



Overview

This chapter describes the Cisco PIX Device Manager (PDM) Version 3.0 and the system requirements for this version.



Note

In this guide, the term “PIX Firewall” refers to all models running PIX Firewall software Version 6.3 unless specifically noted. PIX Firewall software Version 6.3 is required for PDM Version 3.0.

This chapter includes the following sections:

- [Introduction, page 1](#)
- [Data Encryption Overview, page 2](#)
- [PIX Firewall System Requirements, page 4](#)
- [PC/Workstation Requirements, page 6](#)

Introduction

Cisco PIX Device Manager (PDM) is a graphical user interface (GUI) that manages Cisco PIX Firewalls. PDM, a signed Java applet, uses certificates and HTTPS (HTTP over SSL) to securely transmit information between PDM and the PIX Firewall. (Enter “**https**” in your browser to use HTTPS.)

PDM provides the following:

- *GUI*—Lets you configure, manage, and monitor security policies across a network.
- *PDM Startup Wizard*—Creates a basic configuration that allows packets to flow securely through the PIX Firewall from the inside to the outside network.
- *VPN Wizard*—Creates a basic configuration that lets you easily set up a remote access VPN or site-to-site VPN.
- *Monitoring and Reporting Tools*—Provides real-time and historical data, summarizing network activity, resource utilization and event logs, allowing performance and trend analysis. You can detect and interrupt unusual activity with PDM’s logging and notification.
- *Graphical Tools*—Creates graphical summary reports showing real-time usage, security events, and network activity. Data from each graph can be displayed in increments you select (10 second snapshot, last 10 minutes, last 60 minutes, last 12 hours, last 5 days) and refreshed at user-defined intervals. You can view multiple graphs simultaneously to do side-by-side analysis.
 - *System graphs*: Provides detailed status information on the PIX Firewall, including blocks used and free, current memory utilization, and CPU utilization.

- *Connection graphs*: Tracks real-time session and performance monitoring data for connections, address translations, authentication, authorization, and accounting (AAA) transactions, URL filtering requests, and more on a per-second basis.
- *Intrusion Detection System (IDS)*: Provides 16 different graphs to display potentially malicious activity. IDS-based signature information displays activity such as IP attacks, Internet Control Message Protocol (ICMP) requests, and Portmap requests.
- *Interface graphs*: Provides real-time monitoring of your bandwidth usage for each interface. Bandwidth usage is displayed for incoming and outgoing communications, such as packet rates, counts, and errors, as well as bit, byte, and collision counts.
- *Syslog Viewer*—Lets you view specific syslog message types by selecting the desired logging level.
- *Embedded Architecture*—Lets you manage the Cisco PIX Firewall from almost any computer, regardless of the operating system, and works with most browsers, including Microsoft Internet Explorer and Netscape Navigator. There is no application to install and no plug-in required.
- *Secure Communication*—Supports the Secure Sockets Layer (SSL) protocol to provide high-grade encryption from the PIX Firewall to a browser. PDM to PIX Firewall communication is securely encrypted according to these encryption standards: 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or 128-bit Advanced Encryption Standard (AES). You can protect access with a valid username and password, either on the PIX Firewall or through an authentication server.

Data Encryption Overview

This section describes data encryption, including the IPSec, IKE, and certification authority (CA) interoperability features.



Note

For additional information on these features, refer to the “IP Security and Encryption” chapter in the appropriate *Security Configuration Guide* and *Security Command Reference* publications for your specific PIX Firewall.

IPSec is a network level open standards framework, developed by the Internet Engineering Task Force (IETF) that provides secure transmission of sensitive information over unprotected networks such as the Internet. IPSec includes data authentication, antireplay services and data confidentiality services.

Cisco follows these data encryption standards:

- **IPSec**—IPSec is an IP layer open standards framework that provides data confidentiality, data integrity, and data authentication between participating peers. IKE handles negotiation of protocols and algorithms based on local policy, and generates the encryption and authentication keys to be used by IPSec. IPSec protects one or more data flows between a pair of hosts, between a pair of security systems, or between a security system and a host.
- **IKE**—Internet Key Exchange (IKE) is a hybrid security protocol that implements Oakley and Skeme key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE can be used with IPSec and other protocols. IKE authenticates the IPSec peers, negotiates IPSec security associations, and establishes IPSec keys. IPSec can be configured with or without IKE.

- CA—Certification authority (CA) interoperability supports the IPsec standard, using Simple Certificate Enrollment Protocol (SCEP) and Certificate Enrollment Protocol (CEP). CEP permits PIX Firewall devices and CAs to communicate to permit your PIX Firewall device to obtain and use digital certificates from the CA. IPsec can be configured with or without CA. The CA must be properly configured to issue certificates.

