



# Release Notes for the PIX Firewall Manager Version 4.3(2)h

---

July 2001

## Contents

This document includes the following sections:

- Introduction
- System Requirements
- New and Changed Information
- Installation Notes
- Limitations and Restrictions
- Important Notes
- Caveats
- Troubleshooting
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance



# Introduction

The PIX Firewall Manager (PFM) lets you administer one or more PIX Firewall units, view syslog messages, and define customized alarms for each type of syslog message. You can use PFM to view, add, and modify the configuration of each PIX Firewall unit.

This version of PFM supports a subset of the PIX Firewall command set. Features in PIX Firewall version 4.3(2) are supported, but no new features are supported from versions 4.4, 5.0, 5.1, 5.2, or 5.3. Refer to the respective PIX Firewall release notes for information on the new features in those releases that are not supported by PFM. PIX Firewall documentation is available online at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>.


**Note**

If you have a problem with PFM, copy the pfm.log file immediately after a problem occurs so you can send the copy of pfm.log to Cisco's Technical Assistance Center (TAC).

Refer to "New Software Features in Version 4.3(2)h" for information on version 4.3(2)h.


**Note**

PFM provides support for only four interfaces, not the six supported by versions 4.4, 5.0, 5.1, or the eight supported by versions 5.2 and 5.3.


**Note**

PFM cannot be installed on a system or in the same network in which the PIX Firewall Syslog Server (PFSS) is installed.

## Components

PFM software includes these components:

- Management Server—a Windows NT service that runs in the background and receives requests from the Management Client, sends them to the specified PIX Firewall unit, and then passes the PIX Firewall's responses back to the Management Client. The Management Server starts automatically when the installation completes. An icon for the server does not display in the task bar.
- Management Client—a Java applet that you access from the network browser. The Management Client network browser must be Java 1.02 compliant. Refer to "Management Client Requirements" for more information.

PFM provides two access levels: user-level with read-only (non-modifying) access and administrator-level with read and write access.

Diskettes for installing PFM are provided in the PIX Firewall accessory kit.

If you are upgrading from a previous version of PFM software, refer to the documentation supplied with the PIX Firewall for configuration information.

PFM can be installed and uninstalled on Workstation and Server versions of Windows NT 4.0.

# System Requirements

This section includes the following topics:

- Windows NT Requirements
- PIX Firewall Requirements
- Management Server Requirements
- Management Client Requirements

## Windows NT Requirements

The Windows NT system on which you install the Management Server requires the following:

- Windows NT Workstation or Windows NT Server version 4.0 or later with Service Pack 3 or later.
- The Windows NT system must contain a Pentium processor and at least 32 MB RAM.
- TCP/IP must be enabled and the system's IP address must not be dynamically allocated, such as with DHCP.
- The Windows NT system must be on the PIX Firewall's inside network.
- Users must be part of the PIX Admins or PIX Users groups on the Windows NT system. These two user groups and two temporary user accounts are created by the PFM installation program. Refer to "Limiting Access to the Management Client" for more information on how to add users to these groups.

## PIX Firewall Requirements



### Note

---

Each PIX Firewall you manage must have been configured with the PIX Firewall **telnet** command or the PIX Firewall Setup Wizard to permit the Management Server to access the PIX Firewall. The PIX Firewall Setup Wizard is not available in version 4.4.

---

All PIX Firewall units managed by PFM must be running PIX Firewall software version 4.3(2), 4.4, 5.0, 5.1, 5.2, 5.3, or later. To check the version of the PIX Firewall software, go to the PIX Firewall console and enter the **show version** command.

If you are using version 4.3 and 4.4 and intend to manage PIX Firewall units on the outside network, each foreign unit must run Private Link and at least one firewall on the local network must also run Private Link. The local PIX Firewall must be configured to communicate with the foreign Private Link firewalls.

You must have console access to each local and foreign PIX Firewall you manage in order to perform the configuration required to run PFM. If you are managing remote firewalls, work with the site administrator to get the PIX Firewall to communicate with PFM.

To configure each PIX Firewall unit from the Setup Wizard, follow the instructions in the *Installation Guide for the Cisco Secure PIX Firewall Version 5.3*.

Follow these steps to configure each PIX Firewall unit from the command line at the PIX Firewall console:

- 
- Step 1** **enable**—to enter privileged mode. When prompted, enter the privileged mode password. The default is no password and you can press the **Enter** key at the prompt.
- Step 2** **configure terminal**—to enter configuration mode.
- Step 3** **nameif**—to specify the name or security level of the outside or optional third interface on the PIX Firewall. The inside interface cannot be renamed or given a different security level. Each security level must be a unique number between 0 and 99.
- Step 4** **interface**—to set options for the Ethernet or Token Ring network interfaces.
- Step 5** **ip address**—to assign IP addresses and network masks to each interface.
- Step 6** **telnet**—to let the PIX Firewall communicate with PFM:
- ```
: Telnet for PIX Firewall Manager
telnet Windows_NT_IP_Address 255.255.255.255
```
- Replace *Windows\_NT\_IP\_Address* with the IP address of the Windows NT system.
- Add the comment before the **telnet** statement to ensure that the next person configuring the firewall knows the purpose of this **telnet** statement.
- Step 7** **link** and **linkpath**—if you are managing remote PIX Firewall units, configure each for Private Link access. This feature is available in version 4.4, but was removed from version 5.0 and later.
- Step 8** **write memory**—save the configuration in Flash memory.
- 

All commands are described in the configuration guide supplied with the PIX Firewall and online at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>.

## Management Server Requirements

The Management Server has the following requirements:

- Windows NT Workstation or Windows NT Server version 4.0.
- All machines running the Management Server must be on the PIX Firewall's inside network.
- PFM comes with a sound file, T1.AU, for the syslog audio alarm. All sound files must be in .AU format as follows:
  - mu-low: 8 bit
  - Sample Rate: 8000 Hz
  - Channel: mono

Follow these steps to use another .AU format sound file:

- 
- Step 1** Place the sound file on the Windows NT system running the Management Server in the JClient\Netscape subdirectory of the Management Server's target directory.
- Step 2** Click the Management Client's **Setting** tab to modify the audio filename.
- 

## Management Client Requirements

The Management Client has the following requirements:

- All machines running the Management Client must be on the PIX Firewall's inside network.
- The Management Client network browser must be Java 1.02 or 1.1 compliant.
- The following browsers are supported:
  - Microsoft Internet Explorer 4.0 version 4.72.3110.8; updated version: SP1.
  - Netscape Navigator version 3.0 or 3.01.
  - Netscape Navigator Gold version 3.0 or 3.01.
  - Netscape Communicator version 4.0, 4.01, 4.02, 4.04, 4.05.
  - Netscape Navigator (standalone) version 4.0, 4.01, 4.02, 4.04, 4.05.



**Note** Using Netscape Navigator and Communicator version 4.04 or 4.05 with the JDK 1.1 Patch are not compatible with the Management Client. Additionally, Netscape Navigator and Communicator version 4.06 or later is not compatible with the Management Client. Earlier versions of Netscape browsers are available for download at the following URL:

<ftp://archive:oldies@archive.netscape.com/archive/index.html>.

The system running the browser must use Windows 95, Windows NT 4.0 Workstation, Windows NT 4.0 Server, or Solaris. On Windows 95 or Windows NT 4.0, 32 MB RAM is highly recommended.

## New and Changed Information

### New Software Features in Version 4.3(2)h

Caveat CSCds70535 was resolved for PIX Firewall version 4.3(2)h. Refer to “Resolved Caveats - Version 4.3(2)h” for more details.

Refer to “New Software Features in Version 4.3(2)f” for information that also applies to PIX Firewall Manager version 4.3(2)h.

