



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, page 22-1](#)
- [Upgrades, Downgrades, and System Images, page 22-2](#)
- [Supported FTP and HTTP/HTTPS Servers, page 22-3](#)
- [Upgrading the Sensor, page 22-4](#)
- [Configuring Automatic Upgrades, page 22-8](#)
- [Downgrading the Sensor, page 22-11](#)
- [Recovering the Application Partition, page 22-12](#)
- [Installing System Images, page 22-13](#)

Upgrade Notes and Caveats

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

- Anomaly detection has been disabled by default in IPS 7.1(2)E4 and later. If you did not configure the operation mode manually before the upgrade, it defaults to inactive after you upgrade to IPS 7.1(2)E4 or later. 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.
- This service pack automatically reboots the sensor to apply the changes. During reboot, inline network traffic is disrupted.
- You cannot uninstall IPS 7.1(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 7.1 to 7.0. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.0, you must reimage the sensor.
- 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).

- 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.
- 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 accessing downloads on Cisco.com, see [Obtaining Cisco IPS Software](#), page 21-1.
- For the procedure for using the **upgrade** command to upgrade the sensor, see [Upgrading the Sensor](#), page 22-4.
- For the procedure for configuring automatic upgrades on the sensor, see [Configuring Automatic Upgrades](#), page 22-8.
- For the procedure for using the **recover** command, see [Recovering the Application Partition](#), page 22-12.
- For the procedure for installing the IPS 4240 and IPS 4255 system image, see [Installing the System Images for the IPS-4240 and IPS-4255](#), page 22-15.
- For the procedure for installing the IPS 4260 system image, see [Installing the System Image for the IPS 4260](#), page 22-18.
- For the procedure for installing the IPS 4270-20 system image, see [Installing the System Image for the IPS 4270-20](#), page 22-20.
- For the procedure for installing the IPS 4345 and IPS 4360 system image, see [Installing the System Image for the IPS 4345 and IPS 4360](#), page 22-22.
- For the procedure for installing the IPS 4510 and IPS 4520 system image, see [Installing the System Image for the IPS 4510 and IPS 4520](#), page 22-26.
- For the procedure for installing the ASA 5500 AIP SSM system image, see [Installing the System Image for the ASA 5500 AIP SSM](#), page 22-28.
- For the procedure for installing the ASA 5500-X IPS SSP system image, see [Installing the System Image for the ASA 5500-X IPS SSP](#), page 22-31.
- For the procedure for installing the ASA 5585-X IPS SSP system image, see [Installing the System Image for the ASA 5585-X IPS SSP](#), page 22-32.

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 7.1 to 7.0. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.0, 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).

**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.

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.

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 [Basic Sensor Setup, page 3-5](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).

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 21-1](#).
- For the procedure for configuring automatic updates, see [Configuring Automatic Upgrades, page 22-8](#).

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 7.1 Upgrade Files](#), page 22-4
- [Upgrade Notes and Caveats](#), page 22-4
- [Manually Upgrading the Sensor](#), page 22-4
- [Upgrading the Sensor](#), page 22-5
- [Upgrading the Recovery Partition](#), page 22-7

IPS 7.1 Upgrade Files

The currently supported IPS 7.1(x) versions are 7.1(1)E4, 7.1(2)E4, 7.1(3)E4, and 7.1(4)E4, 7.1(5)E4, and 7.1(6)E4. All IPS sensors are not supported in each 7.1(x) version.

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 21-1.

Upgrade Notes and Caveats

For a list of the upgrade notes and caveats for each IPS version, 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

Manually Upgrading the Sensor



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.



Caution

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.

