
# Configuring PDM

This section describes how to configure your PDM. It includes the following topics:



## Starting PDM with Internet Explorer

Perform the following steps to start PDM with Internet Explorer:

**Step 1** On an Internet Explorer browser running on a workstation connected to the PIX Firewall unit, enter the following:

**https://***pix_inside_interface_ip_address*

where *pix_inside_interface_ip_address* is the IP address of the inside interface of your PIX Firewall, entered in standard (number) format.

For the PIX 501 and PIX 506/506E, the factory default inside interface address is as follows:

```
inside IP address to 192.168.1.1
```

Enter **https://192.168.1.1** for the PIX 501 and PIX 506/506E platforms.

This launches PDM.

**Note** Ensure that you add the "**s**" to "**https**" or the web browser cannot connect. HTTPS (HTTP over SSL) provides a secure connection between your browser and the PIX Firewall that you are using PDM to configure or monitor.

**Step 2** Accept the security certificate. (You must accept the certificate to use PDM.)

To avoid the certificate from appearing in Windows Internet Explorer when the certificate dialog (titled "**Security Alert**") is shown, perform the following steps:

a. Click **View Certificate**.

b. Click **Install Certificate**.

c. Click **next>next>Finish>Yes**.

d. Click **OK** in the certificate dialog box.

e. In the Security Alert dialog box, click **Yes**.

**Note** Subsequent PDM loads will not show the certificate dialog box.

**Step 3** Enter your password. If no password has been set, choose and enter one at this time. Click **OK** to continue.

**Step 4** Answer 'Yes' to the Security Warning asking "Do you want to install and run 'Cisco PIX Device Manager'"?

If you do not want this question to be asked next time you load PDM, check the box with the label 'Always trust content from Cisco Systems.'

**Step 5** Follow the instructions on screen.

PDM starts after the certificates are accepted.

**Step 6** For more information on how to use PDM, see the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

# Starting PDM with Netscape Navigator

Perform the following steps to start PDM with Netscape Navigator:

**Step 1** On a Netscape Navigator browser running on a workstation connected to the PIX Firewall unit, enter the following:

```
https://172.23.59.230/
```

This launches PDM.

**Step 2** Accept the security certificate. (You must accept the certificate to use PDM.)

To avoid the certificate from appearing in Netscape Navigator when the certificate dialog (titled "**Security Alert**") is shown, perform the following steps:

a. Click **Next** at the New Site Certificate screen.

b. Click **Next** at the next New Site Certificate screen.

c. Select **Accept this certificate forever (until it expires)**, and click **Next** at the next New Site Certificate screen.

d. Click **Next** at the next New Site Certificate.

e. Click **Finish** at the next New Site Certificate.

f. Click **Continue** at the Certificate Name Check.

**Step 3** Enter your user name and password. Click **OK**.

**Step 4** Select 'Remember this decision,' and click **Grant** at the next four Java Security screens.

PDM starts after the certificates are accepted.

**Step 5** For more information on how to use PDM, see the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

# PDM Home Page

The PDM home page lets you view, at a glance, important information about your PIX Firewall such as the status of your interfaces, the version you are running, licensing information, and performance. Many of the details available on the PDM home page are available elsewhere in PDM, but this is a useful and quick way to see how your PIX Firewall is running. All information on the Home page is updated every ten seconds, except for the Device Information.

You can access the Home page any time by clicking Home on the main toolbar.

**Note** If the interface is configured to use DHCP or PPPoE to obtain an IP address, and running PIX Firewall Version 6.3 or higher, your IP address will be displayed in the Interface Status table. If you are running an earlier version of the PIX Firewall software, the IP address will not be displayed.

On a PIX 501, the inside interface link will always be displayed as up, because this interface acts as a built-in switch. Be sure to check for physical connectivity on the inside interface of a PIX 501.

The PDM home page displays the following fields:

| Area | Description | |
|---|---|---|
| **Device Information** | This area displays the following information: | |
| | **Host Name**, **PIX Version**, **Device Type**, **License**, **PDM Version**, **Total Memory**, and **Total Flash**. | |
| | **Licensed Features**—This area displays the features your PIX Firewall is licensed to use. | Encryption |
| | | Failover |
| | | Max Interfaces |
| | | Inside Hosts |
| | | IKE Peers |
| | | Max Physical Interfaces |

