01   8086   1079  Ethernet           9
04  02  00   8086   1209  Ethernet           11
04  03  00   8086   1209  Ethernet           5
Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004
Platform IPS-4240-K9
Management0/0
MAC Address: 0000.c0ff.ee01
```

**Step 3** Press **Break** or **Esc** at the following prompt while the system is booting to interrupt boot. Press the spacebar to begin boot immediately.

---

**Note** You have ten seconds to press **Break** or **Esc**.

---

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

The system enters ROMMON mode. The `rommon>` prompt appears.

**Step 4** Check the current network settings:

```
rommon> set
```

The output on the configured system resembles the following:

```
ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
      PORT=Management0/0
      VLAN=untagged
      IMAGE=
```

```
CONFIG=
```

The variables have the following definitions:

- Address—Local IP address of IPS-4240
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by IPS-4240
- Port—Ethernet interface used for IPS-4240 management
- VLAN—VLAN ID number (leave as untagged)
- Image—System image file and pathname
- Config—Unused by these platforms

**Note** Not all values are required to establish network connectivity. The address, server, gateway, and image values are required. If you are not sure of the settings needed for your local environment, contact your system administrator.

**Step 5** If necessary, change the interface used for the TFTP download:

**Note** The default interface used for TFTP downloads is Management0/0, which corresponds to the MGMT interface of IPS-4240.

```
rommon> PORT=interface_name
```

**Step 6** If necessary, assign an IP address for the local port on IPS-4240:

```
rommon> ADDRESS=ip_address
```

**Note** Use the same IP address that is assigned to IPS-4240.

**Step 7** If necessary, assign the TFTP server IP address:

```
rommon> SERVER=ip_address
```

**Step 8** If necessary, assign the gateway IP address:

```
rommon> GATEWAY=ip_address
```

**Step 9** Verify that you have access to the TFTP server by pinging it from your local Ethernet port with one of the following commands:

```
rommon> ping server_ip_address
```

```
rommon> ping server
```

**Step 10** If necessary define the path and filename on the TFTP file server from which you are downloading the image:

```
rommon> IMAGE=path/file_name
```

**Caution** Make sure that you enter the **IMAGE** command in all uppercase. You can enter the other ROMMON commands in either lower case or upper case, but the **IMAGE** command specifically must be all uppercase.

UNIX example:

```
rommon> IMAGE=/system_images/IPS-4240-K9-sys-4.1-4-S91.img
```

**Note** The path is relative to the UNIX TFTP server's default tftpboot directory. Images located in the default tftpboot directory do not have any directory names or slashes in the IMAGE specification.

Windows example:

```
rommon> IMAGE=C:\system_images\IPS-4240-K9-sys-4.1-4-S91.img
```

**Step 11** Type **set** and press **Enter** to verify the network settings.

**Note** You can use the **sync** command to store these settings in NVRAM so they are maintained across boots. Otherwise, you must type this information each time you want to boot an image from ROMMON.

**Step 12** Download and install the system image:

```
rommon> tftp
```

**Caution** To avoid corrupting the system image, do not remove power from IPS-4240 while the system image is being installed.

**Note** If the network settings are correct, the system downloads and boots the specified image on IPS-4240. Be sure to use the IPS-4240 image.

### Using the Recovery/Upgrade CD

You can use the recovery/upgrade CD on appliances that have a CD-ROM, such as the IDS-4210, IDS-4235, and IDS-4250. The recovery/upgrade CD reimages both the recovery and application partitions.

**Caution** You are installing a new software image. All configuration data is overwritten.

After you install the system image with the recovery/upgrade CD, you must use the **setup** command to initialize the appliance. You will need your configuration information. You can obtain this information by generating a diagnostics report through IDM.

Signature updates occur approximately every week or more often if needed. The most recent signature update will not be on the recovery/upgrade CD that shipped with your appliance. Download the most recent signature update and apply it after you have recovered the system image.

To recover the system image with the recovery/upgrade CD, follow these steps:

**Step 1** Obtain your configuration information from IDM:

**a.** To access IDM, point your browser to the appliance you are upgrading.

**b.** Select **Monitoring > Diagnostics**. The Diagnostics panel appears.

**c.** Click **Run Diagnostics**. Running the diagnostics may take a while.

**d.** Click **View Results**. The results are displayed in a report.

**e.** To save the diagnostics report, select **Menu > Save As** in your browser.

**Step 2** Insert the recovery/upgrade CD into the CD-ROM drive.

**Step 3** Power off the appliance and then power it back on. The boot menu appears, which lists important notices and boot options.

**Step 4** Type **k** if you are installing from a keyboard, or type **s** if you are installing from a serial connection.

**Note** A blue screen is displayed for several minutes without any status messages while the files are being copied from the CD to your appliance.

**Step 5** Log in to the appliance by using a serial connection or with a monitor and keyboard.

**Note** The default username and password are both cisco.

**Step 6** You are prompted to change the default password.

**Note** Passwords must be at least eight characters long and be strong, that is, not be a dictionary word.

After you change the password, the `sensor#` prompt appears.

**Step 7** Type the **setup** command to initialize the appliance. For the procedure, see Initializing the Sensor.

**Step 8** Install the most recent service pack and signature update. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

### Installing the NM-CIDS System Image

This section describes how to install the NM-CIDS system image, and contains the following topics:


- Overview
- Installing the NM-CIDS System Image
- Upgrading the Bootloader


### Overview

You can reimage the NM-CIDS using the system image file (IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.pkg). Before you can use the system image file, you must upgrade the bootloader in one of the following ways:

**Note** If NM-CIDS is already running version 5.0, the bootloader has been upgraded. You only need to upgrade the bootloader when upgrading from 4.x to 5.0.

- Instead of installing the system image, use the **upgrade** command to upgrade from 4.x to 5.0 using the major upgrade file (IPS-K9-maj-5.0-1-S149.rpm.pkg).

The 5.0 upgrade also updates the bootloader with the new bootloader file (servicesengine-boot-1.0-17-1_dev.bin), then reimages the hard-disk drive with the new image.

We recommend that you use the **upgrade** command.

- Manually upgrade the boot loader

You must first boot to the old helper file where there is an option to update the boot loader in the helper menu. Then you reboot and reimage the hard-disk drive. Refer to in the 4.x documentation.

**Caution** The 5.0 system image does not work with the old bootloader.

You no longer need to boot to the helper to load the 5.0 system image. The 5.0 system image contains everything needed to reimage the NM-CIDS.

The new bootloader works with the 4.x system image; however, you must boot to the helper to load it.

**Caution** If you upgrade the bootloader, make sure you have the correct file. NM-CIDS does not check to verify that you have the correct file. If you upgrade with the wrong file, when you reboot, NM-CIDS will be inaccessible and you will have to RMA it.

### Installing the NM-CIDS System Image

**Caution** The NM-CIDS bootloader must be at 1.0.17-1 before installing the 5.0 system image file. For the procedure if needed, see Upgrading the Bootloader.

**Note** The bootloader has a timeout of 10 minutes, which means reimages over slow WAN links will fail. To avoid this situation, download the bootloader file to a local TFTP server and have the NM-CIDS reimage from the local TFTP server.

To reimage NM-CIDS, follow these steps:

**Step 1** Download the NM-CIDS system image file (IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.pkg) to the TFTP root directory of a TFTP server that is accessible from your NM-CIDS. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Note** Make sure you can access the TFTP server location from the network connected to your NM-CIDS' Ethernet port.

**Step 2** Log in to the router.

**Step 3** Enter enable mode:

```
router# enable

router(enable)#
```

**Step 4** Session to NM-CIDS:

```
router(enable)# service-module IDS-Sensor slot_number/0 session
```

**Note** Use the **show configuration | include interface IDS-Sensor** command to determine the NM-CIDS slot number.

**Step 5** Suspend the session by pressing **Shift-Ctrl-6 X**. You will see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

**Step 6** Reset NM-CIDS:

```
router(enable)# service-module IDS-Sensor slot_number/0 reset
```

You are prompted to confirm the **reset** command.

**Step 7** Press **Enter** to confirm.

**Step 8** Press **Enter** to resume the suspended session. After displaying its version, the bootloader displays this prompt for 15 seconds:

