

# Cisco PIX Device Manager

Q. What is Cisco PDM?

A. The Cisco PIX<sup>®</sup> Device Manager (PDM) is a browser-based configuration tool that enables you to graphically set up, configure, and monitor your Cisco PIX Firewall without requiring extensive knowledge of the PIX Firewall command-line interface (CLI).

Q. How many devices can Cisco PDM administer?

A. As its name implies, Cisco PDM is a tool for configuring, managing, and monitoring a single Cisco PIX Firewall. Each PIX Firewall running operating system (OS) version 6.0 is accessible via its own copy of PDM.

Q. Is Cisco PDM compatible with other forms of management such as Cisco Secure Policy Manager (CSPM), CLI, and so forth?

A. Yes. Although Cisco PDM is a graphical interface to the PIX Firewall, the resulting commands that it reads and writes are CLI. You can use PDM to read configurations that have been created via CLI or CSPM. Likewise, CLI users can view and alter configurations generated by PDM.

Q. Will Cisco continue to offer management of the Cisco PIX Firewall via CLI?

A. Yes. Cisco will continue to provide access to new and existing features via CLI.

Q. Is PDM a replacement for Cisco Secure Policy Manager (CSPM)?

A. No. PDM and CSPM are complementary management tools. As the name implies, PIX Device Manager is a tool for configuring, managing, and monitoring a single PIX Firewall. CSPM enables centralized management and uniform deployment of network policies. CSPM supports configuration of multiple Cisco security products, such as site-to-site virtual private networks (VPNs), Cisco Secure Intrusion Detection System (IDS), and PIX Firewalls. For more information on CSPM go to:

<http://www.cisco.com/wp/public/cc/pd/sqsw/sqppmn/>

Q. Is PIX Firewall Manager (PFM) going away?

A. Yes. Cisco PIX OS version 5.3 will be the last version to support PIX Firewall Manager.

Q. Does Cisco PIX Device Manager provide secure remote management?

A. Yes. Cisco PDM supports the Secure Socket Layer (SSL) Protocol to ensure that communication with remote PIX Firewalls is secure. SSL is supported in most browsers and enables information to be encrypted through the 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES).



Q. Why does PDM require me to have encryption enabled on my Cisco PIX Firewall?

A. In order for PDM to communicate via the Secure Socket Layer (SSL) Protocol your Cisco PIX Firewall must have an activation key that enables 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES). If your Cisco PIX Firewall is not currently encryption enabled you can request a free DES activation key by completing the form at the following site: <http://www.cisco.com/kobayashi/sw-center/internet/pix-56bit-license-request.shtml/>

3DES keys are available as part of a feature license upgrade.

Q. Why was PDM implemented in Java?

A. There are many reasons PDM was developed using Java. The most notable is the ability to provide a robust real-time monitoring tool. Java also provides the greatest accessibility, meaning it can be run on a variety of platforms. Likewise, Java delivers a consistent user experience without requiring a plug-in or complex software installation.

Q. Where does Cisco PDM reside?

A. Cisco PDM resides in the Flash memory of PIX Firewall units running PIX OS version 6.0 and higher. When you use your browser to access PDM, the applet's code is transferred to your system and executed by the browser's Java Virtual Machine (JVM).

Q. Can I use Cisco PDM on a PIX Firewall that has an existing configuration?

A. Yes. However, there are some atypical configurations that Cisco PDM does not support. See the Cisco PIX Device Manager Installation Guide for additional information on such configurations.

Q. Can I upgrade an existing PIX Firewall to use Cisco PDM?

A. Yes. You can use Cisco PDM with any PIX Firewall that meets PIX OS version 6.0 system requirements. Cisco PIX 506, 515, 525, and 535 platforms meet these requirements. Most Cisco PIX 520 firewalls also meet these requirements, or can be upgraded to do so. For more information on system requirements, consult the Cisco PIX Firewall documentation:

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

Q. Do I have to upgrade to PIX OS version 6.0 in order to use PDM?

A. Yes. Cisco PDM can only be downloaded into the Flash memory of existing PIX Firewall units after upgrading to PIX OS version 6.0 and later.

Q. Does PDM allow me to configure all of the features that are accessible from the CLI?

A. Cisco PDM allows you to configure virtually everything that you can configure via CLI. PDM's graphical monitoring capabilities are actually superior to CLI. The one exception is virtual private networking features, which will be supported in a subsequent release.

Q. Is there a limitation on the size of the configuration that Cisco PDM can handle?

A. Cisco recommends that you use Cisco PDM with configuration files that are 100 KB (approximately 1500 lines) or less in size.

