CHAPTER 1

Getting Started

This chapter describes IPS Manager Express (IME) and how to use it. It contains the following sections:

Introducing IME

Note Beginning with IME 7.0.3, you are required to create a password to access IME.

IME is a network management application that provides system health, events, and collaboration monitoring in addition to reporting and configuration for up to ten sensors. IME monitors sensor health using customizable dashboards and provides security alerts through RSS feed integration from Cisco Security Center. It monitors Global Correlation data, which you can view in events and reports. It monitors events and lets you sort views by filtering, grouping, and colorization. IME also supports tools such, as ping, trace route, DNS lookup, and whois lookup for selected events. It contains a flexible reporting network. It embeds the IDM configuration component to allow for a seamless integration between the monitoring and configuration of IPS devices.

Within IME you can set up your sensors, configure policies, monitor IPS events, and generate reports. IME works in single application mode—the entire application is installed on one system and you manage everything from that system.

Advisory

IME contains cryptographic features and is subject to United States and local country laws governing import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you cannot comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products can be found at the following website:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance, contact us by sending e-mail to export@cisco.com.

Participating in the SensorBase Network

Cisco IPS contains a new security capability, Cisco Global Correlation, which uses the immense security intelligence that we have amassed over the years. At regular intervals, Cisco IPS receives threat updates from the Cisco SensorBase Network, which contain detailed information about known threats on the Internet, including serial attackers, Botnet harvesters, Malware outbreaks, and dark nets. The IPS uses this information to filter out the worst attackers before they have a chance to attack critical assets. It then incorporates the global threat data in to its system to detect and prevent malicious activity even earlier.

If you agree to participate in the SensorBase Network, Cisco collects aggregated statistics about traffic sent to your IPS. This includes summary data on the Cisco IPS network traffic properties and how this traffic was handled by the Cisco appliances. We do not collect the data content of traffic or other confidential business or personal information. All data is aggregated and sent by secure HTTP to the Cisco SensorBase Network servers in periodic intervals. All data shared with Cisco is anonymous and treated as strictly confidential.

Table 1-1 shows how we use the data.

Table 1-1 Cisco Network Participation Data Use

Participation Level	Type of Data	Purpose
Partial	Protocol attributes (TCP maximum segment size and options string, for example)	Tracks potential threats and helps us to understand threat exposure
	Attack type (signature fired and risk rating, for example)	Used to understand current attacks and attack severity
	Connecting IP address and port	Identifies attack source
	Summary IPS performance (CPU utilization, memory usage, inline vs. promiscuous, for example)	Tracks product efficacy
Full	Victim IP address and port	Detects threat behavioral patterns

When you enable Partial or Full Network Participation, the Network Participation Disclaimer appears. You must click **Agree** to participate. If you do not have a license installed, you receive a warning telling you that global correlation inspection and reputation filtering are disabled until the sensor is licensed. You can obtain a license at http://www.cisco.com/go/license.

For More Information

- For detailed information on global correlation, see Chapter 13, "Configuring Global Correlation."
- For detailed information on licensing the sensor, see Configuring Licensing, page 18-12.

IME Home Pane

IME Home opens to the Device List pane where you can configure IME devices. It also has the following other features:

- Video help

  IME has an overall feature presentation video that appears when you launch IME, plus five videos containing procedural help.

  The video help appears in the pane that it pertains to, but you can also access all video help from Help > Show Video Help.

  Note IME contains video help that requires you to have the Adobe Flash Player Internet Explorer plug-in version 8 or later.

- Notice of whether the clocks on your system and the sensor are synchronized.

  In the upper left corner, an icon under the Time column indicates whether the sensor time and local system time are synchronized. If they are not, you must make sure you correct the time on the sensor, otherwise the timestamp for monitoring and reporting is not accurate.

- Events per second

  In the lower right corner of the Home pane, the EPS (events per second) that IME has received recently is shown. The EPS count is updated every five seconds.