## New Software Features in Version 4.3(2)g

PIX Firewall Manager has been updated to work with PIX Firewall version 5.3. One new open caveat was identified. Refer to “Open Caveats - Version 4.3(2)e” for more information. Refer to “New Software Features in Version 4.3(2)f” for information that also applies to PIX Firewall Manager version 4.3(2)g.

Table 1 in this document has been corrected for documentation errors. Signature messages 1101, 3153, 3154, and 8000 are not supported and were removed from the table. Signature message 1102 was supported but not listed and now appears in the table.

## New Software Features in Version 4.3(2)f

PIX Firewall Manager has been updated to accept the PIX Firewall version 5.2 and later Cisco Secure Intrusion Detection System syslog signature messages. These messages appear under the Alarm and Report tab in the Warning Log Messages section of the Syslog Message Folder. Refer to *System Log Messages for the Cisco Secure PIX Firewall Version 5.3* for a description of each Cisco Secure IDS signature message. You can view this document online at the following site:

[http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix\\_v53/syslog/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/index.htm)

When PFM is run with PIX Firewall versions 4.4, 5.0, 5.1, 5.2, and 5.3, the following error messages appear on the network browser:

```
PIX_ip_address: Unable to Show RADIUS Server [cmdCode = 4003]
PIX_ip_address: Unable to Show TACACS Server [cmdCode = 4103]
PIX_ip_address: Unable to show AAA Authentication [cmdCode = 3203]
PIX_ip_address: Unable to show AAA Authorization [cmdCode = 3903]
PIX_ip_address: Unable to show AAA Accounting [cmdCode = 5803]
```

These messages indicate features added after version 4.3(2) that are not compatible with PIX Firewall Manager.

The following caveats are new in version 4.3(2)f:

- Do not click the browser’s **Reload** button while using PFM. Doing so can cause PFM to hang. If PFM hangs in this way, you need to reboot the Windows system on which PFM is running.
- If you add a conduit with an external IP address, when you click **Refresh**, the entry is corrupted and cannot be deleted from PFM. The Operator column for these entries displays “-1”. When you attempt to delete a corrupted conduit, PFM displays the following message in the browser:

```
PIX_ip_address: Unable to Delete conduit [cmdCode = 402]
```

As a workaround, you can delete the conduit from the PIX Firewall command line and PFM will update its display to show the conduit deleted.

- If failover is enabled on the PIX Firewall, PFM is unable to display the failover information, which causes PFM to display the following message in the browser:

```
PIX_ip_address: Unable to show Failover [cmdCode=2103]
```

- The Cisco Secure Intrusion Detection System messages only display the title of the message and not the signature number.

Use Table 1 to determine the correct signature number.

**Table 1 Cisco Secure IDS Syslog Messages**

| <b>Signature Title</b>             | <b>Signature ID</b> | <b>Signature Type</b> |
|------------------------------------|---------------------|-----------------------|
| IP options-Bad Option List         | 1000                | Informational         |
| IP options-Record Packet Route     | 1001                | Informational         |
| IP options-Timestamp               | 1002                | Informational         |
| IP options-Security                | 1003                | Informational         |
| IP options-Loose Source Route      | 1004                | Informational         |
| IP options-SATNET ID               | 1005                | Informational         |
| IP options-Strict Source Route     | 1006                | Informational         |
| IP Fragment Attack                 | 1100                | Attack                |
| Impossible IP Packet               | 1102                | Attack                |
| IP Fragments Overlap               | 1103                | Attack                |
| ICMP Echo Reply                    | 2000                | Informational         |
| ICMP Host Unreachable              | 2001                | Informational         |
| ICMP Source Quench                 | 2002                | Informational         |
| ICMP Redirect                      | 2003                | Informational         |
| ICMP Echo Request                  | 2004                | Informational         |
| ICMP Time Exceeded for a Datagram  | 2005                | Informational         |
| ICMP Parameter Problem on Datagram | 2006                | Informational         |
| ICMP Timestamp Request             | 2007                | Informational         |
| ICMP Timestamp Reply               | 2008                | Informational         |
| ICMP Information Request           | 2009                | Informational         |
| ICMP Information Reply             | 2010                | Informational         |
| ICMP Address Mask Request          | 2011                | Informational         |
| ICMP Address Mask Reply            | 2012                | Informational         |
| Fragmented ICMP Traffic            | 2150                | Attack                |
| Large ICMP Traffic                 | 2151                | Attack                |
| Ping of Death Attack               | 2154                | Attack                |
| TCP NULL flags                     | 3040                | Attack                |
| TCP SYN+FIN flags                  | 3041                | Attack                |
| TCP FIN only flags                 | 3042                | Attack                |
| UDP Bomb attack                    | 4050                | Attack                |
| UDP Snork attack                   | 4051                | Attack                |
| UDP Chargen DoS attack             | 4052                | Attack                |
| DNS HINFO Request                  | 6050                | Attack                |
| DNS Zone Transfer                  | 6051                | Attack                |
| DNS Zone Transfer from High Port   | 6052                | Attack                |

**Table 1 Cisco Secure IDS Syslog Messages (continued)**

| Signature Title                                | Signature ID | Signature Type |
|------------------------------------------------|--------------|----------------|
| DNS Request for All Records                    | 6053         | Attack         |
| RPC Port Registration                          | 6100         | Informational  |
| RPC Port Unregistration                        | 6101         | Informational  |
| RPC Dump                                       | 6102         | Informational  |
| Proxied RPC Request                            | 6103         | Attack         |
| ypserv (YP server daemon) Portmap Request      | 6150         | Informational  |
| yplib (YP bind daemon) Portmap Request         | 6151         | Informational  |
| yppasswdd (YP password daemon) Portmap Request | 6152         | Informational  |
| ypupdated (YP update daemon) Portmap Request   | 6153         | Informational  |
| ypxfrd (YP transfer daemon) Portmap Request    | 6154         | Informational  |
| mountd (mount daemon) Portmap Request          | 6155         | Informational  |
| rex (remote execution daemon) Portmap Request  | 6175         | Informational  |
| rex (remote execution daemon) Attempt          | 6180         | Informational  |
| statd Buffer Overflow                          | 6190         | Attack         |

The following existing caveats affect use of PFM version 4.3(2)f:

- The PIX Firewall **nat 0 access-list** command is interpreted incorrectly as the **nat 0 0 0** command.
- The **established** command information can be added, but not viewed. Clicking **Refresh** causes the information to vanish and the following message appears on the browser:

```
PIX_ip_address: Unable to Show established [cmdCode = 4703]
```

- A TFTP server entry cannot be deleted from PFM. Clicking **Refresh** changes the IP addresses of TFTP servers to 0.0.0.0. The actual configuration is not affected and you can view the correct server information with the **show tftp-server** command.
- If you attempt to add authentication, authorization, or accounting information, the following messages appear on the browser:

```
PIX_ip_address: Unable to Add AAA Authentication [cmdCode = 3201]
PIX_ip_address: Unable to Add AAA Authorization [cmdCode = 3901]
PIX_ip_address: Unable to Add AAA Accounting [cmdCode = 5801]
```

- PFM incorrectly converts any netmask you enter for the PAT IP address to be 255.255.255.255 and sends this value to the PIX Firewall.
- If you specify a global pool configuration without a network mask, PFM cannot parse the command information correctly. The workaround is to always enter a netmask when specifying a global pool. If a global is not specified with a mask, the following error message appears when you attempt to view the global information:

```
PIX_ip_address: Unable to Show Global [cmdCode=103]
```

## New Software Features in Version 4.3(2)e

The following are new in version 4.3(2)e:

- Resolved Caveats - Version 4.3(2)e:
  - CSCdp61981: PFM connection timeout causes PIX Firewall crash.
- Open Caveats - Version 4.3(2)e:
  - CSCdr25532: Unable to view **global** command information when netmask is not specified.