```
Please enter '***' to change boot configuration:
```

**Step 9** Type *** during the 15-second delay. The bootloader prompt appears.

**Step 10** Display the bootloader configuration:

```
ServicesEngine boot-loader> show config
```

**Caution** If the bootloader version is not 1.0.17-1, you must upgrade it before installing 5.0. For the procedure, see Upgrading the Bootloader.

**Step 11** Configure the bootloader parameters:

```
ServicesEngine boot-loader> config
```

**Step 12** You are prompted for each value line by line.

**a.** Specify the IP address—The external fast Ethernet port on NM-CIDS. This must be a real IP address on your network.

**b.** Specify the subnet mask—The external fast Ethernet port on NM-CIDS. This must be a real IP address on your network.

**c.** Specify the TFTP server IP address—The IP address of the TFTP server from which to download the NM-CIDS system image.

**d.** Specify the gateway IP address—The IP address of the default gateway for hosts on your subnet.

**e.** Specify the default helper file—The name of the helper image to boot. The NM-CIDS helper file is boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img.

**Note** 4.x had a separate helper file, NM-CIDS-K9-helper-1.0-1.bin, but in 5.0 the system image file is its own helper file.

**f.** Specify the Ethernet interface—The Ethernet interface is always set to **external**.

**g.** Specify the default boot device—The default boot device is always set to **disk**.

**h.** Specify the default bootloader—The default bootloader is always set to **primary**.

If you made any changes, the bootloader stores them permanently. The bootloader command prompt appears.

**Caution** The next step erases all data from the NM-CIDS hard-disk drive.

**Step 13** Boot the system image:

```
ServicesEngine boot-loader> boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img
```

The bootloader displays a spinning line while loading the system image from the TFTP server. When the system image is loaded, it is booted. The system image installs IPS 5.0(1) on NM-CIDS. When the installation is complete, NM-CIDS reboots. The system is restored to default settings. The user account and password are set to `cisco`.

You must initialize NM-CIDS with the **setup** command. For the procedure, see Initializing the Sensor.

### Upgrading the Bootloader

The NM-CIDS bootloader executes immediately after BIOS completes its POST. The bootloader that originally shipped on NM-CIDS is 1.0.5. This version cannot launch IPS 5.0(1).

**Note** We recommend you upgrade your NM-CIDS to 5.0(1) by applying the 5.0(1) upgrade package (IPS-K9-maj-5.0-1-S149.rpm.pkg). When the upgrade package is applied, the configuration is migrated and the bootloader is upgraded to version 1.0.17-1. For the procedure to use the **upgrade** command, see Upgrading the Sensor. If you upgrade your NM-CIDS with the upgrade file, in the future you will not need to upgrade the bootloader before performing a system upgrade.

The NM-CIDS system image (IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img) does not migrate your existing configuration or upgrade the bootloader. Therefore, you must first manually install bootloader version 1.0.17-1.

The 1.0.17-1 bootloader is backwards compatible with the 1.0.5 bootloader. This means you can boot the IDS 4.1 image with bootloader version 1.0.17-1.

**Note** The bootloader has a timeout of 10 minutes, which means reimages over slow WAN links will fail. To avoid this situation, download the bootloader file to a local TFTP server and have the NM-CIDS reimage from the local TFTP server.

To upgrade the bootloader, follow these steps:

**Step 1** Download the bootloader file (servicesengine-boot-1.0-17-1_dev.bin) and the helper file (NM-CIDS-K9-helper-1.0-1.bin) to the TFTP root directory of a TFTP server that is accessible from your NM-CIDS. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Note** Make sure you can access the TFTP server location from the network connected to your NM-CIDS' Ethernet port.

**Step 2** Log in to the router.

**Step 3** Enter enable mode:

```
router# enable

router(enable)#
```

**Step 4** Session to NM-CIDS:

```
router(enable)# service-module IDS-Sensor slot_number/0 session
```

Use the **show configuration | include interface IDS-Sensor** command to determine which slot NM-CIDS is in.

**Step 5** Suspend the session by pressing **Shift-Ctrl-6 X**. You will see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

**Step 6** Reset NM-CIDS:

```
router(enable)# service-module IDS-Sensor slot_number/0 reset
```

You are prompted to confirm the **reset** command.

**Step 7** Press **Enter** to confirm.

**Step 8** Press **Enter** to resume the suspended session. After displaying its version, the bootloader displays this prompt for 15 seconds:

```
Please enter '***' to change boot configuration:
```

**Step 9** Type *** during the 15-second delay. The bootloader prompt appears.

**Step 10** Display the bootloader configuration:

```
ServicesEngine boot-loader> show config
```

**Step 11** Configure the bootloader parameters:

```
ServicesEngine boot-loader> config
```

**Step 12** You are prompted for each value line by line.

**a.** Specify the IP address—The external fast Ethernet port on NM-CIDS. This must be a real IP address on your network.

**b.** Specify the subnet mask—The external fast Ethernet port on NM-CIDS. This must be a real IP address on your network.

**c.** Specify the TFTP server IP address—The IP address of the TFTP server from which to download the NM-CIDS system image.

**d.** Specify the gateway IP address—The IP address of the default gateway for hosts on your subnet.

**e.** Specify the default helper file—The name of the helper image to boot. The NM-CIDS helper file is NM-CIDS-K9-helper-1.0-1.bin.

**f.** Specify the Ethernet interface—The Ethernet interface is always set to **external**.

**g.** Specify the default boot device—The default boot device is always set to **disk**.

**h.** Specify the default bootloader—The default bootloader is always set to **primary**.

If you made any changes, the bootloader stores them permanently.

**Step 13** Boot the helper image:

```
ServicesEngine boot-loader># boot helper NM-CIDS-K9-helper-1.0-1.bin
```

The bootloader displays a spinning line while loading the helper image from the TFTP server. When the helper is loaded, it is booted. The NM-CIDS helper displays its main menu when it launches.

```
Cisco Systems, Inc.

Services engine helper utility for NM-CIDS

Version 1.0.17-1 [200305011547]

——-

Main menu

1 - Download application image and write to HDD

2 - Download bootloader and write to flash

3 - Display software version on HDD

4 - Display total RAM size

5 - Change file transfer method (currently secure shell)

r - Exit and reset Services Engine

h - Exit and shutdown Services Engine

Selection [1234rh]:
```

**Step 14** Choose the transfer method (SSH is the default):

**a.** For SSH, continue with Step 15.

**b.** For TFTP, continue with Steps 16 and 17.

**Step 15** Download the bootloader image and write it to flash:

**a.** Type 2.

**b.** Specify the SSH server username and password.

**c.** Type the SSH server IP address.

**d.** Type the full pathname of bootloader image from the root directory:

```
Selection [1234rh]:servicesengine-boot-1.0-17-1_dev.bin

Ready to begin

Are you sure? y/n
```

**e.** Type y to continue.

```
The operation was successful
```

You are returned to the main menu with the `Selection [1234rh]:` prompt. Continue with Step 18.

**Step 16** Configure TFTP as the transfer method:

**a.** Type 5.

**b.** Type 2 to change to TFTP.

**c.** Type r to return to the Main menu.

**Step 17** Download the bootloader image and write it to flash:

**a.** Type 2.

**b.** Type the TFTP server IP address.

**c.** Type the path from the TFTP root directory:

```
Selection [1234rh]:servicesengine-boot-1.0-17-1_dev.bin

Ready to begin

Are you sure? y/n
```

**d.** Type y to continue.

You are returned to the main menu with the `Selection [1234rh]:` prompt. Continue with Step 18.

**Step 18** Type r to reboot NM-CIDS:

```
Selection [1234rh]: r

About to exit and reset Services Engine.

