Message Inspector™

Version 4.3

Administrator's Guide

011-MAN-0066

Copyright and Trademarks Notice

The contents of this manual, the associated Message Inspector software, and other computer programs offered by Zix Corporation (hereinafter collectively called the "ZixCorp Materials") are the property of Zix Corporation and are copyrighted. Use of the ZixCorp Materials is governed by the license agreement accompanying the original media. Your right to copy the ZixCorp Materials and related documentation is limited by copyright law. Making copies, adaptations, or compilation works (except copies for archival purposes or as an essential step in the utilization of the program in conjunction with the equipment) without prior written authorization from ZixCorp is prohibited by law.

Copyright 2003 by Zix Corporation.

All Rights Reserved.

Protected Under U.S. Patent Laws.

The "Zix" marks, including ZixVPM, ZixVPM Server Manager, ZixIt, ZixMail, ZixMail.net, ZixWorks, ZixPort, ZixIt Signature, ZixCorp Worldwide Signature Server, ZixSignature Manager, ZixCertified Receipt, ZixAuditor, ZixMessage Center, ZixCorp SecureCenter, ZixSelect, ZixResearch Center, Internet Manager, Message Inspector, the Message Inspector logo, SmartBlock and SmartList are protected by trademark laws under U.S. and international law.

All other brand and product names are trademarks or registered trademarks of their respective holders.

Contacting Zix Corporation

Zix Corporation
2711 N. Haskell Avenue
Suite 2300, LB 36
Dallas, TX 75204-2960
Telephone: (214) 370-2000
Fax (Main): (214) 370-2070

Technical and Customer Support

Email: support@zixcorp.com

Web site: www.zixcorp.com

Disclaimer

Message Inspector's Offensive filter entries contain material that may be very offensive to some people. The offensive items and the categorization of offensive content provided by Message Inspector are not to be taken as exhaustive or definitive. Nor do they in any way represent the views of Zix Corp. or its employees. The material contained is not meant to be viewed or used in any way except in connection with the operation of the product. Zix Corp. disclaims responsibility for any other use made of the material.

U.S. Government Restricted Rights (Applicable to U.S. Users Only):

This software and documentation is provided with RESTRICTED RIGHTS. The use, duplication, or disclosure by the government is subject to restrictions as set forth in paragraph (c)(l)(ii) of the Rights in Technical Data Computer Software clause at DFARS 252.227-7013. The manufacturer of this software is Zix Corporation, 2711 N. Haskell Avenue, Suite 2300, LB 36, Dallas, TX 75204-2960, Telephone: (214) 370-2000, Fax: (214) 370-2070.

Revision Date: December 2003

zixcorp™

Contents

Chapter 1

Welcome to Zix Message Inspector 1
New Features 1
Updated Full Text Analysis (FTA) Engine 1
Retrained Spam Engine 2
Blacklists and Whitelists 2
Integrated installation of MI AntiVirus 2
Support for Microsoft Exchange 2
Support for Lotus Domino 2
Support for LDAP 2
Quarantine Server 2
Additional Features 3
How Message Inspector Works 3
The Challenges Inherent in Language Recognition 3
Ambiguity 4
Context 4
Scalability 4
Message Inspector's Technology: A Superior Approach 4
Applying the Technology to the Problem 4
Addressing Context 5
Addressing Ambiguity 5
Addressing Spam 6
Addressing Offensive Material 6
Moving Target 6
The Message Inspector Advantage 6
Accuracy 6
Flexibility 7
Scalability 7
Conventions in this Guide 7

Chapter 2

Installing Message Inspector 9
Planning 9
Memory and Performance 9
MI Server Minimum Requirements 10
Client Requirements 10
Placement 10
Preparing 12
Upgrading from Previous Versions of MI 13
Installing 13
Launching the Install Wizard 13
Installing Multiple Collectors 15

Installing MI Client Only 15
Enabling LDAP 15
INI and Configuration File Values 16
Updating and Reloading from LDAP on the System Screen17
Routing Mail to the MI/AV Server 18
For email from the Internet 18
Alternate method 18
For email to the Internet 19
Implementing SSL with MI 19
Installing the Certificate and Key 19
Copying the Files 19
Admin Server SSL Configuration 19
MI Collector SSL Configuration 20
Enabling SSL for the GUI 20
Using SSL 21
Installing Internal Email Monitoring 21
Preparing the Exchange Server 21
Installing MI's Exchange or Lotus Components 22
Lotus Domino 22
Microsoft Exchange 22
Installing MAPI 23
Verifying Exchange Monitoring 23
Troubleshooting the Installation 24
Contacting Technical Support 24

Chapter 3

Getting Started 25
Logging Into Message Inspector 25
Logging In Using the Administration Client 25
Logging In Through a Web Browser 26
Using the Interface 26
Understanding the Policy 27
Rule Components 28
Name 28
Rank 28
From 28
To 29
Shift 29
Conditions 29
Actions 29
Reportable 30
Continue 30

Understanding the Default Rules....31
System Page....32
Manage MI....33
Other MI Features....34
Using Adobe Acrobat Reader....34
Adobe Buttons....34
Adobe Help....35

Chapter 4

Creating a Custom Policy....37
Planning Your Policy....37
Attributes and Addresses....37
Creating a New Rule....39
Creating a Rule From Defaults....39
Creating a Rule With the Wizard....40
Modifying a Rule....41
Deleting a Rule....41
Saving a Rule....41
Creating Custom Rule Elements....42
Source and Destination....42
Configuring Attributes....42
Creating an Attribute....43
Domains....44
Users....44
Searching for Elements....45
Viewing Element Usage....45
Modifying an Attribute Element....45
Deleting an Attribute Element....45
Importing Attribute Elements....46
Configuring Shifts....46
Creating a Shift....47
Viewing the Usage of a Shift....48
Editing a Shift....48
Deleting a Shift....48
Configuring Conditions....48
Creating a Condition....49
Viewing the Usage of a Condition....51
Editing a Condition....51
Deleting a Condition....51
Configuring Filters....51
Creating a Filter....52
Modifying a Filter Name....52

Deleting a Filter 52
Configuring Actions 53
Creating a New Action 53
Viewing the Usage of an Action 54
Modifying an Action 54
Deleting an Action 55
Disclaimers 55
Creating a Disclaimer 55
Variables in Disclaimers 55
Modifying a Disclaimer 56
Deleting a Disclaimer 56

Chapter 5

Planning a Policy 57
Full Text Analysis 57
Customizing the FTA Engine 57
Training/Calibrating the System 57
Building Boolean Expressions 59
Constructing Entries 60
Editing Entries 62
Including Spam Management In Your Policy 63
Blocking or Tagging Spam 64
Modifying the Spam Engine 65
Spam Slider Guidelines 66
Monitoring and Controlling Offensive Content 66

Chapter 6

Blacklist/Whitelist Manager 69
Using the Personal Blacklist/Whitelist Manager 69
Directing Messages to the Blacklist/Whitelist Manager 69
Using the Address Management Screen 70
Spam Address Management 71
Adding New Entries Manually 71
Managing Global Blacklist/Whitelist Entries 72
Adding Addresses and Domains 72
Removing Addresses and Domains 72