The component technologies implemented for IPsec include:

- DES and Triple DES—The Data Encryption Standard (DES) and Triple DES (3DES) encryption packet data. Cisco IOS software implements the 3-key Triple DES and DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet.
- AES—The Advanced Encryption Standard, a next-generation symmetric encryption algorithm, used by the U.S. Government and organizations outside the U.S.
- MD5 (HMAC variant)—Message Digest 5 (MD5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.
- SHA (HMAC variant)—Secure Hash Algorithm (SHA) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

IPsec with the PIX Firewall software supports the following additional standards:

- AH—Authentication Header is a security protocol that provides data authentication and optional antireplay services.

The AH protocol uses various authentication algorithms; PIX Firewall software has implemented the mandatory MD5 and SHA (HMAC variants) authentication algorithms. The AH protocol provides antireplay services.

- Explicit IV—Explicit Initialization Vector is a sequence of random bytes appended to the front of a plaintext message before encryption by a block cipher, which eliminates the possibility of having the initial ciphertext block the same for any two messages. For example, if messages always start with a common header (a letterhead or “From” line) their initial ciphertext would always be the same, assuming that the same cryptographic algorithm and symmetric key was used. Adding a random initialization vector eliminates this from happening.
- ESP—Encapsulating Security Payload, a security protocol, provides data privacy services, optional data authentication, and antireplay services. ESP encapsulates the data to be protected. The ESP protocol uses various cipher algorithms and (optionally) various authentication algorithms. PIX Firewall software implements the mandatory 56-bit DES-CBC with Explicit IV, Triple DES, or AES as the encryption algorithm, and MD5 or SHA (HMAC variants) as the authentication algorithms. The updated ESP protocol provides antireplay services.

For more information on PIX Firewall IPsec terms, see [IPsec terms](http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm300lh.pdf) in the online Help at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pdm/v_30/pdm300lh.pdf

PIX Firewall System Requirements

PDM Version 3.0 requires PIX Firewall software Version 6.3.

PDM has the following system requirements:

- PDM Version 3.0 is available on all PIX 501, PIX 506/506E, PIX 515/515E, PIX 520, PIX 525, and PIX 535 platforms running PIX Firewall software Version 6.3.
- PDM works with any configuration, whether created with the PIX Firewall command-line interface (CLI), Cisco Secure Policy Manager (CSPM) or Management Center for PIX Firewall (PIXMC). However, subsequent configuration changes using CSPM or PIXMC overwrites the PDM configuration.



Caution

If you are using CSPM or PIXMC, use PDM for monitoring only. All changes made using PDM will be overwritten the next time CSPM or PIXMC synchronizes with the PIX Firewall.

For more information on earlier versions of PDM, see the appropriate installation guide at: http://www.cisco.com/en/US/products/sw/netmgtsw/ps2032/tsd_products_support_install_and_upgrade.html

This section includes the following topics:

- [PIX Firewall System Interoperability with PDM, page 4](#)
- [Flash Memory Requirements, page 5](#)
- [Maximum Configuration File Size, page 5](#)
- [Software Requirements, page 6](#)
- [Upgrading to a New Software Release, page 6](#)

PIX Firewall System Interoperability with PDM

Table 1-1 lists the PIX Firewall System requirements for PDM Version 3.0.

Table 1-1 PIX Firewall System Requirements for PDM Version 3.0

Type	Description
Hardware	
Platform	PIX 501, 506/506(E), 515/515(E), 520, 525, or 535
Random access memory	16MB
Flash Memory	See Table 1-2
Software	
PIX Firewall operating system	Version 6.3
Encryption	DES, 3DES, or AES-enabled

The PIX Firewall system ships with PIX Firewall software Version 6.3, which includes a pre-installed DES activation key. If your PIX Firewall is not enabled for DES, 3DES, or AES, and you are a registered Cisco user, you can receive a DES, 3DES, or AES activation key by completing the form at the following URL: <http://www.cisco.com/public/sw-center/index.shtml>. To become a registered Cisco user, go to <http://tools.cisco.com/RPF/register/register.do>

Flash Memory Requirements

Table 1-2 lists Flash memory requirements for PIX Firewall software Version 6.3 in conjunction with PDM Version 3.0 by platform.

Table 1-2 Flash Memory Requirements for PDM Version 3.0

PIX Firewall Model	Flash Memory Required
PIX 501	8 MB
PIX 506/506E	8 MB
PIX 515/515E	16 MB
PIX 520	16 MB (Some PIX 520 units may need a memory upgrade because older units had 2 MB, though newer units have 16 MB)
PIX 525	16 MB
PIX 535	16 MB

Maximum Configuration File Size

For optimum performance, we recommend a configuration file of no more than 100 KB (approximately 1500 lines) when using PDM.

PIX Firewall configuration files over 100 KB may interfere with the performance of PDM on your workstation in the following situations:

- While executing commands such as **write term** and **show conf**
- Failover (the configuration synchronization time)
- During a system reload

To determine the size of your configuration file, enter the **show flashfs** command at the PIX Firewall CLI prompt. View the output which begins with “file 1.” The number labeled “length” on the same line is the configuration file size in bytes.

For example:

```
pixfirewall# show flashfs
flash file system: version:3 magic:0x12345679
file 0:origin:      0 length:1925176
file 1:origin:2883584 length:2944
file 2:origin:3014656 length:32
file 3:origin:      0 length:0
file 4:origin:3145728 length:131072
file 5:origin:8257536 length:308
```

PIX Firewall platforms have different configuration file size limitations than PDM. See [Table 1-3](#) for the maximum recommended configuration file size by platform.

Table 1-3 Maximum Recommended Configuration File Size by Platform

PIX Firewall Version	Maximum Configuration
PIX 501	256 KB
PIX 506/506E, 515/515E, 520	1 MB
PIX 525, PIX 535 ¹	2 MB

1. This applies to PIX Firewall software Version 5.3(2) and later versions. The maximum recommended configuration file size for PIX Firewall software Versions 5.3(1) and earlier is 1 MB.

Software Requirements

PIX Firewall software Version 6.3 has the following software requirements:

- The PIX Firewall image no longer fits on a diskette. If you are using a PIX Firewall unit with a diskette drive, download the Boothelper file from [cisco.com](http://www.cisco.com/public/sw-center/index.shtml) (<http://www.cisco.com/public/sw-center/index.shtml>) to get the PIX Firewall image.
- Before upgrading from a previous PIX Firewall version, save your configuration and write down your activation key and serial number. Refer to “[Upgrading to a New Software Release](#)” in this chapter for new installation requirements.
- Before upgrading from Version 4 or earlier, using Auto Update, IPSec, SSH, PDM, or VPN, you will need a new 56-bit DES activation key, which can be sent to you by completing the form at: <http://www.cisco.com/public/sw-center/index.shtml>
- Use the **show version** command to verify the software version of your PIX Firewall unit.

Upgrading to a New Software Release

If you registered Cisco user, refer to the [Upgrading Software for the Cisco Secure PIX Firewall](#) document at the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a0080094a5d.shtml

PC/Workstation Requirements

PDM requirements vary depending on the platform.



Note

PDM is not supported on Macintosh, Windows 3.1, or Windows 95 operating systems.

This section includes the following topic:

- [Supported Platforms, page 8](#)

Note the following when using PDM to access the PIX Firewall unit:

- *Minimum Disk Space Requirement*—PDM requires a minimum of at least 4 MB of temporary disk space to load into the browser.

- *Java Virtual Machine (JVM)*—PDM supports the native Internet Explorer JVM from Microsoft, and the native Java Development Kit (JDK), a Java Plug-in. PDM Version 3.0 supports the Java Plug-in 1.3.1, 1.4.0 and 1.4.1 (recommended).



Note Java Plug-in 1.4.0 includes some JVM bugs that cause it to display some error messages in the Java Console.

To check which Java Virtual Machine (JVM) version you have, launch PDM. In the main PDM menu, click **Help>About Cisco PIX Device Manager**. When the **About PDM** information window appears, it displays your browser specifications in a table. You can download the latest JVM version for Internet Explorer from Microsoft, and you can download the latest Java Plug-in from Sun Microsystems.

- *Disabling the Java Plug-in*—If you are using Microsoft Internet Explorer, and it is necessary to disable the Java Plug-in for your configuration, perform the following steps:



Note This is only available if you are using the Java Plug-in 1.3.1, 1.4.0, and 1.4.1 and not a beta version.

- Click **Tools>Internet Options**.
 - Click the **Advanced** tab.
 - In the Java (Sun) section, clear the **Use Java 2** check box.
- *HTTP 1.1*—Settings for **Internet Options>Advanced>HTTP 1.1 settings** should use HTTP 1.1 for both proxy and non-proxy connections.
 - *Secure Sockets Layer (SSL)*—Browser support for SSL must be enabled. The supported versions of Internet Explorer and Netscape Navigator support SSL without requiring additional configuration.
 - *Load Time Improvement*—If you are using the Java Plug-in and accessing your PIX Firewall using an IP address instead of a host name, the performance of PDM is dramatically slower. This occurs if the PIX Firewall host name is not in DNS or in the local hosts file.

The workaround is to assure that the PIX Firewall host name is in DNS. If you are running Windows, and there is no DNS in your network or your DNS does not have the PIX Firewall entry, modify the “hosts” file.

- On Windows NT, 2000, and XP, the hosts file is located at C:\WINNT\system32\drivers\etc\hosts.
- On Windows 98 and ME, it is at C:\Windows\hosts.

Each line in the hosts file is in the format “<ip> <hostname>”. For example:

```
192.168.1.1    pixfirewall.example.com
```

Supported Platforms

This section includes the following topics:

- [Windows, page 8](#)
- [PDM Version 3.0 does not support Windows 3.1 or Windows 95., page 8](#)
- [Red Hat Linux, page 9](#)

Windows

[Table 1-4](#) and [Table 1-5](#) list the requirements for Windows platforms using PDM 3.0.

Table 1-4 Hardware Requirements and Network Connectivity for Windows Platforms for PDM 3.0

Type	Requirements
Hardware	
Processor	Pentium III or equivalent running at 450 Mhz or higher
Random Access Memory	256 MB
Display Resolution and Colors	1024 x 768 pixels and 256 colors
Network Connection	
Connection speed	56 Kbps; 384 Kbps (DSL or cable) recommended

Table 1-5 Supported and Recommended Windows Platforms for PDM 3.0

Operating System	Browser	JVM
Supported Windows Platforms		
Windows 98	Internet Explorer 5.5 or 6.0	Native ¹ JVM (VM 3167 or higher)
Windows NT 4.0 (Service Pack 4 and higher)	Internet Explorer 5.5 or 6.0	Java 1.3.1, 1.4.0, or 1.4.1
Windows 2000 (Service Pack 3)	Netscape 4.7x	Native ¹ JVM 1.1.5
Windows ME	Netscape 7.0x	Java Plug-in 1.4.0 or 1.4.1
Windows XP		
Recommended Windows Platforms		
Microsoft Windows 2000 (Service Pack 3), or Microsoft Windows XP	Internet Explorer 6.0	Native ¹ JVM (VM 3809) or Java Plug-in 1.4.1_02
	Netscape 7.0x	Java Plug-in 1.4.1_02

1. Native refers to the built-in JVM that ships with the browser.



Note

PDM Version 3.0 does not support Windows 3.1 or Windows 95.

Sun Solaris

Table 1-5 and Table 1-6 list the requirements for Sun Solaris platforms using PDM 3.0.

Table 1-6 Hardware and Network Connectivity Requirements for Sun Solaris Platforms for PDM 3.0

Type	Requirements
Hardware	
Processor	SPARC
Random Access Memory	At least 128 MB
Display Resolution and Colors	At least 1024 x 768 pixels and 256 colors
Network Connection	
Connection speed	56 Kbps; 384 Kbps (DSL or cable) recommended

Table 1-7 Supported and Recommended Sun Solaris Platforms for PDM 3.0

Operating System	Browser	JVM
Supported Sun Solaris Platforms		
Sun Solaris 2.8 or 2.9 running CDE window manager	Netscape 4.78 ¹	Native ² JVM
Recommended Sun Solaris Platforms		
Sun Solaris 2.8 running CDE window manager	Netscape 4.78 ¹	Native ² JVM

1. Netscape Communicator 4.79 is not supported.
2. Native refers to the built-in JVM that ships with the browser.

Red Hat Linux

Table 1-8 and Table 1-9 list the requirements for Red Hat Linux platforms using PDM 3.0.

Table 1-8 Hardware and Network Connectivity Requirements for Linux Platforms for PDM 3.0

Type	Requirements
Hardware	
Processor	Pentium III or equivalent running at 450 Mhz or higher
Random Access Memory	At least 128 MB
Display Resolution and Colors	At least 1024 x 768 pixels and 256 colors
Network Connection	
Connection speed	56 Kbps; 384 Kbps (DSL or cable) recommended

Table 1-9 Supported and Recommended Red Hat Linux Platforms for PDM 3.0

Operating System	Browser	JVM
Supported Red Hat Linux Platforms		
Red Hat Linux 7.0, 7.1, 7.2, 7.3 or 8.0 running GNOME or KDE	Netscape 4.7x on Red Hat 7.x	Native ¹ JVM
	Mozilla 1.0.1 on Red Hat 8.0	Java Plug-in 1.4.1
Recommended Red Hat Linux Platforms		
Red Hat Linux 8.0	Mozilla 1.0.1	Java Plug-in 1.4.1_02

1. Native refers to the built-in JVM that ships with the browser.