IME contains menu features that help you configure various aspects of IME.

- **File > Export**—Lets you export event data from the IME database in to a CSV file.
- **File > Import**—Lets you import the event data file that you exported from IEV 5.*x*.
- **View > Reset Layout**—Lets you reset the IME panes to their default view.
- **Tools > Preferences**—Lets you configure how the IME database stores event data, lets you enable email notification, and lets you configure other application settings, such as the location of a network sniffer application, the maximum number of real-time events per view, the maximum number of historical events per view, the event polling interval, and whether to show the feature presentation video at startup. You can also delete the cached DNS names.
- **Tools > Ping, Traceroute, Whois, DNS Lookup**—You can use ping to diagnose basic network connectivity. Ping is a simple way to check if a sensor can communicate back. You can use traceroute to display the route an IP packet takes to a destination. You can use whois to determine the owner of a domain name or an IP address. You can use DNS lookup to translate host names to IP addresses, rather like a phone book.

- **Tools > IME Console Window**—Lets you use the IME Java console to view and copy logged entries in a text format, which can help you troubleshoot IME errors. To show the virtual machine memory statistics, enter `m` in the console. To perform garbage collection, enter `g` in the console.

For More Information

- For information on correcting the time on the sensor and configuring time on the sensor, see Configuring Time, page 6-6.
- For the procedure to configure data archiving, see Configuring Data Archiving, page 1-9.
- For the procedure to set up email notification, see Configuring Email Notification, page 1-10.
- For detailed information on configuring general options for IME, see Configuring General Options, page 1-13.

System Requirements

IME has the following system requirements:

- Minimum hardware requirements
  - IBM PC-compatible 2-GHz or faster processor
  - Color monitor with at least 1024 x768 resolution and a video card capable of 16-bit colors
  - 100-GB hard-disk drive
  - 2-GB RAM
- Supported TCP/UDP ports
  - 47002
  - 47003
  - 47006
  - 47007
  - 47008
  - 47009
  - 47010
- Operating Systems
  - Windows Vista Business and Ultimate (32-bit only)
  - Windows XP Professional (32-bit only)
  - Windows 2003 server

IME supports the following Cisco IPS hardware platforms:

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- AIP SSM-10

- AIP SSM-20
- AIP SSM-40
- IDSM2
- NME IPS

Note Although IME also supports IDS-4210, IDS-4215, IDS-4235, IDS-4250, and NM-CIDS, these platforms do support any IPS software past IPS 6.1, and some of the IME features are not supported.

IME supports the following Cisco IPS versions with the following features:

- Cisco IPS 7.0
  - IPv6
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 6.2
  - IPv6
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 6.1
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 6.0
  - Events Dashboard
  - Events Monitoring

  - Reporting
  - Up to 10 devices
  - Up to 100 EPS
- Cisco IPS 5.1
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 10devices
  - Up to 100 EPS
- Cisco IOS IPS 12.3(14)T7 and 12.4(15)T2
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 10 devices
  - Up to 100 EPS

IME Demo Mode

IME provides a demo mode so that you can see the sensor configuration and event monitoring functions without being connected to real devices. We provide a separate IME Demo icon that you can launch from your desktop. IME Demo mode contains sample events and health and security data for demonstrating event monitoring and sensor health and security status.

You can run IME and IME Demo mode simultaneously, but you can only run one instance of IME Demo mode at a time. You cannot add or delete devices in Demo mode. The dashboard works with simulated data; however, the RSS feed works normally because it relies on Internet connectivity. You can add, edit, or delete event views. The views are filled with simulated events.

Installing IME

This section describes how to install and upgrade IME.

Note Beginning with IME 7.0.3, you are required to create a password to access IME.

Cisco IOS IPS and CSM

IME event monitoring is also supported in IOS-IPS versions that support the Cisco IPS 5.x/6.x signature format. We recommend IOS-IPS 12.4(15)T4 if you intend to use IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

Caution Do not install IME on top of existing installations of CSM. You must uninstall CSM before installing IME. Do not install CSM on top of existing installations of IME.

Installation Notes and Caveats

Observe the following when installing or upgrading IME:

- You can install IME 7.0 over all versions of IME. All alert database and user settings are preserved.
- Make sure you close any open instances of IME before upgrading to IME 7.0.
- Disable any anti-virus or host-based intrusion detection software before beginning the installation, and close any open applications. The installer spawns a command shell application that may trigger your host-based detection software, which causes the installation to fail.
- You must be administrator to install IME.
- IME 7.0 coexists with other instances of the MySQL database. If you have a MySQL database installed on your system, you do NOT have to uninstall it before installing IME 7.0.

Installing or Upgrading to IME 7.0

To install IME, follow these steps:

Step 1 Download the IME executable file to your computer, or start IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file.

IME-7.0.1.exe is an example of what the IME executable file might look like.

Step 2 Double-click the executable file.

The Cisco IPS Manager Express - InstallShield Wizard appears.

You receive a warning if you have a previous version of Cisco IPS Event Viewer installed. Acknowledge the warning, and exit installation. Remove the older version of IEV, and then continue IME installation.

Step 3 Click **Next** to start IME installation.

Step 4 Accept the license agreement and click **Next**.

Step 5 Click **Next** to choose the destination folder, click **Install** to install IME, and then click **Finish** to exit the wizard. The Cisco IME and Cisco IME Demo icons are now on your desktop.

Note The first time you start IME, you are prompted to set up a password.

For More Information

- For the procedure for creating and changing the IME password, see Creating and Changing the IME Password, page 1-7.
- For the procedure for obtaining Cisco IPS software, see Obtaining Cisco IPS Software, page 24-2.

Creating and Changing the IME Password

Note Beginning with IME 7.0.3, you are required to create a password to access IME.

When you start IME for the first time, the Password Policy dialog box appears. Enter a password that you will use to access IME. Re-enter the password to confirm, and then click **OK**. From now on when you log in to IME, enter your password in the Enter IME password field and click **OK**. To change the

IME password, choose **Tools > Change User Password**, and enter your existing password, your new password, and then reenter the new password to confirm. When you uninstall and reinstall IME, you must create a new user password. You do not have to restart IME after a password change.

Note IME does not support user roles or multiple sessions, so you do not need to configure a user name.

Password Requirements

The IME password has the following requirements:

- Must contain at least 8 characters and no more than 80
- Must contain characters from at least three of the following classes:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters (! @ $ % & *)
- No single character repeated more than two times consecutively
- All input must be ASCII characters

Note IME performs other checks to make sure that the password is secure. You receive an error message if the password does not pass validation.

For More Information

For the procedures for adding users to IME, see Configuring Authentication and Users, page 6-17.

Recovering the IME Password

To recover the IME password, follow these steps:

Step 1 Stop the IME client.

Step 2 Delete the hosts.cfg file from the installed directory.

Example

```
C:\Documents and Settings\All Users\Application Data\Cisco Systems\IME\iev\hosts.cfg
```

Step 3 Restart the IME client.

Step 4 You are prompted to create a new password.

No events are lost from the database, including new events between the time you deleted hosts.cfg and restarted IME. However, the event account username and password will be used for both events and configuration. If you had different usernames and passwords for the event and configuration roles, you must edit each device to restore them.

Configuring Data Archiving

IME uses the MySQL database to store events. You need to archive the database tables periodically to maintain IME performance. You can customize the archive settings in the Tools > Preferences > Data Archive pane. Each event file contains 1,000,000 events by default and IME can store up to 400 event files. The time-based archive is disabled by default.

Supported User Role

You must be administrator to configure data archiving in IME.

Field Definitions

The following fields are found in the Data Archive pane:

- Maximum number of events in current event file—Lets you set the maximum number events per current event file.

  The default is 1,000,000. The range is 1000 to 1,000,000.
- Maximum number of archived files—Lets you set the maximum number of archived files you want to maintain.

  The default is 100. The range is 10 to 400.
- Enable time schedule for archiving events—Lets you archive event files at certain times.
- Choose the following time schedule:
  - Every—Lets you set the schedule in minutes. The default is 10 minutes.
  - Every—Lets you set the schedule in hours. The default is every hour.
  - Every day at time—Lets you specify a daily time to archive event files.

Configuring Data Archiving

To configure data archiving, follow these steps:

Step 1 From IME, choose **Tools > Preferences > Data Archive**.

Step 2 In the Maximum number of events in current event file field, enter the number of events you want the current event file to contain.

The default is 1,000,000. The range is 1000 to 1,000,000.

Step 3 In the Maximum number of archived files field, enter the number of archived files you want IME to maintain.

The default is 100. The range is 10 to 400.

Step 4 If you want to use a time schedule to archive events, check the **Enable time schedule for archiving events** check box.

Step 5 Under Choose the following time schedule, enter the time schedule you want to use, either in minutes, hours, or a specific daily time.

Tip To undo your changes, click **Cancel**.

Step 6 Click **Apply** to apply your changes and save the revised configuration.

Configuring Email Notification

You can have IME send email notifications when it receives certain types of events. By default, email notification is disabled. You must have the email server, sender, and recipient of the email.

Caution IME email notification does not support SSL authentication for email servers. All emails are sent to port 25 of the specified email server. Most, if not all, public email providers do not accept unauthenticated SMTP emails on port 25 because the email could be spam. Therefore, you should use your company email server.

Supported User Role

You must be administrator to configure email notification for IME.

Field Definitions

The following fields are found in the Notification pane:

- Enable email/epage notifications—When checked, enables email notifications.
- Mail Server (SMTP Host)—Lets you specify the email server of your company.
- From Address—Lets you specify the person you want to send the email notifications.
- Recipient Address(es)—Lets you specify the sensor administrator that you want to receive the email notifications.
- Send notifications for alerts—Lets you specify which level of alerts you want to see and which alerts with the specified risk ratings you want to see.
- Notification Interval—Lets you specify the notification interval in minutes.

  The default is 10 minutes. The range is 1 to 1440 minutes.
- Notification Type—Lets you choose to send summarized notifications, detailed notifications, or both.
- Maximum number of detailed notifications per interval—Lets you choose how many detailed notifications per interval you want to see.
- Content contains—Lets you choose which content to display in the detailed email notifications:
  - Event ID
  - Severity
  - Device
  - Application name
  - Receive time
  - Event time
  - Sensor local time
  - Signature ID
  - Signature name
  - Signature details
  - Signature version
  - Attacker IP address

- Attacker locality
- Victim IP address
- Victim Port
- Victim OS
- Victim Locality
- Summary count
- Initial alert ID
- Summary type
- Is final
- Interface
- VLAN
- Virtual sensor
- Context
- Actions taken
- Alert details
- Risk rating
- Threat rating
- Reputation
- Reputation details
- Protocol

Configuring Email Notification

To configure email notification for IME, follow these steps:

Step 1 From IME, choose **Tools > Preferences > Notification**.

Step 2 Check the **Enable email/epage notifications** check box.

Step 3 In the Mail Server (SMTP Host) field, enter the mail server name.

Use your company mail server, for example, smtp.mycompany.com.

Step 4 In the From Address field, enter the address of the person you want to send the email notifications.

Step 5 In the Recipient Address(es) field, enter the email of the user you want to receive the email notifications from IME.

Step 6 Choose which types of alerts you want to receive notifications about and in the Risk Rating Range field, enter the risk rating range.

The default is 80-100, which is a medium to high risk rating.

Step 7 In the Notification Interval field, enter the interval in minutes.