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 7.1 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-SSP_10-K9-7.1-3-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-SSP_10-K9-7.1-3-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 7.1(3)E4
```

```
Host:
```

```
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S605.0          2011-10-25
OS Version:          2.6.29.1
Platform:            ASA5585-SSP-IPS10
Serial Number:       123456789AB
```

```
No license present
```

```
Sensor up-time is 11 days.
```

```
Using 4395M out of 5839M bytes of available memory (75% usage)
system is using 26.2M out of 160.0M bytes of available disk space (16% usage)
application-data is using 69.6M out of 171.6M bytes of available disk space (43% usage)
boot is using 57.3M out of 70.5M bytes of available disk space (86% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)
```

```
MainApp           S-2011_NOV_16_00_20_7_1_3_46  (Release)  2011-11-16T00:23:0 6-0600
Running
AnalysisEngine    S-2011_NOV_16_00_20_7_1_3_46  (Release)  2011-11-16T00:23:0 6-0600
Running
CollaborationApp S-2011_NOV_16_00_20_7_1_3_46  (Release)  2011-11-16T00:23:0 6-0600
Running
CLI               S-2011_NOV_16_00_20_7_1_3_46  (Release)  2011-11-16T00:23:0 6-0600
```

```
Upgrade History:
```

```
  IPS-K9-7.1-3-E4   00:30:07 UTC Wed Nov 16 2011
```

```
Recovery Partition Version 1.1 - 7.1(3)E4
```

```
Host Certificate Valid from: 16-Nov-2011 to 16-Nov-2013
```

```
sensor#
```

For More Information

- For a list of supported FTP and HTTP/HTTPS servers, see [Supported FTP and HTTP/HTTPS Servers](#), page 22-3.
- For a list of the specific upgrade files, see [IPS 7.1 Upgrade Files](#), page 22-4.
- For the procedure for locating software on Cisco and obtaining an account with cryptographic privileges, see [Obtaining Cisco IPS Software](#), page 21-1.
- For the IDM procedure for upgrading the sensor, refer to [Manually Updating the Sensor](#). For the IME procedure, refer to [Manually Updating the Sensor](#).

Upgrading the Recovery Partition

**Note**

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

**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-SSP_10-K9-r-1.1-a-7.1-3-E4.pkg
```

```
sensor(config)#
```

```
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.1-3-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 22-3](#).
- For a list of the specific recovery filenames, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).
- For the procedure for using the **recover** command, see [Recovering the Application Partition Image, page 22-12](#).

Configuring Automatic Upgrades



Note

For the IDM procedure for automatically upgrading the sensor, refer to [Configuring Automatic Update](#). For the IME procedure, refer to [Configuring Automatic Update](#).



Caution

In IPS 7.1(5)E4 and later the default value of the Cisco server IP address has been changed from 198.133.219.25 to 72.163.4.161 in the Auto Update URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new IP address.

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.

Use the **auto-upgrade-option enabled** command in the service host submode to configure automatic upgrades. The following options apply:

- **cisco-server**—Enables automatic signature and engine updates from Cisco.com.
- **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**— Specifies the directory where upgrade files are located on the file server. A leading '/' indicates an absolute path.
- **file-copy-protocol**— Specifies the 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**—Specifies the IP address of the file server.
- **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 0 to 8760.
 - **start-time**—Specifies the time of day to start the first automatic upgrade. The valid value is *hh:mm[:ss]*.
- **user-name**—Specifies the username for server authentication.
- **user-server**—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.

**Caution**

In IPS 7.1(5)E4 and later the default value of the Cisco server IP address has been changed from 198.133.219.25 to 72.163.4.161 in the Auto Update URL configuration. If you have automatic update configured on your sensor, you may need to update firewall rules to allow the sensor to connect to this new IP address.

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 22-3](#).
- For the CLI procedure for adding the SCP server to the SSH known hosts list, see [Adding Hosts to the SSH Known Hosts List, page 4-46](#).
- For the output of the **show statistics host** command, see [Displaying Statistics, page 17-31](#).
- For the IDM procedure for automatically upgrading the sensor, refer to [Configuring Automatic Update](#). For the IME procedure, refer to [Configuring Automatic Update](#).

Downgrading the Sensor



Caution

You cannot use the **downgrade** command to revert to a previous major or minor version, for example, from Cisco IPS 7.1 to 7.0. You can only use the **downgrade** command to downgrade from the latest signature update or signature engine update. To revert to 7.0, you must reimagine 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. 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 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 more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).
- For the procedure for using the **setup** command to initialize the sensor, see [Basic Sensor Setup, page 3-5](#).
- For the procedure for upgrading the recovery partition to the most recent version, see [Upgrading the Recovery Partition, page 22-7](#).

Installing System Images



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.

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

- [ROMMON, page 22-14](#)
- [TFTP Servers, page 22-14](#)
- [Connecting an Appliance to a Terminal Server, page 22-14](#)
- [Installing the System Images for the IPS-4240 and IPS-4255, page 22-15](#)
- [Installing the System Image for the IPS 4260, page 22-18](#)
- [Installing the System Image for the IPS 4270-20, page 22-20](#)
- [Installing the System Image for the IPS 4345 and IPS 4360, page 22-22](#)
- [Installing the System Image for the IPS 4510 and IPS 4520, page 22-26](#)
- [Installing the System Image for the ASA 5500 AIP SSM, page 22-28](#)
- [Installing the System Image for the ASA 5500-X IPS SSP, page 22-31](#)
- [Installing the System Image for the ASA 5585-X IPS SSP, page 22-32](#)

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 22-14](#).

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 System Images for the IPS-4240 and IPS-4255

**Note**

This procedure is for the IPS 4240, but is also applicable to the IPS 4255. The system image for the IPS 4255 has “4255” in the filename.

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

- Step 1** Download the IPS 4240 system image file 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 the IPS 4240.

