



CHAPTER 14

Upgrading, Downgrading, and Installing System Images

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

- [Upgrades, Downgrades, and System Images, page 14-1](#)
- [Supported FTP and HTTP/HTTPS Servers, page 14-2](#)
- [Upgrading the Sensor, page 14-2](#)
- [Configuring Automatic Upgrades, page 14-7](#)
- [Downgrading the Sensor, page 14-12](#)
- [Recovering the Application Partition, page 14-12](#)
- [Installing System Images, page 14-14](#)

Upgrades, Downgrades, and System Images

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



Caution

You cannot use the **downgrade** command to go from IPS 6.0 to 5.x. To revert to 5.x, you must reimage the sensor.

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.

After you reimage and initialize your sensor, upgrade your sensor with the most recent service pack, signature update, signature engine update, minor version, major version, and recovery partition file.

For More Information

- For the procedure for using the **setup** command to initialize the sensor, see [Initializing the Sensor, page 11-3](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

Supported FTP and HTTP/HTTPS Servers

The following FTP servers are supported for IPS software updates:

- WU-FTPD 2.6.2 (Linux)
- Solaris 2.8.
- Sambar 6.0 (Windows 2000)
- Serv-U 5.0 (Windows 2000)
- MS IIS 5.0 (Windows 2000)

The following HTTP/HTTPS servers are supported for IPS software updates:

- VMS - Apache Server (Tomcat)
- VMS - Apache Server (JRun)

**Note**

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

For More Information

- For the procedure for downloading IPS software updates from Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for configuring automatic updates, see [Configuring Automatic Upgrades, page 14-7](#).

Upgrading the Sensor

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

- [IPS 6.0 Upgrade Files, page 14-3](#)
- [Upgrade Command and Options, page 14-3](#)
- [Using the Upgrade Command, page 14-4](#)
- [Upgrading the Recovery Partition, page 14-6](#)

IPS 6.0 Upgrade Files

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

- Signature updates, for example, IPS-sig-S700-req-E1.pkg
- Signature engine updates, for example, IPS-engine-E2-req-6.0-1.pkg
- Major updates, for example, IPS-K9-7.0-1-E1.pkg
- Minor updates, for example, IPS-K9-6.1-1-E1.pkg
- Service packs, for example, IPS-K9-6.1-3-E1.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



Note

Upgrading the sensor changes the software version of the sensor.



Caution

When you upgrade AIM-IPS NME-IPSAIM-IPS or NME-IPS using manual upgrade, you must disable heartbeat reset on the router before installing the upgrade. You can reenable heartbeat reset after you complete the upgrade. If you do not disable heartbeat reset, the upgrade can fail and leave AIM-IPS NME-IPSAIM-IPS or NME-IPS in an unknown state, which can require a system reimage to recover.

For More Information

For the procedure for disabling heartbeat reset on AIM-IPS, refer to [Enabling and Disabling Heartbeat Reset](#).

Upgrade Command and Options

Use the **upgrade** *source-url* command to apply service pack, signature update, minor version, major version, or recovery partition file upgrades.

The following options apply:

- *source-url*—The location of the source file to be copied.
 - ftp:—Source URL for an FTP network server. The syntax for this prefix is:
ftp:[//[username@] location]/relativeDirectory]/filename
ftp:[//[username@]location]//absoluteDirectory]/filename



Note

You are prompted for a password.

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



Note

You are prompted for a password.

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



Note The directory specification should be an absolute path to the desired file.

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



Note The directory specification should be an absolute path to the desired file.

For More Information

For the IDM procedure for upgrading the sensor, refer to [Updating the Sensor](#).

Using 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 upgrading 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 were not using SNMP **gets** and **sets** with IPS 5.x (for example, **enable-set-get** was set to **false**), there is no problem upgrading to IPS 6.0. If you were using 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 the following 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.
```



Caution

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

To upgrade the sensor, follow these steps:

- Step 1** Download the major update file (for example, IPS-K9-6.0-3-E1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.



Note You must log in to Cisco.com using an account with cryptographic privileges to download the file. Do not change the filename. You must preserve the original filename for the sensor to accept the update.

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

- Step 3** 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-K9-6.0-3-E1.pkg
```

Step 5 Enter the password when prompted:

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

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

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

Step 7 Verify your new sensor version:

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(3)E.1

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S291.0          2007-06-18
  Virus Update        V1.2            2005-11-24
OS Version:          2.4.30-IDS-smp-bigphys
Platform:            ASA-SSM-20
Serial Number:       P300000220
No license present
Sensor up-time is 13 days.
Using 1039052800 out of 2093682688 bytes of available memory (49% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 49.9M out of 166.6M bytes of available disk space (32% usage)
boot is using 37.8M out of 68.5M bytes of available disk space (58% usage)

MainApp              N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
AnalysisEngine       N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
CLI                  N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500

Upgrade History:

  IPS-K9-6.0-3-E.1 15:31:13 UTC Mon Sep 10 2007

Recovery Partition Version 1.1 - 6.0(3)E.1

sensor#
```



Note For IPS 5.x, you receive a message saying 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.

For More Information

- For the IDM procedure for upgrading the sensor, refer to [Updating the Sensor](#).
- For more information on configuring SNMP, for the CLI procedures, refer to [Configuring SNMP](#). For the IDM procedures, refer to [Configuring SNMP](#).
- For more information on configuring overrides, refer to [Adding, Editing, Enabling, and Disabling Event Action Overrides](#).
- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).
- For the procedure for locating software on Cisco.com and obtaining an account with cryptographic privilege, see [Obtaining Cisco IPS Software, page 13-1](#).

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 IPS 6.0(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-6.0-1.pkg) to an FTP, SCP, HTTP, or HTTPS server that is accessible from your sensor.

**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-6.0-1-E1.pkg  
  
sensor(config)#  
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-6.0-1-E1.pkg
```

Step 5

Enter 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 More Information

- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for using the **recover application-partition** command, see [Using the Recover Command, page 14-13](#).

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:

- [Automatic Upgrades, page 14-7](#)
- [Auto-upgrade Command and Options, page 14-8](#)
- [Using the auto-upgrade Command, page 14-9](#)
- [Automatic Upgrade Examples, page 14-11](#)

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 the following information 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.

**Caution**

When you upgrade AIM-IPS using automatic upgrade, you must disable heartbeat reset on the router before placing the upgrade file on your automatic update server. After AIM-IPS has been automatically updated, you can reenable heartbeat reset. If you do not disable heartbeat reset, the upgrade can fail and leave AIM-IPS in an unknown state, which can require a system reimage to recover.

**Caution**

If you are using 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 will download and try to install it, which is the incorrect file for AIM-IPS.

For More Information

- For the IDM procedure for upgrading the sensor automatically, refer to [Updating the Sensor Automatically](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for disabling heartbeat reset on AIM-IPS, refer to [Enabling and Disabling Heartbeat Reset](#).

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.

- **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.

For More Information

- For the IDM procedure for upgrading the sensor automatically, refer to [Updating the Sensor Automatically](#).
- For the procedure for adding a server to the SSH known hosts lists, refer to [Adding Hosts to the SSH Known Hosts List](#).

