Cisco IPS Manager Express

Product Overview

Intrusion prevention systems (IPSs) are critical to protecting your network and assets against worms, Trojans, and other malicious attacks. Cisco® IPS Manager Express is a powerful, all-in-one IPS management application designed to meet the needs of small and medium-sized businesses. With one application, you can provision, monitor, troubleshoot, and generate reports for as many as 10 Cisco IPS sensors. Cisco IPS Manager Express is an integral part of a Cisco IPS solution, providing intuitive, powerful, and secure protection of your network and assets.

- **Intuitive:** Easy-to-use interfaces simplify deployment and management
- **Powerful:** High performance and advanced features provide strong security protection and reduce analysis time
- **Secure:** Security updates delivered by global security intelligence team working 24 hours a day helps provide peace of mind

Features and Benefits

Intuitive Customizable Dashboards

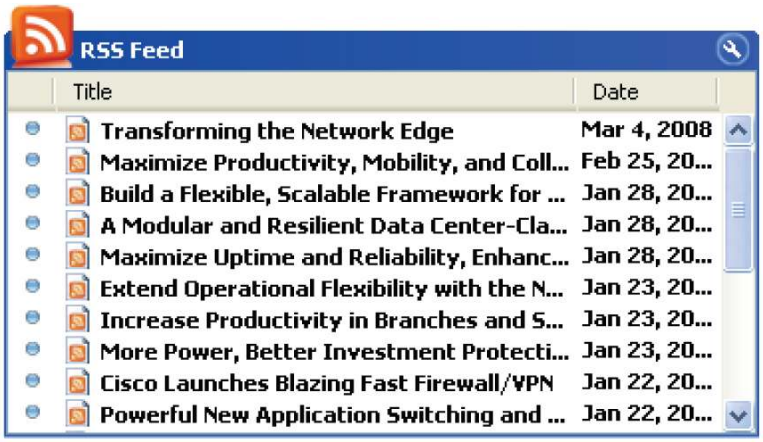
The Cisco IPS Manager Express dashboard (Figure 1) lets you look at the health of both your IPS sensor and the network. Offering numerous drag-and-drop gadgets, the dashboard is customizable and remembers your settings, so you can come back to the same settings the next time you start Cisco IPS Manager Express.

Figure 1. Customizable Dashboard

Live RSS Feeds

Live RSS feeds (Figure 2) keep you informed about the most recent security threats on the network. The feeds can be personalized to your needs and can provide recommendations for securing your network.

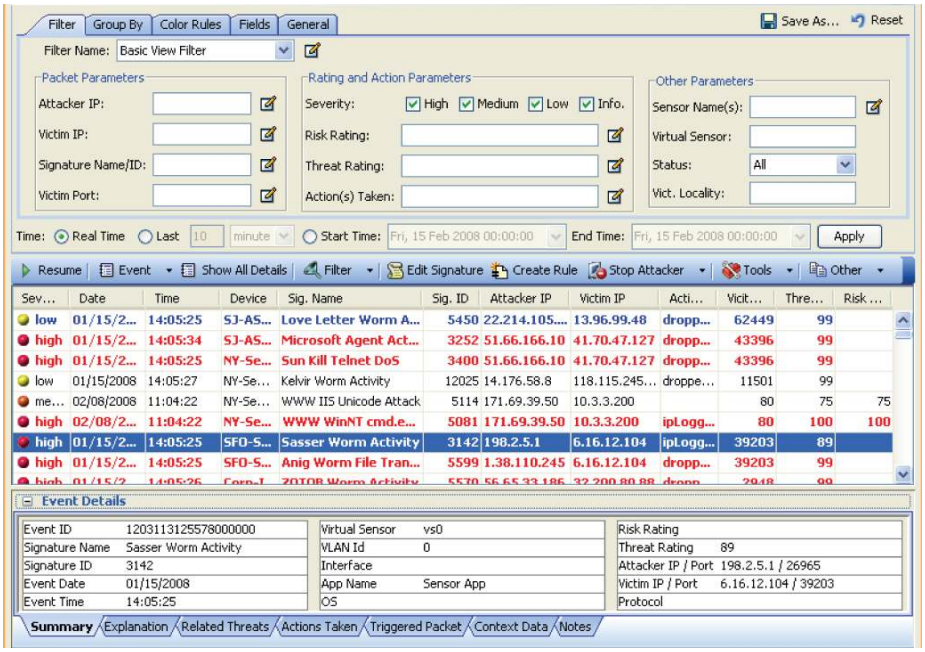
Figure 2. Live RSS Feeds Gadget



Powerful Monitoring of Real-Time and Historical Events with Cisco IPS Manager Express Event Viewer

