Upgrading, Downgrading, and Installing System Images

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

Upgrade Notes and Caveats

Pay attention to the following upgrade notes and caveats when upgrading your sensor:

- Anomaly detection has been disabled by default. If you did not configure the operation mode manually before the upgrade, it defaults to inactive after you upgrade the IPS software. If you configured the operation mode to detect, learn, or inactive, the tuned value is preserved after the upgrade.
- You must have a valid maintenance contract per sensor to download software upgrades from Cisco.com.
- You must be running the following versions to upgrade the following platforms to IPS 7.3(1)E4:
  - For the IPS 4300 series sensors, you must be running IPS 7.1(3)E4 or later.
  - For the IPS 4500 series sensors, you must be running IPS 7.1(4)E4 or later.
- This service pack automatically reboots the sensor to apply the changes. During reboot, inline network traffic is disrupted.
- You cannot uninstall IPS 7.3(x)E4. To revert to a previous version, you must reimage the sensor using the appropriate system image file.

- You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.3 to 7.2. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.2, you must reimage the sensor.

- 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.

Upgrades, Downgrades, and System Images

⚠️

Caution   You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.3 to 7.2. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.2, you must reimage the sensor.

✎

Note   After you upgrade any IPS software on your sensor, you must restart the IDM to see the latest software features.

✎

Note   You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).

✎

Note   During a signature upgrade all signature configurations are retained, both the signature tunings as well as the custom signatures. During a signature downgrade the current signature configuration is replaced with the old signature configuration. So if the last signature set had custom signatures and/or signature tunings, these are restored during the downgrade. Threat profiles may also be upgraded during signature upgrades.

You can upgrade and downgrade the software on the sensor. Upgrading applies a service pack, signature update (which includes threat profile updates), signature engine update, minor version, major version, or recovery partition file. Downgrading removes the last applied service pack or signature update from the sensor. With a signature downgrade, the threat profile is downgraded to the version available in the previous signature version.

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 ROMMON, the bootloader 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 update, major update, and recovery partition files.

For More Information

- For the procedure for initializing the sensor, see Appendix B, "Initializing the Sensor."

- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-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:

- CSM - Apache Server (Tomcat)
- CSM - Apache Server (JRun)

For More Information

- For the procedure for downloading IPS software updates from Cisco.com, see Obtaining Cisco IPS Software, page C-1.
- For the procedure for configuring automatic updates, see Configuring Automatic Upgrades, page D-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 7.3 Upgrade Files, page D-3
- Manually Upgrading the Sensor, page D-4
- Upgrading the Recovery Partition, page D-6

IPS 7.3 Upgrade Files

The currently supported IPS 7.3(x) version is 7.3(1)E4.

For a list of the specific IPS filenames and the IPS versions that each sensor supports, refer to the Release Notes for your IPS version found at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

For More Information

For the procedure for obtaining these files on Cisco.com, see Obtaining Cisco IPS Software, page C-1.

Manually Upgrading the Sensor

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

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

Note   During a signature upgrade all signature configurations are retained, both the signature tunings as well as the custom signatures. During a signature downgrade the current signature configuration is replaced with the old signature configuration. So if the last signature set had custom signatures and/or signature tunings, these are restored during the downgrade. Threat profiles may also be upgraded during signature upgrades.

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

- *source-url*—Specifies 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. You must add the remote host to the SSH known hosts list.

    – http:—Source URL for the web server. The syntax for this prefix is:

    http://[[username@]location][/directory]/filename

    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. The remote host must be a TLS trusted host.

Upgrading the Sensor

> **Note** The CLI output is an example of what your configuration may look like. It will not match exactly due to the optional setup choices, sensor model, and IPS version you have installed.

To upgrade the sensor, follow these steps:

Step 1 Download the appropriate file to an FTP, SCP, HTTP, or HTTPS server that is accessible from 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 Upgrade the sensor.

```
sensor(config)# upgrade url/IPS-4360-K9-7.3-1-E4.pkg
```

The URL points to where the update file is located, for example, to retrieve the update using FTP, enter the following:

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-4360-K9-7.3-1-E4.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.