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:
- 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
```
  - 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/5.1_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.

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.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).
- For the IDM procedure for upgrading the sensor automatically, refer to [Updating the Sensor Automatically](#).
- For the procedure for adding a server to the SSH known hosts lists, refer to [Adding Hosts to the SSH Known Hosts List](#).

Automatic Upgrade Examples

Table 14-1 shows automatic upgrade examples. In these examples, the upgrades are configured hourly starting at 1:00. For example, Cycle 1 begins at 1:00, Cycle 2 begins at 2:00, and Cycle 3 begins at 3:00.

Table 14-1 Automatic Upgrade Example Cases

| Case/Current Version | Files in Remote Directory | Automatic Update Cycle/New Version |
|--|--|--|
| Case 0 5.1(4) E0 S250 | <ul style="list-style-type: none"> IPS-sig-S260-minreq-5.0-6.pkg IPS-engine-E2-req-5.1-4.pkg IPS-sig-S262-req-E2.pkg IPS-sig-S263-req-E2.pkg IPS-engine-E3-req-5.1-4.pkg IPS-sig-S264-req-E3.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-engine-E3-req-5.1-4.pkg. New version is 5.1(4) E2 S250. Cycle 2 installs IPS-sig-S264-req-E3.pkg. New version is 5.1(4) E2 S264. |
| Case 1 5.1(4) E0 S250 | <ul style="list-style-type: none"> IPS-K9-sp-5.1-5.pkg IPS-sig-S260-minreq-5.0-6.pkg IPS-K9-5.1-6-E1.pkg IPS-engine-E2-req-5.1-6.pkg IPS-sig-S262-req-E2.pkg IPS-sig-S263-req-E2.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-K9-5.1-6-E1.pkg. New version is 5.1(6) E1 S260. Cycle 2 installs IPS-engine-E2-req-5.1-6.pkg. New version is 5.1(6) E2 S260. Cycle 3 installs IPS-sig-S263-req-E2.pkg. New version is 5.1(6) E2 S263. |
| Case 2 5.1(6) E5 S300 | <ul style="list-style-type: none"> IPS-K9-6.0-1-E7.pkg IPS-K9-6.0-2-E9.pkg IPS-K9-6.0-3-E11.pkg IPS-engine-E10-req-6.0-2.pkg IPS-engine-E12-req-6.0-3.pkg IPS-sig-S305-req-E12.pkg IPS-sig-S307-req-E12.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-K9-6.0-3-E11.pkg. New version is 6.0(3) E11 S300. Cycle 2 installs IPS-engine-E12-req-6.0-3.pkg. New version is 6.0(3) E12 S300. Cycle 3 installs IPS-sig-S307-req-E12.pkg. New version is 6.0(3) E12 S307. |
| Case 3 5.1(6) E10 S300 | <ul style="list-style-type: none"> IPS-K9-6.0-1-E9.pkg IPS-engine-E11-req-6.0-1.pkg IPS-sig-S305-req-E11.pkg IPS-sig-S307-req-E11.pkg | <ul style="list-style-type: none"> Cycle 1 installs nothing because E9 is less than E10. |
| Case 4 5.1(6) E10 S300 | <ul style="list-style-type: none"> IPS-engine-E11-req-5.1-6.pkg IPS-sig-S301-req-E10.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-engine-E11-req-5.1-6.pkg. New version is 5.1(6) E11 S300. |
| Case 5 5.1(6) E10 S300 | <ul style="list-style-type: none"> IPS-sig-S301-req-E10.pkg IPS-sig-S302-req-E11.pkg IPS-sig-S303-req-E12.pkg IPS-engine-E11-req-5.1-6.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-engine-E11-req-5.1-6.pkg. New version is 5.1(6) E11 S300. Cycle 2 installs IPS-sig-S302-req-E11.pkg. New version is 5.1(6) E11 S302. |
| Case 6 6.0(3)E1 S300 (IPS 4270-20) | <ul style="list-style-type: none"> IPS-K9-6.0-4-E1.pkg IPS-4270_20-K9-6.0-4-E1.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-4270_20-K9-6.0-4-E1.pkg. New version is 6.0(4)E1 S310 |

Table 14-1 Automatic Upgrade Example Cases (continued)

| Case/Current Version | Files in Remote Directory | Automatic Update Cycle/New Version |
|--------------------------------------|--|---|
| Case 7 6.0(4)E3 S330 (AIM-IPS) | <ul style="list-style-type: none"> IPS-K9-6.0-5-E3.pkg IPS-AIM-K9-6.0-5-E3.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-AIM-K9-6.0-5-E3.pkg. New version is 6.0(5)E3 S335. |
| Case 8 6.0(5)E5 S330 (AIM-IPS) | <ul style="list-style-type: none"> IPS-K9-7.0-1-E5.pkg IPS-AIM-K9-7.0-1-E5.pkg | <ul style="list-style-type: none"> Cycle 1 installs IPS-K9-7.0-1-E5.pkg. New version is 7.0(1)E5 S377 |

Downgrading the Sensor

Use the **downgrade** command to remove the last applied service pack or signature upgrade from the sensor.



Caution

You cannot use the **downgrade** command to go from IPS 6.0 to 5.x. To revert to 5.x, you must reimagine the sensor. You can only use the **downgrade** command to downgrade from the latest signature updates and service packs.

To remove the last applied signature update or service pack 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.6.0-2-E1.pkg. Configuration changes made since the last upgrade will be lost and
the system may be rebooted.
```

```
Continue with downgrade?:
```

Step 4 Enter **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:

- [Application Partition, page 14-13](#)
- [Using the Recover Command, page 14-13](#)

Application Partition

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.

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.



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

For More Information

- For the procedure for upgrading the recovery partition to the most recent version, see [Upgrading the Recovery Partition, page 14-6](#).
- For the procedure for using the CD to recover the sensor, see [Using the Recovery/Upgrade CD, page 14-29](#).