Cisco IPS Manager Express provides many advanced event-monitoring capabilities to reduce troubleshooting and analysis time. With the Cisco IPS Manager Express Event Viewer (Figure 3), you can monitor real-time and historical events in the same view. To help you with analysis, the Event Viewer provides filtering, coloring, and grouping capabilities. Events can be colored or filtered using numerous parameters, and can be grouped into tiered levels. To help you better understand an event, the Event Details section provides information about the event and the signature.

Figure 3. Cisco IPS Manager Express Event Viewer



Flexible Reporting Tool

The Cisco IPS Manager Express reporting tool allows you to generate custom and compliance reports in seconds. Choose from predefined templates or create your own report with easy-to-use filters. The reporting tool allows you to choose from pie charts or bar graphs, customize your report to specific time periods, and include IP addresses in the reports. For easier reading, you can use the built-in DNS resolution to convert the IP addresses to DNS names. All reports can be printed or saved to PDF or RTF format for sharing and future viewing.

Advanced Policy Provisioning

The Cisco IPS Manager Express policy provisioning table allows you to quickly and easily define your network security policy based on Risk Rating, an innovative Cisco feature that quantifies the level of risk of each event. Different policy actions can be assigned to different Risk Rating ranges; for example, dropping packets from events with high Risk Ratings and alerting you about events with medium Risk Ratings. You can also create exceptions to your policy using the policy exception table.

Tight Integration Between Application Functions

Tight integration between different application functions within Cisco IPS Manager Express shortens threat response time. With one click, for each event, you can link from the Event Viewer to the policy table or to the signature table. When you link from the Event Viewer to the policy table, you will see pre-populated event information. This simplifies policy provisioning and reduces the chance of mistakes. One-click blocking allows you to stop an attack directly from the Event Viewer.

Intuitive Startup Wizard

The Cisco IPS Manager Express Startup Wizard simplifies IPS sensor setup and reduces deployment time. It provides step-by-step instructions on how to set up an IPS sensor, whether the sensor is a Cisco IPS 4200 Series appliance; an IPS module for a Cisco ASA 5500 Series appliance; or a module for a Cisco Catalyst® switch. With the Cisco IPS Manager Express Startup Wizard, you can set up a fully functional IPS sensor in minutes.

Feature Specifications

Table 1 describes supported features of Cisco IPS Manager Express. Table 2 describes the minimum system requirements for Cisco IPS Manager Express. Table 3 lists the Cisco IPS Manager Express features that are available on different versions of Cisco IPS software.

Table 1. Supported Features

Features	Feature Description	Cisco IPS Sensor Software	Cisco IOS® IPS
Homepage			
Ten-Sensor Dashboard View	Ten-sensor dashboard view of primary sensor statistics, including CPU utilization, memory utilization, IP address, sensor health status, and license expiration for easy at-a-glance viewing.	Yes	No
Sensor Health Meter	An intuitive tri-level (red, yellow, green) meter provides an at-a-glance view of the health of each sensor. Adjustable thresholds on each of six customizable parameters allow the user to customize the meter to the organization's needs.	Yes	No
Security Health Meter	An intuitive tri-level (red, yellow, green) meter provides a Threat Rating based on network security health. Adjustable thresholds allow the user to customize the meter to the organization's needs.	Yes	No