Chapter 7

Quarantine Server 73
Enabling Reviewers 73
Using QS Reviewer 74
User Settings 75

Input Box 75
Message Information 76
Message Attachments 76
Message Disclaimer 76
Limbo Box 77
Output Box 77
Using QS Administrator 78
Adding Reviewers 78
Modifying Reviewers 79

Chapter 8

Managing Message Inspector 81
The Manage Menu 81
Policy 81
License Usage 81
MTA Configuration 81
System 82
Administration Server 83
Updating LDAP 84
MI Product Node 85
Blacklist/Whitelist Manager Options 86
System Logs 86
Admin Users 86
Stopping and Starting 86

Chapter 9

Reporting 89
Report Types 89
Selecting Reports 89
Message Detail 89
Virus Reports 90
Quarantine Reports 90
Attributes 90
Graphs 91
Creating a Graph 92
Statistics 92
Scheduling Text Reports 94
Editing Scheduled Reports 95

Appendix A

Troubleshooting 97
Uninstalling Older Cygwin Versions 97

Standard Cygwin Uninstall....97
Starting MI....97
Policy....98
Quarantine Server....98
Blacklist/Whitelist List....99
Preventing an HTTP Attack on the Admin Server....99

Appendix B

Importing Data....101
Importing Users....101
Importing Domains....102
Importing a File....102

Appendix C

Archiving and Restoring the MI Policy Database....103
Archiving....103
Restoring....103

Appendix D

Backing Up Your Windows 2000 Configuration....105
Saving a Copy of Your Original System Configuration....105

Appendix E

Microsoft Exchange....107
Installing MAPI....107
Outlook 97....107
Outlook 98....107
Outlook 2000....107
Troubleshooting....108
Unable to Locate DLL....108
The Information Store Could Not Be Opened (Case 1)....108
The Information Store Could Not Be Opened (Case 2)....109
Could Not Find Default Information Store....109
This information Service Is Not Installed on Your Computer....110
IMsgSTore::QueryInterface() returned 0x80004002....111
MAPILoginEx() returned 0x80040005....111
Could not get name of Exchange Server #1....112

Appendix F

File Types....113
Glossary....123

Index....137

Chapter 1
Welcome to Zix Message Inspector

Zix Message Inspector (MI) is an intelligent Internet Policy Management solution for email communications. With MI, an organization can stop the leakage of confidential information, reduce legal liability, block spam, and increase employee productivity and network performance. Using Full Text Analysis (FTA) via patented and patent-pending technologies, MI inspects the context of messages and takes appropriate action. MI is superior in three critical aspects of Internet Policy Management:

- Accuracy — MI's Full Text Analysis is measurably more effective than any other content inspection technology.
- Flexibility — MI uses a Policy-based approach, easily adapting to a wide variety of business needs.
- Scalability — MI can effectively operate in organizations with thousands of users with only a minimal impact.

MI's easy-to-use interface and customizable features let you create an electronic communications policy suited to your specific needs.

Read this chapter to understand MI's theory and components. See *Installing Message Inspector on page 9* for how to plan and set up the software. See *Getting Started* on *page 25* if you have already installed MI or are familiar with earlier versions.

New Features

Updated Full Text Analysis (FTA) Engine

MI goes beyond the conventional keyword approaches of address recognition and string matching by applying *Full Text Analysis (FTA),* a suite of technologies designed to use context and previous experiences to overcome ambiguity. FTA incorporates state-of-the-art techniques from computational linguistics, information retrieval, text mining, and lexicography to complement the content analysis step. It integrates all these techniques and technologies into a unified solution. Forming the core of the product are MI's three proprietary, patented, and patent-pending technologies: Automatic Collocation Identification, Automatic Statistics-based Spam

Detection, and Statistical Dynamic Ranking.

The new Full Text Analysis engine includes

- A pre-populated Confidential filter
- Configurable phrase matching and collocation
- Scanning for Social Security and credit card numbers

Retrained Spam Engine

MI's improved, heuristics-based spam engine makes it easy to adjust the engine's aggressiveness depending on your organization's needs. By default, the engine contains four times as many attributes, resulting in a 90 percent accuracy rate.

Blacklists and Whitelists

Administrators can maintain lists of sites that are Always or Never spam. MI goes further, enabling users to configure personal lists that allow or block sites specific to their interests and needs.

Integrated installation of MI AntiVirus

Two AntiVirus options are available with the MI trial version without separate installation. Users who choose either or both AV option can activate them permanently just by entering the license token.

Support for Microsoft Exchange

MI supports MS Exchange 5.5 without requiring an install on the Exchange server. One MI computer can monitor multiple Exchange servers in a domain.

Support for Lotus Domino

MI supports Lotus Domino version 5.0.10 and 5.0.11. One MI computer can monitor multiple Domino servers in a domain.

Support for LDAP

MI's dynamic integration with Lightweight Directory Access Protocol (LDAP) eliminates most manual user and group imports. Once configured, LDAP will update your MI parameters automatically on a regular schedule.

Quarantine Server

You can set up Quarantines from the Policy screen, and take a more detailed look at messages before acting on them.

Additional Features

- Distributed deployment available with multiple collectors.
- More complete reporting, with summary reports and detailed data readily accessible.
- Incorporates PostgreSQL, open source database software from the PostgreSQL Global Development Team
- Hierarchical administration with three levels of users.
- Configurable Rule continuation: more than one rule can apply to a message, and reports reflect all rules affected.
- Filtering on number of attachments or recipients.
- X-header tag option enables tagging source of message.

How Message Inspector Works

MI is an intelligent Internet Policy Management solution. The policy consists of a set of rules that contain conditions on various attributes of email. The policy states what happens when a scanned communication matches all the conditions of a rule. The rules are arranged in the policy according to priority, from highest to lowest.

Rules specify two kinds of actions: policy actions and notification actions. Policy actions modify the message itself. It may be blocked, passed, redirected, or tagged as spam. The notification actions generate reports and messages that record the details of the event, send a copy to another user, or notify the Administrator, sender, or message recipient.

Whenever MI detects a Mail communication, it triggers the highest priority rule that matches the conditions in the message. Once a communication has triggered a rule, it stops if it is not set to continue or keeps processing rules if it is set to continue.

The reports generated from MI's default policy create a clear picture of the traffic on your network, pinpointing potential problems such as bandwidth-consuming use of network resources, unauthorized or inadvertent transmission of confidential information, and potentially embarrassing or litigious transmission of offensive content.

The Challenges Inherent in Language Recognition

To understand the power behind MI's approach, you should first understand the difficulties involved in enabling a computer to accurately filter for content. Software faces three challenges in accurately analyzing messages: ambiguity, context, and scalability.

Ambiguity

Ambiguity means that words can have many different meanings which can only be resolved by understanding them in the context of the full message.

Fruit flies like a banana.

In the sentence above, *flies* can be either a noun or a verb, indicating either the aerodynamic qualities of fruit or the favorite food for *Drosophila melanogaster.* The reader must apply additional information to get the proper meaning, usually by reading the rest of the message for context or by drawing on past experience.

Context

Context refers to the meaning gained from the words surrounding the scanned text.

He was out in left field...when the ball drove down the 3rd base line.

He was out in left field...with that idea.

This metaphor literally refers to a position in baseball, though it usually means that the person referred to is just confused. Without making use of the context, no one could say what the message truly meant. Content cannot be understood without context.

