



Getting Started

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

- [Introducing the IME, page 1-1](#)
- [Advisory, page 1-2](#)
- [Participating in the SensorBase Network, page 1-2](#)
- [IME Home Pane, page 1-3](#)
- [IME System Requirements and Restrictions, page 1-4](#)
- [IME Demo Mode, page 1-4](#)
- [Installing the IME and Migrating Data In to the IME, page 1-4](#)
- [Creating and Changing the IME Password, page 1-6](#)
- [Recovering the IME Password, page 1-7](#)
- [Configuring General Options, page 1-7](#)
- [Configuring the Data Archive, page 1-8](#)
- [Configuring Email Setup, page 1-10](#)
- [Configuring Email Notification, page 1-12](#)
- [Configuring Reports, page 1-14](#)

Introducing the IME

The 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. The IME monitors sensor health using customizable dashboards and provides security alerts through RSS feed integration from the Cisco Security Intelligence Operations site. 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. The 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 the IME you can set up your sensors, configure policies, monitor IPS events, and generate reports. The IME works in single application mode—the entire application is installed on one system and you manage everything from that system.

Advisory

The 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.

Participating in the SensorBase Network

The Cisco IPS contains a security capability, Cisco Global Correlation, which uses the immense security intelligence that we have amassed over the years. At regular intervals, the 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 will collect 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 will be 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 14, “Configuring Global Correlation.”](#)
- For detailed information on licensing the sensor, see [Configuring Licensing, page 20-12](#).

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**—The IME has an overall feature presentation video that appears when you launch the 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 The 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 the IME has received recently is shown. The EPS count is updated every five seconds.

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

- **File > Import**—Lets you import the alarm data file that you exported from the previous version of the IME or IEV 5.x.
- **File > Export**—Lets you export alarm data from the IME database in to a CSV file.
- **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 configure a data archive, set up email and enable email notification and automatic reporting, 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 > Change User Password**—Lets you change your existing password in the Change Password dialog box.

- **Tools > Check Database Integrity**—Lets you perform an immediate database integrity check. You receive a Information dialog box informing you if any errors are found.
- **Tools > Repair Database**—Lets you repair any errors that you find in the database. You receive the following Warning dialog box before you can continue:

```
Database repair may cause data loss in certain circumstances. Do you wish to continue?
```
- **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 6-7](#).
- For the procedure to configure data archiving, see [Configuring the Data Archive, page 1-8](#).
- For the procedure to set up email notification, see [Configuring Email Notification, page 1-12](#).
- For detailed information on configuring general options for the IME, see [Configuring General Options, page 1-7](#).

IME System Requirements and Restrictions

For the list of requirements and restrictions for the IME, refer to the Release Notes for your version of the IME at this URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_release_notes_list.html

IME Demo Mode

The 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 the 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. When the IME is started in demo mode, the IME service continues to receive and store events.

Installing the IME and Migrating Data In to the IME

This section describes how to install and upgrade the IME, and how to migrate data from IEV or a previous version of IME.

Cisco IEV, Cisco IOS IPS, and CSM

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

The 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 the IME to monitor an IOS IPS device. Some of the new IME functionality including health monitoring is not supported.

**Caution**

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

Installation Notes and Caveats**Note**

If you are using Windows 7 or Windows Server 2008, and an IME version earlier than 7.1.1, uninstall IME before upgrading it. Otherwise, just upgrade from your current IME version.

Observe the following when installing or upgrading the IME:

- You can install the IME over all versions of the IME but not over IEV. All alert database and user settings are preserved.
- The IME detects previous versions of IEV and prompts you to manually remove the older version before installing the IME or to install the IME on another system. The installation program then stops.
- Make sure you close any open instances of the IME before upgrading to a new version of the IME.
- 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 the IME.
- The IME 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 the IME.

Installing or Upgrading the IME

To install the IME, follow these steps:

- Step 1** From the Download Software site on Cisco.com, download the IME executable file to your computer, or start the IDM in a browser window, and under Cisco IPS Manager Express, click **download** to install the IME executable file. IME-7.2.1.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 the IME installation.
- Step 3** Click **Next** to start the IME installation.
- Step 4** Accept the license agreement and click **Next**.
- Step 5** Click **Next** to choose the destination folder, click **Install** to install the 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 the IME, you are prompted to set up a password.