Features	Feature Description	Cisco IPS Sensor Software	Cisco IOS® IPS
Customizable Dashboards			
Health and Real-Time Traffic Gadgets	Drag-and-drop gadgets for at-a-glance view of sensor health statistics and real-time traffic statistics. • Sensor information: ◦ Sensor health ◦ Sensor information ◦ CPU, memory, disk, and sensor load ◦ Licensing information ◦ Interface status • Real-time traffic statistics: ◦ Top applications ◦ Network security	Yes	No
Event Statistics and Security News Gadgets	Drag-and-drop gadgets for at-a-glance view of event statistics and security news. • Event statistics: ◦ Top attackers ◦ Top victims ◦ Top signatures ◦ Attacks over time • Security news: ◦ RSS feeds	Yes	Yes
Customizable Gadgets	Customizable graphs (pie chart, bar chart, table) and time intervals for personalization and ease of troubleshooting.	Yes	Yes
Minimize Gadgets	Gadgets can be minimized to save dashboard space.	Yes	Yes
Multiple Dashboard Views	Multiple dashboard views enable customization and flexible viewing.	Yes	Yes
Saved Dashboard Views	Saved dashboard views allow you to see the same view the next time you start Cisco IPS Manager Express.	Yes	Yes
Event Viewer			
Real-Time Event Viewer	Real-time event viewer enables real-time event monitoring.	Yes	Yes
Real-Time Event Viewer Pause	Pause and scroll forward and backward for analysis and troubleshooting.	Yes	Yes
Historical Event Viewer	View events for specified time intervals (date and time) for analysis and troubleshooting.	Yes	Yes
Event Coloring	Event coloring (by signature, severity, attacker/victim IP address, victim port, Risk Rating, Threat Rating, virtual sensor, sensor) improves analysis and troubleshooting.	Yes	Yes
Event Filtering	Event filtering (by signature, severity, attacker/victim IP address, victim port, Risk Rating, Threat Rating, virtual sensor, sensor) simplifies analysis and troubleshooting.	Yes	Yes
Multilevel Event Grouping	Multilevel event grouping (by signature, severity, attacker/victim IP address, Risk Rating, Threat Rating, sensor) simplifies analysis and troubleshooting.	Yes	Yes
Drag-and-Drop Columns	Drag-and-drop columns allow easy column reordering and customized views.	Yes	Yes
Multicolumn Sort	Columns can be sorted alphanumerically for easy viewing on multiple columns.	Yes	Yes
Customizable Views	Create and save customized event views (including filter, color, group settings, and column arrangements) for simplified analysis and troubleshooting.	Yes	Yes
Inline Packet Decode	Under Event Details, you can see the inline packet decode for troubleshooting and forensics.	Yes	Yes
Ethereal Integration Support	Cisco IPS Manager Express can integrate Wireshark Ethereal for advanced troubleshooting and forensics.	Yes	Yes
Dynamic Linkages to Cisco Security Center	Under Event Details, view event information based on data from Cisco Security Center for simplified analysis and troubleshooting.	Yes	Yes
Dynamic Event Linkages to Policy Table	Dynamic event linkages to the policy table provide an easy way to create policy exceptions and simplify provisioning.	Yes	No