```
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

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 4240
- Server—TFTP server IP address where the application image is stored
- Gateway—Gateway IP address used by the IPS 4240
- Port—Ethernet interface used for the 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 Management 0/0, which corresponds to the MGMT interface of the IPS 4240.

```
rommon> PORT=interface_name
```

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

```
rommon> ADDRESS=ip_address
```



Note Use the same IP address that is assigned to the 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-7.0-4-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-4240-K9-sys-1.1-a-7.0-4-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 4240 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 4240. Be sure to use the IPS 4240 image.

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).

Installing the System Image for the IPS 4260

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 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 the 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**.

```
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 Management 0/0 is being used.



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



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

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

```
rommon> address ip_address
```



Note Use the same IP address that is assigned to the 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-7.0-4-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 file location.

Windows Example

```
rommon> file <tftpboot_directory>IPS-4260-K9-sys-1.1-a-7.0-4-E4.img
```

Step 10 Download and install the system image.

```
rommon> tftp
```



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

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).

Installing the System Image for the IPS 4270-20

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 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 the IPS 4270-20.

```
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

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 4270-20.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the IPS 4270-20.
- Port—Specifies the Ethernet interface used for IPS 4270-20 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 local port on the IPS 4270-20.

```
rommon> ADDRESS=ip_address
```



Note Use the same IP address that is assigned to the 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/IPS-4270_20-K9-sys-1.1-a-7.1-3-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-4270_20-K9-sys-1.1-a-7.1-3-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 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 the IPS 4270-20. Be sure to use the IPS 4270-20 image.

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).

Installing the System Image for the IPS 4345 and IPS 4360

**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-7.1-3-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-7.1-3-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 more information about TFTP servers, see [TFTP Servers](#), page 22-14.
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files](#), page 22-4.
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software](#), page 21-1.

Installing the System Image for the IPS 4510 and IPS 4520

**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 Management 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-7.1-4-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-7.1-4-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 more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for locating software on Cisco.com, see [Obtaining Cisco IPS Software, page 21-1](#).

Installing the System Image for the ASA 5500 AIP SSM

This section describes how to install the ASA 5500 AIP SSM system image, and contains the following topics:

- [Reimaging the ASA 5500 AIP SSM, page 22-28](#)
- [Reimaging the ASA 5500 AIP SSM Using the recover configure/boot Command, page 22-28](#)

Reimaging the ASA 5500 AIP SSM

You can reimage the ASA 5500 AIP SSM in one of the following ways:

- From the adaptive security appliance using the **hw-module module 1 recover configure/boot** command.
- 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.