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-6.0-1-E1.pkg) to the tftp root directory of a TFTP server that is accessible from your sensor.



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

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

Step 3 Enter configuration mode:

```
sensor# configure terminal
```

Step 4 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 6.0(2)E1. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

Step 5 Enter **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.



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.

For More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for using the **setup** command to initialize the sensor, see [Initializing the Sensor, page 11-3](#).

Installing System Images

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

- [Understanding ROMMON, page 14-15](#)
- [Supported TFTP Servers, page 14-15](#)
- [Connecting an Appliance to a Terminal Server, page 14-16](#)
- [Installing the IDS-4215 System Image, page 14-17](#)
- [Upgrading the IDS-4215 BIOS and ROMMON, page 14-19](#)
- [Installing the IPS-4240 and IPS-4255 System Image, page 14-21](#)
- [Installing the IPS-4260 System Image, page 14-24](#)
- [Installing the IPS 4270-20 System Image, page 14-26](#)
- [Using the Recovery/Upgrade CD, page 14-29](#)
- [Installing the NM-CIDS System Image, page 14-30](#)

- [Installing the IDSM-2 System Image, page 14-35](#)
- [Installing the AIM-IPS System Image, page 14-47](#)
- [Installing the AIP-SSM System Image, page 14-50](#)

**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 More Information

For the procedure for using the **recover application-partition** command, see [Recovering the Application Partition, page 14-12](#).

Understanding ROMMON

Some Cisco sensors include a preboot CLI called ROMMON, which lets you boot images on sensors where the image on the primary device is missing, corrupt, or otherwise unable to boot the normal application. ROMMON is particularly useful for recovering remote sensors as long as the serial console port is available.

Access to ROMMON is available only through the serial console port, a Cisco-standard asynchronous RS-232C DTE available in an RJ-45F connector on the sensor chassis. The serial port is configured for 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

For More Information

For the procedure for using a terminal server, see [Connecting an Appliance to a Terminal Server, page 14-16](#).

Supported TFTP Servers

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

Some TFTP servers limit the maximum file size that can be transferred to ~32 MB. Therefore, we recommend the following TFTP servers:

- For Windows:
Tftpd32 version 2.0, available at:
<http://tftpd32.jounin.net/>
- For UNIX:
Tftp-hpa series, available at:
<http://www.kernel.org/pub/software/network/tftp/>

Connecting an Appliance to a Terminal Server

A terminal server is a router with multiple, low speed, asynchronous ports that are connected to other serial devices. You can use terminal servers to remotely manage network equipment, including appliances.

To set up a Cisco terminal server with RJ-45 or hydra cable assembly connections, follow these steps:

-
- Step 1** Connect to a terminal server using one of the following methods:
- For IDS-4215, IPS-4240, IPS-4255, IPS-4260, and IPS 4270-20:
 - For terminal servers with RJ-45 connections, connect a 180 rollover cable from the console port on the appliance to a port on the terminal server.
 - For hydra cable assemblies, connect a straight-through patch cable from the console port on the appliance to a port on the terminal server.
 - For all other appliances, connect the M.A.S.H. adapter (part number 29-4077-01) to COM1 on the appliance and:
 - For terminal servers with RJ-45 connections, connect a 180 rollover cable from the M.A.S.H. adapter to a port on the terminal server.
 - For hydra cable assemblies, connect a straight-through patch cable from the M.A.S.H. adapter to a port on the terminal server.

- Step 2** Configure the line and port on the terminal server as follows:

- a. In enable mode, enter the following configuration, where # is the line number of the port to be configured:

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

- b. If you are configuring a terminal server for an IDS-4215, IPS-4240, IPS-4255, IPS-4260, or IPS 4270-20, go to Step 3.

Otherwise, for all other supported appliances, to direct all output to the terminal server, log in to the CLI and enter the following commands:

```
sensor# configure terminal
sensor(config)# display-serial
```

Output is directed to the serial port. Use the **no display-serial** command to redirect output to the keyboard and monitor.

**Note**

You can set up a terminal server and use the **display-serial** command to direct all output from the appliance to the serial port. This option lets you view system messages on a console connected to the serial port, even during the boot process. When you use this option, all output is directed to the serial port and any local keyboard and monitor connection is disabled. However, BIOS and POST messages are still displayed on the local keyboard and monitor.