## New Software Features in Version 4.3(2)d

The following are new in version 4.3(2)d:

- Resolved Caveats - Version 4.3(2)d:
  - CSCdp27150: PFM no longer fails when alert mail is requested.
  - CSCdm88807: PFM no longer stops logging when the SMTP server is unavailable.
- Open Caveats - Version 4.3(2)d:
  - CSCdp95978: The **nat 0 access-list** command appears incorrectly as **nat 0 0 0**.
  - CSCdp95977: The TFTP server address and filename display incorrectly.
  - CSCdp95865: The **established** command can be entered but not displayed.
  - CSCdm86516: Specify only 1 or 2 TCP connections for a static.
- PFM works correctly with the PIX Firewall version 5.1 and later **show interface** command.
- Improved documentation. This document now lists “Frequently Asked Questions” from Cisco’s Technical Assistance Center (TAC).

## New Software Features in Version 4.3(2)

PFM provides the following features:

- Manage up to 10 PIX Firewall units from PFM.
- Configure most PIX Firewall features from the **Administrator** tab in the Management Client.
- Create common configurations for multiple PIX Firewall units from the **Common Configuration** tab in the Management Client.
- Encrypt all communications between the PIX Firewall and PFM.
- Generate reports using the report wizard from the **Alarm and Report** tab by clicking a PIX Firewall folder and then clicking the **Report** button.
- Generate a three-dimensional bar chart report showing network traffic through the PIX Firewall. Information on up to 50 hosts can be reported. Reports can be viewed but not printed from PFM. You can use the extended reporting capability with Microsoft Excel 97 to print and export report information. The PFM Excel database supports up to 64,000 entries.
- Generate reports of FTP and HTTP file transfer activity by host, including source IP address and filename. These reports are not available using Microsoft Excel 97.
- Generate the initial inbound and outbound connection statements in the PIX Firewall configuration using the **Tasks** button in the Management Client to access a series of dialog boxes.

**Note**


---

The Tasks button generates statements in the PIX Firewall configuration that allow connections to or from hosts on internal (protected) networks. If you have additional configuration requirements, such as access control for outbound connections and user authentication or authorization, other configuration commands apply.

---

- Avoid conflicts between OpenSystems.Com Private I and PFM installed on the same system using the **SYSLOG Redirection** button on the **SYSLOG Notification Settings** tab. The **SYSLOG Redirection** button copies syslog event information received from port 514 to port 515.
- Set the time interval for updating syslog message files using an option in the **SYSLOG Notification Settings** tab.

Capture quickly scrolling messages in the SYSLOG Message Window using the **Message Snapshot** button. The snapshot displays up to 200 lines of messages in a separate window. To display the Syslog Message Window, select the **SYSLOG Notification Settings** tab and change the Immediate Syslog Message setting to ON.

## Installation Notes

This section includes the following topics:

- General Notes
- Before Installing
- Installing PFM

**Note**


---

Refer to “Important Notes” for information on using the PIX Firewall Manager.

---

## General Notes

1. Each PIX Firewall you wish to manage must be running PIX Firewall version 4.3(2), 4.4(1), or later.
2. Each PIX Firewall you manage must have previously been configured with the PIX Firewall **telnet** command or PIX Firewall Setup Wizard to permit access to the PIX Firewall from the Management Server for PFM. PIX Firewall Setup Wizard is not available in version 4.4.
3. A PIX Firewall Syslog Server (PFSS) is available for logging PIX Firewall event information on a Windows NT system. PFSS provides logging features not available with PFM, such as using TCP for highly reliable message delivery and control. PFM has features not available with PFSS, such as generating reports from syslog information.  
The PIX Firewall does not support running both PFM and PFSS applications at the same time. You must use either PFM or PFSS, but not both.
4. The Windows NT computer running the PIX Firewall Manager Management Client (graphical user interface) must have a network browser that is Java 1.02 compliant. Refer to “Management Client Requirements” for more information.
5. Selecting a menu item (or screen) is indicated by the following convention:  
Click **screen1>screen2>screen3**.
6. The initial PFM password is set to expire after 42 days. Refer to “Changing Passwords” for more information.

7. PFM encrypts all communication with the PIX Firewall software versions 4.3(2), 4.4, 5.0, 5.1, 5.2, or 5.3. Earlier software versions are not supported.
8. After installation and setup, if you change the IP address of the Windows NT system, you need to update the FIREWALL.HTML file installed on the system. The file is in the JClient\Netscape subdirectory on the Management Server's target directory. In the FIREWALL.HTML file, swap the old IP address with the current IP address, which is only visible from the inside network.

Interface entries can be specified as either IP addresses or domain names; however, you must remember to log on to the management server using the exact entry listed in the FIREWALL.HTML file or an IP address security violation error message can appear. This message indicates the Management Server could not locate the interface specified in the FIREWALL.HTML file, having tried the possible interfaces on the Windows NT computer running the Management Server.

The sections that follow describe other installation topics.

## Before Installing

Before installing PFM, you need to know the following:

- Passwords
  - PIX Firewall privileged mode password. This is set by the **enable password** command at the PIX Firewall console. Once set, the password cannot be viewed and must be obtained from its creator.
  - PIX Firewall Telnet password. The default value is **cisco**, but if this is changed with the **passwd** console command, you must get the password from the PIX Firewall unit's system administrator because you cannot display this value at the PIX Firewall console.
  - Password for a user with Windows NT Administrator privileges.
- Configuration—for each PIX Firewall you manage, you need to configure it as explained in "PIX Firewall Requirements." After configuring the PIX Firewall, determine its inside IP address with the **show ip address** console command.
- Port number—during installation, you are asked to supply a port number for the built-in web server in PFM. The default port for this server is 8080. It is very unlikely, but possible, that this port could be in use by another server. If that is the case, pick another port for the web server. To pick a port, view the IANA web site to determine which port is appropriate:
 

<ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers>
- IP address—you need the IP address of the Windows NT system running PFM. If the computer has more than one network interface and you do not know which one connects to the same network as the PIX Firewall, contact your network administrator.

Follow these steps to view the IP address:

- 
- Step 1** Click **Start>Settings>Control Panel**.
  - Step 2** Double-click the **Network** icon.
  - Step 3** Click the **Protocols** tab and click **TCP/IP Protocols>Properties**.
  - Step 4** When the Microsoft TCP/IP Properties dialog box opens, click the **IP Address** tab. The IP address appears on the lower part of this tab.

- Step 5** If the **Obtain an IP address from a DHCP server** item is checked, click it to disable it. Then click **Specify an IP address** and enter an IP address, subnet mask, and default gateway IP address for this system.

## Installing PFM



### Note

Only users with Windows NT Administrator privileges can run the installer or uninstaller program.