For More Information

- For the procedure for using the **hw-module module 1 recover configure/boot** command, see [Reimaging the ASA 5500 AIP SSM Using the recover configure/boot Command, page 22-28](#).
- For the procedure for recovering the application partition, see [Recovering the Application Partition, page 22-12](#).
- For the procedure for upgrading the recovery image, see [Upgrading the Recovery Partition, page 22-7](#).

Reimaging the ASA 5500 AIP SSM Using the recover configure/boot Command

**Note**

Be sure the TFTP server that you specify can transfer files up to 60 MB in size.

**Note**

This process can take approximately 15 minutes to complete, depending on your network and the size of the image.

If the ASA 5500 AIP SSM suffers a failure and the module application image cannot run, you can transfer application images from a TFTP server to the module using the adaptive security appliance CLI. The adaptive security appliance can communicate with the module ROMMON application to transfer the image.

To install the system image of the ASA 5500 AIP SSM, follow these steps:

- Step 1** Download the system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.



Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of the adaptive security appliance.

- Step 2** Log in to the adaptive security appliance.

- Step 3** Enter enable mode.

```
asa# enable
```

- Step 4** Configure the recovery settings for the ASA 5500 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 5** Specify the TFTP URL for the system image.

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

Example

```
Image URL [tftp://0.0.0.0/]: tftp://192.0.2.0/IPS-SSP-K9-sys-1.1-a-7.1-2-E4.img
```

- Step 6** Specify the command and control interface of the ASA 5500 AIP SSM.



Note The port IP address is the management IP address of the ASA 5500 AIP SSM.

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

Example

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

- Step 7** Leave the VLAN ID at 0.

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

- Step 8** Specify the default gateway of the ASA 5500 AIP SSM.

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

Example

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

Step 9 Execute the recovery.

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

This transfers the image from the TFTP server to the ASA 5500 AIP SSM.

Step 10 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	7.1(1)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 The Status field in the output indicates the operational status of the ASA 5500 AIP SSM. An ASA 5500 AIP SSM operating normally shows a status of “Up.” While the adaptive security appliance transfers an application image to the ASA 5500 AIP SSM, the Status field in the output reads “Recover.” When the adaptive security appliance completes the image transfer and restarts the ASA 5500 AIP SSM, the newly transferred image is running.



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 11 Session to the ASA 5500 AIP SSM and initialize it with the **setup** command.

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for initializing the ASA 5500 AIP SSM, see [Advanced Setup for the ASA 5500 AIP SSM, page 3-14](#).

Installing the System Image for the ASA 5500-X IPS SSP



Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.



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 7.1 version you have installed.

To install the system image on the ASA 5500-X IPS SSP, follow these steps:

Step 1 Download the IPS system image file corresponding to your ASA platform to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.



Note Make sure you can access the TFTP server location from the network connected to the Ethernet port of the adaptive security appliance.

Step 2 Log in to the adaptive security appliance.

Step 3 Enter enable mode.

```
asa> enable
```

Step 4 Copy the IPS image to the disk0 flash of the adaptive security appliance.

```
asa# copy tftp://192.0.2.0/directory/IPS-5545-K9-sys-1.1-a-7.1-3-E4.aip disk0:
```

Step 5 Image the ASA 5500-X IPS SSP.

```
asa# sw-module module ips recover configure image
disk0:/IPS-SSP_5545-K9-sys-1.1-a-7.1-3-E4.aip
```

Step 6 Execute the recovery. This transfers the image from the TFTP server to the ASA 5500-X IPS SSP and restarts it.

```
asa# sw-module module ips recover boot
```

Step 7 Periodically check the recovery until it is complete.

```
asa# show module
```

Mod	Card	Type	Model	Serial No.
0		Cisco ASA 5545 Appliance with 8 GE ports, 1	ASA5545	ABC1234D56E
1		IPS 5545 Intrusion Protection System	IPS5545	ABC1234D56E

