

Upgrading Software for the Cisco Secure PIX Firewall and PIX Device Manager

Document ID: 4801

Note: This document covers how to upgrade the software on a PIX 500 Series Security Appliance. In order to download PIX software, refer to the **Software Center (registered customers only)** . You must log in and possess a valid service contract in order to access the PIX software.

Contents

Introduction

Before You Begin

- Requirements
- Components Used
- Conventions
- Determine Your Upgrade Procedure
- Download Software

Upgrade the PIX Firewall from Versions 4.x.x or 5.0.x

- Appliances with a Floppy Drive
- Appliances without a Floppy Drive (Monitor Mode)
- Upgrade the PIX Firewall from Boothelper or Monitor Mode

Upgrade the PIX Firewall from Versions 5.1.1 or Later

- Use the copy tftp flash Command to Upgrade the PIX
- Upgrade PIX Devices in a Failover Set with Minimal Downtime

Recover from a Faulty Upgrade

Upgrade the Activation Key

- PIX Devices Running Versions 6.1 and Earlier
- PIX Devices Running Versions 6.2 and 6.3

Upgrade the PIX Device Manager

Obtain a Valid Service Contract

Troubleshooting

Related Information

Introduction

This document explains how to upgrade PIX Firewall software and how to upgrade the PIX Device Manager (PDM). This document is relevant for all versions of PIX Firewall Software releases 4.x to 6.3.x.

Note: This document does not cover upgrades to version 7.x. For more information on this, refer to the Cisco Secure PIX Security Appliance 7.x and ASDM Software Upgrade Procedure for version 7.x and the Adaptive Security Device Manager (ASDM).

Before You Begin

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- **Set up a TFTP Server**

In most cases, the use of a TFTP server is required for a software upgrade of the PIX Security Appliance. Cisco strongly recommends that you back up the PIX configuration to a TFTP server prior to the upgrade. Issue the **write net** command in order to back up your configuration.

For example:

```
pixfirewall# write net 10.1.1.10:pixconfig
```

Cisco no longer provides a TFTP server for download, but you can find many easy-to-use, free options through a search engine.

- **Gather Necessary Information**

In order to determine which software upgrade works for your PIX Security Appliance, gather the device specifications. Sometimes, it is necessary to have the activation key of the PIX on-hand during the upgrade procedure. Issue the **show version** command in order to obtain the necessary device information.

For example:

```
pixfirewall# show version

Cisco PIX Firewall Version 6.3(4)
Cisco PIX Device Manager Version 3.0(2)

Compiled on Fri 02-Jul-04 00:07 by morlee

pixfirewall up 29 mins 18 secs

Hardware:   PIX-501, 16 MB RAM, CPU Am5x86 133 MHz
Flash E28F640J3 @ 0x3000000, 8MB
BIOS Flash E28F640J3 @ 0xffffd8000, 128KB

0: ethernet0: address is 0015.2b95.f95c, irq 9
1: ethernet1: address is 0015.2b95.f95e, irq 10
Licensed Features:
Failover:                Disabled
VPN-DES:                 Enabled
VPN-3DES-AES:           Enabled
Maximum Physical Interfaces: 2
Maximum Interfaces:     2
Cut-through Proxy:      Enabled
Guards:                 Enabled
URL-filtering:          Enabled
Inside Hosts:           Unlimited
Throughput:             Unlimited
IKE peers:              10

This PIX has a Restricted (R) license.

Serial Number: 809324870 (0x303d5146)
Running Activation Key: 0x96cb328a 0x15e9aeaf 0xddb832cf 0xb906199e
Configuration last modified by enable_15 at 07:52:05.707 UTC Tue Jul 11 2006
```

Also, be sure to read the relevant release notes for the PIX software version in the Cisco PIX 500 Series Security Appliance Documentation.

525	applicable	applicable	flash	flash	flash	flash
PIX 535	Not applicable	Not applicable	Not applicable	copy tftp flash	copy tftp flash	copy tftp flash

Note: The PIX Firewall Classic, 10000, and 510 are discontinued and cannot run PIX Firewall Software version 6.0 or later. If you have a PIX Classic, 10000, or 510, and you want to run PIX Firewall Software 6.0 or later, contact your local Cisco Account Team or Reseller in order to purchase a newer PIX Firewall.