Are you sure? [y/N]
```

**Step 19** Type **y** to confirm. The bootloader is now upgraded to version 1.0.17-1. Continue only if you want to install the NM-CIDS system image now.

**Step 20** After BIOS POST is completed on NM-CIDS, when you see the following message, type three asterisks:

```
Please enter '***' to change boot configuration:
```

**Caution** The next step erases all data from the NM-CIDS hard-disk drive.

The boot loader prompt appears.

**Step 21** Boot the NM-CIDS system image:

```
ServicesEngine boot-loader> boot helper IPS-NM-CIDS-K9-sys-1.1-a-5.0-1.img
```

The bootloader displays a spinning line while loading the system image from the TFTP server. When the system image is loaded, it is booted. The system image installs IPS 5.0(1) on NM-CIDS. When the installation is complete, NM-CIDS reboots. The system is restored to all default settings. The user account and password are set to `cisco`.

You must initialize your NM-CIDS with the **setup** command. For the procedure, see Initializing the Sensor.

### Installing the IDSM-2 System Image

If the IDSM-2 application partition becomes unusable, you can reimage it from the maintenance partition. After you reimage the application partition of IDSM-2, you must initialize IDSM-2 using the **setup** command. For the procedure, see Initializing the Sensor.

When there is a new maintenance partition image file, you can reimage the maintenance partition from the application partition. This section describes how to reimage the application partition and maintenance partition for Catalyst software and Cisco IOS software.

This section contains the following topics:

- Installing the System Image
- Configuring the Maintenance Partition
- Upgrading the Maintenance Partition

### Installing the System Image

This section describes how to install the IDSM-2 system image, and contains the following topics:

- Catalyst Software
- Cisco IOS Software

### Catalyst Software

To install the system image, follow these steps:

**Step 1** Download the IDSM-2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz) to the FTP root directory of a FTP server that is accessible from your IDSM-2. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Step 2** Log in to the switch CLI.

**Step 3** Boot IDSM-2 to the maintenance partition:

```
cat6k> (enable) reset module_number cf:1
```

**Step 4** Log in to the maintenance partition CLI:

```
login: guest

Password: cisco
```

**Note** You must configure the maintenance partition on IDSM-2. For the procedure, see Configuring the Maintenance Partition.

**Step 5** Install the system image:

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
```

**Step 6** Specify the FTP server password. After the application partition file has been downloaded, you are asked if you want to proceed:

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

**Step 7** Type y to continue. When the application partition file has been installed, you are returned to the maintenance partition CLI.

**Step 8** Exit the maintenance partition CLI and return to the switch CLI.

**Step 9** Reboot IDSM-2 to the application partition:

```
cat6k> (enable) reset module_number hdd:1
```

**Step 10** When IDSM-2 has rebooted, check the software version. For the procedure, see Verifying IDSM-2 Installation.

**Step 11** Log in to the application partition CLI and initialize IDSM-2. For the procedure, see Initializing the Sensor.

---

### Cisco IOS Software

To install the system image, follow these steps:

---

**Step 1** Download the IDSM-2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz) to the TFTP root directory of a TFTP server that is accessible from your IDSM-2. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Step 2** Log in to the switch CLI.

**Step 3** Boot IDSM-2 to the maintenance partition:

```
router# hw-module module module_number reset cf:1
```

**Step 4** Session to the maintenance partition CLI:

```
router# session slot slot_number processor 1
```

**Step 5** Log in to the maintenance partition CLI:

```
login: guest

Password: cisco
```

---

**Note** You must configure the maintenance partition on IDSM-2. For the procedure, see Configuring the Maintenance Partition.

---

**Step 6** Install the system image:

```
guest@hostname.localdomain# upgrade
ftp://user@ftp_server_IP_address/directory_path/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz

–install
```

**Step 7** Specify the FTP server password. After the application partition file has been downloaded, you are asked if you want to proceed:

```
Upgrading will wipe out the contents on the hard disk.

Do you want to proceed installing it [y|n]:
```

**Step 8** Type y to continue. When the application partition file has been installed, you are returned to the maintenance partition CLI.