Mod	MAC Address Range	Hw Version	Fw Version	Sw Version
0	503d.e59c.6dc1 to 503d.e59c.6dca	1.0		8.6.1
ips	503d.e59c.6dcb to 503d.e59c.6dcb	N/A	N/A	7.1(3)E4

Mod	SSM Application Name	Status	SSM Application Version
1	IPS	Up	7.1(3)E4

Mod	Status	Data Plane Status	Compatibility
0	Up	Sys	Not Applicable

```
1 Up Up
```

```
asa#
```



Note The Status field in the output indicates the operational status of the ASA 5500-X IPS SSP. An ASA 5500-X IPS SSP operating normally shows a status of “Up.” While the adaptive security appliance transfers an application image to the ASA 5500-X IPS SSP, the Status field in the output reads “Recover.” When the adaptive security appliance completes the image transfer and restarts the ASA 5500-X IPS SSP, the newly transferred image is running.



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 8 Session to the ASA 5500-X IPS SSP and initialize it with the **setup** command.

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for initializing the ASA 5500-X IPS SSP, see [Advanced Setup for the ASA 5500-X IPS SSP, page 3-18](#).

Installing the System Image for the ASA 5585-X IPS SSP

This section describes how to install the ASA 5585-X IPS SSP system image using the **hw-module** command or ROMMON, and contains the following topics:

- [Installing the ASA 5585-X IPS SSP System Image Using the hw-module Command, page 22-32](#)
- [Installing the ASA 5585-X IPS SSP System Image Using ROMMON, page 22-35](#)

Installing the ASA 5585-X IPS SSP System Image Using the hw-module Command



Note Be sure the TFTP server that you specify can transfer files up to 60 MB in size.



Note This process can take approximately 15 minutes to complete, depending on your network and the size of the image.



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 7.1 version you have installed.

To install the system image, transfer the software image from a TFTP server to the ASA 5585-X IPS SSP using the adaptive security appliance CLI. The adaptive security appliance can communicate with the ROMMON application of the ASA 5585-X IPS SSP to transfer the image. To install the ASA 5585-X IPS SSP software image, follow these steps:

- Step 1** Download the ASA 5585-X IPS SSP system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.



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

- Step 2** Log in to the adaptive security appliance.

- Step 3** Enter enable mode.

```
asa# enable
```

- Step 4** Configure the recovery settings for the ASA 5585-X IPS SSP.

```
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 5** Specify the TFTP URL for the software image.

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

Example

```
Image URL [tftp://0.0.0.0/]: tftp://192.0.2.0/IPS-SSP_40-K9-sys-1.1-a-7.1-3-E4.img
```

- Step 6** Specify the command and control interface of the ASA 5585-X IPS SSP.



Note The port IP address is the management IP address of the ASA 5585-X IPS SSP.

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

Example

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

- Step 7** Leave the VLAN ID at 0.

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

- Step 8** Specify the default gateway of the ASA 5585-X IPS SSP.

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

Example

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

- Step 9** Execute the recovery. This transfers the software image from the TFTP server to the ASA 5585-X IPS SSP and restarts it.

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

Step 10 Periodically check the recovery until it is complete.



Note The status reads `Recovery` during recovery and reads `Up` when installation is complete.

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:                ASA5585-SSP-IPS40
Hardware version:     1.0
Serial Number:        JAF1350ABSL
Firmware version:     2.0(1)3
Software version:     7.1(3)E4
MAC Address Range:   8843.e12f.5414 to 8843.e12f.541f
App. name:            IPS
App. Status:          Up
App. Status Desc:     Normal Operation
App. version:         7.1(3)E4
Data plane Status:    Up
Status:               Up
Mgmt IP addr:         192.0.2.0
Mgmt Network mask:    255.255.255.0
Mgmt Gateway:         10.89.148.254
Mgmt Access List:    10.0.0.0/8
Mgmt Access List:    64.0.0.0/8
Mgmt web ports:       443
Mgmt TLS enabled     true
asa#
```



Note The Status field in the output indicates the operational status of the ASA 5585-X IPS SSP. An ASA 5585-X IPS SSP operating normally shows a status of “Up.” While the adaptive security appliance transfers the software image to the ASA 5585-X IPS SSP, the Status field in the output reads “Recover.” When the adaptive security appliance completes the software image transfer and restarts the ASA 5585-X IPS SSP, the newly transferred image is running.