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

Step 7 Verify your new sensor version.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(1)E4

Host:
    Realm Keys            key1.0
Signature Definition:
    Signature Update      S741.0          2013-09-10
    Threat Profile Version  2
OS Version:               2.6.29.1
Platform:                 IPS-4360
Serial Number:            FGL1702401M
Licensed, expires:        21-Nov-2014 UTC
Sensor up-time is 22:09.
Using 14372M out of 15943M bytes of available memory (90% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.6M out of 376.4M bytes of available disk space (24% usage)
```

```
boot is using 63.1M out of 70.2M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)


MainApp          C-2013_12_16_14_00_7_3_0_143   (Release)   2013-12-16T14:06:20-0600
Running
AnalysisEngine   C-2013_12_16_14_00_7_3_0_143   (Release)   2013-12-16T14:06:20-0600
Running
CollaborationApp C-2013_12_16_14_00_7_3_0_143   (Release)   2013-12-16T14:06:20-0600
Running
CLI              C-2013_12_16_14_00_7_3_0_143   (Release)   2013-12-16T14:06:20-0600

Upgrade History:

  IPS-K9-7.3-1-E4   11:22:07 UTC Sat Jan 19 2013

Recovery Partition Version 1.1 - 7.3(1)E4

Host Certificate Valid from: 09-Oct-2014 to 09-Oct-2016

sensor#
```

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see Supported FTP and HTTP/HTTPS Servers, page D-3.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-1.

Upgrading the Recovery Partition

Note   You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).

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

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

Step 1   Download the appropriate recovery partition image file 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-4360-K9-r-1.1-a-7.3-1-E4.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-4360-K9-r-1.1-a-7.3-1-E4.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 D-3.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-1.
- For the procedure for using the **recover** command, see Upgrading the Recovery Partition, page D-6.

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:

- Understanding Automatic Upgrades, page D-7
- Automatically Upgrading the Sensor, page D-8

Understanding 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.

For More Information

For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-1.

Automatically Upgrading the Sensor

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

The following options apply:

- **cisco-server {disabled | enabled}**—Enables automatic signature and engine updates from Cisco.com.

- **cisco-url** *cisco_url*—Specifies the Cisco server locator service. You do not need to change this unless the www.cisco.com IP address changes.

- **default**— Sets the value back to the system default setting.

- **directory** *directory*— Specifies the directory where upgrade files are located on the file server. A leading '/' indicates an absolute path.

- **file-copy-protocol {ftp | scp}**— Specifies the file copy protocol used to download files from the file server.

    ✎
    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*—Specifies the IP address of the file server.

- **password** *password*—Specifies the user password for Cisco server authentication.

- **schedule-option**—Specifies the schedules for when Cisco server automatic upgrades occur. Calendar scheduling starts upgrades at specific times on specific days. Periodic scheduling starts upgrades at specific periodic intervals.

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

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

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

    - **interval**—Specifies the number of hours to wait between automatic upgrades. Valid values are 1 to 8760. The default value is 24.

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

- **user-name** *user_name*—Specifies the username for server authentication.

- **user-server {disabled | enabled}**—Enables automatic upgrades from a user-defined server.

Configuring Automatic Upgrades

If you get an unauthorized error message while configuring an automatic update, make sure you have the correct ports open on any firewalls between the sensor and Cisco.com. For example, you need port 443 for the initial automatic update connection to www.cisco.com, and you need port 80 to download the chosen package from a Cisco file server. The IP address may change for the Cisco file server, but you can find it in the lastDownloadAttempt section in the output of the **show statistics host** command.

Note To check the status of the last automatic update or the next scheduled automatic update, run the **show statistics host** command and check the Auto Update Statistics section.

To schedule automatic upgrades, follow these steps:

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

Step 2 Enter automatic upgrade submode.

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

Step 3 Configure the sensor to automatically look for new upgrades either on Cisco.com or on your file server:

a. On Cisco.com. Continue with Step 4.

