



Upgrading PIX Firewall Software

This chapter describes how to upgrade the software image on your Cisco PIX Firewall. It contains the following sections:

- [Before You Start](#)
- [Getting a Console Terminal](#)
- [Downloading the Current Software](#)
- [Installing and Recovering PIX Firewall Software](#)
- [Upgrading Failover from a Previous Version](#)
- [TFTP Download Error Codes](#)

Before You Start

PIX Firewall displays a warning message if the configuration file (stored in Flash memory) is newer than the PIX Firewall software version currently being loaded. This message warns you of the possibility of unrecognized commands in the configuration file. For example, if you install version 5.3 software when the current version is 6.0, the following message appears at startup:

```
Configuration Compatibility Warning:  
The config is from version 6.0(1).  
but the image is version 5.3(2).
```

In the message, “config” is the version in Flash memory and “image” is the version you are installing.



Caution

Before upgrading from a previous version, save your configuration and write down your activation key.

Getting a Console Terminal

If the computer you are connecting to runs Windows, the Windows HyperTerminal accessory provides easy-to-use software for communicating with the PIX Firewall. If you are using UNIX, refer to your system documentation for a terminal program.

HyperTerminal also allows you to cut and paste configuration information from your computer to the PIX Firewall console.

Follow these steps to configure HyperTerminal:

-
- Step 1** Connect the serial port of your PC to the console port of the PIX Firewall with the serial cable supplied in the PIX Firewall accessory kit.
- Step 2** Locate HyperTerminal by opening the Windows 95 or Windows NT **Start** menu and clicking **Programs>Accessories>HyperTerminal**.
- Step 3** Double-click the Hypertrm accessory. The New Connection window opens with the smaller Connection Description dialog box in the center.
- Step 4** Enter the name of the connection. You can use any name such as PIX Console. Click **OK** when you are ready to continue.
- Step 5** At the Phone Number dialog box, ignore all the fields except “Connect using.” In this field, click the arrow at the right to view the choices. Click “Direct to Com 1,” unless you are using another serial port. Click **OK** to continue.
- Step 6** At the COM1 Properties dialog box, set the following fields:
- Bits per second to 9600.
 - Data bits to 8.
 - Parity to None.
 - Stop bits to 1.
 - Flow control to Hardware.
- Step 7** Click **OK** to continue.
- Step 8** The HyperTerminal window is now ready to receive information from the PIX Firewall console. If the serial cable is connected to the PIX Firewall, power on the PIX Firewall and you should be able to view the console startup display.
- If nothing happens, first wait 60 seconds. The PIX Firewall does not send information for about 30 seconds. If messages do not appear after 60 seconds, press the **Enter** key. If still nothing appears, ensure that the serial cable is attached to COM1 and not to COM2 if your computer is so equipped. If garbage characters appear, ensure that the bits per second setting is 9600.
- Step 9** On the **File** menu, click **Save** to save your settings.
- Step 10** On the **File** menu, click **Exit** to exit HyperTerminal. HyperTerminal prompts you to be sure you want to disconnect. Click **Yes**.
-

HyperTerminal saves a log of your console session that you can access the next time you use it.

To restart HyperTerminal, double-click the connection name you chose in the HyperTerminal folder. When HyperTerminal starts, drag the scroll bar up to view the previous session.

Downloading the Current Software

This section includes the following topics:

- [Getting a TFTP Server](#)
- [Downloading Software from the Web](#)
- [Downloading Software with FTP](#)

If you registered cisco.com user, you can obtain software from the following site:

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>

To become a registered user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

The software available at this website includes the following items:

- **bh5nn.bin**—Allows you to create a “Boothelper” installation diskette required to download version 6.1 PIX Firewall software from a TFTP server.
- **pix60n.bin**—The latest software image. Place this image in the TFTP directory so it can be downloaded to the PIX Firewall unit.
- **pfss6nn.exe**—Contains the PIX Firewall Syslog Server (PFSS), which installs on a Windows NT Server so that it can receive syslog messages from the PIX Firewall and store them in daily log files. The PIX Firewall sends messages to the PFSS via TCP or UDP and can receive syslog messages from up to 10 PIX Firewall units.
- **rawrite.exe**—A program you use to create a Boothelper diskette for the PIX Firewall.

