# IMlogic IM Manager
A Technical Overview

Table of Contents

1.0 Introduction .................................................. 3  
  1.1 Instant Messaging in the Enterprise ...................... 3  
  1.2 Instant Messaging and Security ........................... 3  
  1.3 Instant Messaging and Regulatory Compliance .......... 4  

2.0 IMlogic IM Manager Features and Benefits ................. 5  
  2.1 Introduction ................................................. 5  
  2.2 Security ...................................................... 5  
    2.2.1 Threat Protection .................................... 5  
    2.2.2 Authentication and Access control .................. 6  
    2.2.3 Usage control and Monitoring ...................... 6  
  2.3 Archiving and Regulatory Compliance ................. 7  
  2.4 Deployment and Scalability .............................. 8  

3.0 IMlogic IM Manager Architecture .......................... 9  
  3.1 IM Manager Ecosystem .................................... 9  
  3.2 IM Manager Product Architecture ....................... 10  
    3.2.1 Overview .............................................. 10  
    3.2.2 Public IM ............................................. 10  
    3.2.3 Enterprise IM ....................................... 12  
    3.2.4 Additional Components ............................... 13  
    3.2.5 Complete Picture .................................... 15  
  3.3 IM Manager Message Capture ................................ 16  
  3.4 Conversation Exports / Archiving ....................... 17  
  3.5 Anti Virus Scans for File Transfers .................... 18  
  3.6 High Availability ....................................... 19  
    3.6.1 A sample 85,000 seat deployment .................. 20  

4.0 Minimum Hardware Requirements ....................... 21  

5.0 Minimum Software Requirements .......................... 21  

6.0 Additional Requirements ................................. 21
1.0 Introduction

1.1 Instant Messaging in the Enterprise

Instant Messaging (IM) is the fastest growing communications medium of all time, with enterprise business use growing at nearly 200% per year. First popularized as a tool for simple text messaging, IM has now become an indispensable tool for business communication — enabling employees to communicate and collaborate in real-time with colleagues, partners and customers around the world.

As a result, businesses are now being challenged to safely enable IM use while simultaneously satisfying the manageability, security and compliance requirements associated with this mission critical communications medium.

IMlogic IM Manager, the leading secure IM management solution, delivers real-time threat protection, rapid deployment, management, and records compliance for enterprise-wide IM usage. As the only secure IM management solution designed to deliver enterprise-class scalability, reliability and extensibility, IM Manager offers the most comprehensive support available for public, enterprise and hosted IM networks. With technology certifications from instant messaging industry leaders such as Microsoft®, AOL®, IBM®, Reuters, Yahoo!, and Jabber, Inc.®, businesses can now easily and securely support the broad use of IM for real-time communications.

1.2 Instant Messaging and Security

The rapid growth of IM has also exposed organizations to numerous security risks because corporate IM usage often goes unmanaged and unmonitored. These security risks include:

- Blended threats that use IM as a means to bypass traditional gateway antivirus software
- Identity theft, spoofing and phishing over IM
- Advanced spyware and SPAM over IM
- Proprietary information security leaks over IM
- Targeted attacks on enterprise domains

The IMlogic Threat Center, the industry’s first global consortium to provide threat detection and protection for instant messaging, tracks the emerging threats and real-time security risks associated with instant messaging. These findings are
based on research and analysis of reported incidents and events on the global IM networks. Incidents reported to the IMlogic Threat Center include open forum submissions from the general public, IMlogic enterprise customer events, IMlogic Threat Center Global honey-pot network events, and data contributed from consortium members, representing industry leaders in security and IM.

To further protect customers against IM threats, IMlogic provides the industry’s first preemptive protection against IM worms and viruses through the IMlogic Real-Time Threat Protection System (RTTPS). RTTPS is the most advanced IM threat protection system for predictive, automatic threat identification and prevention. IMlogic’s patent-pending RTTPS technology moves IM threat protection beyond traditional reactive security systems and safeguards, preventing IM virus, worm and malware outbreaks before they occur.

The IMlogic Real-Time Threat Protection System passively monitors all enterprise IM traffic and looks for network anomalies and potential malicious behavior. Once a potential threat is recognized, the RTTPS predictive protection filter identifies the new threat signature and stops the potential outbreak by blocking it at the point of propagation.