Download Software

PIX Security Appliance Software is only available to users with a CCO account and associated service contract. Refer to the Software Center (registered customers only) in order to download PIX software. You must log in to access the PIX software.

Upgrade the PIX Firewall from Versions 4.x.x or 5.0.x

Appliances with a Floppy Drive

These steps apply only to PIX devices that have a floppy drive. Specifically, this group is limited to the PIX Classic, 10000, 510 and 520.

- Create a bootable diskette in Windows.
- Follow the instructions in the Upgrade the PIX Firewall from Boothelper or Monitor Mode section of this document.

Complete these steps in order to create a bootable diskette in Windows:

1. Go to the PIX Software Download page (registered customers only) and download the **rawrite.exe** utility. Use this utility in order to write the PIX binary image onto a floppy diskette.
2. Download the PIX binary image (**.bin** file) that corresponds to the software version to which you want to upgrade. PIX image filenames are in the **pixnnx.bin** format, where *nn* is the version number and *x* is the release number.

Example: The file **pix611.bin** is for PIX Software release 6.1.1.

3. If you upgrade to PIX Software version 5.2 or later, you also need to download the corresponding boothelper binary file.

Example: If you upgrade from PIX Software version 4.4(8) to 6.1(1), you must download these three files:

- ◆ **rawrite.exe**
- ◆ **pix611.bin**
- ◆ **bh61.bin**

4. Locate a high-density, IBM-formatted diskette that does not contain any files.

Note: Do not use the PIX Firewall boot diskette that came with the original PIX Firewall purchase. You need this diskette for system recovery if you choose to reinstall the original version. The **rawrite.exe** program erases all the files on the diskette.

If you format the diskette from Windows, choose the long version, not the quick format. The quick format does not adequately prepare the diskette for **rawrite**. The best way to format the diskette is from the MS-DOS command prompt. Issue the **format a:command**, where *a* is the letter of the

floppy drive where the diskette is located.

5. Place the blank diskette in the floppy drive of your computer and bring up a DOS prompt. Change to the directory where you saved the **rawrite.exe** utility and the PIX files.
6. Run the **rawrite.exe** program. In order to do this, issue the **rawrite** command at the DOS prompt. When prompted, type the name of the file that you want written to the floppy diskette.

Note: If you upgrade to PIX Software version 5.1 or earlier, specify the file for the PIX image itself. It is in the format of **pixnxx.bin**. If you upgrade to PIX versions 5.2 or later, specify the PIX boot helper file, in the format of **bhnn.bin**.

Example: Create a Bootable Diskette from Windows

```
C:\>rawrite
RaWrite 1.2 - Write disk file to raw floppy diskette
Enter source file name: bh61.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: 11 Head: 1 Sector: 16
Done.
C:\>0
```

7. Once the **rawrite** process finishes, eject the diskette and insert it in the PIX Firewall diskette drive. Perform one of these actions in order to make the PIX boot from the image on the diskette.

- ◆ Power cycle the PIX.

or

- ◆ Use the reset switch of the PIX.

or

- ◆ Issue the **reload** command from the PIX console.

8. When the PIX completes the reboot, perform the appropriate step listed:

- ◆ If you upgrade to PIX Software version 5.1 or earlier, remove the floppy diskette from the drive, and you are finished.

- ◆ If you upgrade to PIX Software version 5.2 or later, then when you load the boot helper program on the floppy, the PIX comes up in boot helper mode. Proceed to the Upgrade the PIX Firewall from Boot helper or Monitor Mode section of this document in order to complete the upgrade.

Appliances without a Floppy Drive (Monitor Mode)

PIX devices that do not have an internal floppy drive come with a ROM boot monitor program that is used for the upgrade of the PIX Firewall image. Complete these steps in order to enter monitor mode on devices without a floppy drive:

1. Power cycle or reload the PIX. During bootup, you are prompted to use **BREAK** or **ESC** to interrupt Flash boot. You have ten seconds to interrupt the normal boot process.
2. Press the **ESC** key or send a **BREAK** character in order to enter monitor mode.

- ◆ If you use Windows HyperTerminal, you can press the **ESC** key or send a **BREAK** character by with the **Ctrl+Break** keystroke.

- ◆ If you Telnet through a terminal server in order to access the console port of the PIX, you must press **Ctrl]** in order to get to the Telnet command prompt. Then enter the **send break** command.