During installation, if a previous version of PFM is found, the installation program replaces the old version with the new. Follow these steps to install PFM:

- Step 1** If you used the PIX Firewall Setup Wizard to configure the PIX Firewall with the IP address and network mask of the Windows NT computer running PFM, skip to Step 2. If you have not set up the IP address for the Windows NT computer, verify network connectivity before starting by following these steps:
- a. From each PIX Firewall you intend to manage, ping the Windows NT system. Use the PIX Firewall **ping inside** command. The ping is successful if the “response received” message appears. If the ping is unsuccessful, verify the IP address of the Windows NT system and check the network cabling. For example, if the Windows NT system has an IP address of 192.168.42.42, you would use the following commands from the PIX Firewall to enter privilege mode and run the **ping** command:
 

```
enable
Password: (press Enter)
ping inside 192.168.42.42
```
  - b. From the Windows NT system, ping the inside interface of each PIX Firewall. To ping from Windows NT, click **Run** on the Start menu and enter the **ping** command, or click the **Programs>Command Prompt** and enter the command there. The ping is successful if the “Reply from” message appears. If the ping is unsuccessful, verify the IP address of the inside interface of the PIX Firewall and check the network cabling. For example, if a PIX Firewall has an inside IP address of 192.168.42.54, you would enter this command:
 

```
ping 192.168.42.54
```
  - c. From the Windows NT system, establish a Telnet session with each target PIX Firewall. The Telnet is successful if the “PIX password” prompt appears. The default password is **cisco**. Enter the password to receive access to the PIX Firewall command prompt. If the Telnet is unsuccessful, go to the PIX Firewall console and use the **show telnet** command to ensure that the configuration has a **telnet** command entry for the IP address of the Windows NT system. Refer to “PIX Firewall Requirements” for information on how to enter the PIX Firewall console commands to get to configuration mode, give Telnet access, and store the configuration in Flash memory. For example,

if a PIX Firewall has an IP address of 192.168.42.54, enter these commands to access configuration mode, let administrators start Telnet sessions with the PIX Firewall console, and store the configuration in Flash memory:

```
enable
Password: (press Enter)
configure terminal
: Created for PIX Firewall Manager
telnet 192.168.42.54
write memory
```

- Step 2** Exit all Windows programs.
- Step 3** Log in to the Windows NT system as **Administrator** or as any user who is a member of the **Administrator** group or who has Windows NT Administrator privileges.
- Step 4** From the Windows NT system, insert the first PFM diskette in the diskette drive. You can install the software:
- Click **Start>Settings>Control Panel>Add/Remove Programs**.
  - From My Computer by double-clicking the diskette icon and then double-clicking the miniature computer Setup icon.
  - Click **Start>Run** and enter the starting filename as **a:\setup.exe**. (If the diskette is in another drive, use that drive letter instead.)
- Step 5** Once the installation program starts, you are prompted with a series of dialog boxes. You can simply click **Next** and the installation will proceed without interruption. Alternately, you can designate an installation directory other than the default.
- Step 6** During the installation you are prompted for a port number for the built-in web server in PFM; use the default, 8080, unless that port is in use already. Any port between 1025 and 64000 can be entered as an alternative. To pick another port, view <ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers> to find the ports in use.
- The installation program then copies its files and prompts you to insert the second diskette. Insert the diskette and the remaining files are copied.
- Step 7** At the last dialog box, click **Finish**. The Management Server starts automatically.
- Step 8** To check whether the Management Server is running, click **Start>Settings>Control Panel** and double-click the **Services** icon. Look for the “PIX Firewall Management Server” service name. A server is running if its status appears as Started. If the status field is blank, you may run the server by selecting its name and then clicking **Start**. If you need to stop the Management Server, refer to the instructions for doing so in “Management Client Requirements.”
- Step 9** After the software setup completes, change the default passwords of the **pixadmin** and **pixuser** users with the Windows NT User Manager program described in the following section, “Changing Passwords.”

# Limitations and Restrictions

1. PFM cannot be installed or uninstalled under Windows NT domain administration logins. If you attempt to install PFM on this type of login, the following message appears:

```
You are not authorized to run this installer.
Terminating...
```

2. When installing PFM on a backup domain controller, be sure that the backup domain controller has connectivity with the primary domain controller. If connectivity is lost between the backup domain controller and the primary domain controller, the following message appears:

```
Could not find the domain controller for the domain.
```

In this case, the installation procedure cannot add the PFM users and groups to the Windows NT Security Account Manager database, and attempts to use PFM will fail.

3. PFM does not support the following PIX Firewall commands:
  - All commands and features new to versions 4.4, 5.0, 5.1, 5.2, 5.3, and later. Refer to the PIX Firewall release notes for more information on new commands.
  - **aaa authentication enableserialtelnet console tacacs+radius —aaa authentication enable console** requires authentication to access the PIX Firewall console and lets you log changes made to the PIX Firewall configuration from a serial console session.
  - **clear logging disabled**—lets you enable all previously disabled system messages.
  - **clock set**—lets you set the clock in the PIX Firewall that is used in conjunction with adding a timestamp to syslog messages that will be received by the syslog server.
  - **config net**—read the configuration from the TFTP server.
  - **hostname**—change the PIX Firewall host name.
  - **name** or **names**—permit users to map hostnames to IP addresses, thus allowing users to specify host names in the places where IP addresses are permitted.
  - **ping**—determine if other IP addresses are visible from the PIX Firewall.
  - **sysopt**—tune advanced PIX Firewall TCP cut through proxy features and enable or disable the PIX Firewall IP FragGuard feature.

To view, add, or change these configuration features, use the PIX Firewall unit's console port or start a Telnet session to access the PIX Firewall.




---

**Note** The **established** command in the command line interface is same as the multimedia feature in the Management Client. To use this feature, click **Administrator>Administration>Multimedia**.

---

4. The following configuration features can be viewed on the Management Client but must be added or changed at the PIX Firewall's console port or Telnet session:
  - MTU size. You only need to change this if you have a Token-Ring interface. Use the **mtu** command.
  - Interface configuration. Use the **interface**, **nameif**, and **ip address** commands to change the values if needed.
  - Failover. Use the **failover** command if needed.
  - Private Link. Use the **link** and **linkpath** commands.

5. ICMP protocol services, such as ping, are initially blocked in both directions by the PIX Firewall and require a **conduit** configuration. To configure a **conduit**, click **Inbound>Static>Conduit**.

If a help topic is not available, information on the topic can be found in the documentation supplied with your PIX Firewall or online at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>

## Important Notes

This section includes the following topics:

- Changing Passwords
- Limiting Access to the Management Client
- Starting the Management Client
- Using the Management Client
- Navigating the Management Client
- Stopping the Management Client
- Stopping the Management Server
- Generating and Printing Syslog Reports
- Usage Notes

## Changing Passwords

Follow these steps to change passwords for the **pixadmin** and **pixuser** default usernames:

- 
- Step 1** Click **Start>Programs>Administrative Tools (Common)>User Manager**. If your Windows NT system is a domain controller, click **User Manager for Domains**.
  - Step 2** When the User Manager starts, locate the two users, **pixadmin** and **pixuser** in the Username section of the screen.
  - Step 3** Click the **pixadmin** username, and click **User>Properties**.
  - Step 4** In the User Properties dialog box, enter the new password in the Password and Confirm Password fields.
  - Step 5** In the User Properties dialog box, select the **Password Never Expires** check box to prevent the password from expiring. If the box is not cleared, the password expires after the number of days set in the Account Policy Maximum Password Age configured in the Windows NT system. The default value set during Windows NT system installation is 42 days. Click **OK** to exit.
  - Step 6** Click the **pixuser** username and click **User>Properties**. Enter the new password in the Password and Confirm Password fields.
  - Step 7** In the User Properties dialog box, select the **Password Never Expires** check box to prevent the password from expiring.
  - Step 8** Click **OK** to exit, and click **User>Exit** to leave the User Manager.
-

## Limiting Access to the Management Client

You can specify which users can access the Management Client by creating user accounts on the Windows NT system on which PFM is installed and giving the user either PFM administrative or read-only access privileges. When the Management Client starts, users enter their login ID and password and, if accepted, they can then run PFM.




---

**Note** Before limiting access to the Management Client, change the default password to a new value as described in the preceding section, “Changing Passwords.”