Scalability

Conventional keyword searches tax the resources of any machine because they scan for each word in every message, reducing your ability to scan for content effectively. Even the most sophisticated system can slow down your network unless the software efficiently manages the challenge of constantly and consistently analyzing messages.

Message Inspector's Technology: A Superior Approach

The English language's high degree of ambiguity means that any system of language recognition based on string matching will produce a large number of false hits, making such a system highly unreliable. MI has a better approach.

MI starts with *content analysis.* This finely-tuned technique is based both on word frequency and the relative position of words within a sentence. Content analysis operates on the meaning of the messages rather than strings of characters or some secondary, potentially irrelevant, aspect of a message such as an email or IP address.

Applying the Technology to the Problem

MI's content identification relies on three key elements: the filtering engine, a set of filters, and a linguistic database. Together, these elements enable MI to evaluate a

new message with a high degree of accuracy to determine how closely it matches a particular filter.

MI contains predefined filters developed and maintained by the lexicographers at Zix Corp. The research and development process involves identifying, testing, and ranking the words and phrases based on the results of scientific testing and rigorous discussion of the findings.

The administrator has the ability to edit these filters and create new filters that pertain to the organization's specific needs. All filters reference the linguistic database. This unique capability enables MI to use the power of FTA, but keep the filter-creation interface simple and intuitive.

Addressing Context

The linguistic database recognizes language patterns and structures. It is trained on hundreds of thousands of messages and contains statistics and standard deviations on frequencies of words, probabilities of words co-occurring, and collocation characteristics (pairs of words with special meanings that occur together more often than statistically probable).

When MI's filtering engine determines the presence of the filter content in a new message, it compares the characteristics and statistics associated with the occurrence of the content in the message with the statistics of the same content in the linguistic database. As a result, MI assigns each "matching" message a relevance score that indicates the *extent* to which it matches the original filter criteria. Each filter includes a sensitivity value, and only those messages whose ranking is above that value are considered true matches. This statistical modeling proves highly accurate in identifying suspect content.

Addressing Ambiguity

MI addresses the problem of language ambiguity by identifying strong and weak matches between incoming messages and a filter. If a match between a filter and a message containing ambiguous words is weak, this indicates that the message does not contain the content you want to identify. If the match between them is strong, the message is likely to contain the content you want to identify. This is particularly relevant to preventing false hits and false positives.

Ambiguity issues are reduced if features of context and statistical probability can be taken into account. In order to identify offensive language, MI's technology uses a linguistic database that contains statistics about the word frequencies and collocations of plain language and about the word frequencies and collocations specifically characteristic of offensive language.

The statistics in this database provide the basis for making highly accurate judgements about the language in any particular new message.

The following sources are used:

- Print sources of slang and offensive language
- Text from Web sites containing offensive language

Addressing Spam

MI employs Automated Statistics-based Spam Detection that delivers extremely accurate lexical identification of spam based on statistical filters that identify the actual content of a message. Applied to all incoming email, this technique enables highly accurate identification based on the actual content of the message, as well as other attributes. Spam detection and prevention is reliable and requires virtually no administrative attention.

Addressing Offensive Material

One of the prominent risks of electronic communications is the risk of liability from the use of offensive and inappropriate language. To address this risk, MI uses a sophisticated process of offensive language recognition to determine if a particular message should be acted upon. Work done on offensive language recognition was performed by Zix Corp.'s staff of linguistics experts.

Moving Target

Spammers do not sit idle while we bring technology to bear. They find new ways of disguising their spam and trying to sneak it through mail systems.

MI includes spam-signature technology to keep pace with the ever-changing spam. As new spam enters the Internet, we identify the distinguishing characteristics of each. By default, MI updates

The Message Inspector Advantage

Accuracy

All filtering technologies must balance between two critical measures: *sensitivity* and *precisio*n. Sensitivity measures the avoidance of false negatives, messages that should be filtered. Precision measures the avoidance of false positives, messages that should not be filtered.

MI is measurably more accurate at every level of sensitivity and precision. MI's engine maximizes accurate detection and minimizes false positives. In test results, MI

shows roughly a 3% false hit/false positive rate. Other products that use keyword techniques generate much higher error rates, typically between 25% and 50%.

Flexibility

MI lets the system administrator control the sensitivity/precision balance by adjusting the sensitivity parameter of the filters. The sensitivity and precision performance of MI can be easily modified to suit the needs of a wide variety of organizations. For example, in environments where there are large amounts of email containing confidential information, MI can be precisely tuned to deliver a high level of sensitivity, effectively making sure that false negatives are minimized. As another example, an organization that wants to reduce large amounts of inappropriate email can tune MI to deliver a high level of precision, effectively ensuring the false positives are minimized.

Scalability

As the volume of electronic communications increases in an organization, and as an organization adds more end users, the requirements increase for:

- The number of filters that need to run concurrently
- The range of actions to employ upon discovery of suspect content
- The volume of traffic to manage

MI's Full Text Analysis can analyze language accurately with a minimal burden on the host system. MI uses thousands of categories, entries, and definitions, effectively creating an index for each message as it passes. MI's speed can be compared to the difference between reading a document for a specific word versus finding the word immediately from the index.

Conventions in this Guide

We use the following in this guide:

- **Bold type** indicates a choice, such as something you click or type
- *Italic* indicates a title or what you see on a screen
- This style of number on an illustration (1) indicates a step to follow

Chapter 2
Installing Message Inspector

This chapter provides the steps necessary to install MI in any configuration. To ensure a successful installation, plan the installation, prepare the MI computer, install the software, and then route the mail to the MI server.

In addition, MI can track and control internal Lotus Domino and Microsoft Exchange email. See "Installing Internal Email Monitoring" on page 21.

You can access MI through a standard Microsoft Internet Explorer or Netscape Navigator browser.

The Message Inspector CD or the compressed MI executable that you download from our Web site provides the necessary files to install the above components.

Important: *If you use the Quarantine Server or Blacklist/Whitelist Manager, install each of these on a separate computer from the MI Administration Server. Depending on your usage, these can be very compute intensive.*

Important: *MI 4.3 supports Lotus Domino versions 5.0.10 and 5.0.11 only.*

Planning

There are four steps to planning your installation:

1. Determine the projected number of monitored users, the number of messages per day and approximate attachment sizes to establish the minimum requirements.
2. Decide what components are you installing.
3. Select a computer to meet the minimum requirements.
4. Review your network. This includes knowing the mail server's Mail Exchanger (MX), Address (A) and Pointer (PTR) records. When you use our embedded Mail Transfer Agent (MTA,) you must change these after installing MI.

Memory and Performance

MI can operate on a server with 256 MB of RAM. However, we recommend at least 512 MB for best performance.

MI Server Minimum Requirements

- Single 800 MHz or faster processor. For high mail volume, at least a single 1 GHz processor. We recommend dual processors for enterprise environments. Contact our Technical Support for details.
- At least 512 megabytes (MB) of RAM for best performance; we recommend 1gigabytes (GB) or more and for high mail volume, 2 GB.
- 10 GB disk space. For high mail volume, heavy quarantine server usage or large amounts of detailed report data, we recommend at least 20 GB or 60 GB for best performance.
- Windows 2000 with Service Pack 2 or higher, and Internet Explorer 6 or above, Netscape 6 or above or Mozilla 1.4 or above browser.
- A static IP address.
- (Optional) A CD-ROM drive.
- (Optional) A network or local printer installed, if you want to print the installation worksheet.