```
sensor(config-hos-aut)# cisco-server enabled
```

b. From your server.

```
sensor(config-hos-aut)# user-server enabled
```

c. Specify the IP address of the file server.

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

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

```
sensor(config-hos-ena)# directory /tftpboot/sensor_updates
```

e. 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 4 Specify the username for authentication.

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

Step 5 Specify the password of the user.

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

Step 6 Specify the scheduling:

a. For calendar scheduling (starts upgrades at specific times on specific day):

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

b. For periodic scheduling (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 7 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/6.1_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   -----------------------------------------------
sensor(config-hos-ena)#
```

Step 8 Exit automatic upgrade submode.

```
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

Step 9 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 D-3.

- For the procedure for adding a remote host to the trusted hosts list, for IDM refer to Defining Known Hosts Keys, for IME refer to Defining Known Host Keys, and for the CLI, refer to Adding Hosts to the SSH Known Hosts List.

Downgrading the Sensor

⚠

Caution You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.3 to 7.2. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.2, you must reimage the sensor.

> **Note** You cannot downgrade the sensor using the recovery partition. To downgrade to an earlier version, you must install the appropriate system image file (.img file).

Use the **downgrade** command to remove the last applied signature upgrade or signature engine upgrade from the sensor. The signature upgrade includes threat profiles. When you downgrade the signature update, the threat profile reverts to the one found in the previous signature upgrade.

To remove the last applied signature update or signature engine update 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 downgrade the system to IPS-K9-7.3-0.136-E4.
Configuration changes made since the last upgrade will be lost and the system may be
rebooted. Signature threat profile mapping to signature instances will be reverted to the
previous configuration.
Continue with downgrade? []: yes

Broadcast Message from root@qa-ff-4510-133-163
        (somewhere) at 23:47 ...

Un-installing IPS-sig-S760-req-E4.



Broadcast Message from root@qa-ff-4510-133-163
        (somewhere) at 23:47 ...

Un-install complete.

sensor#
```

Step 4   Display the current version after the downgrade.

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(0.136)E4

Host:
    Realm Keys             key1.0
Signature Definition:
    Signature Update       S760.0            2013-12-12
    Threat Profile Version 5
OS Version:                2.6.29.1
Platform:                  IPS-4510-INC-K9
Serial Number:             JAF1539CLTL
Licensed, expires:         17-Sep-2014 UTC
Sensor up-time is 1 day.
Using 22470M out of 24019M bytes of available memory (93% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 85.4M out of 377.5M bytes of available disk space (24% usage)
boot is using 62.9M out of 70.5M bytes of available disk space (94% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)
```

```
MainApp            C-2013_11_20_12_52_7_3_1   (Release)   2013-11-20T12:57:43-0600
Running
AnalysisEngine     C-2013_11_20_12_52_7_3_1   (Release)   2013-11-20T12:57:43-0600
Running
CollaborationApp   C-2013_11_20_12_52_7_3_1   (Release)   2013-11-20T12:57:43-0600
Running
SwitchApp          C-2013_11_20_12_52_7_3_1   (Release)   2013-11-20T12:57:43-0600
Running
CLI                C-2013_11_20_12_52_7_3_1   (Release)   2013-11-20T12:57:43-0600

Upgrade History:

* IPS-K9-7.3-0.136-E4      07:40:07 UTC Sun Jan 20 2013
  IPS-sig-S760-req-E4.pkg  16:57:01 UTC Sat Jan 11 2014

