



# Intelligent Event Module™ for Cisco® PIX® Firewall 6.3

## INTELLIGENT EVENT MODULE BASICS

The Cisco PIX Firewall 6.3 Intelligent Event Module (IEM) enables you to automate real-time monitoring of the Cisco® PIX® Firewall appliance (version 6.3) and capture the critical information you need for enterprise security management.

The Cisco PIX Firewall 6.3 IEM provides ConsoleWorks® with a watch-list of baseline infrastructure messages, including intrusion detection alerts, suspicious traffic alarms, and system error codes, produced by PIX firewalls. ConsoleWorks watches for these messages, called Events, in the data streams of your PIX appliances.

### Events

When ConsoleWorks detects an Event, it alerts you to the Event as it is happening, records the circumstances surrounding the Event, and automatically performs the default or customer-configured responses associated with that Event.

### Scans

IEMs come with Events pre-arranged in logical groupings, called Scans™. Working with a Scan—or a combination of Scans—instead of hundreds of individual Events simplifies managing Events across your enterprise.

## CISCO PIX FIREWALL 6.3 IEM AT A GLANCE

Events:	391
Scans:	1 Master 7 Event Severity
Filename:	<code>cw_iem-cisco_pix63-0003.bin</code>
License Required:	<code>CONWRKS-DB-PIX.lic</code>
Connector Required:	Serial, Telnet or Telnet on Demand

## USING THE CISCO PIX FIREWALL 6.3 IEM

To use this IEM, complete the following tasks:

1. Download the IEM from the TDi web site.
2. Import the IEM into ConsoleWorks.
3. Associate the Scans from the IEM with the appliances you want to manage.

### Download the IEM

1. Obtain a license for the Cisco PIX Firewall 6.3 IEM. To obtain this license, contact your TDI Regional Sales Manager ([sales@tditx.com](mailto:sales@tditx.com)).
2. Move to the TDI web site ([www.tditx.com/support\\_iemdownloads.asp](http://www.tditx.com/support_iemdownloads.asp)).
3. On the Product Downloads page, locate and click **Cisco PIX Firewall 6.3**.
4. In the Connect to support2.tditx.com dialog box, enter your User name and Password, and click **OK**. To obtain a User name and Password, contact TDI Support ([support@tditx.com](mailto:support@tditx.com)).
5. Save the file (`cw_iem-cisco_pix63-0003.bin`) to a directory accessible from your client workstation.

### Import the IEM

1. On the main menu:
  - (ConsoleWorks 3.x) click **Admin > Database > Import IEM**.
  - (ConsoleWorks 4.0) click **Events > IEMs**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-cisco_pix63-0003.bin`.
4. On the Import IEM page, click **Import IEM**, and wait for the **IEM Import Completed** message to appear before attempting to associate Scans.

### Associate the Scan


Associate the Scans from the Cisco PIX Firewall 6.3 IEM with the PIX appliances you want monitored. When you associate Scans with an appliance, you are specifying that ConsoleWorks scan the data streams of that appliance for the Events contained in the Scans.

### Example: To associate Scan PIX63\_ALERT (ConsoleWorks 3.x)

1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **PIX63\_ALERT**.
3. On the Scan: PIX63\_ALERT page, in the Unassociated Consoles column, select the check boxes next to the names of the managed appliances you want to associate with the Scan.
4. Click **Update Scan**.



### Example: To associate Scan PIX63\_ALERT (ConsoleWorks 4.0)

1. On the main menu, click **Events > Scans > Edit**.  
*The Edit Scan page appears.*
2. On the Name drop-down list, click **PIX63\_ALERT**.
3. Click , then click **Add**.  
*The Add Consoles selector appears.*
4. Select the Consoles you want associated with the Scan, review your choices in the Selected Consoles window, and click **OK**.
5. Click **Save**.

### SCANS AVAILABLE IN THE CISCO PIX FIREWALL 6.3 IEM

The Cisco PIX Firewall 6.3 IEM contains a Master Scan and seven Event Severity Scans.

#### Master Scan

The Master Scan, **PIX63**, is the top-level Scan. It references all the other Scans in the IEM. When you associate the Master Scan with an appliance, you are specifying that ConsoleWorks scan the data streams of that appliance for any of the IEM's 391 Events.

#### Event Severity Scans

The Cisco PIX Firewall 6.3 IEM contains seven Event Severity Scans. Use one or more of these Scans to monitor PIX Firewalls for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

- PIX63\_ALERT 41 Events
- PIX63\_CRITICAL 21 Events
- PIX63\_ERROR 75 Events
- PIX63\_WARNING: 112 Events
- PIX63\_NOTIFICATION 22 Events
- PIX63\_INFORMATIONAL 104 Events
- PIX63\_DEBUGGING: 16 Events

### SAMPLE CISCO PIX FIREWALL 6.3 IEM EVENTS

The Cisco PIX Firewall 6.3 IEM provides you with names, message texts, Severity ratings, causes, explanations, and responses for Events produced by the Cisco PIX Firewall appliance.

The following section displays samples of the information you receive for each Event in the Cisco PIX Firewall 6.3 IEM.

#### Sample Event 1

- Name:** PIX63\_106017
- Message:** %PIX-2-106017
- Severity:** CRITICAL
- Cause:** Denied IP because of Land Attack from *IP\_address* to *IP\_address*.
- Explanation:** This message appears when the firewall receives a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This indicates a spoofed packet designed to attack systems. This attack is referred to as a Land Attack.
- Response:** If this message persists, an attack may be in progress. The packet does not provide enough information to determine where the attack originates.

- Additional Information:** You may also want to reference information at one of the following sites:

[Cisco PIX Firewall Documentation Site](#)

[Cisco PIX Firewall System Log Messages, Version 6.3](#)

#### Sample Event 2

- Name:** PIX63\_105036
- Message:** %PIX-1-105036
- Severity:** ALERT
- Cause:** PIX dropped a LAN Failover command message.
- Explanation:** The firewall dropped an unacknowledged LAN failover command message, indicating a connectivity problem on the LAN failover interface.
- Response:** Check that the LAN interface cable is connected.

©2008 TDI. The information in this document is provided by TDI as-is without warranty of any kind and is subject to change without notice. The warranties for TDI solutions are set forth in the limited warranty statements accompanying such solutions. Nothing herein shall be construed as constituting an additional warranty. All products or company names mentioned in this document are trademarks or registered trademarks of their respective owners. Portions of the technology within the ConsoleWorks server are protected under US Patent number 6,505,245. ConsoleWorks is a registered trademark of TDI.