Client Requirements

- Pentium 350 MHz or faster processor
- 256 MB of RAM
- Windows 95, 98, NT 4.0 Workstation or Server with Service Pack 3 or higher, Windows 2000 with Service Pack 2 or higher, and Internet Explorer 6 or higher, Netscape 6 or above or Mozilla 1.4 or higher browser.
- HTTP access to the MI Administration Server

Important: *For best display of management screens, use screen area settings of 1024X768 or above, and a color setting of 24 bit True Color or better. To change, go to* ***Control Panel > Display > Settings****.*

Placement

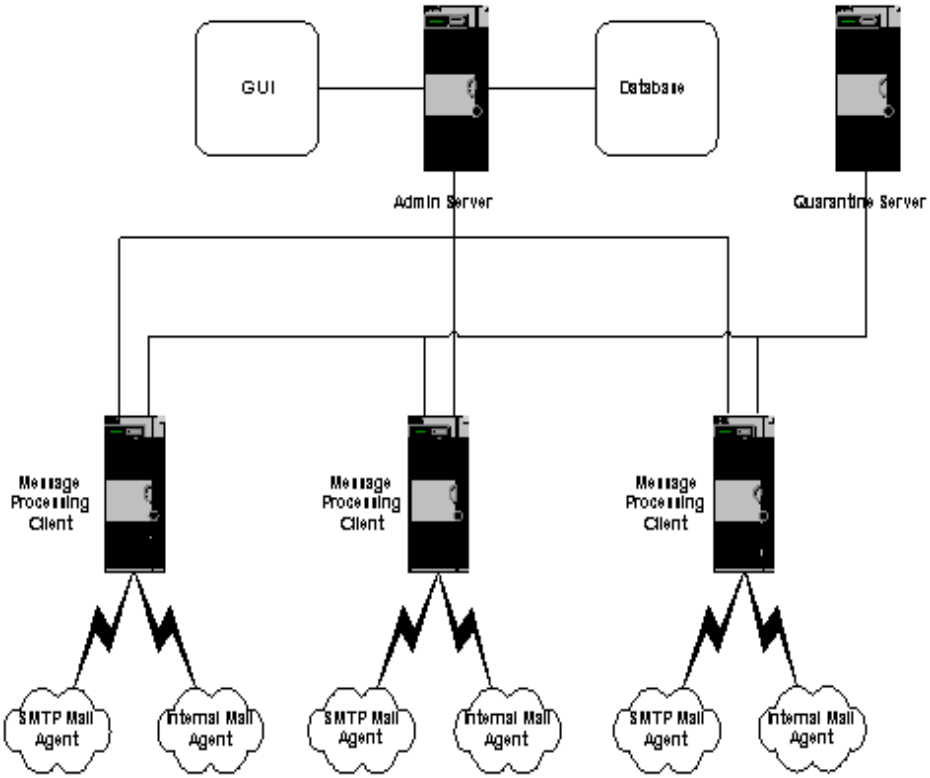
Message Inspector is made up of one or more installations, each handling email messages which are analyzed and processed according to a single distinct policy.

A complete MI system consists an Administration Server, a Sendmail Switch, one or more Filter Servers, and one or more clients. Optionally, you can add a Quarantine Server or Black/White Manager Server or both on separate computers.

- Install the Administration Server on a computer that can connect to the Filter Servers.
- Load the Administration Client on a computer that can connect to the Administration Server.

- Install Quarantine Server on any computer that can connect to the Filter Servers.
- Install the Filter Server, AntiVirus and Sendmail Switch (the MTA) with either Client or Server.
- Place the Blacklist/Whitelist Manager with either Client or Server.

Important: *We strongly recommend installing the Administration Server on a separate computer from any other MI components. This help insure best performance.*



The diagram shows secure network connections (SSL on TCP/IP), and the computers represent processes that may be running on different computer systems. These processes may be located together in a LAN or they may be geographically separate in a WAN. Message processing clients can all be deployed either on the same or on separate computers as desired. You can deploy the database separately, but not with secure communications between it and the Administration Server. One MTA and/or Filter Server can be present on each computer, which may also contain any combinations of the already mentioned servers.

Important: *Do not install MI on:*

- a computer already running Internet-related services or other large programs. Doing so might prevent proper installation and limit MI's effectiveness. The same network can use IPX and other protocols in addition to IP; this does not affect MI's operation.
- the same computer as the internal email server, if you will monitor internal email traffic with Lotus Domino or Microsoft Exchange. See "Troubleshooting the Installation" on page 24 and "Installing Internal Email Monitoring" on page 21.

Preparing

Before installing MI, be sure you have the necessary rights, user names and passwords.

- If you want to back up your current system configuration before you install MI, see "Backing Up Your Windows 2000 Configuration" on page 105.
- Check the computer against the minimum requirements listed on page 10.
- Before installation, verify that you have a DNS suffix defined and that the computer can resolve itself. To confirm this:
  - Be sure you are logged in as the local server Administrator.
  - Right-click **My Computer > Properties** or go to **Control Panel > System.**
  - Open **Network Identification > Properties> More > Primary DNS suffix of this computer.**
  - If the DNS suffix is correctly entered in the text field, click **Cancel** on each dialog to exit or
  - Fill in the correct DNS suffix.
- Confirm that no additional services are running on the MI computer. Uninstall or permanently disable network monitoring tools, Internet servers, communication programs, or other programs that affect processor or network card utilization.
- If you plan to enable Secure Socket Layer (SSL) with MI, be sure you have the necessary certificate and key. See "Implementing SSL with MI" on page 19.
- If you will monitor Microsoft Exchange mail, you must have MAPI on the MI server before you begin MI installation. For details, see "Microsoft Exchange" on page 107.

Upgrading from Previous Versions of MI

You can up install MI 4.3 on top of MI 4.2. See our support Web site for information about earlier versions. If you use MI 3.1.7, technical article #10617 describes which data you can convert and how to upgrade. See http://www.zixcorp.com/support/im_softwaresupport.php and visit the Message Inspector section.

Installing

Install all MI components using either the MI CD or the downloaded file. If you need to download the file, point your browser too:

http://www.zixcorp.com/compro/download_trials.php

Launching the Install Wizard

To install MI from the CD, insert it into the drive. The installation process starts automatically after a few seconds. If it does not, double-click **setup.exe** in the CD's root directory.

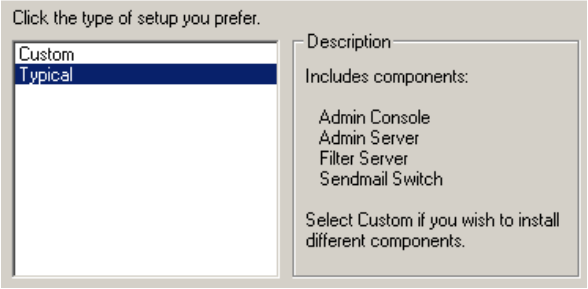
If you do not have the CD:

1. Download the self-extracting zipped archive that contains the MI files to a directory on the computer where you intend to install MI
2. Double-click the file.
3. When the unzip utility screen appears, click **OK**. The utility decompresses the software into the directory shown unless you change this.
4. Click **Unzip** to continue.
5. When the dialog tells you when the files have decompressed, click **OK**.