Getting a TFTP Server



Note

If you are using a PIX Firewall unit that contains a diskette drive, use a “Boothelper” diskette to download the PIX Firewall image with TFTP. If your site has a Cisco router, the use of TFTP is similar to the way you download Cisco IOS software to your router.

You should have a TFTP server to install the PIX Firewall software. If your computer runs the Windows operating system and you are a registered cisco.com user, you can download a TFTP server from Cisco from the Web or by FTP.

You can download the server from the Web at the following website:

<http://www.cisco.com/cgi-bin/tablebuild.pl/tftp>

To become a registeredcisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

Follow these steps to download the server by FTP:

- Step 1** Start your FTP client and connect to **cco.cisco.com**, using your cisco.com username and password.
- Step 2** You can view the files in the main directory by entering the **ls** command.
- Step 3** Enter the **cd cisco** command to move to the top level software directory. Then enter **cd tftp** to access the TFTP software directory. Use the **ls** command to view the directory contents.

- Step 4** Use the **get** command to copy the TFTP executable file to your directory.
-

Downloading Software from the Web

You can obtain PIX Firewall software by downloading it from Cisco's website or FTP site. If you are using FTP, refer to "Downloading Software with FTP."

Before downloading software, you need to be a registered cisco.com user. You can register at the following website:

<http://tools.cisco.com/RPF/register/register.do>

Follow these steps to install the latest PIX Firewall software:

- Step 1** Use a network browser, such as Netscape Navigator to access <http://www.cisco.com>.
- Step 2** If you are a registered cisco.com user, click **LOGIN** in the upper area of the page. If you have not registered, click **REGISTER** and follow the steps to register.
- Step 3** After you click **LOGIN**, a dialog box appears requesting your Username and Password. Enter these and click **OK**.
- Step 4** Access cisco.com at <http://www.cisco.com> and log in. Then access the PIX Firewall software downloads at the following website:
<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>
- Step 5** Obtain the software you need. If you have a PIX Firewall unit with a diskette drive, obtain the Boothelper binary image file bh512.bin so you can store a PIX Firewall image on a diskette. If you have a PIX 506, PIX 515, PIX 525, or PIX 535 you can skip the discussion of the Boothelper diskette.
-

Downloading Software with FTP

Before using FTP, you need to be a registered cisco.com user. To register, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

Once you have registered, set your FTP client for passive mode. If you are not running in passive mode, you can log in and view the Cisco presentation messages, but entering commands will cause your client to appear to suspend execution.

The Windows 95 and Windows NT command line FTP programs do not support passive mode.

Follow these steps to get the most current software with FTP:

- Step 1** Start your FTP client and connect to **cco.cisco.com**, using your cisco.com username and password.
- Step 2** You can view the files in the main directory by entering the **ls** command.
- Step 3** Enter the **cd cisco** command to move to the top level software directory. Then enter **cd internet** and **cd pix** to access the PIX Firewall software directory. Use the **ls** command to view the directory contents.
- Step 4** Use the **get** command to copy the proper file to your workstation as described at the start of the current section.

- Step 5** If you have not done so already, you can also download a TFTP server for use with Windows by using the `cd ..` command to return to the **internet** directory. Then use the `cd tftp` command to access the TFTP software directory. Use the `get` command to copy the TFTP executable file to your directory.
- Step 6** If you want documentation, use the `cd documentation` command from the `pix` directory and copy the files you need to your workstation. Files with the `.pdf` suffix can be viewed with Adobe Acrobat Reader, which you can download from the following website:
<http://www.adobe.com/prodindex/acrobat/readstep.html>
- Step 7** When you are done, enter `quit` to exit.
-

Installing and Recovering PIX Firewall Software

This section contains the following topics:

- [Installing Image Software from the Command Line](#)
- [Using Monitor Mode to Recover the PIX Firewall Image](#)
- [Using Boothelper](#)
- [Downloading an Image with Boothelper](#)

Installing Image Software from the Command Line

To use TFTP to install a software image from the PIX Firewall command line, enter the following command:

```
copy tftp flash
```

You can use this command with any PIX Firewall running Version 5.1 or higher. When you enter this command, the PIX Firewall prompts for the specific values required to complete the operation. You can also use a colon (:) to take the parameters from the `tftp-command` settings, or you can explicitly specify each parameter. For details, refer to the `copy tftp flash` command in the [Cisco PIX Firewall Command Reference](#).