1.3 Instant Messaging and Regulatory Compliance

Instant messaging has become pervasive throughout all industries and is generally accepted as a form of “electronic messaging” as defined by governmental and industry bodies. As such, in many instances IM faces the same retention requirements as e-mail and other enterprise messaging systems and must be archived. Additionally, many organizations are being exposed to HR and legal risk associated with unmanaged and unmonitored IM communications that can contain inappropriate, damaging or illegal information.

Important regulatory requirements relevant to IM include:

- **SEC Rule 17a-3 and 17a-4**: Instant messages are characterized as a “book or record” to be retained as an “internet communication.”
- **NASD Rule 3010 and 3110**: Firms must maintain a “system to supervise and review” IM conversations and demonstrate compliance procedures for “electronic correspondence.”
- **NYSE Rules 440 and 342**: “Instant Messaging” is explicitly outlined in NYSE Information Memo #03-7 as a type of communication that must be archived under SEC regulations.
- **DOD Directive 5015.2**: Sets standards for records retention, including IM.
• Sarbanes-Oxley (SOX) 404: SOX brings with it a vast requirement for monitoring and reporting on the communication and documentation related to the company’s finances.

• HIPAA: Requires retention of patient records during clinical trials by med/pharma companies and privacy of patient records, including information shared over IM.

• FERC: Federal Energy Regulatory Commission requires the logging and auditing of transaction-related information, including IM.

• FCC: Federal Communications Commission requires extensive record keeping and storage requirements. Supervision and index of books and records is required.

• Corporate Communication Policy for IM: Instant messaging must be monitored and controlled in order to meet corporate compliance requirements for employee communications.

2.0 IM Manager Features and Benefits

2.1 Introduction

IM use in the enterprise has proliferated through grass roots adoption, devoid of the compliance and security considerations traditionally factored into the deployment of mission-critical enterprise communication tools. IMlogic IM Manager directly addresses these concerns by providing a centralized solution for management, security, and policy enforcement for IM usage.

2.2 Security

2.2.1 Threat Protection

• Automatic Security Updates from the IMlogic Threat Center: Receive automatic security updates for worms and SPAM lists from the IMlogic Threat Center.

• Predictive Threat Protection: Prevent zero-day attacks by using the IMlogic Real-Time Threat Protection System (RTTPS) to detect malicious content using heuristic and behavior-based monitoring to recognize and block potential IM threat outbreaks.

• URL Filtering and Redirection: Redirect the recipient of a URL to a web page that educates them on the risks of IM worms, and informs them of the reputation of the particular URL that they have received.
• **File Transfer Control:** Apply advanced file filtering controls to screen file transfers across multiple IM protocols, including support for restrictions based on file type and user location.

• **Virus Scanning for File Transfers:** Out-of-the-box integration with industry leading technologies from McAfee™, Sybari™ and Symantec™.

• **SPAM Watch:** Dynamically detect, identify and block spammers at the user, network and domain levels, combined with advanced detection and protection from the IMlogic Threat Center.

• **IM Client Version Control:** Prevent the usage of unauthorized versions of public IM clients that have not been patched or upgraded to address known security vulnerabilities.

2.2.2 **Authentication and Access control**

• **IM Screen Name Registration:** Require users to register their IM screen name with their corporate LDAP identity. Map real employee IDs and attributes to their IM screen names.

• **User Access Restrictions:** Selectively disable specific users or groups from accessing the IM networks.

• **Ethical Boundaries:** Create and extend boundaries to internal or external IM users to block unauthorized / inappropriate IM conversations.

• **Authentication Enforcement:** Enforce user authentication and authorization policies, including support for identifying and profiling users based on enterprise corporate directories.

• **Trusted Domain Communications:** Securely federate with external users and enterprise organizations for trusted domain communications.

• **Internal Network Routing:** Route internal IM communications within your network to preserve privacy and protect intellectual property.

2.2.3 **Usage control and Monitoring**

• **Content Filtering:** Filter messages for inappropriate content or sensitive information. Optionally block transmission of the message and/or notify responsible parties when it occurs.
• **Regular Expression Pattern Matching**: Leverage a complete regular expression pattern engine to create filtering and blocking strings, such as credit card or social security numbers.