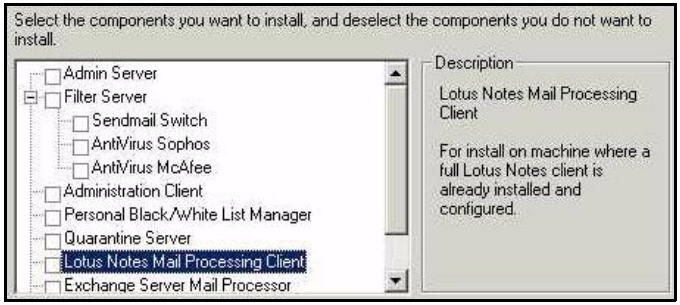
The installation program begins. It runs identically from downloaded files or CD.

1. Click **Next** on the welcome screen.
2. Read the License Agreement, then the Maintenance and Support Agreement. Click **Yes** at each and continue.

3. Choose setup type: for a standard installation on one computer, select *Typical*. To include Quarantine Server, Away Never Manager or other options from the menu of MI components, select *Custom*.



4. If you select *Typical,* click **Next**. If you select *Custom,* choose components and click **Next.**



Note: *In a custom installation, keep in mind that the Quarantine Server and the Personal Blacklist/Whitelist Manager software should each go on its own separate computer.*

Depending on which type of installation and which components you choose, you will receive prompts for server names, and IP and email addresses. For each, enter the information and click **Next** to continue. Prompts will include some or all of the SMTP server, quarantine server, and administrator email return address.

Note: *Answer a prompt for a server name with either the IP address of the computer or a fully qualified domain name.*

5. When prompted, click **Install.** The installation runs for several minutes.
6. At the opening screen of the PostgreSQL portion of the installation. Click **Next.**
7. Accept the licensing agreement and click **Next** again.

8. Click **Finish** at the end of the PostgreSQL installation to resume the main installation.
9. Enter the MTA configuration information at the prompt:
   - *SMTP Domain*: Type the domain name, for example, *mycompany.com*, for which MI will accept mail. Press **Enter** to finish.
   - *SMTP Server*: Enter the IP address of the mail server for which MI is to relay mail to after it filters it. Confirm the entries and press **Enter**. Repeat the process for any additional SMTP domains and SMTP servers.
   - *IP addresses*: Enter the IP address of any systems from which MI will accept relayed mail. If this includes an entire subnet, specify the entry with the common octets of that subnet and without the trailing dot. For example if the subnet is *192.168.1.1 - 192.168.1.254*, type '*192.168.1*' in the entry. Confirm the entry and press **Enter**. Repeat the process for any additional IP addresses or subnets.
10. Click **Finish** at the end of the installation and reboot.

Installing Multiple Collectors

To install more than one collector, restart the installation on each server. Choose **Custom** and check the *Filter Server* box. This includes the *Sendmail Switch*.

During the installation, when you enter the IP address of the Administration Server, MI will configure the collector properly to communicate with it.

Tip: *If you add many additional collectors, you may need to increase the power of the Administration Server. The additional reporting load can require extra processors, processor speed and RAM.*

Installing MI Client Only

1. Run setup and select *Administration Client*.
2. At the prompt, enter the IP address of the MI Admin Server.
3. Click **Finish** when installation is complete.

Enabling LDAP

If you are an LDAP user, enable LDAP after installation as follows:

1. Start Cygwin.
2. From its prompt screen, change to the MI directory. By default, this is “program files\message inspector”.

3. In the following shell script command, replace the first DC with your domain and the second with the .com portion. If you use a three-part domain such as test.appropriateuse.com, add an additional “DC=”.
4. Also change “cn=ldap” to show the valid user who has rights to the Active Directory server.
5. Then change the password to that valid user’s.
6. At the prompt, enter the script in the form:

   $ sh ./bin/ldap-config --host 190.168.1.55 --basedn cn=users,DC=appropriateuse,DC=com --binddn cn=ldap,cn=users,DC=appropriateuse,DC=com --password ldappw

7. Restart the MI admin server.

This script updates *admin.ini* with the options shown, and puts several records in the *CSystemObjectSub* table to activate the *Update from LDAP* and *Replace from LDAP* buttons on the MI System screen.

INI and Configuration File Values

If you will use LDAP imports, we strongly recommend that you change a line in the admin.ini file to allow importing of user with only email addresses and no other attributes. To do this:

1. Open *//Message Inspector/etc/admin.ini* in a text editor.
2. Find the line *#skip_nomail_users=0*
3. Remove the # comment marker and change the value to 1, so that the line reads: **skip_nomail_users=1**
4. Save the file.

You should not need to edit the *ldap-config* file. However, if you choose to open it in a text editor, you will see the following values in it:

usage="$0 [options]

--host host Hostname of LAP server

--file file Admin server config file. (default: $inifile, in current dir)

--port port LDAP port on server (default: $ldapport)

--basedn DN Base DN for queries

--binddn dn DN admin server can bind as. (optional; skip to use anonymous)

--password P Password admin server can bind with.

--print Print LDAP section of configuration file

Important: *If base DN not specified, assume anonymous binding. Specify '-' for host to disable LDAP.*

Updating and Reloading from LDAP on the System Screen

For more information on the System screen, see "Managing Message Inspector" on page 81.

Important: *Before updating, be sure the admin server and LDAP server systems clocks are in sync. For example, if the admin server is five minutes ahead of the LDAP server and you do the following in under five minutes:*

- *An update from LDAP on admin server GUI.*
- *A change in LDAP.*
- *Update from LDAP again.*

The admin server will not pick up the change. It remembers update times in the database, but according to its own clock.

1. Click **Manage >System**
2. Select the top node in the left frame if it is not already selected.
3. Scroll down in the right frame until you can see the *Update from LDAP* and *Replace from LDAP* buttons.
4. Click *Replace from LDAP.*

   This brings in users and groups as they exist in LDAP. MI will now use these as its users.

Important: *If you have changed or moved LDAP groups, use the* Replace from LDAP *button. This will delete existing users and groups, replacing them with the current ones in LDAP. The* Update from LDAP *button will bring over changes and is appropriate if you have added and deleted users from existing groups.*

5. To ensure that LDAP DNs appear in the *Policy* screen and wizards:
   - Cycle the *System* screen after making the updates
   - or click **Edit >Reload from Server** on the *Policy* screen

You are ready manage your organization's mail communications. The following chapters describe how to understand and create an electronic communications policy and to use MI's reports to intelligently monitor email traffic on your network. When you are ready to begin managing through IM, see "Getting Started" on page 25.

Routing Mail to the MI/AV Server

MI or MI/AV must process inbound and outbound email before the mail server(s) deliver it. The recommended choice of using MI's embedded requires changing DNS records (preferred) or switching IP addresses for incoming email and routing SMTP traffic to the MI server for outbound email.

For email from the Internet

The first method requires the following records to be added to the Primary DNS for the domain.

- An MX record of *lower* preference than that of the MX record for the existing, internal email (SMTP) server. The lower preference MX record is used to represent the MI system.
- An A record and the appropriate PTR record.

After installing MI and creating an MX record of lower preference, this method ensures that SMTP servers on the Internet route email to MI. After MI processes the incoming email in accordance with the policies defined, MI forwards email to the existing SMTP server for delivery to the appropriate recipients.

