Installing PDM

This chapter describes how to install Cisco PIX Device Manager (PDM) Version 3.0 on your PIX Firewall unit.

This chapter includes the following sections:

- Downloading the PDM Software, page 1
- Installing PDM, page 2
- Loading the PDM Image, page 4

Downloading the PDM Software

You can download PDM using either of the following options:

- Downloading PDM from Cisco.com, page 1
- Downloading PDM Using FTP, page 2

Downloading PDM from Cisco.com

Perform the following steps to install PDM from Cisco.com (the Web):

Step 1 Go to http://www.cisco.com using a web browser.

Step 2 On the menu bar, click **LOGIN**.

Step 3 Enter your Cisco.com username and password and click **OK**.

Note To register as a Cisco.com user, and obtain a username and password, go to this URL: http://tools.cisco.com/RPF/register/register.do

Step 4 Enter **http://www.cisco.com/cgi-bin/tablebuild.pl/pix** in the web address area of your web browser and press the **Return** or **Enter** key on your keyboard. (If you are prompted again for a username and password, enter your Cisco.com username and password.)

Step 5 On the Cisco Secure PIX Firewall Software page, find the section titled "Select a File to Download", click **pdm-*nnn*.bin** (where *nnn* represents the PDM software image version that you want to install) and follow the instructions presented.

Downloading PDM Using FTP

Perform the following steps to install PDM using FTP:

Step 1 Set your FTP client to passive mode by selecting the Properties button on the Connect to FTP Site screen, selecting the Connection tab, checking **Use Passive Mode**, and clicking **Apply**.

Step 2 Start your FTP client and connect to **ftp.cisco.com**. Enter your Cisco.com username and password when prompted.

Step 3 Enter **`cd cisco`**.

Step 4 Enter **`cd ciscosecure`** and then enter **`cd pix`** to access the PIX Firewall software directory.

Step 5 Copy the **pdm-*nnn*.bin** file (where *nnn* represents the PDM version) to a folder where it can be accessed from your TFTP server. (You can use the **ls** command to view the directory contents.)

Step 6 To download PIX Firewall and PDM documentation, enter **`cd documentation`**, locate the .pdf files for the documents you want, and copy the files to your workstation. (Files with the .pdf file extension are viewed with Adobe Acrobat Reader, which is free and available at http://www.adobe.com/products/acrobat/readstep2.html.)

Step 7 Enter **`quit`** to exit.

Installing PDM

Perform the following steps to install PDM:

Step 1 Follow these steps to set up a console connection from a Microsoft Windows workstation to your PIX Firewall unit, unless you already have a console connection:

- **a.** Power off your PIX Firewall unit.
- **b.** Connect the serial port of a Microsoft Windows workstation to the console port of the PIX Firewall with the serial cable supplied in the PIX Firewall accessory kit.
- **c.** Power on the PIX Firewall unit. If a failover PIX Firewall unit is present, configure the primary unit first.

Step 2 Locate the Windows **HyperTerminal** accessory by looking for it on the Windows **Start** menu. It is usually located under **Programs>Accessories>Communications>HyperTerminal**.

Step 3 Click **HyperTerminal** to open the **New Connection** window; the **Connection Description** dialog box appears.

Step 4 Enter a name for the connection and click **OK**.

Step 5 In the **Connect To** dialog box, leave the area code and phone number blank.

Step 6 In the **Connect using** drop-down menu, select **Com 1** (unless you are using another serial port to connect, in which case select that port) and click **OK**.

Step 7 Set the values in the following table:

Field Name	Value to Set
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Step 8 Click **OK** to continue.

The HyperTerminal window is now ready to receive information from the PIX Firewall console. Wait 30 seconds for the PIX Firewall startup messages to display. These messages should appear similar to the following example:

```
Rebooting....
Cisco Secure PIX Firewall BIOS (4.0) #0: Thu Mar  2 22:59:20 PST 2000
Platform PIX-515
Flash=i28F640J5 @ 0x300

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 1507840 bytes of image from flash.
############################################################################
64MB RAM
Flash=i28F640J5 @ 0x300
BIOS Flash=AT29C257 @ 0xfffd8000
mcwa i82559 Ethernet at irq 10  MAC: 0050.54ff.3772
mcwa i82559 Ethernet at irq  7  MAC: 0050.54ff.3773
mcwa i82559 Ethernet at irq 11  MAC: 00d0.b792.409d

  ------------------------------------------------------------------------
                              ||        ||
                              ||        ||
                             ||||      ||||
                          ..:||||||:..:||||||:..
                          c i s c o S y s t e m s
                         Private Internet eXchange
  ------------------------------------------------------------------------
                         Cisco PIX Firewall

Cisco PIX Firewall Version 6.3
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 6
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
```

Step 9 Press the **Enter** key if it takes more than a minute for the PIX Firewall command prompt to appear.

If irrelevant characters appear, reset the **Bits per second** to 9600 and try to connect again.

Note If it still does not appear, power off the PIX Firewall and ensure that the serial cable is attached to COM1 and not to COM2, if your computer is so equipped. Power the PIX Firewall back on and try to connect again.

Step 10 Enter the **enable** command if your PIX Firewall unit is being run for the first time.

