

Cisco PIX Device Manager v3.0

Overview

Cisco PIX[®] Device Manager is a feature-rich, graphical tool providing enterprise and service providers an easy-to-use management facility for Cisco PIX Firewalls. Bundled with the PIX operating system (OS), it features an intuitive graphical user interface (GUI) with integrated online help and intelligent wizards to greatly simplify setup and configuration of your Cisco PIX Firewall. In addition, a wide range of informative, real-time, and historical reports provide critical insight into usage trends, performance baselines, and security events. Furthermore, administrative and device security is assured through user passwords (with optional authentication via a RADIUS or TACACS server) and encrypted communications to the local or remote Cisco PIX Firewall.

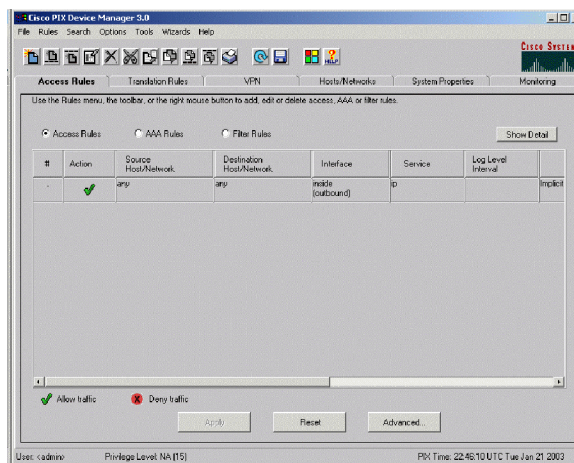
In short, Cisco PIX Device Manager simplifies the configuration, operation, and monitoring of Cisco PIX Firewalls, making it a highly effective productivity tool to manage network security and save both time and money.

In this release, Cisco PIX Device Manager v3.0 provides easy access to virtually all PIX firewall functions, including support for more than 20 new features available in PIX OS v6.3. Cisco PIX Device Manager v3.0 also extends its firewall management capabilities with support for new browsers and operating systems, batching of command-line interface (CLI) commands, and use of the Sun Java Plug-in. Table 1 provides a summary of the features and benefits described here.

Intuitive User Interface

Many security vulnerabilities are caused by poor configuration. Consequently, implementing security policy must be as straightforward as possible. Cisco PIX Device Manager includes wizards, point-and-click configuration, and online help to simplify administration. Cisco PIX Device Manager also provides a table showing exactly what traffic is permitted or denied between a source and destination, so that security professionals can focus on enforcing security and defining policy, rather than on mastering the tools required to get the job done.

Figure 1





Cisco PIX OS v6.3 Feature Support

Cisco PIX Device Manager v3.0 gives you point-and-click access to virtually every feature available in this feature-packed PIX OS release. Popular new functions such as virtual LAN (VLAN), Open Shortest Path First (OSPF) routing, Advanced Encryption Standard (AES), enhanced Easy VPN Remote, and voice over IP (VoIP), are all fully integrated into the rich graphical environment of Cisco PIX Device Manager, thus simplifying overall systems management.

Java Plug-in

Cisco PIX Device Manager 3.0 adds support for Sun's Java Plug-in. This allows Cisco PIX Device Manager to coexist more easily with other browser-based applications.

Improved Cisco PIX Device Manager Load Times

Reduce File Size

Thanks to a customized Cisco Java class loader, Cisco PIX Device Manager can selectively choose which files are needed for specific browsers. This reduces overall file size, improves Cisco PIX Device Manager load times, and allows support of more browsers and platforms.

Caching

The caching feature allows Cisco PIX Device Manager files to be securely loaded from a user's local hard drive, rather than from across the network. When enabled, Cisco PIX Device Manager launch times are nearly cut in half. An initial check ensures that the local Cisco PIX Device Manager version matches that of your PIX firewall, or it will initiate download of the current version. Users who wish to load Cisco PIX Device Manager from the PIX firewall are given the ability to clear the cache or disable this feature.

CLI Execution Enhancements

CLI command batching allows Cisco PIX Device Manager to send more than one command at a time to the PIX firewall and overcomes the CLI 1024-character length limit. This improves the performance of wizards and virtual private network (VPN) dialogs which often result in the execution of multiple commands. Batching also allows you to maintain connectivity in instances where an initial interface or addressing change may cause users to lose connectivity.

Wizards

Startup Wizard

Cisco PIX Device Manager offers a helpful wizard for setting up a new PIX deployment. With just a few steps, the Cisco PIX Device Manager Startup Wizard enables you to efficiently create a basic configuration that allows packets to flow through the PIX firewall from the inside network to the outside network securely. You can also perform optional tasks such as configuring interface parameters, Easy VPN Remote, Auto Update, Network and Port Address Translation (NAT/PAT), and Dynamic Host Configuration Protocol (DHCP) server settings. After you complete the initial setup, intuitive pull-down menus and icons enable you to easily add and delete services and rules, as well as access other feature settings.



VPN Wizard

Cisco PIX Device Manager's VPN wizard can help you easily create VPN policy with step-by-step configuration and policy application. It can create site-to-site VPNs, which can be used to securely connect a PIX firewall to another VPN device, or remote access VPNs (including hardware clients), which can be used to securely connect mobile users and telecommuters to a PIX firewall.

Graphical User Interface

Using Cisco PIX Device Manager, you can easily configure, manage, and monitor security policies across your network. Cisco PIX Device Manager's GUI provides a familiar, tabbed layout with one-click access to common tasks. The point-and-click design is simple for even novice users, reducing training time. The result is cost savings through significant reductions in management time and maximum efficiency in network security management.

Object Grouping

To simplify your configuration, object grouping enables you to define groups of objects such as hosts, IP addresses, or network services. You can use these groups, for example, when you create and apply access rules. When you include a Cisco PIX Firewall object group in a PIX firewall command, it is the equivalent of applying every element of the object group to the PIX firewall command.

Monitoring and Reporting

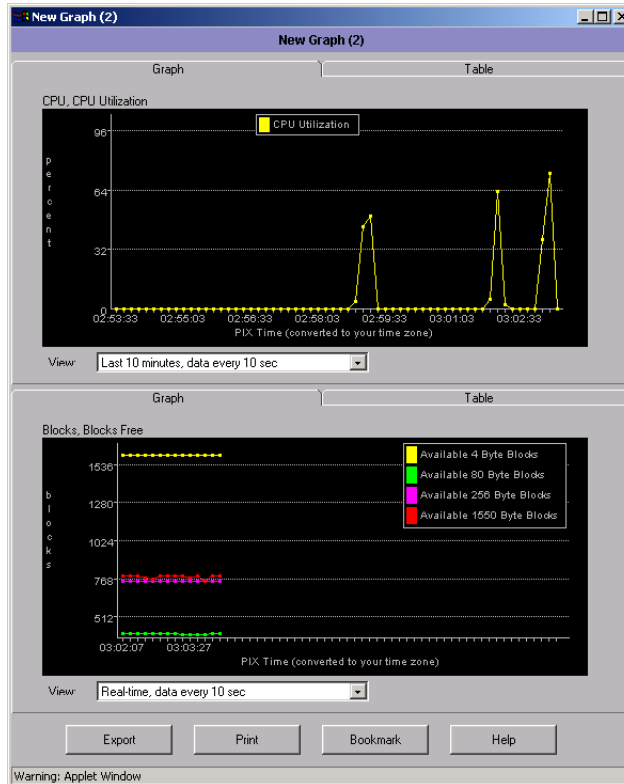
Cisco PIX Device Manager offers robust reporting and monitoring tools that provide you with real-time and historical insights. At a glance, administrators can view graphical reports or tables summarizing network activity, resource utilization, and event logs, allowing performance and trend analysis. Cisco PIX Device Manager's logging and notification features allow security staff to detect and interrupt suspicious activity.

Monitoring Tools

Cisco PIX Device Manager monitoring tools create 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. The ability to view multiple graphs simultaneously allows you to do side-by-side analysis.



Figure 2



System graphs: Provide detailed status information on the Cisco PIX Firewall, including blocks used and free, current memory utilization, and CPU utilization.

Connection graphs: Track 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. Stay fully informed of your network connections and activities, without being overwhelmed.

Intrusion detection system (IDS): 16 different graphs are available 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: Provide real-time monitoring of your bandwidth usage for each interface. Bandwidth usage is displayed for incoming and outgoing communications. You can view packet rates, counts, and errors, as well as bit, byte, and collision counts, and more.

VPN statistics and connection graphs: View detailed information and counters for Internet Key Exchange (IKE) and IPSec security associations, as well as Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) VPN. Use the VPN connection graphs to get a real-time graphical view of VPN performance statistics.

Syslog Viewer

Cisco PIX Device Manager's integrated syslog viewer allows you to view specific syslog message types by selecting the desired logging level.



Embedded Architecture

The embedded design of Cisco PIX Device Manager allows customers to manage their Cisco PIX Firewalls from almost any computer, regardless of their operating system—a critical requirement for many of today's e-businesses. Similarly, Cisco PIX Device Manager provides a consistent experience by working with most of today's popular browsers, including Microsoft Internet Explorer and Netscape Navigator and Communicator. With Cisco PIX Device Manager, there is no application to install and no plug-in required. An authorized network administrator can securely manage and monitor their PIX firewalls from a Web browser.

Secure Communication

Cisco PIX Device Manager supports the Secure Sockets Layer (SSL) protocol to provide high-grade encryption for all communication between a PIX firewall and a browser. Your PIX firewall, combined with 56-bit Data Encryption Standard (DES) or the more secure 168-bit Triple DES (3DES), helps ensure that communication with remote PIX firewalls is secure.

Similar to Telnet usage, Cisco PIX Device Manager enables you to protect access with a valid username and password. This can either be on the PIX firewall or through an authentication server.

Table 1 New Features and Benefits Summary

New Features	Benefits
Cisco PIX OS v6.3 feature support	<ul style="list-style-type: none">• Gives administrators increased flexibility for defining and enforcing security policies using the latest PIX firewall features such as VLAN and OSPF
Cisco custom Java class loader, and caching	<ul style="list-style-type: none">• Provides users quicker and more efficient Cisco PIX Device Manager access to their PIX firewalls
Java Plug-in	<ul style="list-style-type: none">• Allows Cisco PIX Device Manager to coexist more easily with other browser-based applications
Batch CLI commands	<ul style="list-style-type: none">• Provides a performance enhancement for wizards and IPSec rule changes• Maintains connectivity when making interface and addressing changes• Eliminates CLI 1024-character length limit
Support for Netscape Communicator 7, Red Hat Linux 8, and Mozilla	<ul style="list-style-type: none">• Gives users the flexibility to use the latest operating systems and browsers

Licensing

Cisco PIX Device Manager v3.0 is included as part of Cisco PIX operating systems version 6.3 and higher (v1.x is included with PIX OS v6.0 or v6.1, Cisco PIX Device Manager v2.x requires PIX OS v6.2). A separate license for Cisco PIX Device Manager is not required. A DES or 3DES license is required. If your PIX firewall is not currently encryption-enabled, you can request a free DES activation key by completing the following form:

<http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl?pid=221&fid=324>

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



Technical Specifications

Cisco PIX Firewall System Requirements

Hardware

Platform: Cisco PIX 501, 506/506E, 515/515E, 520, 525, or 535 firewalls

Random Access Memory: 32 MB

Flash Memory: 16 MB (PIX 501, 506/506E Firewall require 8 MB)

Software

PIX Firewall operating system: Version 6.3 (Cisco PIX Device Manager v1.x requires PIX OS v6.0 or v6.1, Cisco PIX Device Manager v2.x requires PIX OS v6.2)

Encryption: DES or 3DES-enabled

User System Requirements

Hardware

Processor: Pentium III 450 MHz, Pentium IV or equivalent 500 MHz recommended

RAM: 128 MB, 192 MB recommended

Display resolution: 800 x 600 pixels, 1024 x 768 pixels recommended

Display colors: 256, high color (16-bit) recommended

Table 2 Software

Operating Systems	Browsers (JavaScript and Java enabled)
Windows 2000 (Service Pack 1)	Microsoft Internet Explorer 5.5 or higher with JVM (VM 3167 or higher) or Java Plug-in v1.4.1 Netscape Communicator 4.7x with native JVM 1.1.5 Netscape Communicator 7.0x with Java Plug-in v1.4.1
Windows NT 4.0 (Service Pack 6a)	
Windows 98 (original or 2nd edition)	
Windows ME	
Windows XP	
Sun Solaris 2.8 or higher running CDE or OpenWindows window manager on SPARC microprocessor	Netscape Communicator 4.7x
Red Hat Linux 7.0, 7.1, 7.2, 7/3 or 8.0 running GNOME or KDE 2.0 desktop environment	Netscape Communicator 4.7x Mozilla 1.1 with Java Plug-in 1.4.1

Network Connection

Connection speed: 56 kbps, 384 kbps recommended

Additional Information

For more information about Cisco PIX Firewalls and Cisco PIX Device Manager, 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
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • 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

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, the Cisco Systems logo, and PIX are registered trademarks or 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.
(0301R) TS/LW4130 02/03