Note that until the Time-to-Live (TTL) value expires, SMTP servers on the Internet continue to route email to the existing SMTP server. Once the TTL value has passed, all email is routed to the MI system.

Alternate method

The second method requires switching IP addresses between the MI system and the existing SMTP server. In addition, the following records should be added to the Primary DNS for the domain.

- An MX record of *higher* preference than the existing MX record. The higher preference MX record is used to represent the existing SMTP server.
- An A record and the appropriate PTR record.

After you switch the IP addresses and install MI, SMTP servers on the Internet immediately route all email to MI, regardless of the TTL value.

Note: *The ability to assign MI the IP address previously specified on the SMTP server may be prohibited by the existing SMTP server having services requiring the IP address in question. While you switch IP addresses and until MI has been installed, it is highly probable that you will not receive email from the Internet.*

For email to the Internet

There is only one method to allow MI to filter email going *to* the Internet. You must configure the existing SMTP server to forward email to the MI system. For assistance in configuring common mail servers such as MS Exchange or Lotus Notes, visit our Technical Support web site at http://www.internetmanager.com**.**

Implementing SSL with MI

You can enable Secure Socket Layer (SSL) with MI at any time after installation. The following instructions cover configuring MI once you have the necessary certificate.

Important: *You must install a digital certificate and private key pair from a trusted Certificate Authority (CA), such as Entrust, Thawte, or VeriSign, before you configure MI for SSL. This certificate must include the common name of the MI admin server. For help in creating your certificate, contact your chosen CA.*

Installing the Certificate and Key

After you receive your certificate and key from the CA to enable SSL:

1. Copy them to the certificates subdirectory.
2. Modify configuration files on the MI admin server and collector.
3. Import the files onto MI client(s) computers.
4. Modify each client's MI properties.im file.

Copying the Files

On the MI admin server and on each MI collector, copy the certificate and key files to the */certificates* subdirectory under MI's root installation directory.

On the client(s), copy the key file to the home directory of the computer. In Windows 2000, this is *C:\Documents and Settings*.

Admin Server SSL Configuration

On the admin server, in the MI install root, open in the *//Message Inspector/etc/admin.ini* file in an ASCII editor.

1. Under [im_admin], modify the value for enabling SSL. Set:

   security=SSL

2. Under [SSL], modify the values for keypath and certpath to point to the location of the key and certificates. Set:

keypath=./certificates/testkey.key

certpath=./certificates/testcert.pem

where testkey.key and testcert.pem are your key and certificate file names.

3. Save the file and exit the editor.

MI Collector SSL Configuration

On each collector, in the MI install root, open the *config.ini* file in an ASCII editor.

1. Uncomment (remove the #) from the following lines:

   AdminServerUseSSL = true

   AdminServerCACertPath = ./certificates/CACert.pem

   AdminServerCommonName = networkaddress.domain.com

2. Modify the *AdminServerCACertPath* to be the location of the CA certificate
3. Set the *AdminServerCommonName* to the name of the admin server.

Important: *This must be the same name as in the certificate. For example, the common name will appear at the top of the certificate in the form "CN=networkaddress.zixcorp.com".*

4. Save the file and exit the editor.

Enabling SSL for the GUI

Likewise, you need to make the certificate available on each computer that will access MI through the management console. This uses a utility provided in the Java package installed with the client software. You then edit the *properties.im* file.

Important: *Close the GUI when making changes to* properties.im.

1. After you have copy your certificate into your home directory, locate *keytool.exe*. This is in the *bin* subdirectory under the JavaSoft\JRE*version* directory.
2. Use this utility to import your key into a Java format. The following example uses Windows paths. Use the import command in the form:

   keytool -import -trustcacerts -alias mykey -file "c:\documents and settings\administrator\cacert.pem" -keystore "c:\documents and settings\administrator\trustStore" -storepass mycode

Note: *By default, no trustStore reference appears. The MI client software looks for the trustStore file under the home directory. You can specify any path, alias name or password.*

Note: *Entering* keytool *without any arguments displays the available commands. Detailed documentation is available from Sun Microsystems at http://java.sun.com.*

3. From the home directory, open the *properties.im* file in an ASCII editor.
4. Modify the SSL line to read:

   use.ssl=true
5. Modify the trustStore line to equal the path and name of the certificate.
6. Save the file and exit the editor.

Using SSL

Restart the admin server. Now when you load the management console, you will be able to connect by SSL.

Installing Internal Email Monitoring

MI can track and control internal email on Microsoft Exchange or Lotus Domino servers. To do so, you must run the separate setup from the subdirectory *InternalMail,* located in the directory in which you placed MI setup.

Before you run the setup, be sure that:

- MI has installed successfully by confirming that it is monitoring mail.
- your system meets Domino or Exchange requirements.

Note: *For details on installing MAPI and troubleshooting an Exchange installation,* see "Microsoft Exchange" on page 107.

Preparing the Exchange Server

Before you install the MI Exchange component, set up your Exchange 2000 Server. To do this:

1. Log onto the Exchange server as a Domain Administrator.
2. In the *Active Directory Users and Computers* tool, add a user, *miadmin*.
3. Right click **miadmin**, choose **Properties**, and on the *Member of* tab, make this user a member of *Domain Admins* and *Exchange Domain Servers*.
4. Remove *miadmin* from the *Domain users* group.
5. Open the *Exchange System Manager.*
6. In the left tree, right click on your Exchange Server and choose **Properties**.

7. On the *Security* tab, verify that both *Domain Admins* and *Exchange Domain Servers* have full access (check each box in the left column).
8. In the left tree, under *Servers* expand the *First Storage Group*.
9. Right click on **Mailbox Store** and choose **Properties.**
10. On the *Security* tab, add *miadmin* as a user, and verify that it has full rights.

Installing MI's Exchange or Lotus Components

1. Run MI setup as above beginning with "Installing" on page 13.

Important: *If you are including the Exchange component, log onto the MI server with the* miadmin *domain account.*

2. Choose *Custom* setup type.
3. In *Select Components*, check the boxes for Lotus or Exchange options (**Lotus Notes Mail Processing Client** and **Lotus Notes Server Extmgr**, or **Exchange Server Mail Processor**).

Important: *Be sure that all the other MI components you want to install are checked as well.*

Lotus Domino

1. Setup looks for the Domino client. If it does not detect it, exit, install the Domino client, and restart setup.
2. Enter the hostname of the Domino server. Click **Next**.

3. Enter the associated password. Click **Next**.
4. A maintenance screen appears when the process is complete. Click **Finish.**

Microsoft Exchange

1. The Internal Mail setup verifies that MAPI is installed and loads its file.
2. When prompted, enter **miadmin** and the password. Then click **Next**.

3. In the next screen, enter the hostname of the Exchange server. Then click **Next**.
4. When prompted for the user, enter **miadmin** again.
5. Continue with the MI installation.

Installing MAPI

You cannot install MI's Exchange component without MAPI on the server. If the installation prompts you to install MAPI, you can do so by installing Microsoft Outlook (not Outlook Express).

- Outlook 97 - Use Typical install or Custom with Microsoft Exchange Service Support selected.
- Outlook 98 - Use Minimal, Standard, or Full installation. On the E-mail Service Options screen, select Corporate or Workgroup.
- Outlook 2000 - Use any installation.