**Step 9** Exit the maintenance partition CLI and return to the switch CLI.

**Step 10** Reboot IDSM-2 to the application partition:

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

**Step 11** Verify that IDSM-2 is online and that the software version is correct and that the status is ok:

```
router# show module module_number
```

**Step 12** Session to the IDSM-2 application partition CLI:

```
router# session slot slot_number processor 1
```

**Step 13** Initialize IDSM-2. For the procedure, see Initializing the Sensor.

---

### Configuring the Maintenance Partition

This section describes how to configure the maintenance partition on IDSM-2, and contains the following topics:

- Catalyst Software
- Cisco IOS Software

### Catalyst Software

To configure the IDSM-2 maintenance partition, follow these steps:

---

**Step 1** Log in to the switch CLI.

**Step 2** Enter privileged mode:

```
cat6k# enable

cat6k(enable)#
```

**Step 3** Session to IDSM-2:

```
cat6k# session 9

Trying IDS-9...

Connected to IDS-9.

Escape character is '^]'.

Cisco Maintenance image
```

---

**Note** You cannot Telnet or SSH to the IDSM-2 maintenance partition.You must session to it from the switch CLI.

---

**Step 4** Log in as user guest and password cisco.

---

**Note** You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM-2 application partition for some reason, you will have to RMA IDSM-2.

---

```
login: guest

Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

**Step 5** View the IDSM-2 maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74

Subnet Mask     : 255.255.255.128

IP Broadcast    : 10.255.255.255

DNS Name        : idsm2.localdomain

Default Gateway : 10.89.149.126

Nameserver(s)   :

guest@idsm2.localdomain#
```

**Step 6** Clear the IDSM-2 maintenance partition host configuration (ip address, gateway, hostname):

```
guest@idsm2.localdomain# clear ip

guest@localhost.localdomain# show ip

IP address      : 0.0.0.0

Subnet Mask     : 0.0.0.0

IP Broadcast    : 0.0.0.0

DNS Name        : localhost.localdomain

Default Gateway : 0.0.0.0

Nameserver(s)   :

guest@localhost.localdomain#
```

**Step 7** Configure the maintenance partition host configuration:

**a.** Specify the IP address:

```
guest@localhost.localdomain# ip address ip_address netmask
```

**b.** Specify the default gateway:

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

**c.** Specify the hostname:

```
guest@localhost.localdomain# ip host hostname
```

**Step 8** View the maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74

Subnet Mask     : 255.255.255.128

IP Broadcast    : 10.255.255.255

DNS Name        : idsm2.localdomain

Default Gateway : 10.89.149.126

Nameserver(s)   :

guest@idsm2.localdomain#
```

**Step 9** Verify the image installed on the application partition:

```
guest@idsm2.localdomain# show images

Device name             Partition#              Image name

-----------             ----------              ----------

Hard disk(hdd)          1                       5.0(1)

guest@idsm2.localdomain#
```

**Step 10** Verify the maintenance partition version (including the BIOS version):

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)

mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :

integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL

Number of Pentium-class Processors : 2

BIOS Vendor: Phoenix Technologies Ltd.

BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB

Size of compact flash: 61 MB

Size of hard disk: 19077 MB

Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

**Step 11** Upgrade the application partition:

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz

Downloading the image. This may take several minutes...

Password for jsmith@10.89.146.114:

500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
(unknown size)

/tmp/upgrade.gz           [|]   28616K

29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file

ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
is downloaded.

Upgrading will wipe out the contents on the storage media.

Do you want to proceed installing it [y|N]:
```

**Step 12** Type y to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.

If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...

Applying the image, this process may take several minutes...

Performing post install, please wait...

Application image upgrade complete. You can boot the image now.

guest@idsm3.localdomain#
```

**Step 13** Display the upgrade log:

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005

Downloaded upgrade image

ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz

Extracted the downloaded file

Proceeding with image upgrade.

Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1

Fri Mar 11 21:22:06 2005 : Creating IDS application image file...

Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX

Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729

Fri Mar 11 21:22:06 2005 : image: 0000000029323770

Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770

Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1

Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz

Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1

Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1

Fri Mar 11 21:22:07 2005 : Initializing the hard disk...

Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)

Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)

Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.

Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.

Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.

Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.

Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.

Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.

Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...

Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.

Fri Mar 11 21:22:20 2005 : Performing post install, please wait...

Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.

Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.

Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.

Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.

Application image upgrade complete. You can boot the image now.

Partition upgraded successfully

guest@idsm2.localdomain#
```

**Step 14** Clear the upgrade log:

```
guest@idsm2.localdomain# clear log upgrade
```

```
Cleared log file successfully
```