Caution

Never download a PIX Firewall image earlier than Version 4.4 with TFTP. Doing so will corrupt the PIX Firewall Flash memory unit.

Using Monitor Mode to Recover the PIX Firewall Image

You can use monitor mode to recover the PIX Firewall image when it has been lost or corrupted and you do not have access to the PIX Firewall command line.



Note

You must use a 1FE or 4FE card installed in a 32-bit slot for installing image software with monitor mode. You cannot use monitor mode to connect to a TFTP server through a Gigabit Ethernet card, a 4FE-66 card, or a Fast Ethernet card installed in a 64-bit slot.

Use the following steps to download an image over TFTP using the **monitor** command:

-
- Step 1** Immediately after you power on the PIX Firewall and the startup messages appear, send a BREAK character or press the **Esc** (Escape) key.
The monitor> prompt appears.
 - Step 2** If desired, enter a question mark (?) to list the available commands.
 - Step 3** Use the **address** command to specify the IP address of the PIX Firewall unit's interface on which the TFTP server resides.
 - Step 4** Use the **server** command to specify the IP address of the host running the TFTP server.
 - Step 5** Use the **file** command to specify the filename of the PIX Firewall image. In UNIX, the file needs to be world readable for the TFTP server to access it.
 - Step 6** If needed, enter the **gateway** command to specify the IP address of a router gateway through which the server is accessible.
 - Step 7** If needed, use the **ping** command to verify accessibility. Use the **interface** command to specify which interface the ping traffic should use. If the PIX Firewall has only two interfaces, the **monitor** command defaults to the inside interface. If this command fails, fix access to the server before continuing.
 - Step 8** Use the **tftp** command to start the download.

An example follows:

```
Rebooting...
PIX BIOS (4.0) #47: Sat May 8 10:09:47 PDT 2001
Platform PIX-525
Flash=AT29C040A @ 0x300

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Flash boot interrupted.
0: i8255X @ PCI(bus:0 dev:13 irq:11)
1: i8255X @ PCI(bus:0 dev:14 irq:10)

Using 1: i82558 @ PCI(bus:0 dev:14 irq:10), MAC: 0090.2722.f0b1
Use ? for help.
monitor> addr 192.168.1.1
address 192.168.1.1
monitor> serv 192.168.1.2
server 192.168.1.2
monitor> file pix601.bin
file cdisk
monitor> ping 192.168.1.2
Sending 5, 100-byte 0x5b8d ICMP Echoes to 192.168.1.2, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
monitor> tftp
tftp pix601.bin@192.168.1.2.....
Received 626688 bytes

PIX admin loader (3.0) #0: Mon Aug 7 10:43:02 PDT 1999
Flash=AT29C040A @ 0x300
Flash version 6.0.1, Install version 6.0.1

Installing to flash
...
```

Using Boothelper

If your PIX Firewall unit has a diskette drive, you need to obtain the Boothelper binary image file `bh521.bin` and create a diskette.

This section contains the following topics:

- [Get the Boothelper Binary Image](#)
- [Preparing a Boothelper Diskette with UNIX, Solaris, or LINUX](#)
- [Preparing a Boothelper Diskette on a Windows System](#)

Get the Boothelper Binary Image

Use the following steps to download the Boothelper binary image:

-
- Step 1** Log in to cisco.com and continue to the PIX Firewall software directory, as described in the previous section, “[Downloading Software from the Web](#)” or “[Downloading Software with FTP](#).”
- Step 2** Download the `bh521.bin` Boothelper image from cisco.com and prepare a diskette as described in the sections that follow.



Note The Boothelper installation only supports PIX Firewall version 5.1, 5.2, 5.3, 6.0, and later. After Boothelper downloads the PIX Firewall image via TFTP, it verifies the checksum of the image. If it is not version 5.1 or later, it displays the message “Checksum verification on flash image failed” and reboots the PIX Firewall.