**Note**

There are no keyboard or monitor ports on an IDS-4215, IPS-4240, or IPS-4255. Keyboard and monitor ports are not supported on IPS-4260 or IPS 4270-20. Therefore, the **display-serial** and **no display-serial** commands do not apply to those platforms.

Step 3 Be sure to properly close a terminal session to avoid unauthorized access to the appliance.

If a terminal session is not stopped properly, that is, if it does not receive an exit(0) signal from the application that initiated the session, the terminal session can remain open. When terminal sessions are not stopped properly, authentication is not performed on the next session that is opened on the serial port.

**Caution**

Always exit your session and return to a login prompt before terminating the application used to establish the connection.

**Caution**

If a connection is dropped or terminated by accident, you should reestablish the connection and exit normally to prevent unauthorized access to the appliance.

For More Information

For the procedure for displaying BIOS and POST messages on the local monitor, see [Directing Output to a Serial Connection, page 1-19](#).

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.

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-6.0-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IDS-4215.

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.

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/IPS-4215-K9-sys-1.1-a-6.0-1-E1.img
```



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

Windows example:

```
rommon> file <tftpboot_directory>IPS-4215-K9-sys-1.1-a-6.0-1-E1.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.

For More Information

- For the procedure for upgrading the IDS-4215 BIOS and ROMMON, see [Upgrading the IDS-4215 BIOS and ROMMON, page 14-19](#).
- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

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.



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 Enter **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.

For More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

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-6.0-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS-4240.



Note

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

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/path name
- 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-1.1-a-6.0-1-E1.img
```



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

Windows example:

```
rommon> IMAGE=\system_images\IPS-4240-K9-sys-1.1-a-6.0-1-E1.img
```

Step 11 Enter **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 enter 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.

For More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

Installing the IPS-4260 System Image

You can install the IPS-4260 system image by using the ROMMON on the appliance to TFTP the system image onto the flash device.

To install the IPS-4260 system image, follow these steps:

Step 1 Download the IPS-4260 system image file (IPS-4260-K9-sys-1.1-a-6.0-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS-4260.

Make sure you can access the TFTP server location from the network connected to your IPS-4260 Ethernet port.

Step 2 Boot IPS-4260.

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:

```
Assuming IPS-4260-K9 Platform
 2 Ethernet Interfaces detected

Cisco Systems ROMMON Version (1.0(11)1c) #26: Mon Mar 13 18:05:54 CST 2006

Platform IPS-4260-K9
Management0/0
Link is UP
MAC Address: 0004.23cc.6047

Use ? for help.
rommon #0>
```

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

```
rommon #1> interface name
```

The port in use is listed just after the platform identification. In the example, port Management0/0 is being used.



Note The default port used for TFTP downloads is Management0/0, which corresponds with the command and control (MGMT) interface of the IPS-4260.



Note Ports Management0/0 (MGMT) and GigabitEthernet0/1 (GE 0/1) are labeled on the back of the chassis.

Step 5 Specify an IP address for the local port on IPS-4260:

```
rommon> address ip_address
```



Note Use the same IP address that is assigned to IPS-4260.

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 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/IPS-4260-K9-sys-1.1-a-6.0-1-E1.img
```



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

Windows example:

```
rommon> file <tftpboot_directory>IPS-4260-K9-sys-1.1-a-6.0-1-E1.img
```

Step 10 Download and install the system image:

```
rommon> tftp
```



Note IPS-4260 reboots once during the reimaging process. Do not remove power from IPS-4260 during the update process or the upgrade can become corrupted.

For More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

Installing the IPS 4270-20 System Image

You can install the IPS 4270-20 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4270-20 system image, follow these steps:

Step 1 Download the IPS 4270-20 system image file (IPS4270-20-K9-sys-1.1-a-6.0-1-E1.img) to the tftp root directory of a TFTP server that is accessible from your IPS 4270-20.



Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4270-20.

Step 2 Boot IPS 4270-20.

The console display resembles the following:

```
Booting system, please wait...
Cisco Systems ROMMON Version (1.0(12)10) #7: Thu Jun 21 13:50:04 CDT 2007

ft_id_update: Invalid ID-PROM Controller Type (0x5df)

ft_id_update: Defaulting to Controller Type (0x5c2)
```



Note The controller type errors are a known issue and can be disregarded.