**Step 15** Display the upgrade log:

```
guest@idsm2.localdomain# show log upgrade

guest@idsm2.localdomain#
```

**Step 16** Ping another computer:

```
guest@idsm2.localdomain# ping 10.89.146.114

PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.

64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec

64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec

64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec

64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec

64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms

guest@idsm2.localdomain#
```

**Step 17** Reset IDSM-2:

**Note** You cannot specify a partition when issuing the **reset** command from the maintenance partition. IDSM-2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, IDSM-2 boots to the application partition.

```
guest@idsm2.localdomain# reset

guest@idsm2.localdomain#

2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in progress. Do
not remove module until shutdown completes

Broadcast message from root Fri Mar 11 21:55:47 2005...

The system is going down for system halt NOW !!

cat6k> (enable)
```

### Cisco IOS Software

To configure the IDSM-2 maintenance partition, follow these steps:

**Step 1** Log in to the switch CLI.

**Step 2** Session to IDSM-2:

```
router# session slot 11 processor 1

The default escape character is Ctrl-^, then x.

You can also type 'exit' at the remote prompt to end the session

Trying 127.0.0.111 ... Open

Cisco Maintenance image
```

**Note** You cannot Telnet or SSH to the IDSM-2 maintenance partition.You must session to it from the switch CLI.

**Step 3** Log in as user guest and password cisco.

**Note** You can change the guest password, but we do not recommend it. If you forget the maintenance partition guest password, and you cannot log in to the IDSM-2 application partition for some reason, you will have to RMA IDSM-2.

```
login: guest
```

```
password: cisco
Maintenance image version: 2.1(2)
guest@idsm2.localdomain#
```

**Step 4** View the maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip
IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :
guest@idsm2.localdomain#
```

**Step 5** Clear the maintenance partition host configuration (ip address, gateway, hostname):

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip
IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :
guest@localhost.localdomain#
```

**Step 6** Configure the maintenance partition host configuration:

**a.** Specify the IP address:

```
guest@localhost.localdomain# ip address ip_address netmask
```

**b.** Specify the default gateway:

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

**c.** Specify the hostname:

```
guest@localhost.localdomain# ip host hostname
```

**Step 7** View the maintenance partition host configuration:

```
guest@idsm2.localdomain# show ip
IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :
guest@idsm2.localdomain#
```

**Step 8** Verify the image installed on the application partition:

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------               ----------
Hard disk(hdd)          1                       5.0(1)
guest@idsm2.localdomain#
```

**Step 9** Verify the maintenance partition version (including the BIOS version):

```
guest@idsm2.localdomain# show version
Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
```

```
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL

Number of Pentium-class Processors : 2

BIOS Vendor: Phoenix Technologies Ltd.

BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB

Size of compact flash: 61 MB

Size of hard disk: 19077 MB

Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

**Step 10** Upgrade the application partition:

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz

Downloading the image. This may take several minutes...

Password for jsmith@10.89.146.114:

500 'SIZE WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
(unknown size)

/tmp/upgrade.gz           [|]   28616K

29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file

ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz
is downloaded.

Upgrading will wipe out the contents on the storage media.

Do you want to proceed installing it [y|N]:
```

**Step 11** Type y to proceed with the upgrade.

```
Proceeding with upgrade. Please do not interrupt.

If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...

Applying the image, this process may take several minutes...

Performing post install, please wait...

Application image upgrade complete. You can boot the image now.

guest@idsm3.localdomain#
```

**Step 12** Display the upgrade log:

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005

Downloaded upgrade image

ftp://jsmith@10.89.146.114//RELEASES/Latest/5.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-5.0-1.bin.gz

Extracted the downloaded file

Proceeding with image upgrade.

Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1

Fri Mar 11 21:22:06 2005 : Creating IDS application image file...

Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX

Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729

Fri Mar 11 21:22:06 2005 : image: 0000000029323770

Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770

Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
```

```
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

**Step 13** Clear the upgrade log:

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

**Step 14** Display the upgrade log:

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

**Step 15** Ping another computer:

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec
--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

**Step 16** Reset IDSM-2:

---

**Note** You cannot specify a partition when issuing the **reset** command from the maintenance partition. IDSM-2 boots to whichever partition is specified in the boot device variable. If the boot device variable is blank, IDSM-2 boots to the application partition.

---

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
```

```
Broadcast message from root Fri Mar 11 22:04:53 2005...

The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]

router#
```