---

Follow these steps to limit access to the Management Client:

- 
- Step 1** Start the User Manager as described in Step 1 in the preceding section, “Changing Passwords.” The User Manager dialog box appears. If you want to authorize access for users who already have accounts on the Windows NT system, proceed to Step 2. To add new users to the Windows NT system, click **User>New User**. Specify the information for the user including the user’s login name, full name, and password.
  - Step 2** To give a user access to the Management Client, locate the Groups area at the bottom of the User Manager dialog box.
  - Step 3** From the Groups area, if you want users to be able to change PIX Firewall settings, double-click **PIX Admins**. If you want users only to have read access and no change privileges, double-click **PIX Users**. The Local Group Properties dialog box then appears.
  - Step 4** Click **Add** to add an existing user to the selected group. The Add Users and Groups dialog box appears.
  - Step 5** From the Names field, choose the name of the user you wish to add, click **Add**, and then click **OK** to complete adding this user. Control returns to the Local Group Properties dialog box where you can continue adding users. To exit back to the User Manager dialog box, click **OK**. Then exit User Manager by clicking **OK**.




---

**Note** Do not assign a user to both the **PIX Admins** and **PIX Users** groups.

---

## Starting the Management Client

Follow these steps to start the Management Client, restart the network browser, disable proxies, and then access the Management Client:

### Windows 95, Windows NT, Solaris Netscape Navigator Version 3.x

---

- Step 1** Click **Network Preferences** on the **Options** menu.
- Step 2** Click the **Proxies** tab, select the **No Proxies** check box, and click **OK**.
- Step 3** Click **Open Location** on the **File** menu, enter **^L**, or click **Open**, and enter the following:  
`http://IP_address:port`

where *IP\_address* is the system running PFM Server, and *port* is the Management Server's web server port that you defined in "Installation Notes."

---

### Windows 95, Windows NT, Solaris Netscape Communicator 4.0, 4.01, 4.02, 4.04, 4.05, Netscape Navigator 4.0, 4.01, 4.02, 4.04, 4.05

---

- Step 1** Click **Preferences** on the **Edit** menu. A dialog box appears.
- Step 2** In the hierarchy display at the left, double-click the **Advanced** item. (In Solaris, click the arrow beside **Advanced**.) The hierarchy expands to display additional choices.
- Step 3** Click **Proxies** from the expanded hierarchy list.
- Step 4** Select the **Direct connection to the Internet** check box, and click **OK**.
- Step 5** Click **Open Location** on the **File** menu, enter **^L**, or click **Open**, and enter the following:  
`http://IP_address:port`

where *IP\_address* is the system running PFM Server, and *port* is the Management Server's web server port that you defined in "Installation Notes."

---

### Windows 95 or Windows NT Microsoft Internet Explorer 4.0 Version 4.72.3110.8; Updated Version: SP1

---

- Step 1** Click **Internet Options** on the **View** menu.
- Step 2** Click the **Connections** tab.
- Step 3** In the **Proxies Server** group box, clear **Access the Internet using a proxy server**.
- Step 4** Return to the main menu and enter the following:  
`http://IP_address:port`

where *IP\_address* is the system running PFM Server, and *port* is the Management Server's web server port that you defined in "Installation Notes."

---

## Using the Management Client

Follow these steps to view the Management Client applet with any network browser described in “Management Client Requirements.”

- 
- Step 1** After you have disabled browser proxies as described in “Starting the Management Client” and started the Management Client, the home page appears.
  - Step 2** You can generate reports using Microsoft Excel 97 by following the instructions on the home page.
  - Step 3** Click **Run Management Client**.
  - Step 4** After the Management Client is loaded, you are then prompted for a username and password. For the username, enter **pixadmin** for read-write access, or **pixuser** for read-only access. Enter either the default password, **cisco**, or the new password entered in “Installation Notes.”

You can also use any username that is in either the **PIX Admins** or **PIX Users** group. When you complete entering a username and password, click **OK**. The Management Client then opens after it loads into memory.




---

**Note** When the program is loading, do not minimize the web browser.

---

- Step 5** If you need to restart the applet, you can click the browser's **Reload** button.
- 

## Navigating the Management Client

After you enter your login credentials, the Management Client window appears.

Follow these steps to navigate in the Management Client:

- 
- Step 1** To view or modify the PIX Firewall configuration, go to the Main Tree window on the left side of the Management Client window and double-click a PIX Firewall folder. If the Main Tree window is empty, click **Add A PIX Firewall** in the Contents window to add PIX Firewall units to the Main Tree. Click the **Reload Configuration** button in the Contents window to get the most current configuration.




---

**Note** Any change to the configuration of a PIX Firewall made in the Management Client is sent immediately to the PIX Firewall and automatically saved in the PIX Firewall unit's RAM.

---




---

**Note** If you have made changes to the configuration, click the **Reload Configuration** button following the upgrade to get the current configuration information.

---

The areas of the Management Client window are as follows:

- The tabs:
  - **Administrator** tab lets you view and change information for a firewall unit.
  - **Alarm and Report** tab lets you receive notification when errors occur and display system usage reports.
  - **Common Configuration** tab lets you configure specific authentication and administration information for multiple PIX Firewall units at the same time.
  - **SYSLOG Notification Settings** tab lets you set information used by the **Alarm and Report** tab.
- The **Tasks** button provides a wizard-like function that allows you to generate inbound and outbound connection statements in the PIX Firewall configuration from a series of dialog boxes.
- The **Save to Flash Mem of PIX** button saves all configuration changes to Flash memory in the PIX Firewall. Flash memory retains configuration information when the system power is lost for any reason.
- The Main Tree lists the PIX Firewall folders. PFM assigns a folder icon to each PIX Firewall unit available on the network. When you double-click the top-level firewall icon, it displays the possible task areas for which you can view or change information. By double-clicking each subsequent folder, you work down to the individual task options.
- The PIX Firewall IP Addresses area keeps interface information visible at all times while configuring the PIX Firewall unit. Use the scroll bar to view all interfaces.
- The Contents area displays task information based on the PIX Firewall folder selection from the Main Tree. This area has several functions:
  - Displays help information on PIX Firewall folders and on other task selections.
  - Displays the configuration for the current task.
  - Provides button selections for viewing and changing configuration settings. Button selection varies based on the task selection. Buttons include Add, Delete, Help, Refresh, Edit, and Cancel. Click the **Save to Flash Mem of PIX** button to save all changes made in this area.

**Step 2** Double-click the configuration option you want from the folder in the Main Tree. The folder then opens into a series of subfolders or files for each configuration feature. The Contents area displays information about each configuration feature. Use the button selections to get help information, view current configuration information, or change configuration settings.

**Step 3** To ensure that the firewall can reload the new configuration after reboot, save the configuration in the firewall unit's Flash memory by clicking the **Save to Flash Mem of PIX** button.

To back up the configuration to a diskette, follow these steps:

- a. Place an IBM-formatted diskette in the PIX Firewall's drive.
- b. In the Main Tree window in PFM, click the PIX Firewall folder's **Administration** folder.
- c. Click **Save/Erase Config**, and click **to Floppy**.

## Stopping the Management Client

To stop the Management Client, stop the network browser on which it runs.

## Stopping the Management Server

Follow these steps if you need to stop the Management Server:

- 
- Step 1** Click **Start>Settings>Control Panel>Services**.
- Step 2** When the Services dialog box opens, select the PIX Firewall Management Server item from the Service list. You can stop this service by clicking the **Stop** button.
- 

## Generating and Printing Syslog Reports

The PIX Firewall generates syslog messages for system events, such as security alerts and resource depletion. Syslog messages are stored in log files and can be used to create alerts and reports.

PFM provides two ways to view syslog connection information: using the PIX Firewall Management Client graphical user interface, or using a Microsoft Excel macro and data files provided for Microsoft Excel 97. Options for printing reports are available only using Microsoft Excel 97.