3. The `monitor>` prompt displays.
4. Proceed to the Upgrade the PIX Firewall from Boothelper or Monitor Mode section of this document.

Upgrade the PIX Firewall from Boothelper or Monitor Mode

Note: Be sure that you have followed the instructions for either section presented, Security Appliances with a floppy drive or Security Appliances without a floppy drive, before you proceed with these steps.

If you upgrade the PIX from versions 5.0.x or earlier to versions 5.1.x or later, you must use the boothelper or monitor mode method for the upgrade. This is because before version 5.1, the PIX Firewall software does not provide a way to TFTP an image directly into the Flash. Follow these steps to upgrade PIX Security Appliances with or without a floppy drive:

1. Copy the PIX Firewall binary image (`pixnnn.bin`) to the root directory of the TFTP server.
2. For PIX Classic, 10000, 510 and 520s be sure that you have already used the procedure for Creating a Bootable Diskette. Use the boothelper file that most closely corresponds to the PIX image to which you upgrade. Boot the PIX from the boothelper floppy to enter the boothelper mode.

All other PIX devices (501, 506, 515, 525 and 535) do not contain a floppy drive. Instead, they have an internal boot monitor mode. See the instructions in this document for how to Enter Monitor Mode on a PIX 501, 506, 515, 525 or 535.

Once in monitor or boothelper mode, you can use the `?` key to see a list of available options.

3. Issue the **interface** *number* command. The **interface** command specifies which PIX interface the TFTP server is connected out of. The default is interface 1 (inside).

Note: The PIX cannot initialize a Gigabit Ethernet interface from monitor or boothelper mode. Use a Fast Ethernet or Token Ring interface instead.

4. Issue the **address** *pix_interface_ip_address* command. The **address** command specifies the IP address of the PIX unit interface.
5. Issue the **server** *tftp_server_ip_address* command. The **server** command specifies the IP address of the TFTP server.
6. Issue the **file** *filename* command. The **file** command specifies the filename of the PIX Firewall image.
7. Issue the **ping** *tftp_server_ip_address* command. Ping the server in order to verify accessibility. If this command fails, double-check your cables, IP address of the server and of the PIX, and IP address of the gateway (if needed). The pings must succeed before you can continue.

Note: Issue the **gateway** command in order to specify the IP address of a router gateway through which the server is accessible:

`gateway ip_address of the gateway interface`

8. Issue the **tftp** command in order to start the download of the image from the TFTP server.
9. After the image downloads, you are prompted to install the new image. Enter **y** in order to install the image to Flash.
10. When prompted to enter a new activation key, enter **y** if you wish to enter a new activation key, or **n** to keep the existing activation key. See the Upgrade the Activation Key section of this document for more information about the activation key and how to obtain a new one.
11. If you use the boothelper mode, you are prompted to remove the boothelper diskette. You have thirty seconds to remove the diskette before the PIX automatically reboots. Remove the diskette now. Once the PIX reboots, it loads the new image from Flash.

This completes the upgrade process.

Once the PIX is upgraded to 5.1 or later, it is no longer necessary to use a floppy diskette to load new images onto the PIX. In PIX Software version 5.1 and later, the **copy tftp flash** command allows you to TFTP your new PIX image directly to the PIX from a TFTP server. Refer to the PIX Command Reference for further details.

Example – Upgrade the PIX Firewall from Boothelper or Monitor Mode

```
monitor>interface 1
0: i8255X @ PCI(bus:0 dev:14 irq:10)
1: i8255X @ PCI(bus:0 dev:13 irq:11)

Using 1: i82557 @ PCI(bus:0 dev:13 irq:11), MAC: 0002.b945.a23c
monitor>address 172.18.124.154
address 172.18.124.154
monitor>server 172.18.125.3
server 172.18.125.3
monitor>file pix611.bin
file pix611.bin
monitor>ping 172.18.125.3
Sending 5, 100-byte 0xcde2 ICMP Echoes to 172.18.125.3, timeout is 4 seconds:
!!!!
Success rate is 100 percent (5/5)
monitor>tftp
tftp pix611.bin@172.18.125.3.....
Received 2562048 bytes

Cisco Secure PIX Firewall admin loader (3.0) #0: Tue Dec 517:35:46 PST 2000
System Flash=E28F128J3 @ 0xffff0000
BIOS Flash=am29f400b @ 0xd8000
Flash version 6.1.1, Install version 6.1.1
Do you wish to copy the install image into flash? [n] y

Installing to flash

Serial Number: 480380761 (0x1ca20759)
Activation Key: 760754d0 39f62229 a4a0245f b5b87e80

Do you want to enter a new activation key? [n] n
Writing 2469944 bytes image into flash...
```