• **IM Network Control**: Selectively disable access to specific public IM networks.

• **User, Group & Domain Management**: Manage single users, user groups or entire user domains, supported with a configurable, prioritized rules engine.

• **Identity Management & Screen Name Registration**: Provision IM user accounts, including support for single-user administration directly from the management console.

• **Real-Time Systems Management Dashboard**: Monitor and manage real-time services across the enterprise, including support for overall performance and availability of the solution.

### 2.3 Archiving and Regulatory Compliance

• **Inject Disclaimers into Conversations**: Require disclaimers to be appended to conversation threads. Administrator can configure message to disclose archiving and monitoring.

• **Archive 100% of IM Conversations**: Capture all IM messages across the multiple networks. Continue to allow and log messages even in the event of a database failure.

• **Web Based Search and Retrieval Interface**: Search, retrieve, and reconstruct IM conversations. Searching can be done by content, date, name, screen name, or LDAP attribute.

• **Configurable Access to Archives**: Restrict reviewers to access only particular data sets (such as legal, research, or investment banking) to enforce privacy or regulatory policies.

• **Index Conversations with Directory Data**: Ensure that IM conversations are appropriately indexed by department, title, cost center code, etc.

• **Audit Statistics and Compliance Reporting**: Append comments and mark messages as “reviewed” to ensure that your reviewers are satisfying compliance procedures. Demonstrate compliance with audit trail reporting.

• **Print or E-mail Compliance Reports and IM Conversations**: Use the web based reviewers’ UI to generate hardcopies, or emails containing IM conversations and audit statistics.
• **Export to 3rd Party Archives:** Export logged IM conversations to 3rd party archiving solutions, including Entelagent, iLumen, Iron Mountain, Symantec/VERITAS, IXOS, Legato, Persist, Zantaz, and others.

• **Globalized for Non-English Operating Environments:** Deploy in non-English operating environments, with full support for double-byte and mixed-byte encoding, and i18n standards.

### 2.4 Deployment and Scalability

• **Rapid Deployment & Automatic Configuration:** Deploy IM management without costly implementation or configuration barriers through IM Manager's Intelligent Installer, which automatically detects and configures IM Manager for initial installation and deployment.

• **End User Transparency:** Option to deploy IM Manager without involving the end user. Use IM Manager to detect inappropriate or irresponsible use of IM within your enterprise.

• **No Client Software or Configuration:** Deploy IM Manager without having to deploy any software or make any configuration changes on the client desktop.

• **Proven Fortune 1000 Performance & Scalability:** Deployed in the most demanding IT environments with the industry's most reliable, secure IM management system, architected for zero message loss and without a single point of failure.

• **LDAP Directory Synchronization, Performance & Scalability:** Synchronize with large, complex user directories, including custom object classes and attributes.

• **Extensible Architecture:** Support for IM application plug-ins, such as the IMlogic Broadcast Buddy that allows you to broadcast messages to groups of users on enterprise IM systems.
3.0 IMlogic IM Manager Architecture

3.1 IMlogic IM Manager Ecosystem

In a typical IMlogic IM Manager deployment there are several optional 3rd party components that can contribute to the overall solution:

1. **Multiple IM protocols:**
   a. **Public IM Clients:** Free IM clients, typically including AOL, MSN, Yahoo!, and ICQ
   b. **Enterprise IM systems:** Locally deployed IM solutions, including Microsoft Office Live Communications Server, IBM Sametime, and Jabber.

2. **IM “Cloud” Servers:** Servers that reside on the internet and relay public IM messages. Examples include: login.oscar.aol.com; messenger.hotmail.com, and scs.msg.yahoo.com.

3. **Anti Virus Scan Engines:** If IM Manager is configured to allow file transfers for one or more users, it can have the files scanned by a best-of-breed scan engine, such as Symantec, Sybari or McAfee.