### Upgrading the Maintenance Partition

This section describes how to upgrade the maintenance partition, and contains the following topics:

- Catalyst Software
- Cisco IOS Software

#### Catalyst Software

To upgrade the maintenance partition, follow these steps:

**Step 1** Download the IDSM-2 maintenance partition file (c6svc-mp.2-1-1.bin.gz) to the FTP root directory of a FTP server that is accessible from your IDSM-2. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Step 2** Log in to the IDSM-2 CLI.

**Step 3** Enter configuration mode:

```
idsm2# configure terminal
```

**Step 4** Upgrade the maintenance partition:

```
idsm2# upgrade ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-1.bin.gz
```

You are asked whether you want continue.

**Step 5** Type y to continue. The maintenance partition file is upgraded.

#### Cisco IOS Software

To upgrade the maintenance partition, follow these steps:

**Step 1** Download the IDSM-2 maintenance partition file (c6svc-mp.2-1-1.bin.gz) to the FTP root directory of a FTP server that is accessible from your IDSM-2. For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software.

**Step 2** Log in to the switch CLI.

**Step 3** Session in to the application partition CLI:

```
router# session slot slot_number processor 1
```

**Step 4** Enter configuration mode:

```
idsm2# configure terminal
```

**Step 5** Upgrade the maintenance partition:

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-1.bin.gz
```

**Step 6** Specify the FTP server password:

```
Password: ********
```

You are prompted to continue:

```
Continue with upgrade?:
```

**Step 7** Type yes to continue.

### Installing the AIP-SSM System Image

You can reimage the AIP-SSM in one of the following ways:

- From ASA using the **hw-module module 1 recover configure/boot** command. See the following procedure.
- Recovering the application image from the sensor's CLI using the **recover application-partition** command. For the procedure, see Recovering the Application Partition.
- Upgrading the recovery image from the sensor's CLI using the **upgrade** command. For the procedure, see Upgrading the Recovery Partition.

To install the AIP-SSM system image, follow these steps:

**Step 1** Log in to the ASA.

**Step 2** Enter enable mode:

```
asa> enable
```

**Step 3** Configure the recovery settings for AIP-SSM:

```
asa# hw-module module 1 recover configure
```

**Note** If you make an error in the recovery configuration, use the **hw-module module 1 recover stop** command to stop the system reimaging and then you can correct the configuration.

**Step 4** Specify the TFTP URL for the system image:

```
Image URL [tftp://0.0.0.0/]:
```

Example:

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.0-1.img
```

**Step 5** Specify the command and control interface of AIP-SSM:

```
Port IP Address [0.0.0.0]:
```

Example:

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

**Step 6** Leave the VLAN ID at 0.

```
VLAN ID [0]:
```

**Step 7** Specify the default gateway of the AIP-SSM:

```
Gateway IP Address [0.0.0.0]:
```

Example:

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

**Step 8** Execute the recovery:

```
asa# hw-module module 1 recover boot
```

**Step 9** Periodically check the recovery until it is complete:

**Note** The status reads `guest@localhost.localdomain#` during recovery and reads `guest@localhost.localdomain#` when reimaging is complete.

```
asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5540 Adaptive Security Appliance         ASA5540            P2B00000019
  1 ASA 5500 Series Security Services Module-20  AIP-SSM-20         P1D000004F4
Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7b1c to 000b.fcf8.7b20  0.2          1.0(7)2      7.0(0)82
  1 000b.fcf8.011e to 000b.fcf8.011e  0.1          1.0(7)2      5.0(0.22)S129.0
Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa#
```

**Note** To debug any errors that may happen in the recovery process, use the **debug module-boot** command to enable debugging of the system reimaging process.

**Step 10** Session to AIP-SSM and initialize AIP-SSM with the **setup** command. For the procedure, see Initializing the Sensor.

Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks