

# Symantec™ IM Manager

Secure instant messaging (IM) management and policy enforcement of public and enterprise IM for enterprise risk management

---

## Overview

Symantec IM Manager seamlessly manages, secures, logs, and archives corporate IM traffic with certified support for consumer IM services and enterprise IM platforms and with granular policy controls for text messaging, file transfers, audio, video, VoIP, application sharing, and other real-time communication capabilities associated with IM. Symantec IM Manager secures corporate networks against external threats such as IM viruses, worms, and malware through the use of real-time content filtering, worm and virus signature detection, behavior-based threat protection, and file-based antivirus scanning. It also protects organizations against the loss of sensitive information or intellectual property over IM through granular policy controls for internal IM usage, including internal message routing, regular expression pattern matching, and real-time user monitoring.

Integrated with Symantec Security Response, Symantec IM Manager offers the industry's first zero-day threat protection from IM-borne viruses and worms.<sup>1</sup> Utilizing a patent-pending behavior- and signature-based system, Symantec IM Manager provides automatic protection for new and emerging IM viruses. In addition, it provides a tool to enforce content and regulatory compliance policies for all aspects of IM, including the ability to selectively log

messages based on user, group, or domain attributes; selectively insert customer message disclaimers; and capture 100 percent of message traffic for internal or external third-party archiving.<sup>2</sup>

---

## Key features

### *Manage instant messaging to drive business results*

- **User management and access control**—Manage and control IM user, group, and domain access to disparate IM systems, including integration with enterprise directory structures.
  - **Priority-based policy enforcement**—Establish consistent IM usage policy enforcement, including real-time content filtering, granular file transfer, and advanced client feature controls.
  - **Real-time analytics and reporting**—Obtain visibility into IM usage and growth patterns with real-time altering, trend reporting, and custom monitoring.
- 

### *Protect the organization with security and usage control*

- **Zero-day protection**—Take advantage of patent-pending technology for detection and protection against zero-day attacks.
- **Automatic threat updates**—Automatically update virus and spam signatures from the industry-leading Symantec Security Response Team.

1. See the Symantec Real-Time Threat Protection System (RTTPS) press release, July 2005.

2. Message queue technology is a transacted system that helps ensure high performance and message integrity by acting as a persistent, networkable buffer between the point of capture and the archive. If a message is not accepted by the queue, it is not sent.

- **Virus scanning and file transfer control**—Scan file transfers leveraging the Symantec AntiVirus™ Scan Engine to prevent infected or confidential files from traversing your network.
- 

### **Comply with legal and corporate accountability standards**

- **Rich message archive**—Selectively capture and retain IM conversations with direct links to employee data from the corporate directory for enhanced retention and discovery.
  - **Real-time content filtering**—Block messages and/or notify administrators when messages containing restricted phrases or inappropriate content are sent.
  - **Integration with Symantec Enterprise Vault™**—Deliver IM conversations to Symantec Enterprise Vault via out-of-the-box, transactional integration with Enterprise Vault. This allows organizations to review IM and email conversations in one centralized store.
- 

### **System requirements**

#### **Recommend IM manager server**

- 3.0 GHz Intel® Xeon® processor
- 1 GB RAM
- 60 GB hard disk

#### **Recommended database server**

- 3.0 GHz Intel Xeon processor
- 1 GB RAM
- 100 GB hard disk

### **Minimum recommended software requirements**

- Microsoft® Windows® 2000 with SP3 or Windows 2003
- MDAC 2.5 or later
- Microsoft Internet Explorer 5.5 or later
- Microsoft XML Core Services (MSXML) 4.0 SP2
- Microsoft IIS Web Service
- Access to Oracle® (Oracle 9i v 9.2.0.5 with ODBC drivers 9.2.0.63, Oracle Enterprise Client 9.2.01), Microsoft SQL Server 2005, Microsoft SQL Server 2000 SP4, or MSDE installed database

### **Sample of supported IM networks**

- AIM 6.5
- Yahoo 8.1
- Windows LiveMessenger 8.5
- Google Talk
- ICQ 6.0
- Sametime 8.0
- Office Communications Server 2007

For a full list, visit:

<http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2007082917260454>

## Data Sheet: Messaging Security Symantec™ IM Manager

### *Visit our website*

<http://enterprise.symantec.com>

### *To speak with a Product Specialist in the U.S.*

Call toll-free 1 (800) 745 6054

### *To speak with a Product Specialist outside the U.S.*

For specific country offices and contact numbers, please visit our website.

### *About Symantec*

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

### *Symantec World Headquarters*

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

[www.symantec.com](http://www.symantec.com)

Confidence in a connected world.