4. **Email Archiving Solution:** If you own or are deploying an email archiving solution, IM Manager can export logged IM conversations as emails and push them to the archiving store. This allows you to consolidate storage on all electronic communication. For more information, see section 3.4 “Conversation Exports / Archiving” below.
5. Network Security Solutions: IMlogic provides its customers with prescriptive guidance and support with regards to hardening the IM environment. By properly configuring your firewall you can block rogue users and applications without investing in any additional technology. Additionally, many companies use web proxies and packet inspection devices that can assist in hardening the IM environment without requiring the IM solution to be in line with other protocols, such as HTTP, SMTP and FTP.

3.2 IMlogic IM Manager Product Architecture

3.2.1 Overview

IM Manager is a software proxy for securing, managing, and logging multiple instant messaging protocols. The IM Manager software is typically installed on a server behind one or more corporate firewalls. The only additional software that IM Manager requires is a database. The database is used to store meta data (such as policy definitions) and logged IM conversations.

3.2.2 Public IM

To control public IM protocols, simple port monitoring is not sufficient because many public IM clients will attempt to connect on multiple ports. However, public IM clients only seek to connect to a very short list of hosts, for example: login.oscar.aol.com and messenger.hotmail.com.

Because of this, the easiest and most thorough way to handle public IM messages is through DNS redirection:
A typical transaction:

1. A user signs onto a public IM client with their screen name and password. During the authentication, the client attempts to connect to the public relay.

2. The local DNS server has several zones for each of the public IM protocols that will forward this request directly to the IM Manager server rather than allowing the client to connect to the internet and directly access the public relay.

3. IM Manager ascertains who the user is through LDAP integration and registration. IM Manager then applies all applicable policies to the message (content filtering, virus scanning, etc…) and logs the message to the data repository.

4. IM Manager decides on an appropriate action:
   
   i. **Block the Message**: If the message contains a virus or contains content that triggers a block policy
   
   ii. **Route the Message Internally**: If this conversation is between two internal users, the conversation is routed internally without having to traverse the internet
   
   iii. **Route the Message Externally**: If the conversation is between an internal and external participant.

5. The corporate firewall is configured to block any rogue IM connections that are attempting to bypass the IM Manager server. Essentially, a firewall policy ensures that the only internal machine that can connect to login.oscar.aol.com, or any other public relay, is the IM Manager server.

This architecture has three key advantages:

1. It requires no client-side configuration changes or software installation.

2. It is not dependant on inspecting specific ports that a client might circumvent.

3. IM Manager is not managing IM conversations through deep packet inspection. So, it is not inline with other internet bound protocols, such as HTTP, SMTP, and FTP.
3.2.3 Enterprise IM

Because Enterprise IM (EIM) servers are deployed locally, DNS redirection is not required. Enterprise IM vendors, such as Microsoft, IBM, and Jabber all provide API integration with their messaging infrastructure. IMlogic has developed enterprise security and management agents that run on the enterprise messaging server and capture IM messages in-stream to apply policies after the message had been sent, but before it is relayed to the intended recipient.

A typical transaction:

1. An EIM user signs onto their client and sends a message to a contact.
2. The IMlogic IM Manager capture agent, running on the EIM server, intercepts the message.
3. The IM Manager server checks the identity of the sender and recipient against the corporate LDAP directory and applies any appropriate policies to the message.
4. IM Manager logs the message to the data repository.
5. IM Manager decides on an appropriate action:
   i. Block the Message: If the message contains a virus or contains content that triggers a block policy.
   ii. Allow the Message to Proceed: If the message passes all applicable policies.
2. Admin and Reporting User Interface (UI): Administrators and reviewers interact with IMlogic IM Manager through easy to use, web based user interfaces. IM Manager offers three distinct interfaces:

- **Administrator's UI**: Used to administer the product, run reports, configure policies, and manage users and groups.

- **Reviewer's UI**: Delegated to any individual who needs to review IM conversations. Typically this would include compliance officers, HR, and legal employees. Access can be restricted to allow a reviewer to only view conversations held by particular individuals. For example, a VP of sales might be able to review only conversations had by sales employees.

- **Person Archive UI**: When enabled, this UI can be delegated to allow every IM user to search IM conversations that they participated in. Participants can only view conversations they were involved with, and they can not modify any of the messages.