Migrating IEV Data

To migrate IEV 5.x events to the 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 the IME, you can import these files to the new IME system.

**Note**

The IME 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 the IME, follow these steps:

-
- Step 1** From the 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 the IME.
-

For More Information

- For the procedure for creating and changing the IME password, see [Creating and Changing the IME Password, page 1-6](#).
- For instructions on how to obtain Cisco IPS software, see [Obtaining Cisco IPS Software, page 26-1](#).

Creating and Changing the IME Password

When you start the IME for the first time, the Password Policy dialog box appears. Enter a password that you will use to access the IME. Reenter the password to confirm, and then click **OK**. From now on when you log in to the 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 the IME, you must create a new user password. You do not have to restart the IME after a password change.

**Note**

The 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**

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

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
```

**Note**

This example location may be different depending on which Windows version you have.

- 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 the IME. However, the event account user name and password will be used for both events and configuration. If you had different user names and passwords for the event and configuration roles, you must edit each device to restore them.

Configuring General Options

In the General dialog box, 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 the IME.

Field Definitions

The following fields are found in the General dialog box:

- 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 the 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 the IME, follow these steps:

-
- Step 1** From the 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**.
-

Configuring the Data Archive

The 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** dialog box. Each event file contains 1,000,000 events by default and the IME can store up to 400 event files. You can configure IME to send you an email when the event archive reaches a specified limit.

**Note**

You must have an email server configured to receive emails.

Field Definitions

The following fields are found in the Data Archive dialog box:

- **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 Notification:**
 - **When number of archived files reach**—Configures the IME to email you when a specified percent of maximum number of archived files is reached. The default is disabled and the default percentage is 80%.

For example, when you set the maximum number of archived files to 10, and you set the percentage the archived files should reach to 30%, you receive an email when the number of event files created reaches three. Once an email has been sent for a configured percentage, the IME never sends an email again, unless you change the percentage field or the maximum number of archived files field. If you change these two fields, the percent value is recalculated, and once it reaches the new calculation, an email is sent.

- **When number of archived files reach maximum**—Configures the IME to email you when the number of archived files reaches the specified maximum. The default is disabled.

Once the maximum value is reached for every new event archive file creation, an email is sent. To stop receiving notification, uncheck this option. If you change the maximum number of archived files value to a higher value than the old configured value, the notification stops until it reaches the new threshold value. If it is less than the old value, the notifications never stop.

- **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 the 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 the IME to maintain. The default is 100. The range is 10 to 400.
 - Step 4** Check the **When number of archived files reach** checkbox and enter a percentage in the % of Max field to receive emails when a specific percent of the maximum number of archived files is reached. The default is enabled and the default percentage is 2%.

Example Email:

The configured maximum archived event file limit is 10.

The configured percentage threshold value for the archived event file is 2%. This is a notification to inform you that this percent threshold value has been reached. The oldest event data files are overwritten once the maximum archive file limit is reached.

- Step 5** Check the **When number of archived files reach maximum** checkbox to receive emails when the number of archived files reaches the specified maximum number.

Example Email:

The configured maximum archived event file limit is 10. This is a notification to inform you that this limit is just about to be reached. The next event file creation from the system will overwrite the oldest event file.

Example Email:

The configured maximum archived event file limit is 10. This is a notification to inform you that this limit was reached. The new event file creation from the system is overwriting the oldest event files.

- Step 6** If you want to use a time schedule to archive events, check the **Enable time schedule for archiving events** check box. The default is enabled.
- Step 7** 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 8** Click **Apply** to apply your changes, save the revised configuration, and continue editing the dialog box, or click **OK** to save the changes and exit the dialog box.

For More Information

For the procedure for setting up an email server for the IME, see [Configuring Email Setup, page 1-10](#).

Configuring Email Setup

In the Email Setup dialog box, you can configure a mail server, and sender and recipient email addresses so that the IME can send email notifications to specified users.

Field Definitions

The following fields are found in the Email Setup dialog box:

- Allow mail to be sent from IME (required for email notifications)—When checked, lets you have the IME send email notifications.
- Send Test Email—Lets you test email setup. You must specify a mail server and sender/recipient email addresses before you can test the email setup.
- Server Settings—Lets you specify the mail server settings:
 - Mail Server (SMTP Host)—Specifies the mail server of your company. Check the **Using SSL** checkbox to use SSL on this server.
 - Using authentication—When checked, enables user authentication.
 - Username—Specifies the username of the user authorized to access the mail server.

- Password—Specifies the password of the authorized user.
- Sender/Recipient Settings—Lets you specify emails for the senders and recipients:
 - Sender Address—Lets you specify the person who sends the email notifications.
 - Recipient Address(es)—Lets you specify the sensor administrator that you want to receive the email notifications.

Setting Up Email

To set up email, follow these steps:

-
- Step 1** From the IME, choose **Tools > Preferences > Email Setup**.
- Step 2** Check the **Allow mail to be sent from IME (required for email notifications)** checkbox.
- Step 3** Configure the mail server settings:
- a. In the Mail Server (SMTP Host) field, enter the mail server address for your company. Use your company mail server, for example, smtp.mycompany.com.
 - b. To use SSL, check the **Using SSL** checkbox.
 - c. To require user authentication, check the **Using authentication** checkbox.
 - d. In the Username field, enter the username of the user who will access the mail server.
 - e. In the Password field, enter the password for this user.
- Step 4** Configure the sender and recipient settings:
- a. In the Sender Address field, enter the email address of the user who will send email from the IME.
 - b. In the Recipient Address(es) field, enter the email addresses you want to send email notifications to, for example, admin@mycompany.com or ips@mycompany.com.



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

- Step 5** Click **Apply** to save your changes.
- Step 6** To test the email setup, **Send a Test Email**.
- If you have correctly set up email, 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, you receive an error message stating either that the IME could not connect to the SMTP host because the wrong SMTP server is configured, or that the IME failed to authenticate the server because the user credentials are incorrect.
- Step 7** Click **OK** to save your changes and exit the dialog box.
-

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)

Configuring Email Notification

Email notifications are sent periodically to the recipient address for the events that correspond to the criteria you defined in the Send notifications for alerts field. By default, email notification is disabled. You must have the email server, sender, and recipient addresses for the email. You must set up email first by entering that information in the **Tools > Preferences > Email Setup** dialog box.

Field Definitions

The following fields are found in the Notifications dialog box:

- Enable email/epage notifications—When checked, enables email notifications.
- Send Test Notification—Lets you test IME email notification. You must have at least one severity level and at least one field selected to test email notification.
- 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 the IME, follow these steps:

-
- Step 1** From the IME, choose **Tools > Preferences > Notification**.
 - Step 2** Check the **Enable email/epage notifications** check box.
 - Step 3** 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 4** In the Notification Interval field, enter the interval in minutes. Notification is sent as one summary for each sensor per each interval. The default is 1 to 100 minutes.
 - Step 5** Under Notification Type, choose what type of notification you want to receive, summarized or detailed.
 - Step 6** If you choose detailed notifications, under Maximum number of detailed notifications per interval, enter how many detailed notifications you want per summary, and then enter which fields you want in the summary content.