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=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

The variables have the following definitions:

- Address—Local IP address of IPS 4270-20
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by IPS 4270-20
- Port—Ethernet interface used for IPS 4270-20 management
- VLAN—VLAN ID number (leave as untagged)
- Image—System image file/path name
- 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, assign an IP address for the local port on IPS 4270-20:

```
rommon> ADDRESS=ip_address
```



Note Use the same IP address that is assigned to IPS 4270-20.

Step 6 If necessary, assign the TFTP server IP address:

```
rommon> SERVER=ip_address
```

Step 7 If necessary, assign the gateway IP address:

```
rommon> GATEWAY=ip_address
```

Step 8 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 9 If necessary define the path and filename on the TFTP file server from which you are downloading the image:

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

UNIX example:

```
rommon> IMAGE=/system_images/IPS4270-20-K9-sys-1.1-a-6.0-1-E1.img
```



Note The path is relative to the UNIX TFTP server 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=\system_images\IPS4270-20-K9-sys-1.1-a-6.0-1-E1.img
```

Step 10 Enter **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 enter this information each time you want to boot an image from ROMMON.

Step 11 Download and install the system image:

```
rommon> tftp
```



Caution

To avoid corrupting the system image, do not remove power from IPS 4270-20 while the system image is being installed.



Note If the network settings are correct, the system downloads and boots the specified image on IPS 4270-20. Be sure to use the IPS 4270-20 image.

For More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

Using the Recovery/Upgrade CD

You can use the recovery/upgrade CD on appliances that have a CD-ROM, such as 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:
- To access IDM, point your browser to the appliance you are upgrading.
 - Choose **Monitoring > Diagnostics Report**.
The Diagnostics Report pane appears.
 - Click **Generate Report**.
Running the diagnostics may take a while.
 - Click **View Results**.
The results are displayed in a report.
 - To save the diagnostics report, click **Save**.
- 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** Enter **k** if you are installing from a keyboard, or Enter **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** Enter the **setup** command to initialize the appliance.
- Step 8** Install the most recent service pack and signature update.

For More Information

- For the procedure for using the **setup** command to initialize the appliance, see [Initializing the Appliance, page 11-3](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

Installing the NM-CIDS System Image

You can reimage the NM-CIDS using the system image file (IPS-NM-CIDS-K9-sys-1.1-a-6.0-1-E1.img). If NM-CIDS is already running IPS 5.x, the bootloader has been upgraded. If NM-CIDS is not running 5.x, you must upgrade the bootloader before installing the 6.0 image.

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

- [Installing the NM-CIDS System Image, page 14-30](#)
- [Upgrading the NM-CIDS Bootloader, page 14-32](#)

Installing the NM-CIDS System Image



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-6.0-1-E1.img) to the TFTP root directory of a TFTP server that is accessible from your NM-CIDS.



Note

Make sure you can access the TFTP server location from the network connected to the 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 should 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 Enter ******* 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 1.0.17-3, you must upgrade it before installing IPS 6.0.

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. 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-6.0-1-E1.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 6.0(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 More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for upgrading the bootloader, see [Upgrading the NM-CIDS Bootloader, page 14-32](#).
- For the procedure, for using the **setup** command to initialize NM-CIDS, see [Initializing NM-CIDS, page 11-32](#).

Upgrading the NM-CIDS Bootloader

The NM-CIDS bootloader executes immediately after BIOS completes its POST. Make sure you have the most recent version of the bootloader. The current one is `servicesengine-boot-1.0-17-3.bin`.

We recommend you upgrade your NM-CIDS to 6.0(1) by applying the 6.0(1) update (IPS-NM-CIDS-K9-sys-1.1-a-6.0-1-E1.img). When the update is applied, the configuration is migrated and the bootloader is upgraded to version 1.0.17-3. If you update your NM-CIDS with the update file, in the future you do not need to upgrade the bootloader before performing a system update.

The NM-CIDS system image file (IPS-NM-CIDS-K9-sys-1.1-a-6.0-3-E1.img) does not migrate your existing configuration or upgrade the bootloader. Therefore, you must first manually install bootloader version 1.0.17-3.



Note

The bootloader has a timeout of 10 minutes, which means reimages over slow WAN links 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-1.0-17-3.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.



Note

Make sure you can access the TFTP server location from the network connected to the Ethernet port of NM-CIDS.

- 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 Press **Shift-Ctrl-6 X** to suspend the session.

You will see the `router#` prompt. If you do not see this prompt, press **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-1.0-17-3_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-1.0-17-3_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 1.0.17-3. 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-6.0-3-E1.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 6.0(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 More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure to use the **upgrade** command, see [Upgrading the Sensor, page 14-2](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure, for using the **setup** command to initialize NM-CIDS, see [Initializing NM-CIDS, page 11-32](#).

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.

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. It contains the following topics:

- [Installing the IDSM-2 System Image for Catalyst Software, page 14-36](#)
- [Installing the IDSM-2 System Image for Cisco IOS Software, page 14-37](#)
- [Configuring the IDSM-2 Maintenance Partition for Catalyst Software, page 14-38](#)
- [Configuring the IDSM-2 Maintenance Partition for Cisco IOS Software, page 14-42](#)
- [Upgrading the IDSM-2 Maintenance Partition for Catalyst Software, page 14-46](#)
- [Upgrading the IDSM-2 Maintenance Partition for Cisco IOS Software, page 14-46](#)

Installing the IDSM-2 System Image for Catalyst Software

To install the IDSM-2 system image, follow these steps:

Step 1 Download the IDSM-2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-6.0-0.190-E0.1.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM-2.

Step 2 Log in to the switch CLI.

Step 3 Boot IDSM-2 to the maintenance partition:

```
console> (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.

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-6.0-0.190-E0.1.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 Enter **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:

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

Step 10 When IDSM-2 has rebooted, check the software version.

Step 11 Log in to the application partition CLI and initialize IDSM-2.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for configuring the maintenance partition on IDSM-2, see [Configuring the IDSM-2 Maintenance Partition for Catalyst Software, page 14-38](#).
- For the procedure, for using the **setup** command to initialize IDSM-2, see [Initializing IDSM-2, page 11-12](#).

Installing the IDSM-2 System Image for Cisco IOS Software

To install the IDSM-2 system image, follow these steps:

Step 1 Download the IDSM-2 system image file (WS-SVC-IDSM2-K9-sys-1.1-a-6.0-0.190-E0.1.bin.gz) to the TFTP root directory of a TFTP server that is accessible from your IDSM-2.

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.

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-6.0-0.190-E0.1.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 Enter **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 More Information

- For a list of recommended TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for configuring the maintenance partition, see [Configuring the IDSM-2 Maintenance Partition for Catalyst Software, page 14-38](#).
- For the procedure, for using the **setup** command to initialize IDSM-2, see [Initializing IDSM-2, page 11-12](#).

Configuring the IDSM-2 Maintenance Partition for 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:

```
console# enable
console(enable)#
```

Step 3 Reload IDSM-2:

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

Step 4 Session to IDSM-2:

```
console# 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 5 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, IDSM-2 requires an RMA.

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

Step 6 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 7 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 8 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 9 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 10 Verify the image installed on the application partition:

```
guest@idsm2.localdomain# show images
```

| Device name | Partition# | Image name |
|----------------|------------|------------|
| Hard disk(hdd) | 1 | 6.0(1) |

```

-----
-----
-----
guest@idsm2.localdomain#

```

Step 11 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 12 Upgrade the application partition:

```

guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.0-0/WS-SVC-IDS2-K9-sys-1.1-a-6.0-0.190-E0.1.bin.gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'WS-SVC-IDS2-K9-sys-1.1-a-6.0-0.190-E0.1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.0-0/WS-SVC-IDS2-K9-sys-1.1-a-6.0-0.190-E0.1.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/6.0-0/WS-SVC-IDS2-K9-sys-1.1-a-6.0-0.190-E0.1.bin.gz is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:

```

Step 13 Enter **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 14 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/6.0-0/WS-SVC-IDS2-K9-sys-1.1-a-6.0-0.190-E0.1.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: XXXXXXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 00000000000031729
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 15 Clear the upgrade log:

```

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

```

Step 16 Display the upgrade log:

```

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

```

Step 17 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 18 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 !!
console> (enable)#

```

For More Information

For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers](#), page 14-2.

Configuring the IDSM-2 Maintenance Partition for 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              6.0(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/6.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.0-1-E1.img

```

```

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-6.0-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.0-1-E1.img
(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/6.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.0-1-E1.img
is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:

```

Step 11 Enter **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/6.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.0-1-E1.img
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: XXXXXXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 000000029323770
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#
```

For More Information

For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).