3. IMLogic Threat Center: IM Manager integrates with the IMlogic Threat Center for auto-updates of virus, worm, and SPAM definitions, and for connectivity to RTTPS. Using auto-updates, IM Manager will periodically call the IMlogic Threat Center to pull the latest list of virus definitions, worm signatures, and spam signatures to each local deployment. Additionally, RTTPS will receive high priority threat information from the global, RTTPS community and the IMlogic Threat Center. This threat information and worm signatures will be automatically sent to IM Manager to block any suspicious activity in your environment. Any malicious content signatures will be analyzed by the IMlogic Threat Center to validate and confirm the behavior is associated with a known or new outbreak. For more information on RTTPS and the IMlogic Threat Center, please see:


Additionally, the IMlogic Threat Center, when used with RTTPS, offers URL filtering and redirection for URLs sent over IM. Because the majority of threats sent over IM are initiated as URLs, it is essential to educate users on the risks of clicking on links received over IM. When a user receives a link, and clicks on it in the IM client, IM Manager is capable of redirecting them to a page on the IMLogic Threat Center that provides two important messages:
3.2.4 Additional Components

In addition to the scenarios above, several additional components make up the IMlogic IM Manager solution, including:

1. **Corporate LDAP / Active Directory Server:** IM Manager performs read-only operations from your corporate LDAP directory, and can work with any custom object class or attribute. This integration provides two key features:

   - **Accountability:** IM Manager registers a user’s screen names against his/her corporate profile. This allows IM Manager to log all conversations with the user’s actual name, rather than an anonymous IM screen name.

   - **Policy Enforcement:** By associating a user’s screen name to their LDAP user profile, IM Manager can look up a user’s group memberships and apply the appropriate policies for that user’s role. For example, a sales rep may be able to have external conversations, but file transfers are blocked, and a disclaimer is inserted into every conversations. However, an IT employee may not have external conversations, can use file transfers, and does not receive a legal disclaimer.
• Education on the risks inherent in clicking links in IM conversations: Many IM users are not aware of the risk involved with links in IM conversations. When a user receives a link, IMlogic IM Manager masks the URL to redirect them to a page that educates them on these risks.

• Reputation score of the particular URL that is received: After being redirected to the IMlogic Threat Center’s warning page, the IMlogic Threat Center will indicate the reputation of the particular URL that was received. If a user has received a link to a domain that has been known to host malware, then the reputation will be highlighted in red and indicated as “RISKY”. After reviewing the reputation of the link, the recipient can optionally navigate to the intended target.

3.2.5 Complete Picture

Below is a complete picture of an IM Manager deployment, including public IM clients and an enterprise IM system:
3.3 IMlogic IM Manager Message Capture

In a typical organization, for compliance and legal purposes, it is critical that 100% of IM Messages are captured. Likewise, the productivity gained by using IM as a communications protocol requires that IM is available at all times.

Because of these two concerns, IM Manager can not have a real-time dependency on the underlying database. On occasion database servers become unavailable, or perform slower while being utilized by other applications. In this scenario it is critical that IM Manager be capable of still allowing IM messages to be sent and received, without any performance impact, and while still applying policies. Similarly, it is critical that IM Manager be capable of archiving IM messages, regardless of the connectivity to the database server.

To accomplish this, IM Manager uses two techniques:

1. **Advanced User and Policy Caching:** IM Manager caches all user information and policy definitions from the database into local memory, and will continue to apply these policies regardless of connectivity to the database server. This cache is updated regularly to ensure that the most recent policy definitions are applied. Applying policies from local memory also enhances throughput of IM messages.

2. **Message Queuing:** In order to ensure message archiving, regardless of the connectivity to the database server, IMlogic IM Manager leverages a persistent, transactional message queue as a buffer to write to the database:
A typical transaction:

1. A user types an IM message into their client and hits “send”

2. IM Manager examines the message and applies all applicable policies. The message is then inserted into the message queue with its associated meta data.

3. If the message is not blocked due to a policy violation, it is then relayed to the intended recipient.

4. As soon as possible, a logging service then logs the message into the database for permanent retention. Under normal operating conditions this step is done in real-time. However, if the connection to the database server is limited for any reason, the logged message can reside in the message queue until the database server recovers. Upon recovery, IM Manager will push all queued messages into the database.

