

Symantec IM Manager™

Secure instant messaging (IM) management of public and enterprise IM, and legal and corporate governance policies compliance

Symantec IM Manager seamlessly manages, secures, logs, and archives corporate IM traffic with certified support for public and enterprise IM networks, including granular policy controls for files, 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 usage of real-time content filtering, worm and virus signature detection, behavior-based threat protection, and file-based antivirus scanning. Symantec IM Manager 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 the Symantec™ Security Response, Symantec IM Manager offers the industry's first zero-day threat protection from IM-borne viruses and worms.¹ Utilizing a patent-pending behavior- and signature-based system, Symantec IM Manager provides automatic protection for new and emerging IM viruses.

In addition, Symantec IM Manager 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; guarantee 100% message capture and logging through integrated message queuing; selectively insert message disclaimers; and capture 100% of message traffic managed by IM Manager for internal or external third-party archiving.²

Key features

Manage instant messaging to drive business results

- **Powerful, Flexible Group Policy**—Manage single users or large enterprise groups with predefined, configurable rules within a configurable hierarchy.
- **User Access Control**—Manage employee IM use behind your firewall and control access to external IM networks by user or group.
- **Transparency to End Users**—Deploy IM Manager without touching the desktop and use Symantec IM Manager to detect inappropriate use of IM.

Protect the organization with security and usage control

- **Zero-Day Protection**—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™ Response Team.
- **Virus Scanning and File Transfer Control**—Scan file transfers leveraging Symantec AntiVirus™ Scan Engine to prevent infected or confidential files from traversing your network.

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

2. Message queue technology is a transacted system that does not allow messages to be sent if they are not written to an archive first. If it is not captured and stored it is not sent.



Comply with legal and corporate accountability standards

- **Rich Message Archive**—Capture all messages and enrich message archive with employee data from the corporate directory for enhanced search capability and reporting.
- **Compliance Auditor Workflow**—Review conversations, append audit comments, and mark messages as reviewed to demonstrate compliance review procedures.
- **Real-time Content Filtering**—Block messages and/or notify administrators when messages containing restricted phrases are sent.

System requirements

- Intel® Pentium® III or compatible; 30 GB hard drive
- Windows Server 2003, Windows 2000 Server Service Pack 4 or later; Red Hat Enterprise Server 3.0 for the pass through relay (for DMZ deployment)
- Microsoft Core Services XML 4.0 SP2; Internet Information Services 5.0 or greater
- 512 MB RAM
- SQL Server 2000 SP3; oracle 9iR2 (9.2.0.4); MSDE (8.00.761 included)
- Microsoft® Internet Explorer v6.0 or later

More information

Visit our Web site

www.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 Web site.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