Upgrading the IDSM-2 Maintenance Partition for Catalyst Software

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

-
- Step 1** Download the IDSM-2 maintenance partition file (c6svc-mp.2-1-2.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM-2.
- Step 2** Session to IDSM-2 from the switch:
- ```
console>(enable) session slot_number
```
- Step 3** Log in to the IDSM-2 CLI.
- 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.2-1-2.bin.gz
```
- You are asked whether you want continue.
- Step 6** Enter the FTP server password.
- Step 7** Enter **y** to continue.
- The maintenance partition file is upgraded.
- 

### For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

## Upgrading the IDSM-2 Maintenance Partition for Cisco IOS Software

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

- 
- Step 1** Download the IDSM-2 maintenance partition file (c6svc-mp.2-1-2.bin.gz) to the FTP root directory of an FTP server that is accessible from your IDSM-2.
- 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** Log in to IDSM-2.
- Step 5** Enter configuration mode:
- ```
idsm2# configure terminal
```
- Step 6** Upgrade the maintenance partition:
- ```
idsm2(config)# upgrade  
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

Step 7 Specify the FTP server password:

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

You are prompted to continue:

```
Continue with upgrade?:
```

Step 8 Enter **yes** to continue.

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers, page 14-2](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).

Installing the AIM-IPS System Image

To install the AIM-IPS system image, follow these steps:

Step 1 Download the AIM-IPS system image file (IPS-AIM-K9-sys-1.1-6.0-1-E1.img), and place it on a TFTP server relative to the tftp root directory.



Note Make sure the network is configured so that AIM-IPS can access the TFTP server.

If no TFTP server is available, you can configure the router to operate as a TFTP server.

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-AIM-K9-sys-1.1-6.0-1-E1.img
router(config)# exit
router#
```

Step 2 Disable the heartbeat reset.

```
router# service-module IDS-Sensor 0/slot_number heartbeat-reset disable
```



Note Disabling the heartbeat reset prevents the router from resetting the module during system image installation if the process takes too long.

Step 3 Session to AIM-IPS.

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



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

Step 4 Suspend the session by pressing **Shift-Ctrl-6 X**.

You should see the `router#` prompt. If you do not see this prompt, try **Ctrl-6 X**.

Step 5 Reset AIM-IPS.

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

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

Step 6 Press **Enter** to confirm.

Step 7 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 8 Enter ******* during the 15-second delay.

The bootloader prompt appears.

Step 9 Press **Enter** to session back to AIM-IPS.

Step 10 Configure the bootloader.

```
ServicesEngine bootloader> config
```

```
IP Address [10.89.148.188]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

For each prompt, enter a value or accept the previously stored input that appears inside square brackets by pressing **Enter**.



Note The gateway IP address must match the IP address of the IDS-Sensor *slot/port* interface.



Note If you set up the module interfaces using the **unnumbered** command, the gateway IP address should be the IP address of the other router interface being used as part of the unnumbered command.



Caution The pathname for the AIM-IPS image is full but relative to the tftp server root directory (typically /tftpboot).

Step 11 Start the bootloader.

```
ServicesEngine bootloader> upgrade
```

Step 12 Follow the bootloader instructions to install the software (choose option 1 and follow the wizard instructions).



Note In the following example, the AIM-IPS IP address is 10.1.9.201. The imaging process accesses the AIM-IPS image from the router TFTP server at IP address 10.1.9.1.

Example:

```
Booting from flash...please wait.
```


Step 15 Enable the heartbeat reset.

```
router# service-module IDS-sensor 0/slot_number heartbeat-reset enable
```

For More Information

- For a list of supported TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 13-1](#).
- For the procedure for configuring an unnumbered IP address, refer to [Using an Unnumbered IP Address Interface](#).

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 CLI using the **recover application-partition** command.
- Upgrading the recovery image from the sensor CLI using the **upgrade** command.

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 (enable)# 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-6.0-1-E1.img
```

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



Note The port IP address is the management IP address 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 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 `Recovery` during recovery and reads `Up` 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 | ASA-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 More Information

- For the procedure for using the `recover application-partition` command, see [Recovering the Application Partition, page 14-12](#).
- For the procedure for using the `upgrade` command, see [Upgrading the Recovery Partition, page 14-6](#).
- For a list of recommended TFTP servers, see [Supported TFTP Servers, page 14-15](#).
- For the procedure for using the `setup` command to initialize AIP-SSM, see [Initializing AIP-SSM, page 11-25](#).