1. After the install, start Outlook to finish configuring MAPI.
2. At E-mail Service Options select Corporate or Workgroup.
3. Select Microsoft Exchange Server information service.
4. After completing the configuration, start Outlook.
5. At the prompt, make Outlook your default mail manager.
6. Start the installation of MI's Exchange component.

Verifying Exchange Monitoring

After MI installation and rebooting, you can verify the Exchange monitoring. Do this on the MI server in its *Services*. To do this:

1. In the *Control Panel*, *Administrative Tools*, open *Services*.
2. Right click on the *IM Exchange Mail Processor Client* service and select **Properties**.
3. On the *Log On* tab, inspect the *Log on as:* section to verify that it is **miadmin**.

You can also verify that the Exchange server account and name are correct in the *mpexchange.ini* file. You will find this in the *\\Program Files\Message Inspector\etc* folder.

MI identifies the Exchange Server by its NetBIOS name. If the server is *EXCH1*, for example, the entry for the account in the file might be *imadmin@EXCH1*.

When you check this entry, also verify that there are no trailing spaces after the name of the server.

Finally, you can view the *mpexchange.log* file in *\\Program Files\Message Inspector\var\log* folder. This should show a successful connection to each mailbox.

Troubleshooting the Installation

Complications may arise during or after your installation if your dedicated MI server does not meet the listed requirements (see "MI Server Minimum Requirements" on page 10).

- If the CPU is not fast enough or the computer does not have enough RAM, traffic monitoring and blocking will be sporadic and the browser component may fail when running reports.
- If the MI Server does not have at least 150MB of free disk space for the software, the installation will fail before finishing.
- If the MI Server does not have up to 150MB additional free disk space for database storage, either the operating system or MI (or both) will stop when the hard drive runs out of space.
- If *MS Exchange Server Name and Mailbox* dialog remains on the screen, check behind it on the desktop for a *utils.h* error message. This Microsoft message indicates the wizard could not find the MAPI server. Verify that the MI server is on the same network segment as the MAPI server and in the same domain. Then reinstall MI.

Contacting Technical Support

We strongly suggest that all MI administrators thoroughly read "Creating a Custom Policy" on page 37. For the most current technical notes, visit our Web support site at:

http://www.zixcorp.com/support

You can reach our technical support team Monday through Friday, 8 a.m. to 6 p.m., Eastern U.S. Time, at:

(888) 283-8725

To email a question to the support team, use the following address:

MIsupport@zixcorp.com

Chapter 3
Getting Started

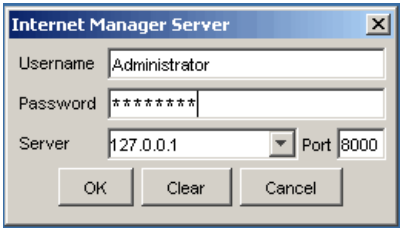
This chapter introduces MI's interface by walking through its basic functions. The default rules begin collecting data as soon as the software starts. The report data provide guidelines for customizing a policy for your organization's specific needs.

Logging Into Message Inspector

You can connect to the MI interface through a standard Web browser or the Administration Client. We recommended using the Administration Client, but if you have not installed the client on a particular workstation, any Web browser will work. See "Client Requirements" on page 10.

Logging In Using the Administration Client

The MI server includes a client for accessing the GUI. You can use this or a browser as described in the next section.



1. Double-click the **Administration Client** icon on your desktop.
2. Log in using the Administrator login and password for the computer on which you installed the Administration Server.
3. Enter the IP address for the Message Inspector computer and the port number it uses. If Message Inspector is on the computer you are connecting from, the loopback address of 127.0.0.1, or *localhost*, will also work. The default for the installation is port 8000.

Important: *The username and the password are case sensitive.*

Logging In Through a Web Browser

On the MI server or from a remote computer without MI, you can log into the admin server through a Web browser.

1. In the **Address** or **Location** field, enter the IP address or name of the computer on which you installed MI, a colon immediately after the address, and the port number, typically 8000.

   for example: `http://localhost:8000`

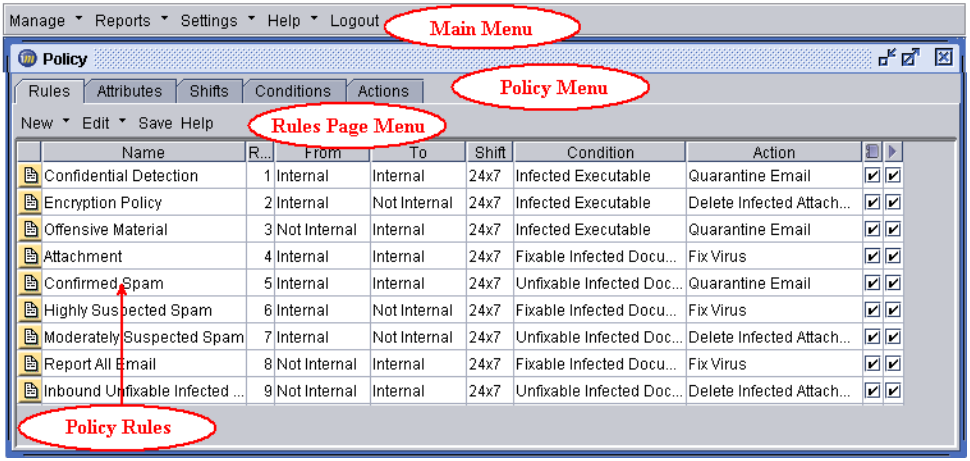
2. Click **Please Click Here to Login.**

3. In the **User Name and Password** dialog boxes, the Administrator login and password for the computer on which you installed MI. The username and the password are case sensitive.

4. Click **OK**.

Using the Interface

The policy displays all the *Rules* currently in effect and lets you create new ones. (Rules are sets of conditions that specify what will happen to a message that meets those conditions: see Rule Components on page 28.) If the *Policy* page does not open when you log in for the first time, click **Manage/Policy on** the main menu to display the **Rules** tab. MI contains default rules which you can use from the beginning, modify to suit your needs, or augment with new rules that meet your particular requirements.



Understanding the Policy

When MI examines a message, it passes that message through the rules in rank order, from top to bottom. Each rule states a set of conditions and specifies what will happen to a message that meets these conditions. The message triggers the highest ranked rule that matches the conditions in the message. Then the action from the matching rule, and that rule only, runs on the message.

In the example above:

The first rule, *Confidential Detection*, takes any message that contains information that matches the Confidential filter, makes a note of it in the database, and passes it through to its destination. The third rule, *Offensive Material*, performs the same action on traffic that matches the Offensive filter. Because the rules are accessed in order, an offensive and confidential message triggers the first rule and is categorized in the reports as confidential. However, if you select **Continue**, the message will trigger every rule it matches. See "Rule Components" on page 28.

Placed in the proper order, the rules combine to effectively enforce your organization's Acceptable Usage Policy. MI refers to this collection of rules as the Message Inspector Policy.

Rule Components

Each rule is composed of a set of parameters that you can select directly from the rule screen or create in a policy tab. Essentially, these parameters break down the conditions that trigger the rule and the action to be taken on the message. The parameters that make up a rule are described below.