This section includes the following topics:

- Configuration Requirements
- Viewing Reports

Refer to “Troubleshooting Syslog Reporting Problems” for additional syslog reporting information.

### Configuration Requirements

Prior to using the Alarm and Report features, you must configure each PIX Firewall to generate syslog messages and send them to a syslog server host, one of which can be the host running PFM. The syslog server in PFM listens for messages from the PIX Firewall on UDP port 514. Messages are stored in daily log files on the Windows NT computer running PFM. PFM uses the information in the daily log files to generate reports. To configure each PIX Firewall unit from the Management Client, click **Administrator>SYSLOG** to view options for configuring syslog host and message information.

### Viewing Reports

To view syslog reports from the PIX Firewall Management Client, follow the instructions for “Navigating the Management Client.” From the Management Client, click the **Alarm and Report** tab to view options for generating reports.

To view and print syslog reports from the macro, follow the instructions for “Starting the Management Client” to display the PFM home page. From the home page, follow the instructions on how to log in and generate reports.

The procedure for generating and printing syslog reports uses the Microsoft Excel macro REPORT.XLS. To use this file, start the Microsoft Excel application and open the file from within the application. If you try to open the file directly by double-clicking it, the following error message appears:

```
Cannot open the corresponding DBF file
```

**Note**

When downloading the files from the web browser, be sure to save all files (report.xls, dns.dbf, monday.dbf, sunday.dbf, and so on) to the same directory on the local drive. After all the files are in the same directory, use Microsoft Excel 97 to open the report.xls file.

**Note**

The macro does not support viewing or printing detailed reports of FTP and HTTP file transfers as provided in reports generated by the PIX Firewall Management Client.

PFM saves syslog information in daily log files. For example, PIX Firewall syslog information for Monday is saved in the *monday.log* file. The log files are located in *\PIX Firewall Manager\protect\<weekday>.log* on the Windows NT computer.

Log files are retained for one week, allowing a separate log file for each day of the week. After one week, daily log files are overwritten, starting with the daily file that was created first. For example, if log files were first started on Monday, the Monday log file will be overwritten in seven days. This also means that you can access a six-day archive of log information for a given day.

- For reporting purposes, hosts on a perimeter network are considered “outside.” When setting up syslog reports from the PIX Firewall Management Client, you must specify “outside” to include the hosts on the perimeter network in the report.

## Usage Notes

1. When a Management Client is running, only the following configuration changes to the PIX Firewall units made through the console or Telnet sessions are reflected in the client applet: **conduit**, **static**, **global**, **nat**, **outbound**, **apply**, and **alias**. To view the updated configuration for any other PIX commands modified via the console or Telnet sessions, click a PIX Firewall folder, then click the **Reload Configuration** button.
2. If a client is already connected to a Management Server and a second client on the same machine tries to connect to the same Management Server, then the first client will be disconnected and the second client will be connected.
3. PFM incorrectly converts any netmask you enter for the PAT IP address to be 255.255.255.255 and sends this value to the PIX Firewall.
4. All members in the PIX Admins group have read and write access, and all members in the PIX Users group have only read access; do not change the PIX Firewall configurations. Usernames that do not belong to one of these two groups cannot use the Management Client applet.
5. When accessing the Management Server from the Management Client, do not use the loopback address (127.0.0.1) in the URL. Using the loopback address causes an “I/O Exception” error on all online help and description pages. Refer to “Starting the Management Client” for more information on using the Management Client.
6. If you change the PIX Firewall enable password in **Administrator>Administration>Password**, wait for confirmation of password change prior to entering additional commands. If you enter an invalid password, confirmation of the change can take several minutes while the server tries to validate the entry. In the case of an invalid password, additional commands can appear to hang until the server returns confirmation that the change was unsuccessful.

7. Initially, no syslog setting information displays in the **Administration>SYSLOG** panel. Press the Refresh button to display the current information. Syslog information in the daily syslog file is now saved every 10 minutes by default. You can change the time interval for saving syslog information by setting the value in the **SYSLOG Notification Settings** tab.
8. You can specify that syslog messages be marked with the current time. To configure each PIX Firewall unit with the timestamp option, click **Administrator>SYSLOG**, set the logging type to **Timestamp** and set the status to **Enable**.
9. You must set the date and time from the PIX Firewall command line interface using the **clock set** command before timestamp information will appear in syslog messages. You cannot set the date and time from the PFM Management Client.

## Caveats

The sections that follow describe open and resolved caveats.

### Open Caveats - Version 4.3(2)e

The following caveats are open:

- CSCdr05227 and CSCdr25532

If you specify a global pool configuration without a network mask, PFM cannot parse the command information correctly. The workaround is to always enter a netmask when specifying a global pool. If a global is not specified with a mask, the following error message appears when you attempt to view the global information:

```
PIX_ip_address: Unable to Show Global [cmdCode=103]
```

### Open Caveats - Version 4.3(2)d

The following caveats are open:

- CSCdp95978

PFM interprets and displays the **nat (inside) 0 access-list** command, which is used to bind an access list to NAT 0 (NAT disabled) on the PIX Firewall, as follows:

```
nat (inside) 0 0.0.0.0 0.0.0.0 0 0
```

- CSCdp95977

When a TFTP server's IP address and filename are entered on PFM, PIX Firewall receives the information correctly, but if you click Refresh, the IP address appears in PFM as 0.0.0.0.

- CSCdp95865

The **established** command can be added, but not displayed. If you attempt to view the command information, the following error message appears:

```
Unable to show established [cmdCode=4703]
```

- CSCdm86516

When trying to specify a maximum number of connections on a static, PFM displays the “Max TCP connections cannot be higher than 2” error message. The maximum value you can specify with PFM is one connection.

As a workaround, you can set a higher value from the PIX Firewall configuration mode command line. From the PIX Firewall, use the **show static** command to view the **static** command statements, use the **no static** command to remove the **static** command statement, and then re-enter the **static** command with the correct value for the maximum number of connections.

## Resolved Caveats - Version 4.3(2)h

The following caveat is resolved:

- CSCds70535

PFM version 4.3(2)h saves the Syslog Notification Option for the following syslog groups under the Alarms and Notifications tab in the PFM client:

- All the groups under Critical Log Messages
- Groups under Error Log Messages:
  - Connection
  - Translation
  - SMTP error
  - PIX IP Fragment
  - Logical Update (error)
  - SNMP Error
  - VPDN
  - RIP
  - ICMP Info
  - RTSP Gateway Provider

## Resolved Caveats - Version 4.3(2)e

The following caveat was resolved:

- CSCdp61981

PFM no longer causes the PIX Firewall to fail when the PFM connection times out.

## Resolved Caveats - Version 4.3(2)d

The following caveats were resolved:

- CSCdp27150  
PFM no longer fails when alert mail is requested for the following events:
  - Connection denied by outbound list
  - Translation denied by outbound
  - Translation for to denied by outbound
- CSCdm88807  
PFM no longer stops logging when the SMTP server is unavailable.