Notification is sent as one summary for each sensor for each interval. The default is 1 to 100 minutes.

Step 8 Under Notification Type, choose what type of notification you want to receive, summarized or detailed.

Step 9 If you choose detailed notifications, under Maximum number of detailed notifications per interval, enter how many detailed notifications you want for each summary, and then enter which fields you want in the summary content.

Step 10 Click **Apply**.

Step 11 To test the email setup, click **Send a Test Mail**.

If you have correctly set up email notification, you receive an information dialog box stating that the test email has been sent and you should check to see that you received it.

If you have not correctly set up email notification, you receive an error message stating that the SMTP host is unknown.

Step 12 Click **OK** to save your changes.

Sample Email Configuration

```
Flag this message
high 2004-0 ICMP Echo Request (10.2.2.2)
Wednesday, March 10, 2010 3:13 PM
From abc@def.com Wed Mar 10 23:13:38 2010
Date:                     Wed, 10 Mar 2010 23:13:38 GMT
From:
abc@def.com
To:                          jsmith@cisco.com
To:                          jimsmith2010@yahoo.com
Subject:                               high 2004-0 ICMP Echo Request (10.2.2.2)

Jim
```

Email Notification Examples

The following example shows the notification sent as one summary for each sensor per each interval:

```
low 9698-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*) Total:
284
high 35786-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 276
high 40971-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 251
low 8813-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*) Total:
565
high 21357-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 279
high 41528-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 554
```

The following example shows the detailed information for each event:

```
event_id=1186174940758000000
severity=high
device_name=shark
event_time=1186174940758000000
sig_id=21357
sig_name=Signature Example
```

For More Information

- For more information about risk categories, see Configuring Risk Category, page 12-32.
- For information on how the risk rating is calculated, see Calculating the Risk Rating, page 12-2.

Configuring General Options

In the General pane, you can configure certain general options, such as, specifying a network sniffer application, specifying the maximum number of events you want a real time or historical event to contain, specifying the event polling interval, whether you want to see the feature presentation video every time at startup, and whether you want to clear cached DNS names.

A network sniffer application, such as Wireshark, is useful for showing captured data packets for an event. Wireshark is a free network protocol analyzer for UNIX and Windows. It lets you examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Wireshark has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, see http://www.wireshark.org.

DNS enables you to convert human-readable names into the IP addresses needed for network packets. To optimize speed, the DNS names are cached. You can clear the DNS lookup results.

Supported User Role

You must be administrator to configure the general settings in IME.

Field Definitions

The following fields are found in the General pane:

- Network Sniffer Application Location—Lets you specify the path to your network sniffer application, or you can click **Browse** and locate the path.
- Maximum Real-time Events Per View—Lets you specify the number of events that a real-time event view should contain. When this number is reached, old events are removed from the view.

  The default is 2000.
- Maximum Historical Events Per View—Lets you specify the number of events that a historical event view should contain.

  The default is 50,000.
- Event Polling Interval—Lets you specify the number of seconds per interval for event polling.
- Show feature presentation video at startup—The IME feature video starts up by default every time you start IME. You can disable it here.
- Delete cached DNS names—Lets you clear cached DNS names.

Configuring the General Settings

To configure the general settings for IME, follow these steps:

Step 1 From IME, choose **Tools > Preferences > General**.

Step 2 In the Network Sniffer Application Location field, enter the location of your network sniffer application, or click **Browse** to locate the path.

Step 3 In the Maximum Real-time Events Per View field, enter the number of events you want a real-time event view to contain.

Step 4 In the Maximum Historical Events Per View field, enter the number of events you want a historical event view to contain.

Step 5 In the Event Polling Interval field, enter the number of seconds you want event polling intervals to have.

Step 6 Check the **Show feature presentation video at startup** check box to disable the feature presentation video.

The default is enabled.

Step 7 To delete cached DNS names, click **Delete cached DNS names**.