| Area | Description |
|---|---|
| **Interface Status** | **Interface**—Displays the interface name as configured in the Interfaces panel. You can click any of the table headings to sort by that value. |
| | **IP Address/Mask**—Displays the IP address of the associated interface. |
| | **Link**—Displays the link status of the interface. A red icon is displayed if the physical status of the link is down, and a green icon is displayed if the physical status of the link is up. Note that on a PIX 501, the inside interface link will always be displayed as up, because this interface acts as a built-in switch. Be sure to check for physical connectivity on the inside interface of a PIX 501. |
| | **Current Kbps**—Displays the current number of kilobits per second that cross the interface. |
| **VPN Status** | This area displays the status of your VPN tunnels, if they are configured. |
| **Traffic Status** | **Connection Per Second Usage**—Displays the information about Connections Per Second (TCP, UDP, and total) of traffic going through the device. |
| | **outside Interface Traffic Usage (Kbps)**—Displays the input and output traffic going through '**outside'** interface in Kilobits per second. |
| **System Resources Status** | **CPU**—Displays the percentage of CPU being utilized at the moment. |
| | **CPU Usage (percent)**—Displays the real time status of CPU usage and history for the last five minutes. |
| | **Memory**—Displays the total amount of memory being utilized at the moment. |
| | **Memory Usage (percent)**—Displays the real time memory usage and history for the last five minutes, in megabytes. |
| | **Memory (MB)**—Displays information about free, used and total memory in megabytes. Note that one megabyte is equal to 1,048,576 bytes. |

# Using the PDM Startup Wizard

By completing this wizard, your PIX Firewall is immediately enabled.

**Note** You can configure PDM manually using the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

After PDM launches, you can access the PDM Startup Wizard at any time from the main PDM control panel as follows:

**Step 1** On the PDM top menu, click **Wizards>Startup Wizard**.

**Step 2** Read the **Welcome to the Startup Wizard** page and click **Next** when ready to continue.

**Step 3** Fill in the configuration prompts according to your network security policies. Click **Next** at the end of each wizard page to go to the next set of prompts, or click **Back** to go back to the previous prompts.

For assistance with deciding what to enter into the Startup Wizard dialog boxes, click **Help**.

**Step 4** When you have completed all the wizard pages, the **Startup Wizard Completed** page displays. To send the configuration to your PIX Firewall and exit the wizard, click **Finish**. Otherwise, click **Back** to make changes to previous pages.

# VPN Wizard

Use the VPN Wizard panel to select the type of Virtual Private Network (VPN) tunnel that you are defining and to identify the interface on which the tunnel will be enabled. A VPN tunnel provides secure communication over an insecure network, such as the public Internet, by encrypting traffic between two IPSec peers, such as your local PIX Firewall and a remote PIX Firewall or VPN concentrator.

To configure a secure tunnel, first decide if you are using your PIX Firewall to provide remote access to your local area network (LAN), or to provide connectivity to a LAN in another geographic location. Next, identify the interface to use to connect to the remote IPSec peer. If your PIX Firewall has only two interfaces, this will always be the lower security interface, which is named "outside" by default. If your PIX Firewall has multiple interfaces, you should plan your VPN configuration before running this wizard and identify the interface to use for each remote IPSec peer with which you need to establish secure connectivity.

To set up your PIX Firewall as a remote access client in relation to another PIX Firewall or Cisco VPN Concentrator, select the Startup Wizard from the Wizards menu.

You can configure the VPN Wizard as follows:

- Site-to-Site VPN, page 4-5
- Remote Access VPN, page 4-5
- Select Interface, page 4-6

## Site-to-Site VPN

This configuration is used between two IPSec security gateways, which can include PIX Firewalls, VPN concentrators, or other devices that support site-to-site IPSec connectivity. When you select this option, a series of panels are displayed lets you enter the configuration required for this type of VPN. With a site-to-site VPN, your local PIX Firewall provides secure connectivity between your LAN and a LAN in a different geographic location.

## Remote Access VPN

This configuration is used to allow secure remote access for VPN clients, such as mobile users. A remote access VPN lets remote users securely access centralized network resources. When you select this option, the system displays a series of panels that let you enter the configuration required for this type of VPN. With a remote access VPN, your local PIX Firewall provides secure connectivity between individual remote users and the LAN resources protected by your local PIX Firewall.

## Select Interface

Use the selection list to select the interface on which the current VPN tunnel will be enabled. The outside interface is the lower security interface on your PIX Firewall, while the inside interface is the higher security interface.

# Configuring VPN Tunnels

If you have never configured VPN tunnels before, use the VPN Wizard to begin: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf. By completing this wizard, your PIX Firewall is immediately configured to enforce network security policy as specified by you during the wizard prompts.

For information on configuring VPN tunnels, see the online Help for VPN Wizard at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm30olh.pdf

# Configuration Recommendations

For best performance when running Windows, use Internet Explorer versions 5.5 or 6.0 without the Java plug in or with the Java Plug in, but not as the default JVM. PDM Version 3.0 supports the Java plug in for browsers.

When using Windows 2000 or later, fastest loading of PDM can be achieved by editing the Windows configuration file "`hosts`".

**Step 1** Locate the hosts file. Under Windows 2000, the location of the hosts file is:

```
C:\WINNT\system32\drivers\etc\hosts
```

**Step 2** Select the file, right click, and select **Open With>Notepad**.

**Step 3** Follow the Microsoft instructions in the hosts file to add your PIX Firewall IP address and host name.

**Step 4** Save the hosts file to the original location.

```
Copyright (c) 1993-1999 Microsoft Corp.
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.

This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.

Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.

For example:

102.54.94.97 rhino.example.com # source server
38.25.63.10 x.example.com # x client host
```