## Resolved Caveats - Version 4.3(2)c and Version 4.3(2)b

The following caveats were resolved:

- CSCdm82184  
Notification messages now correctly match the content of the syslog messages. Previously, because of a table pointer error, a message sent as a notification would be different than the one PFM received from the PIX Firewall.
- CSCdm82126  
Syslog messages are now handled correctly; however, if multiple messages are received within one minute, notifications (if enabled) are not processed after the first message during the one-minute interval. Formerly a one-minute timer attempted to separate messages from arriving simultaneously, but the timer interfered with normal message processing.
- CSCdm70502  
Notifications for the syslog messages “deny send,” “deny use of network,” and “cannot ping PAT address” now correctly stay in the PFM configuration, which PFM stores in the syslog.ini file.
- CSCdm00640  
Upgrades from a previous PFM version now work correctly. Previously, if you did not want to overwrite a previous version, the install script would fail and issue the following error message:  
Severe: General file transfer error. Please check your target location and try again.  
Error Number:- 37
- CSCdk89537  
PFM now correctly handles **nat** and **static** commands for PIX Firewall versions 4.3(2), 4.4, 5.0, 5.1, 5.2, and 5.3.
- CSCdk88558  
Authorization page access no longer displays the following message:  
Port must be a +ve integer  
  
(“+ve” means positive.) Authorization page access is not available in versions 4.4, 5.0, 5.1, 5.2, and 5.3 because PFM does not support the AAA changes in these later versions.

- CSCdk88554  
When configuring multiple PIX Firewall units, in the authentication and authorization window under common configurations, the first IP address from the list of available PIX Firewall units is already selected. This is considered a feature so that one unit is always selected. You can unselect it by clicking the selected entry.
- CSCdk87760  
Authorization port and protocols are now handled correctly.
- CSCdk86999  
An extra space is no longer added after a mail recipient's name when PFM sends an email notification. With the extra space, LotusMail rejected the messages from PFM.
- CSCdk85823  
Timestamps now appear correctly in syslog messages.
- CSCdk85806  
Refresh now works correctly on the Administration>SYSLOG Output page.
- CSCdk84974  
Failover information now displays correctly. Formerly, the browser displayed the following message when a user would attempt to display failover information:  

```
PIXIPADDRESS: Unable to show Failover (cmdCode=2103)
```
- CSCdk68634  
You can now delete a conduit after deleting an associated static.

## Troubleshooting

This section includes the following topics:

- Frequently Asked Questions
- Installation Troubleshooting
- Using Microsoft Excel 97 Offline Reporting Features
- Troubleshooting Syslog Reporting Problems
- Tips

## Frequently Asked Questions

The following questions are frequently asked in Cisco's Technical Assistance Center (TAC):

- Why does PFM not install correctly?  
You may not be logged in locally as "administrator" on the Windows NT system. Users with administrative rights can install the product; however, users in the administrator group generally do not have enough rights to install the product.

While it may work, Cisco recommends that you not install PFM on a PDC (Primary Domain Controller) or BDC (Backup Domain Controller) for these reasons:

- PFM installation needs to create a local SAM (Security Access Management) database, which is required for PFM access. This is usually not possible on default PDC or BDC installations.
- When configured for logging, PFM places a heavy load on a system. Most administrators do not want to put such tasks on critical network servers like PDCs or BDCs that handle additional services.
- Why does the Windows NT system beep continuously after installing PFM?

Continuous beeping indicates a port conflict between applications. Usually a syslog application such as, CiscoWorks, PFSS (PIX Firewall Syslog Server), or a third-party application already has access to UDP port 514 or a web server has access to the default TCP port 8080. Follow these steps to remove the conflict:

- 
- Step 1** Completely uninstall PFM and remove the install directory with Windows Explorer.
  - Step 2** Reboot the Windows system.
  - Step 3** Log in to the Windows system *locally* (not the domain) as “administrator” (use this login name, not the login of someone with administrator rights).
  - Step 4** *Do not run setup yet.* At a command prompt, run the **netstat -a** command to verify both TCP 8080 and UDP 514 are not listed.  
  
If they are listed, uninstall the application that is using UDP port 514 or in the case of TCP 8080, choose an alternate TCP port such as 8081.
  - Step 5** If you uninstalled an application to remove the port conflict, repeat Steps 2 through 4, and reboot the Windows system.
  - Step 6** Check for any error messages in the event viewer and take the appropriate actions. You can search for the meaning of specific error messages at the following site:  
  
<http://support.microsoft.com/support>
  - Step 7** Click **Start>Settings>Control Panel>Services** to verify that the “server” service is running.
  - Step 8** *Now* reinstall PFM.
  - Step 9** Reboot. You can log in to the domain at this time.
- 

- Why does PFM not run after installing it? (The banner page does not display.)

The following may cause this event:

- You might be browsing the incorrect address. Enter one of these sites:

[http://the\\_nt\\_ip\\_address:8080](http://the_nt_ip_address:8080)

<http://127.0.0.1:8080>

If you chose an alternate port for the web server on the Windows system, enter that port instead of 8080. *Do not* attempt to run index.html because this will not work.

- Make sure your Windows NT IP Stack is *not* set to use DHCP. You must be assigned a static IP address. Make sure this static IP address has not changed after installation of PFM.
- Make sure the Windows NT server service is running by clicking **Start>Settings>Control Panel>Services**. This is especially important on a Windows NT Workstation.
- From the **Services** item, make sure the **PIX Firewall Manager service** started.

- Why does the error message “Security violation in all five IP addresses in firewall.html” appear after clicking the configuration link from the banner page?

The following may cause this message:

- You might be browsing the incorrect address. Enter one of these sites:

`http://the_nt_ip_address:8080`

`http://127.0.0.1:8080`

If you chose an alternate port for the web server on the Windows system, enter that port instead of 8080. *Do not* attempt to run `index.html` because this will not work.

- If your Windows NT system is multihomed, has more than one network interface card (NIC), or has multiple IP addresses associated with the NIC installed, make sure all IP addresses of the machine are listed in the following file:

`c:\Program Files\Cisco\PIX Firewall Manager\jclient\netscape\firewal.html`

You can edit this file with a text editor such as Notepad. In some rare cases, you may need to add the Windows NT NetBios host name of the Windows NT system as one of the IP address entries in this file. Reboot the Windows NT system after you edit this file.

- Is there a log file I can look at for troubleshooting PFM problems?

Yes, it is called `pfm.log`.

- What is the banner page that appears and prompts for a username and password?

You need to enter a username and password to use PFM. The default administrator username is **pixadmin** and the default password is **cisco**. The administrator has read and write permission to change the configuration. Alternately, you can use the **pixuser** username to view but not change the configuration.

The User Manager on the Windows NT system lets you add, change, or delete users in the `pixadmin` or `pixuser` groups. See “Changing Passwords” for more information.

- Why does PFM display numerous error messages or does not load the configuration after installing it?

The following can help:

- You must a supported browser that is listed on the PFM banner page. Any variations of version from these browsers are not supported. Versions of Netscape browsers are downloadable from their FTP site:

`ftp://archive:oldies@archive.netscape.com/archive/index.html` HINT:

- If you do not want to install the required browser on the Windows NT system on which PFM is installed, you can access the PFM server from another workstation or over your network using a supported browser.
- Another possibility is that your PIX Firewall contains an unsupported network interface card. Only use Cisco upgrades in your PIX Firewall.
- Configure your PIX Firewall to allow Telnet from PFM. To verify, go to a command line and Telnet to the PIX Firewall interface, enter the password, and then access enable mode.

## Installation Troubleshooting

If you have problems installing or using PFM, check the following items:

- Installing PFM generates the following error message:

A version of the PIX Firewall SYSLOG SERVER is detected on this machine. You must uninstall PIX Firewall SYSLOG SERVER before installing the PIX Firewall Manager.

If the PFM installation detects the presence of the PIX Firewall Syslog Server application on the same system, it displays a message warning you that both applications exist. The PIX Firewall does not support running both PFM and PFSS applications at the same time. You must use either PFM or PFSS, but not both.

- PFM reports that it cannot connect with the PIX Firewall unit.

Verify that the PIX Firewall has been configured for Telnet access from the Windows NT computer where the PIX Firewall Manager Server is installed.

- PFM denies user login access.