Q. Does Cisco PDM require a license or separate fee?

A. Cisco PDM is included as part of PIX OS version 6.0 and later. A separate license for Cisco PDM is not required. A DES or 3DES license is required because Cisco PDM supports only encrypted communication. If your Cisco PIX Firewall is not currently encryption enabled you can request a free DES activation key by completing the form at the following site:

<http://www.cisco.com/kobayashi/sw-center/internet/pix-56bit-license-request.shtml>

3DES keys are available as part of a feature license upgrade.



Q. Will Cisco PDM come preloaded on new PIX Firewalls that I order?

A. If you order a new Cisco PIX Firewall unit with OS version 6.0, the operating system and PDM are already loaded into Flash memory for you. If you are upgrading from a previous version of PIX Firewall, you must use the Trivial File Transfer Protocol (TFTP) from the Cisco PIX Firewall unit's inside interface to upgrade to version 6.0 and copy the Cisco PDM image to your Cisco PIX Firewall. This is explained in the section "Installing PDM on an Existing PIX Firewall Unit" in the Cisco PIX Device Manager Installation Guide.

Q. Where does Cisco PDM store the configuration information it generates?

A. PDM saves all configuration changes to Flash memory in the PIX Firewall. Flash memory will retain configuration information if the system power is lost for any reason.

Q. Can I use PDM to access more than one PIX at a time from the same machine?

A. Yes. You can run several PDM sessions on a single workstation. The maximum number of PDM sessions you can run varies depending on your workstation's resources such as memory, CPU speed, and browser type.

Q. Can multiple users access PDM on the same PIX simultaneously?

A. Yes. Up to five administrators can use PDM to access a given PIX Firewall at the same time.

Q. What techniques are used to secure Cisco PDM?

A. Several safeguards are available to ensure that access to a PIX Firewall via PDM is secure. Among them are administrator authentication, definition of allowed hosts, use of signed applets, and SSL.

*Administrator Authentication*—When you access PDM, PIX Firewall prompts you for login credentials. You can restrict access via the enable password, which is encrypted and stored locally on the PIX. You can also use an external authentication server to store username and password information.

*Allowed Hosts*—PDM allows you to specify the IP address of hosts or networks that can access the PIX Firewall.

*Signed Applets*—Java features include digital signatures for applets, so that you can ascertain the origin of an applet, and limit entry into your system to applets that have been signed by trusted entities. For more information about Java security features, go to <http://www.sun.com/960901/feature3/javasecure.html>

*SSL*—Communication between your workstation and PIX Firewall is secured via the Secure Socket Layer (SSL). SSL is supported in most browsers and enables information to be encrypted through the 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES).

Q. What are the minimum system requirements for a workstation that will be used to access Cisco PDM?

A. Current guidelines are listed below. Complete system requirements are detailed in the Cisco PIX Device Manager Installation Guide.

#### Hardware

Processor:	300 MHz, 500 MHz recommended
Random Access Memory:	128 MB, 192 MB recommended
Display Resolution:	800 x 600 pixels, 1024 x 768 pixels recommended
Display Colors	256, 256 color recommended

## Software

Operating Systems	Browsers
Windows 2000 (Service Pack 1) Windows NT 4.0 (Service Pack 6a) Windows 98 (original or 2nd addition)	<ul style="list-style-type: none"><li>• MS Internet Explorer 5.01 (Service Pack1) or higher (5.5 recommended)</li><li>• Netscape Communicator 4.51 or higher (4.76 recommended)</li></ul>
Sun Solaris 2.6 or 2.8 running CDE or OpenWindows window manager	<ul style="list-style-type: none"><li>• MS Internet Explorer 5.0 or higher (5.5 recommended)</li><li>• Netscape Communicator 4.51 or higher (4.76 recommended)</li></ul>
Redhat Linux 6.2 or 7.0 running GNOME or KDE 2.0 desktop environment	<ul style="list-style-type: none"><li>• Netscape Communicator 4.76</li></ul>

## Network Connection

Connection speed: 56 Kbps, 128 Kbps recommended

## Additional Information

For more information about Cisco PIX Firewall, go to <http://www.cisco.com/go/pix>



### Corporate Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

### European Headquarters

Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy Les Moulineaux  
Cedex 9  
France  
[www.cisco.com](http://www.cisco.com)  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia  
[www.cisco.com](http://www.cisco.com)  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

**Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the**

**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The  
Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia  
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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. (00010R)