- Step 3** Download the PIX Firewall software binary image file `pix601.bin` from cisco.com and store this file in a directory accessible by your TFTP server.
-

Preparing a Boothelper Diskette with UNIX, Solaris, or LINUX

Follow these steps to prepare a Boothelper diskette:

-
- Step 1** To prepare a UNIX, Solaris, or LINUX TFTP server to provide an image to the PIX Firewall, edit the `inetd.conf` file to remove the `#` (comment character) from the start of the “`tftp`” statement.
- Step 2** Use the `ps aux | grep inetd` command string to determine the process ID of the current `inetd` process.
- Step 3** Use the `kill -HUP process_id` command to kill the process. The process will restart automatically.
- Step 4** Use the `dd` command to create the Boothelper diskette for the PIX Firewall unit. For example, if the diskette device name is `rd0`, use the following command:

```
dd bs=18b if=./bh510.bin of=/dev/rd0
```

This command copies the binary file to the output device file with a block size of 18 blocks.



Note The diskette may have a name other than `rd0` on some UNIX systems.

- Step 5** Eject the diskette, insert it in the PIX Firewall diskette drive, and power cycle the unit. Alternately, if available, use your unit's Reset switch, or enter the reload command from the PIX Firewall console. The PIX Firewall then boots from the new diskette.
-

Preparing a Boothelper Diskette on a Windows System

Follow these steps to create the Boothelper diskette from a Windows system:

- Step 1** Locate an IBM formatted diskette that does not contain useful files. Do not use the PIX Firewall boot diskette that came with your original PIX Firewall purchase—you will need this diskette for system recovery should you need to downgrade versions.
- Step 2** Enter **rawrite** at the MS-DOS command prompt and you are prompted for the name of the .bin binary file, the output device (**a:** or **b:** for a 3.5-inch diskette), and to insert a formatted diskette. A sample **rawrite** session follows.

```
C:\pix> rawrite
RaWrite 1.2 - Write disk file to raw floppy diskette

Enter source file name: bh512.bin
Enter destination drive: a:
Please insert a formatted diskette into drive A: and press -ENTER- :
Number of sectors per track for this disk is 18
Writing image to drive A:. Press ^C to abort.
Track: 78 Head: 1 Sector: 16
Done.
C:\pix>
```

Ensure that the binary filename is in the "8.3" character format (8 characters before the dot; 3 characters after the dot).

- Step 3** When you are done, eject the diskette, insert it in the PIX Firewall diskette drive, and power cycle the unit. Alternately, if available, use your unit's Reset switch, or enter the reload command from the PIX Firewall console. The PIX Firewall then boots from the new diskette.
-

Downloading an Image with Boothelper

Follow these steps to use the Boothelper diskette to download an image from a TFTP server:

- Step 1** Download a PIX Firewall image from cisco.com and store it on the host running the TFTP server.
- Step 2** Start the TFTP server on the remote host and point the TFTP server to the directory containing the PIX Firewall image. On the Cisco TFTP Server, access the **View>Options** menu and enter the name of the directory containing the image in the **TFTP server root directory** field.
- Step 3** Connect a console to the PIX Firewall and ensure that it is ready.
- Step 4** Put the Boothelper diskette you prepared in the PIX Firewall and reboot it. When the PIX Firewall starts, the `pixboothelper>` prompt appears.

- Step 5** You can now enter commands to download the binary image from the TFTP server. In most cases, you need only specify the **address**, **server**, and **file** commands, and then enter the **tftp** command to start the download. The commands are as follows:
- If needed, use a question mark (?) or enter the **help** command to list the available commands.
 - Use the **address** command to specify the IP address of the network interface on which the TFTP server resides.
 - Use the **server** command to specify the IP address of the host running the TFTP server.
 - Use the **file** command to specify the filename of the PIX Firewall image.
 - If needed, use the **gateway** command to specify the IP address of a router gateway through which the server is accessible.
 - If needed, use the **ping** command to verify accessibility. If this command fails, fix access to the server before continuing. You can use the **interface** command to specify which interface the ping traffic should use. The Boothelper defaults to the interface 1 (one).
 - Use the **tftp** command to start the download.
- Step 6** After the image downloads, you are prompted to install the new image. Enter **y**.
- Step 7** When you are prompted, enter your activation key.
- Step 8** After you enter your activation key, PIX Firewall prompts you to remove the Boothelper diskette. You have 30 seconds to remove the diskette. During this time you have three options:
- Remove the diskette and reboot the unit with the reboot switch.
 - Use the **reload** command while the diskette is in the unit.
 - After the interval, the PIX Firewall will automatically boot from the Boothelper diskette.
- After Boothelper downloads the PIX Firewall image via TFTP, it verifies the checksum of the image. If it is not version 5.1 or later, it displays the message “Checksum verification on flash image failed” and reboots the PIX Firewall.
- Keep the Boothelper diskette available for future upgrades. You will need to repeat these steps whenever you download an image to your PIX Firewall unit. Alternatively, you can use the **copy tftp flash** command to download an image directly from the PIX Firewall command line.
-