 - Step 7** In the Content contains field, check the checkbox of each field that you want included in the email notifications.
 - Step 8** Click **Apply** to save your changes.
 - Step 9** To test the email notification, click **Send Test Notification**.

If you have correctly set up notification, you receive an information dialog box stating that the test notification has been sent and you should check to see that you received it. If you have not correctly set up notification, you receive an error message.
 - Step 10** Click **OK** to save your changes and exit the dialog box.
-

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 12-31](#).
- For information on how the risk rating is calculated, see [Calculating the Risk Rating, page 12-2](#).

Configuring Reports

The IME send reports once a day, week, or month based on the schedule you configure. By default, automatic reporting is disabled. The IME sends an email with the report as a PDF attachment. The email lets you know the success or failure of the reports you wanted to generate.

Field Definitions

The following fields are found in the Reports dialog box:

- Enable automatic reporting—When checked, enables automatic reporting.
- Send Test Report(s)—Lets you test IME automatic reporting. You must have a time specified, at least one type of report selected, and email notifications set up to test automatic reporting.
- Choose a time schedule—Lets you specify when you want to receive automatic reports:
 - Daily—Specifies a daily automatic report. Choose the time you want to receive it from the drop-down list.
 - Weekly—Specifies a weekly automatic report. Choose the day and time you want to receive it from the drop-down list.
 - Monthly—Specifies a monthly automatic report. Choose time you want to receive it from the drop-down list and enter the day of the month you want to receive it in the Day of each month field.
- Report(s) to include—Lets you choose which types of reports you want to receive.

- Top Attacker Reports—Shows top attacker IP addresses for a specified time. You specify the top number of attacker IP addresses. There are four predefined top attacker reports:
 - Basic Top Attacker
 - Top 10 Attackers Last 1 Hour
 - Top 10 Attackers Last 8 Hours with High Severity
 - Top 20 Critical Attackers Last 24 Hours
- Top Victim Reports—Shows top victim IP addresses for a specified time. You specify the top number of victim IP addresses. There are four predefined top victim reports:
 - Basic Top Victim
 - Top 10 Victims Last 1 Hour
 - Top 10 Victims Last 8 Hours with High Severity
 - Top 20 Victims with Action Denied Attacker
- Top Signature Reports—Shows top signatures fired for a specified time. You specify the top number of signatures. There are four predefined top signature reports:
 - Basic Top Signature
 - Top 10 Signatures Last 1 Hour
 - Top 10 Signatures Last 8 Hours with High Severity
 - Top 20 Critical Signatures Last 24 Hours
- Attacks Over Time Reports—Shows the attacks over a specified time. There are five predefined reports:
 - Basic Over Time Attack
 - Attacks Blocked in Last 24 Hours
 - Attacks Dropped in Last 24 Hours
 - Attacks Over Time Last 1 Hour
 - Critical Attacks Over Last 24 Hours
- Filtered Events vs All Events Reports—Displays a set of events against the total events for a specified time period. There is one predefined report:
 - Negative Reputation Events
 - My Reports—Displays your user-defined reports.
- Preferred chart type—Lets you view the reports as bar charts or pie charts.

Configuring Automatic Reporting

To configure automatic reporting for the IME, follow these steps:

-
- Step 1** From the IME, choose **Tools > Preferences > Reports**.
- Step 2** Check the **Enable automatic reporting** check box.
- Step 3** Choose a time schedule:
- Daily
 - Weekly
 - Monthly

Step 4 In the Report(s) to include field, check the checkbox of each report that you want included in the automatic reports.

Step 5 From the Preferred chart type drop-down list, choose either Bar Chart or Pie Chart.

Step 6 Click **Apply** to save your changes.

Step 7 To test the automatic reporting, click **Send Test Report(s)**.

If you have correctly set up automatic reporting, you receive an information dialog box stating that the test report has been sent and you should check to see that you received it. If you have not correctly set up automatic reporting, you receive an error message.

Step 8 Click **OK** to save your changes and exit the dialog box.

Automatic Reports Email Example

```
From: ime@cisco.com [mailto:ime@cisco.com]
Sent: Monday, October 31, 2011 4:30 AM
To: John Smith (jsmith)
Subject: IME Auto-Generated Report - 2011-10-31T04:30:08.085-0500
```

Please find attached a report summarizing recent sensor activity registered with Cisco IME.

The following reports were not generated due to missing data:

- Top 10 Attackers last 8 hours with High Severity
- Top 20 Critical Attackers last 24 hours
- Top 10 Victims last 8 hours with High severity
- Top 20 Victims with Action as denied
- Top 10 Signatures last 8 hours with High Severity
- Top 20 Critical Signatures last 24 hours