Features	Feature Description	Cisco IPS Sensor Software	Cisco IOS® IPS
Dynamic Linkages to Signature Table	Dynamic event linkages to signature table simplify signature tuning.	Yes	No
One-Click Block/Deny	In a single click, block or deny attacker packets for immediate threat prevention.	Yes	No
Integrated Network Tools	Network tools, including ping, trace-route, DNS lookup, and whois, are integrated into the Event Viewer for simplified analysis and troubleshooting.	Yes	Yes
Event Incident Handling	Event incident handling settings help you simplify your incident handling process. You can assign incident handling settings (assigned, acknowledged, closed) to events, filter events based on these settings, and create notes for each event.	Yes	Yes
Event Save and Export	Save all events or selected events to HTML or CSV for further analysis or recordkeeping. Events can be exported from Cisco IPS Manager Express for sharing and recordkeeping.	Yes	Yes
Events per Second (EPS) Meter	The EPS meter gives you an indication of the number of events Cisco IPS Manager Express is processing per second. Users can also view EPS per sensor.	Yes	Yes
Email Notification	Email notification keeps you informed about threats when you are away. You can specify email notification intervals and events. Events can be filtered based on severity and Risk Rating.	Yes	Yes
Data Archive	On-box data archive with customizable archive schedule allows faster data analysis.	Yes	Yes
Configuration			
Policy Provisioning	Provision policies based on Risk Rating. IPS actions are assigned to different Risk Rating ranges.	Yes	No
Policy Exceptions	Provision policy exceptions based on Risk Rating, attacker IP address/port, victim IP address/port, and signature.	Yes	No
Anomaly Detection Provisioning	Configure a sensor to send alerts upon abnormal network behavior. Cisco anomaly detection provides zero-day attack protection.	Yes	No
Signature Provisioning			
Signature Action Assignment	Choose from 14 actions to assign to signatures (“deny packets,” “alert,” etc.).	Yes	No
Signature Enable and Disable	Enable and disable signatures based on your requirements.	Yes	No
Auto-Signature Updates	Sensor automatically retrieves and applies new signature updates at user-specified times, for enhanced security and ease of deployment.	Yes	No
Signature Wizard	Signature wizard provides a step-by-step guide to creating custom signatures.	Yes	No
Signature Filtering	Intuitive signature filtering (by signature, severity, fidelity, Risk Rating, and action) simplifies signature provisioning.	Yes	No
Drag-and-Drop Columns	Drag-and-drop columns allow easy column reordering and customized views.	Yes	No
Column Sort	Columns can be sorted alphanumerically for easy viewing.	Yes	No
Signature Export	Signature export allows you to export signature tables to CSV or HTML format.	Yes	No
Reporting			
Predefined Report Templates	More than 10 predefined report templates simplify report generation. Predefined report templates include top 10 attacker last 1 hour, top 10 victims last 1 hour, and attacks over last 1 hour.	Yes	Yes
Customizable Reports	Create customized reports based on specified timeframe and filter criteria such as attacker IP address, victim IP address, victim port, signature, Risk Rating, Threat Rating, signature, and action taken.	Yes	Yes
Customizable Graphs	Specify graph types (pie chart or bar graph) for personalized reporting.	Yes	Yes
Report Save	Save report to PDF or RTF format for compliance reporting or recordkeeping.	Yes	Yes

Features	Feature Description	Cisco IPS Sensor Software	Cisco IOS® IPS
Setup and Help			
Startup Wizard	Intuitive startup wizard provides step-by-step instructions on setting up an IPS, including network settings, time setting, and interface configuration.	Yes	No
Administrator Password Requirements	Specify minimum administrator password requirements, including number of attempts, minimum number of characters, minimum character types, and number of historical passwords.	Yes	No
Video Help	Video help provides visual step-by-step guide on using primary features in Cisco IPS Manager Express.	Yes	Yes

Table 2. Minimum System Requirements

Component	Minimum Requirements
System Hardware	• IBM PC-compatible with 2-GHz or faster processor ◦ Color monitor with at least 1024x768 resolution and a video card capable of 16-bit colors
Hard Drive	100 GB
Memory (RAM)	2 GB
Supported Operating Systems	• Windows Vista Business and Ultimate (32-bit only) • Windows XP Professional (32-bit only) • Windows 2003 server **Note:** Cisco IPS Manager Express supports only the 32-bit U.S. English version of Windows.

Table 3. Supported IPS Sensors and IPS Sensor Software

Sensor	IPS Software
• Cisco IPS 4240, 4255, 4260, and 4270 Sensors • Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Modules and Cards • Cisco ASA 5500 Series IPS Security Services Processors • Cisco ASA 5500 Series Adaptive Security Appliances • Cisco IPS Advanced Integration Module (AIM) • Cisco Catalyst® 6500 Series Intrusion Detection System (IDSM-2) Services Module	Cisco IPS Sensor Software Version 6.1 and higher

Ordering Information

This product is included with Cisco IPS Sensor Software. To download the software, visit http://www.cisco.com/cisco/software/navigator.html?mdfid=277026257&i=rm.

For More Information

For more information about Cisco IPS Manager Express, visit http://www.cisco.com/go/ime or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-459033-03 09/12