Upgrading Failover from a Previous Version

This section describes how to upgrade PIX Firewalls configured for the failover feature. It includes the following topics:

- [Upgrading Failover Systems](#)
- [Upgrading Failover Systems with Boothelper](#)

Upgrading Failover Systems

Complete the following steps for a PIX Firewall with a bios extension installed, which can TFTP from the monitor mode:

-
- Step 1** Connect a separate console to the primary unit and one to the secondary unit.
 - Step 2** Reload both PIX Firewall units, and bring them to monitor mode.
 - Step 3** On the primary unit, use monitor mode TFTP to load the new PIX Firewall image. You will want to save the image to Flash memory and let it boot up. Enter a **show failover** command to ensure everything looks fine.
 - Step 4** Repeat Step 3 on the secondary unit.
 - Step 5** Once the standby (secondary) unit completes booting and is up, the active (primary) unit will start to synchronize the configuration from the primary unit to the secondary. Wait until the configuration replication is finished, then use the **show failover** command on both PIX Firewall units to ensure the failover is running correctly.
-

Upgrading Failover Systems with Boothelper

Use the steps that follows to upgrade failover for a PIX Firewall system with a floppy diskette drive.

-
- Step 1** Connect a separate console to the primary unit and one to the secondary unit.
 - Step 2** Place the boothelper diskette in the diskette drive of the primary unit and reboot the system.
When the PIX Firewall starts, the `pixboothelper>` prompt appears.
 - Step 3** As the primary unit reboots, PIX Firewall prompts you to write the image to Flash memory. Before entering a reply, read the next three substeps and be ready to move quickly to complete them. When ready, enter **y** for yes at the prompt.
 - a.** Immediately remove the diskette from the primary unit and insert it into the standby unit. Locate the reset button on the front of the standby unit.
 - b.** When the PIX Firewall Cisco banner appears on the primary unit's console, press the reset button on the standby unit to load the new image.
 - c.** On the primary unit, enter the **show failover** command to make sure the primary unit is active and the secondary unit is in Standby mode after the upgrade of the primary unit.
 - Step 4** Wait for the standby unit to finish booting. Once the standby unit is up, the two units synchronize during which time the primary unit's console does not accept input. On the standby unit, use the **show failover** command to monitor progress. When both PIX Firewall units report Normal, the replication is done.
-

TFTP Download Error Codes

During a TFTP download, if tracing is on, non-fatal errors appear in the midst of dots that display as the software downloads. The error code appears inside angle brackets. [Table 9-1](#) lists the code values.

For example, random bad blocks appear as follows:

```
....<11>..<11>.<11>.....<11>...
```

Also, tracing will show “A” and “T” for ARP and timeouts, respectively. Receipt of non-IP packets causes the protocol number to display inside parentheses.

[Table 9-1](#) lists the TFTP error codes.

Table 9-1 Error Code Numeric Values

Error Code	Description
-1	Timeout between the PIX Firewall and TFTP server.
2	The packet length as received from the Ethernet device was not big enough to be a valid TFTP packet.
3	The received packet was not from the server specified in the server command.
4	The IP header length was not big enough to be a valid TFTP packet.
5	The IP protocol type on the received packet was not UDP, which is the underlying protocol used by TFTP.
6	The received IP packet's destination address did not match the address specified by the address command.
7	The UDP ports on either side of the connection did not match the expected values. This means either the local port was not the previously selected port, or the foreign port was not the TFTP port, or both.
8	The UDP checksum calculation on the packet failed.
9	An unexpected TFTP code occurred.
10	A TFTP transfer error occurred.
-10	The image filename you specified cannot be found. Check the spelling of the filename and that permissions permit the TFTP server to access the file. In UNIX, the file needs to be world readable.
11	A TFTP packet was received out of sequence.

Error codes 9 and 10 cause the download to stop.

