CHAPTER 1

Getting Started

This chapter describes IME and how to get started using it. It contains the following sections:

Introducing IME

IME is a network management application that provides system health monitoring, events monitoring, reporting, and configuration for up to five sensors. IME monitors sensor health using customizable dashboards and provides security alerts through RSS feed integration from Cisco Security Center. 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.

Note IME 6.1 replaces IEV 5.*x*.

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 are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may 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.

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 right 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**—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.

For More Information

For information on correcting the time on the sensor and configuring time on the sensor, see Configuring Time, page 6-6.

System Requirements

IME has the following system 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
- 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
- NME-IPS
- IDSM-2

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

- Cisco IPS 6.1
  - Sensor Configuration
  - Sensor Health Dashboard
  - Events Dashboard
  - Event Monitoring
  - Reporting
  - Up to 5 devices
  - Up to 75 events per second (EPS)
- Cisco IPS 6.0
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 5 devices
  - Up to 75 events per second (EPS)

- Cisco IPS 5.1
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 5 devices
  - Up to 75 events per second (EPS)
- Cisco IOS IPS 12.3(14)T7 and 12.4(15)T2
  - Events Dashboard
  - Events Monitoring
  - Reporting
  - Up to 5 devices
  - Up to 75 events per second (EPS)

Before Installing IME 6.1

IME 6.1 detects previous versions of IEV and prompts you to manually remove the older version before installing IME 6.1 or to install IME on another system. The installation program then stops.

Caution IME does not automatically uninstall IEV.

IME 6.1 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 6.1.

Migrating IEV Data

To migrate IEV 5.*x* events to IME, you must exit the installation and manually export the old events by using the IEV 5.*x* export function to move the data to local files. After installing IME 6.1, you can use the import function to import these files to the new system.

Note IME 6.1 does not support import and migration functions for IEV 4.*x*.

To export event data from IEV 5.*x* to a local file:

Step 1 From IEV 5.*x*, choose **File > Database Administration > Export Database Tables**.

Step 2 Enter the file name and select the table(s).

Step 3 Click **OK**.

The events in the selected table(s) are exported to the specified local file.

Importing IEV Event Data In to IME

To import event data in to IME, follow these steps:

Step 1 From IME, choose **File > Import**.

Step 2 Select the file exported from IEV 5.*x* and click **Open**.

The contents of the selected file are imported in to IME.

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

If you have a version of Cisco IPS Event Viewer installed, the Install wizard prompts you to remove it before installing IME.

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 or IEV. You must uninstall these applications before installing IME.

Caution 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.

Note You must be administrator to install IME.

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-6.1.1.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.

Step 3 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 4 Double-click the executable file.

The Cisco IPS Manager Express - InstallShield Wizard appears.

Step 5 Click **Next** to start IME installation.

Step 6 Accept the license agreement and click **Next**.

Step 7 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.