Upgrade the PIX Firewall from Versions 5.1.1 or Later

If the PIX Security Appliance is running PIX Software releases 5.1.1 or later, you can use the **copy tftp flash** command in order to download a software image with TFTP. The **copy tftp flash** command can be used with any PIX Firewall model that is running PIX Software versions 5.1.1 or later. The image you download is made available to the PIX on the next reload (reboot). Refer to the PIX Command Reference for more information on this command.

Use the copy tftp flash Command to Upgrade the PIX

Complete these steps in order to upgrade the PIX with the use of the **copy tftp flash** command.

1. Copy the PIX Firewall binary image (pix nnn .bin) to the root directory of the TFTP server.
2. Issue the **copy tftp flash** command from the PIX prompt.
3. Enter the remote host IP address.
4. Enter the PIX binary filename (has the pix nnn .bin name format).
5. Type **yes**.

Example – Upgrade the PIX Firewall with the copy tftp flash Command

```
pixfirewall#copy tftp flash
Address or name of remote host [127.0.0.1]? 172.18.125.3
Source file name [cdisk]?pix611.bin
copying tftp://172.18.125.3/pix611.bin to flash
[yes|no|again]?yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 2562048 bytes.
Erasing current image.
Writing 2469944 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed.
pixfirewall#
```

Upgrade PIX Devices in a Failover Set with Minimal Downtime

In order to use this procedure, the PIX devices must be running PIX Software version 5.1.x or later. These instructions are valid for all PIX devices that are capable of running in a failover set. Refer to How Failover Works on the Cisco Secure PIX Firewall for more information about failover.

Two different options are listed to help you upgrade the PIX with minimal downtime. The first option is the safest way to upgrade your failover set. If anything goes wrong with the upgrade process, you always have one operational PIX to pass your network traffic. The second option is simpler but involves more risk. The risk resides in the possibility that the new image that loads on the PIX devices is corrupt in some way. Both options are presented so that you can choose the best method for your specific network.

Note: If you want to upgrade the failover set from 6.x to 7.x, refer to the Upgrade PIX Appliances in a Failover Set section of Cisco Secure PIX Security Appliance 7.x and ASDM Software Upgrade Procedure.

Option 1

This is the safer way to upgrade the failover set:

1. Copy the PIX Firewall binary image (pix nnn .bin) to the root directory of the TFTP server.
2. Power off the Primary (this causes the Secondary to become active).
3. Disconnect all cables from the Primary (including the failover cable).
4. Power on the Primary and attach a PC with a TFTP server on it.
5. Issue the **copy tftp flash** command in order to upgrade the Primary.
6. Reload the Primary and verify the new version and configuration.
7. Power off the Primary.
8. Reconnect all cables back to the Primary.
9. Quickly power off the Secondary, and then immediately power on the Primary.

Note: A period of downtime occurs while the Primary boots up.

Once the Primary is up, it is active and passes traffic.

10. Repeat steps 2 through 7 for the Secondary PIX.
11. Power on the Secondary. It comes up as Standby.
12. Both PIX devices now run the upgraded version and are back to normal operation.

Option 2

This is the quicker way to upgrade the failover set:

1. Copy the PIX Firewall binary image (pix nnn .bin) to the root directory of the TFTP server.

2. Issue the **copy tftp flash** command in order to copy the new PIX image to the Primary PIX.
3. Issue the **copy tftp flash** command in order to copy the new PIX image to the Secondary PIX.
4. Power off both PIX devices.
5. Power on the Primary PIX.
6. Wait ten seconds. This ensures that the Primary PIX becomes the Active PIX.
7. Power on the Secondary PIX. It comes up at Standby.
8. Both PIX devices now run the upgraded version and are back to normal operation.