Recovery Partition Version 1.1 - 7.3(0.136)E4

Host Certificate Valid from: 10-Jan-2014 to 11-Jan-2016

sensor#
```

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

You can recover the application partition image for the sensor 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 sensor. 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   When you reconnect to the sensor after recovery, you must log in with the default username and password **cisco**.

Recovering the Application Partition Image

To recover the application partition image, follow these steps:

Step 1   Download the recovery partition image file to an FTP, HTTP, or HTTPS server that is accessible from 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 7.1(x)E4. 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 sensor with the **setup** command.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.

For More Information

- For the procedure for upgrading the recovery partition to the most recent version, see Upgrading the Recovery Partition, page D-6.

- For a list of supported TFTP servers, see TFTP Servers, page D-14.

- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-1.

- For the procedure for using the **setup** command, see Appendix B, "Initializing the Sensor."

Installing System Images

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

- ROMMON, page D-14
- TFTP Servers, page D-14
- Connecting an Appliance to a Terminal Server, page D-14
- Installing the IPS 4345 and IPS 4360 System Images, page D-15
- Installing the IPS 4510 and IPS 4520 System Image, page D-18

⚠ **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.

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 D-14.

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

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 terminal servers with RJ-45 connections, connect a 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.

Step 2   Configure the line and port on the terminal server. 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
```

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.

Installing the IPS 4345 and IPS 4360 System Images

✎

Note   This procedure is for IPS 4345, but is also applicable to IPS 4360. The system image for IPS 4360 has "4360" in the filename.

You can install the IPS 4345 and IPS 4360 system image by using the ROMMON on the appliance to TFTP the system image on to the compact flash device. To install the IPS 4345 and IPS 4360 system image, follow these steps:

Step 1   Download the IPS 4345 system image file to the tftp root directory of a TFTP server that is accessible from your IPS 4345.

✎

Note   Make sure you can access the TFTP server location from the network connected to the Ethernet port of your IPS 4345.

Step 2   Boot the IPS 4345.

```
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-4345-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

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 the IPS 4345.

- Server—TFTP server IP address where the application image is stored.

- Gateway—Gateway IP address used by the IPS 4345.

- Port—Ethernet interface used for the IPS 4345 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 Management 0/0, which corresponds to the MGMT interface of the IPS 4345.

```
rommon> PORT=interface_name
```

Step 6   If necessary, assign an IP address for the local port on the IPS 4345.

```
rommon> ADDRESS=ip_address
```

> **Note**   Use the same IP address that is assigned to the IPS 4345.

Step 7   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-4345-K9-sys-1.1-a-7.3-1-E4.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-4345-K9-sys-1.1-a-7.3-1-E4.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 the IPS 4345 while the system image is being installed.

> ✎
>
> **Note**   If the network settings are correct, the system downloads and boots the specified image on the IPS 4345. Be sure to use the IPS 4345 image.

For More Information

- For a list of supported TFTP servers, see TFTP Servers, page D-14.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-1.

Installing the IPS 4510 and IPS 4520 System Image

> ✎
>
> **Note**   The following procedure references the IPS 4510 but it also refers to the IPS 4520.

You can install the IPS 4510 and IPS 4520 system image by using the ROMMON on the appliance to TFTP the system image onto the compact flash device.

To install the IPS 4510 system image, follow these steps:

Step 1   Download the IPS 4510 system image file to the tftp root directory of a TFTP server that is accessible from your IPS 4510.

> ✎
>
> **Note**   Make sure you can access the TFTP server location from the network connected to the Management port of your IPS 4510.

Step 2   Boot the IPS 4510.

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

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—Specifies the local IP address of the IPS 4510.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the IPS 4510.
- Port—Specifies the Ethernet interface used for IPS 4510 management.
- VLAN—Specifies the VLAN ID number (leave as untagged).
- Image—Specifies the 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 Managment port on the IPS 4510.

```
rommon> ADDRESS=ip_address
```

> ✎
>
> **Note**   Use the same IP address that is assigned to the IPS 4510.

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/IPS-4510-K9-sys-1.1-a-7.3-1-E4.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\IPS-4510-K9-sys-1.1-a-7.3-1-E4.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 the IPS 4510 while the system image is being installed.

> **Note**   If the network settings are correct, the system downloads and boots the specified image on the IPS 4510. Be sure to use the IPS 4510 image.

For More Information

- For a list of supported TFTP servers, see TFTP Servers, page D-14.
- For the procedure for locating software on Cisco.com, see Obtaining Cisco IPS Software, page C-1.