3.4 Conversation Exports / Archiving

IM Manager is capable of exporting all logged IM conversations to a third party archiving solution, such as Symantec/VERITAS, EMC Legato, Zantaz, AXS-One, HP-RISS and others. This allows organizations to consolidate the storage of all electronic communications into a single data store, and leverage a unified reviewer’s interface.

Because archiving solutions are typically optimized to store emails, IM Manager converts logged IM conversations into an STMP compliant format and then sends the message to a predefined journaling inbox:
A typical transaction:

1. An administrator defines an export task in the administrator’s UI, and schedules it to run at an appropriate time (typically once per night). Upon execution, IMlogic IM Manager polls its database and generates one XML file for each IM conversation that occurred since the last archive event. This XML file is put into a temporary directory on the server.

2. IM Manager then applies a custom XSLT transform to the XML messages to convert the XML documents into SMTP compliant messages. The XSLT transform is selected based upon the intended archiving solution.

3. The resulting SMTP message contains a transcript of an IM conversation and attributes about the participants. It is then dropped into a pickup directory to be sent to a predefined journaling inbox that will be archived by the archiving solution.

3.5 Antivirus Scans for File Transfers

IM Manager offers policies to control file transfers through IM clients. Administrators can control who is allowed to send files over IM, whether they can be sent externally, and what types of files can be transferred.

If file transfers are going to be allowed, IM Manager is capable of leveraging a best-of-breed antivirus scan engine to determine if the file is infected. This scan is performed on the IM Manager / AV server before the file is sent to the intended recipient’s desktop, adding an additional layer of virus protection. Supported anti virus vendors include:

1. Symantec: During file transfers, IM Manager can make an API level call to the Symantec scan engine to have the file scanned on the server. IM Manager simply requires the location of the Symantec installation, and the preferred port.
2. McAfee: IMlogic IM Manager can request a scan from the McAfee scan engine. Administrators simply indicate the location of the McAfee virus definition files (DAT).

3. Sybari: Sybari offers Antigen for Instant Messaging. This engine can be installed on the IM Manager server to provide complete file transfer antivirus scanning for public IM and Microsoft Office Live Communications Server.

3.6 High Availability

In a typical IM Manager deployment, high availability is configured through three key architectural techniques:

1. No Single Point of Failure: Architected with message queuing and advanced caching, IM Manager creates redundancy and system recovery from failure of any individual components. In a distributed environment, IT managers often do not control database infrastructure or messaging platforms. When these systems fail or connections are lost, IM Manager continues to manage IM traffic. If the database fails or becomes unavailable, IM Manager’s proxies continue to function completely. By locally caching the necessary security and identity services on each proxy component, users are not impacted if individual components or the database fails.

2. Zero Message Loss: Many regulated customers must archive all IM communications. Every IM Manager component has redundant and reliable logging — even in the event of database failure. As an IM message passes through IM Manager it is immediately captured in real-time and stored to a persistent, transactional message queue.

3. Load Balancing and Failover: IM Manager can be load balanced with existing IT infrastructure components, including TCP / IP session aware load balancers using DNS round robin. This redundant infrastructure ensures employees can continue to use IM even if an IM Manager server fails.
3.6.1 A sample 85,000 seat deployment

Below is a sample architecture from an IMlogic IM Manager 85,000 named-seat deployment which includes both public IM users and an enterprise IM system.

This deployment includes: Deployment of "Pass-Through" Relays to ensure that no inbound ports are required in the DMZ; "Partner-Relays" proxy consumer IM services for management, security, and compliance archiving; Enterprise IM Systems; Enterprise LDAP directories; and Web-Based Administration Tools.
4.0 Minimum Hardware Requirements

• 1.8GHz Pentium III
• 30GB Hard Drive
• 512 MB RAM

5.0 Minimum Software Requirements

Server Operating System

• Windows Server 2003
• Windows 2000 Server, Service Pack 4
• Red Hat Enterprise Server 3.0

Database Management System

• SQL Server 2000 SP3
• Oracle 9iR2 (9.2.0.4)
• MSDE (8.00.761 included)

6.0 Additional Requirements

• Microsoft Core Services XML 4.0 SP2
• Internet Information Services 5.0 or greater
• Internet Explorer 6.0