Recover from a Faulty Upgrade

Complete these steps in order to recover the PIX when there is an upgrade from PIX Software version 6.x to 6.x, and you end up with a faulty upgrade:

1. As noted earlier, be sure to copy down your activation key before you attempt this procedure.
2. Follow the steps to boot the PIX into monitor mode.
3. Follow the steps to upgrade the PIX from Monitor Mode to load the erasedisk.bin file using TFTP.
You need to get this file from Cisco Technical Support.
4. When the system re-starts, boot the PIX into monitor mode again.
5. Follow the steps for how to upgrade the PIX from Monitor Mode in order to load the new 6.x version file in the PIX using TFTP.

Upgrade the Activation Key

There are several reasons that you could need to upgrade the activation key on the PIX:

- The PIX does not currently have VPN-DES or VPN-3DES encryption enabled.

Note: VPN-DES encryption must be enabled in order for you to manage the PIX with the PDM. Registered users can obtain a free 56-bit VPN-DES activation key when they complete the PIX 56-bit License Upgrade Key form. Complete the Cisco ASA 3DES/AES License Registration to obtain a 3DES/AES key.

- The PIX currently does not have failover activated.
- The upgrade from a connection-based license to a feature-based license.

If you fall into one of these categories and have obtained a new activation key for your PIX, the next step is to connect to the PIX, issue the **show version** command, and save the output to a text file. The output of the **show version** command contains your existing version, serial number, and activation key. You need this information if there are any problems with the upgrade of the activation key.

The PIX activation key is based on the serial number of the PIX and is therefore unique for each PIX. The activation key tells the PIX what features it is licensed for. The serial number of your PIX is saved in Flash. If you replace the Flash card in your PIX, then your PIX contains a new serial number (different from the number shown on the sticker on the outside of the box). Always use the serial number displayed in the output of the **show version** command.

Note: You must manually enter activation keys. **Do not** use copy and paste, as this can cause errors which can cause the activation key to fail.

Note: Add additional numbers to 9-digit serial numbers that start with either the number 4 or 8 in order to make them 11-digit numbers. For example, the number 4xxxxxxx appears as 444xxxxxxx in the Activation Key. Likewise, numbers that start with an 8 require that you add two additional 8s.

PIX Devices Running Versions 6.1 and Earlier

Follow the instructions in Upgrade the PIX Firewall from Boothelper or Monitor Mode if the PIX currently runs versions 6.1 or earlier. Step 10 is where you are prompted to enter a new activation key.

PIX Devices Running Versions 6.2 and 6.3

Issue the **activation-key** command in order to change your activation key if the PIX currently runs versions 6.2 or 6.3. Refer to the PIX Command Reference for more information.

Example: Upgrade the Activation Key on a PIX that Runs Versions 6.2 or 6.3

```
pixfirewall(config)#activation-key 54bf4b80 b7237e20 05022c63 f09e3302
Updating flash...Done.
Serial Number: 480490644 (0x1ca3b494)

Flash Activation Key: 0x54bf4b80 0xb7237e20 0x05022c63 0xf09e3302
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 10
Cut-through Proxy: Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

The flash activation key has been modified.
The flash activation key is now DIFFERENT from the running key.
The flash activation key will be used when the unit is reloaded.
pixfirewall(config)#
pixfirewall(config)#reload
```

Upgrade the PIX Device Manager

The PDM upgrade procedure is the same as that used for a new installation. For detailed instructions, refer to the installation guide in the PDM product documentation for the appropriate version.

Obtain a Valid Service Contract

You must have a valid service contract in order to download the PIX software. In order to obtain a service contract, perform these steps:

- Contact your Cisco Account team if you have a Direct Purchase Agreement.
- Contact a Cisco Partner or Reseller in order to purchase a service agreement.
- Use the Profile Manager in order to update your Cisco.com profile and request association to a service agreement.

Troubleshooting

Problem:After an upgrade, the user receives the `Cannot select private key` error when the PIX reboots.

Workaround/Solution: Re-generate the rsa key for SSH:

```
ca zero rsa
ca generate rsa key 1024
ca save all

write mem
reload
```

For more information on SSH key generation, refer to [PIX/ASA 7.x: SSH on the Inside and Outside Interface Configuration Example](#)

Related Information

- [PIX 500 Series Security Appliances](#)
 - [Cisco Secure PIX Firewall Frequently Asked Questions](#)
 - [Cisco PIX Device Manager](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 4801