Step 11 When prompted, enter your PIX Firewall password. (After starting a new PIX Firewall, you should change the password to secure administrative access to the unit.) If no password has been set, you can choose one and enter it at this time.

Step 12 Start your TFTP server. See Appendix A, "Using a TFTP Server." for more information on the TFTP server.

Step 13 Check the IP address of the computer running the TFTP server, as described in "Determining the IP Address of Your Server" in Chapter 2, "Preparing to Install PDM."

Loading the PDM Image

Perform the following steps to load the PDM image file onto the PIX Firewall:

Step 1 Enter the following at the command prompt to load the PDM image file:

```
pixfirewall# copy tftp://Your_TFTP_Server_IP_Address/Your_pdmfile_name flash:pdm
```

Or you can enter the generic command and follow the prompts:

```
pixfirewall# copy tftp flash:pdm
```

Step 2 Enter the following command at the prompt to enter configuration mode:

```
pixfirewall# configure terminal
```

Caution If your PIX Firewall is running a pre-existing configuration, refer to the *Cisco PIX Device Manager Release Notes Version 3.0* for information on the configuration commands supported for use with PDM.

Note If you have a PIX 501 or PIX 506/506E, you can use the factory default configuration loaded on the unit and skip to "Starting PDM with Internet Explorer" in Chapter 4, "Configuring PDM," instead of entering setup.

Step 3 To enter setup, use the **setup** command as shown in the following example:

```
pixfirewall (config)# setup
```

Step 4 Load the PDM image by following the steps in Table 3-1:

Note Press **Enter** to accept the default values.

Table 3-1 Setup Command Prompts

Step	Command	Purpose
Step 1	`Enable Password [<use current password>]:`	Enter an alphanumeric password, up to 16 characters in length, to protect the PIX Firewall privileged (access) mode. Record the password in accordance with your security policy. If you assign a password here, then it is used for authentication every time you launch PDM unless you configured your PIX Firewall to use another AAA server for authentication, in which case the AAA server provides the authentication.

Step 2	`Clock (UTC)`
	`Year [2001]:`
	`Month [Aug]:`
	`Day [27]:`
	`Time [22:47:37]:`
		Set the PIX Firewall clock to Universal Coordinated Time (UTC, also known as Greenwich Mean Time, or GMT). For example, if you are in the Pacific Daylight Savings time zone, set the clock 7 hours ahead of your local time to set the clock to UTC. Enter the year, month, day, and time. Enter the UTC time in 24-hour time as hour:minutes:seconds.

Step 3	`Inside IP address:`	Specify the IP address of the PIX Firewall unit's inside interface. Ensure that this IP address is unique on the network and not used by any other computer or network device, such as a router.
Step 4	`Inside network mask:`	Specify the network mask for the inside interface. An example mask is 255.255.255.0. You can also specify a subnetted mask, for example: 255.255.255.224. Do not use all 255s, such as 255.255.255.255. This prevents traffic from passing on the interface.
Step 5	`Host name:`	Specify up to 16 characters as a name for the PIX Firewall unit.
Step 6	`Domain name:`	Specify the domain name for the PIX Firewall.
Step 7	`IP address of host running PIX Device Manager:`	Specify the IP address of the workstation designated to run PDM. This is the IP address of any workstation running supported web browser software, which you will use for accessing PDM over the network.

After you enter the IP address of the workstation running PDM, PIX Firewall displays the information you just entered.

The following is a sample display:

```
The following configuration will be used:
Enable Password: ciscopix
Clock (UTC): 14:22:00 Aug 28 2001
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: accounting_pix
Domain name: example.com
IP address of host running PIX Device Manager: 192.168.1.2
```

Step 5 Enter **n** to edit the values, or enter **y** to save the information to the PIX Firewall Flash memory.

```
Use this configuration and write to flash? y
```

Or, enter **y** at the prompt to save the information to the PIX Firewall Flash memory.

Step 6 Click **Save** to save your settings.

Step 7 Click **Exit**.

Step 8 Click **Yes** to exit HyperTerminal.

RSA Key

The setup process generates an RSA key automatically. To generate an RSA key manually, follow these steps:

Step 1 Enter configuration mode:

```
pixfirewall# configure terminal
```

Step 2 Remove the existing RSA key, if applicable:

```
pixfirewall (config)# ca zeroize rsa
```

Step 3 Generate a new RSA key:

```
pixfirewall (config)# ca generate rsa key 512
```

Note It might take 30 or more seconds for the command prompt to return.

Step 4 Display the new RSA key:

```
pixfirewall (config)# show ca mypubkey rsa
```

Step 5 For access to PDM, you must specify a client that is permitted to access the PIX Firewall HTTP server and then enable the HTTP server. Use the following command to specify a client that is permitted to access the HTTP server:

```
pixfirewall (config)# http ip_address [netmask] [if_name]
```

- *ip_address*—The host or network authorized to initiate an HTTP connection to the PIX Firewall.
- *netmask*—The network mask for the HTTP IP address.
- *if_name*—The interface name on which the host or network initiating the HTTP connection resides.

Step 6 Enable the HTTP server:

```
pixfirewall (config)# http server enable
```

Step 7 Save the RSA key:

```
pixfirewall (config)# ca save all
```

Step 8 Save the configuration:

```
pixfirewall (config)# write memory
```