Note To debug any errors that may happen during this process, use the **debug module-boot** command to enable debugging of the software installation process.

Step 11 Session to the ASA 5585-X IPS SSP.

Step 12 Enter `cisco` three times and your new password twice.

Step 13 Initialize the ASA 5585-X IPS SSP with the **setup** command.

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for initializing the ASA 5585-X IPS SSP, see [Advanced Setup for the ASA 5585-X IPS SSP, page 3-21](#).

Installing the ASA 5585-X IPS SSP System Image Using ROMMON

You can install the ASA 5585-X IPS SSP system image by using the ROMMON on the adaptive security appliance to TFTP the system image onto the ASA 5585-X IPS SSP.

To install the ASA 5585-X IPS SSP system image, follow these steps:

- Step 1** Download the ASA 5585-X IPS SSP system image file to the tftp root directory of a TFTP server that is accessible from your adaptive security appliance.



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

- Step 2** Boot the ASA 5585-X IPS SSP.

Booting system, please wait...

```
CISCO SYSTEMS
Embedded BIOS Version 0.0(2)10 11:16:38 04/15/10
Com KbdBuf SMM UsbHid Msg0 Prompt Pmrt Cache1 LowM ExtM HugeM Cache2 Flg Siz0 Amrt PMM
PnpDsp Smbios Lpt0 Npx1 Apm Lp1 Acpi Typ Dbg Enb Mp MemReduce MemSync1 CallRoms MemSync2
DriveInit
```

```
Total memory : 12 GB
Total number of CPU cores : 8
Com Lp1 Admgr2 Brd10 Plx2 OEM0=7EFF5C74
Cisco Systems ROMMON Version (1.0(12)10) #0: Thu Apr 8 00:12:33 CDT 2010
```

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

```
Management0/0
Link is UP
MAC Address: 5475.d029.7fa9
```

- 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 #0> 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=4
RETRY=20
```

The variables have the following definitions:

- Address—Specifies the local IP address of the ASA 5585-X IPS SSP.
- Server—Specifies the TFTP server IP address where the application image is stored.
- Gateway—Specifies the gateway IP address used by the ASA 5585-X IPS SSP.
- Port—Specifies the ethernet interface used for the ASA 5585-X IPS SSP management.
- VLAN—Specifies the VLAN ID number (leave as untagged).
- Image—Specifies the system image file/path name.
- Config—Specifies the 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 management interface of the ASA 5585-X IPS SSP.

```
rommon> PORT=interface_name
```

Step 6 If necessary, assign an IP address for the local port on the ASA 5585-X IPS SSP.

```
rommon> ADDRESS=ip_address
```



Note Use the same IP address that is assigned to the ASA 5585-X IPS SSP.

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-SSP_10-K9-sys-1.1-a-7.1-3-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-SSP_10-K9-sys-1.1-a-7.1-3-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
```

**Note**

If the network settings are correct, the system downloads and boots the specified image on the ASA 5585-X IPS SSP. Be sure to use the ASA 5585-X IPS SSP image.

**Caution**

To avoid corrupting the system image, do not remove power from the ASA 5585-X IPS SSP while the system image is being installed.

For More Information

- For more information about TFTP servers, see [TFTP Servers, page 22-14](#).
- For a list of the specific system image files, see [IPS 7.1 Upgrade Files, page 22-4](#).
- For the procedure for initializing ASA 5585-X IPS SSP, see [Advanced Setup for the ASA 5585-X IPS SSP, page 3-21](#).