Verify that the user is a member of the PIX Admins or PIX Users groups on the Windows NT computer. If the user is not a member of a group, add the user.

- PFM installs but does not run.

This can indicate that the client portion of the application is not communicating with the server portion. To determine where errors might be occurring, use the following procedure to launch PFM to the desktop:

- 
- Step 1** Click **Start>Settings>Control Panel>Services** on the Windows NT computer.
  - Step 2** Scroll through the services to locate the PIX Firewall Manager Server.
  - Step 3** Double-click **PIX Firewall Manager Server**, which displays the Service dialog box.
  - Step 4** In the Service dialog box, check **Allow Service to Interact with Desktop**, and click **OK**.
  - Step 5** In the Services dialog box, click **Stop** to halt the PIX Firewall Manager Server; then click **Start** to restart the service.
  - Step 6** Start PFM. Errors generated by the application appear in the PIX Management dialog box. Copy the errors messages in the dialog boxes and use Cisco Connection Online (CCO) for additional support.
- 

- The Management Client stops running and reports Java applet errors in the status bar.

If the Management Client appears to stop working and reports Java applet errors, use the following procedure to launch the Java console from the web browser.

- From Netscape Navigator, click **Communicator>Java Console** on the browser menu.
- From Internet Explorer, click **View>Internet Options>Advanced**, and click **Java Console** from the menu options.

The error messages appear in the Java console panel. If the error messages report security violations, it can mean that the Management Client is having trouble communicating with the Management Server.

In such cases, try the following:

- Close the Management Client and enter the client location in the browser again using the HTTP protocol as shown here:

`http://local_host_ip_address:8080`

Do not click **File>Open** on the browser menu to access the Management Client.

- Verify that you have not changed the IP address of the Windows NT workstation running the Management Client. Changing this address can generate security violation messages. If you change the IP address of the Windows NT workstation, you must edit the IP address of the Management Client in the following file on your local disk:

`\Program Files\Cisco\PIX Firewall\jclient\netscape\firewall`

If the problems persist, use Cisco Connection Online (CCO) for additional support.

## Using Microsoft Excel 97 Offline Reporting Features

- Can Excel 95, 98 or 2000 be used?  
Excel 95, no; the macros are incompatible with PFM. Excel 98 and 2000 are not officially supported but customer support has created reports in both versions without error.
- Why do the .dbf files required for offline reporting not open?  
You cannot generate reports from PFM active files (report.xls, stat.dbf, dns.dbf, monday.dbf, and so on). You must copy these files to a separate directory to run them then with Excel 97.
- What prevents download *day.dbf* files from being downloaded?  
You will be unable to copy Monday.dbf to another directory until Tuesday, and Tuesday.dbf until Wednesday, and so on have occurred.
- When *day.dbf* files are downloaded, why does a message appear stating that report.xls contains no data?  
You most likely have not configured logging properly. Follow these steps:

- 
- Step 1** Logging traps output must be set to debugging or these files will not populate.
  - Step 2** Verify that logging host is pointed at the PFM server.
  - Step 3** Make sure your configuration shows logging on.
  - Step 4** Test successful logging by clicking “Immediate syslog notification” to “on” in PFM, generating traffic through the PIX Firewall, then verifying activity in the GUI pop-up window.
- 

- After opening report.xls, why does Excel display a message stating that it cannot find the .dbf files it needs to run?  
You are most likely using most recently used (MRU) or double-clicking report.xls. Excel 97 tracks MRU files at the bottom of the file menu and Windows also tracks these in the start/documents menu. Do not open report.xls from those locations. If you do, the macros embedded in report.xls will not function properly. You must click the **File>Open** menu to browse and open report.xls. Excel associates that directory with the application. When you use MRU, Excel keeps the directory association with the “My Documents” folder and the attempt to open report.xls results in no access to the needed .dbf files.
- Why is the password to access and modify the macros embedded in report.xls not available?  
The report.xls file is password protected to protect the integrity of the embedded macros.

## Troubleshooting Syslog Reporting Problems

Problems generating syslog reports can mean that one or both of the configuration settings for the syslog host or Message type is not correct, or that data is not reaching the syslog host. If you have problems displaying syslog report information, or you receive a “Database Empty” error message, check the following items:

- Review the section “Generating and Printing Syslog Reports” for configuration requirements. Configure the SYSLOG Host and Message Types settings.
- Verify that messages are occurring at the PIX Firewall. From the Management Client, click the **Alarm and Report** tab. Under the heading, **Immediate SYSLOG Message**, click **ON** to display a syslog message window that reports messages as they are received at the syslog host. If no messages appear in the SYSLOG Message Window, it might indicate that no syslog messages are being generated by the PIX Firewall. This can be normal if no activity is occurring at the PIX Firewall. To generate a syslog message, use Telnet to log in to a PIX Firewall that has been configured with the IP address of the syslog host running this PFM. If configured properly, a message should appear in the SYSLOG Message Window indicating that the connection was permitted.



**Note**

---

Close the SYSLOG Message Window after you have verified that information is being received at the syslog host. These messages can fill up system memory on the host, slowing performance.

---

- Verify that the Message Type is set to capture level 7 messages. PFM requires you to set the Message Type to level 7 before generating reports. From the Management Client, click the **Administration** tab and click **Administration>SYSLOG** from the Main Tree. Click **Edit** to display the Edit SYSLOG Output dialog box, and change the Message Types level if necessary.



**Note**

---

The Facility setting in the Edit SYSLOG Output dialog box is not used by PFM Management Client for generating reports. The report wizard provided with the Management Client references hosts by IP address.

---

If syslog reports display both host names and IP addresses, verify that the Windows NT system running the Management Server is able to resolve host names. PFM attempts to resolve IP addresses with host names when the Management Server receives syslog messages. If it finds a host name for an IP address, the address and host name pair is stored in a database on the Management Server. This database is used to create syslog reports. If the Management Server is unable to resolve the IP address with a host name within 15 seconds, only the IP address is logged in the database. As a result, syslog reports might include both host names and IP addresses.

## Tips

The following tips can help ensure PFM works correctly:

1. Do not install on a Windows NT system running Microsoft IIS. If you must, do not let PFM occupy any server ports being used by MS IIS. (Carefully following the previous directions will eliminate that.)
2. If any error messages appear during installation of PFM, capture them and call customer support immediately. *Do not* attempt to proceed.

You capture error messages from Windows as follows:

- a. Press and hold the Alt key and then press the Print Screen key to take a snapshot of the screen and copy it to the clipboard.
  - b. Start Wordpad and paste the screen image into a document.
  - c. Save the file and send it to customer support.
3. If any errors in the event viewer cannot be resolved, contact Microsoft support for assistance at the following site:  
<http://support.microsoft.com/support>
  4. Ensure that the most current Service Pack is installed on your Windows NT system before installing PFM. All Windows NT Service Packs through SP5 work on all PFM versions, but the browser that installs with the Service Pack may not be supported.
  5. Verify that your browser is compatible with PFM. Supported browsers are described on the PFM banner page that displays after you start PFM.
  6. Make sure you have properly configured a PIX Firewall to allow Telnet from PFM. To verify, Telnet to the PIX Firewall and start enable mode.
  7. If your Windows NT system is multihomed (more than one NIC) make sure all IP addresses for the system are listed in firewall.html, which you can edit with a text editor. Reboot the Windows NT system after you edit this file.

## Related Documentation

Use this document in conjunction with the PIX Firewall documentation at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm>

Cisco provides PIX Firewall technical tips at the following site:

<http://www.cisco.com/warp/public/110/index.shtml#pix>

## Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered CCO users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

### Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

### Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R)

Copyright © 2000-2001, Cisco Systems, Inc.  
All rights reserved.