Rules | Attributes | Shifts | Conditions | Actions

New Edit Save Help

	Name	...	From	To	Shift	Condition	Action		
	Report All Email	1	Everyone	Everyone	24x7	All Messages	Pass	☑	☑
	Infected Executable	2	Everyone	Everyone	24x7	Infected Executable	Delete Infected Attachment	☑	☐
	Fixable Infected Document	3	Everyone	Everyone	24x7	Fixable Infected Document	Fix Virus	☑	☐
	Unfixable Infected Document	4	Everyone	Everyone	24x7	Unfixable Infected Document	Delete Infected Attachment	☑	☐
	Confidential Detection	5	Everyone	Everyone	24x7	Confidential	Pass	☑	☑
	Encryption Policy	6	Everyone	Everyone	24x7	Encrypted	Pass	☑	☑
	Offensive Material	7	Everyone	Everyone	24x7	Extreme Offensive	Pass	☑	☑
	Attachment	8	Everyone	Everyone	24x7	Known Attachment	Pass	☑	☑
	Never Spam	9	Not Internal	Internal	24x7	Never Spam	Pass	☑	☐
	Always Spam	10	Not Internal	Internal	24x7	Always Spam	Pass	☑	☐
	Known Spam	11	Not Internal	Internal	24x7	Known Spam	Pass	☑	☐
	Highly Suspected Spam	12	Not Internal	Internal	24x7	Highly Suspected Spam	Pass	☑	☐
	Moderately Suspected Spam	13	Not Internal	Internal	24x7	Moderately Suspected Spam	Pass	☑	☐
	Spam Expressions	14	Not Internal	Internal	24x7	Spam Expressions	Pass	☑	☐

Name

The Name parameter contains the name of the rule. A good rule name should be straightforward and easy to remember, like *Trade Secrets*.

Rank

The Rank parameter shows the priority of the rule. The rules are arranged in the policy according to priority rank, the highest ranking rule (1) at the top, the lowest ranking rule (7) at the bottom.

From

The *From* (source) parameter matches the email address or domain in the rule to the address of the person sending the message.

This source parameter uses *Attributes* to identify the range of users to monitor. The default attribute *Everyone* matches any message from any source. You can create new attributes for more specific rules. For details, see "Configuring Attributes" on page 42.

To

The *To* (destination) parameter matches the email address or domain in the rule to the address of the person receiving the message.

The Destination parameter uses *Attributes* to identify the range of users to monitor. The default attribute *Everyone* matches any message to any address. You can create new attributes for more specific rules.For details, see"Configuring Attributes" on page 42.

Note: *MI tags messages that have been analyzed by at least one rule, so that they will not be re-examined. To ensure this, keep at least one default rule set to* From Everyone *and* To Everyone*, which will analyze all messages.*

Shift

The Shift parameter sets the hours in which the rule operates. For a rule to apply to a message, the message must be processed by MI during the shift selected in the rule.

MI ships with a number of pre-defined shifts. All the default rules use the shift ***24x7***, which runs 24 hours a day, 7 days a week. You can create new shifts for more specific rules. For more, see "Configuring Shifts" on page 46.

Conditions

The Conditions field sets the parameters required to trigger the rule, such as

- File name, type, and content
- Size of message
- Size of attachment
- Number of attachments
- Recipients

For example, you can create a condition called *Financial Data* set to detect spreadsheets over 500K in size that match the confidential filter. The pre-defined conditions cover offensive material, encrypted data, spam, and other basics.

You can create new conditions for more specific rules. For details on creating conditions, see "Configuring Conditions" on page 48.

Actions

The *Actions* field decides how MI directs or reports a message that matches the rule parameters. Each Action can comprise notification actions and policy actions. These include:

- **Block —** Prevent the delivery of the message.

- **Bounce —** Return the message to the sender or redirects it to a specified address. This should include a notification.
- **Delete Attachment —** Removes one or more attachments and delivers the rest of the email.
- **Delete Infected Attachment —** Removes virus-infected attachment(s).
- **Fix Virus —** Repairs attachment(s) with a virus and includes the *Fixed Virus* message.
- **Pass —** Delivers the email.
- **Pass and Alert —** Delivers the email and notifies an address, by default the administrator.
- **Pass and Notify Confidential Alert —** Delivers the email and notifies an address, by default the administrator, that the email has violated the *Confidential* rule and what MI did with email.
- **Pass and Notify Sender —** Delivers the email, but notifies the sender, by default the disclaimer warns that the email violates company policy.
- **Pass and Outgoing Disclaimer —** Delivers the email with the notice that it is intended only for the addressed recipient(s).
- **Quarantine Email —** Sends the email the quarantine server for further evaluation.
- **Spam Tag —** Delivers the email with a header notice that it is *Suspected SPAM*.
- **Delete** — Prevent the message from reaching the recipient.
- **Deliver** — Allow the message through.
- **Quarantine** — Send the message to the Quarantine Server for further review.
- **X-Header**— Add a custom *x header* to a message, to allow blocking or delivery of a message regardless of its spam-like characteristics, without an indicator visible to users

Reportable

Selecting **Reportable** directs MI to place a report on this rule in the database

Continue

If you select **Continue**, MI will go on reviewing email for rule matches after the first match is triggered. If you do not, the review ends with the first match.

Important: *Use care when choosing* Continue*. If a message triggers rules with contradictory actions, MI generates two or more conflicting reports.*

Understanding the Default Rules

MI automatically begins processing the email communications on your network as soon as the installation process is complete. It scans and processes all incoming mail with a valid email domain regardless of the license count. Mail is blocked only when a user outside of your defined access list attempts to use the mail server as a relay.

The default policy contains basic rules designed to track and categorize your traffic and also to demonstrate how MI operates. Review these reports to help you determine how to customize your policy.

We recommend that you use MI in conjunction with a clearly stated acceptable usage policy concerning electronic communications on your organization's network.

Note: *When presenting this default policy and discussing policies anywhere in the product literature, We do not advocate nor advise use of any particular policy. This responsibility rests solely with the user of the software. The rules and policies that appear are intended for illustrative purposes only.*

None of the rules that install with MI are set to control traffic. Every rule is set to allow messages through and track them in the database. In selected order, the rules detect confidential information (defined by the user), encrypted files, offensive material, email attachments, spam or other junk mail, and place all other email under *Report All Email.*

- **Confidential Information —** To make this rule effective, you must create several confidential entries specific to your needs and add them to the filter.
- **Encryption Policy** — MI can detect and alert you to several types of encrypted files. The *Encryption* condition specifies the files detected.
- **Offensive Material** — Detects messages with potentially offensive sexual, abusive, or other highly inappropriate material
- **Email Attachments** — Detects file types commonly attached to email messages. The fact that there is a rule for email attachments does not mean that other rules ignore email attachments.
- **Never Spam** — Use this rule to catch mail you do not want tagged as spam before the spam engine examines it.
- **Always Spam** — The spam rules use three pre-defined filters to identify spam and tag targeted email messages before they go to the intended recipient. *Always Spam* identifies confirmed spam addresses and domains loaded in the MI database by default, or by administrators. The others are:
- **Highly Suspected Spam**

- **Moderately Suspected Spam**
- **Report All Email** — This rule detects every email message no matter what the content or file type. It is meant to detect and report any message not detected by one of the other rules. Keep this at the lowest priority.

The following default rules are available during the MI trial, and remain active if you purchase MI AntiVirus:

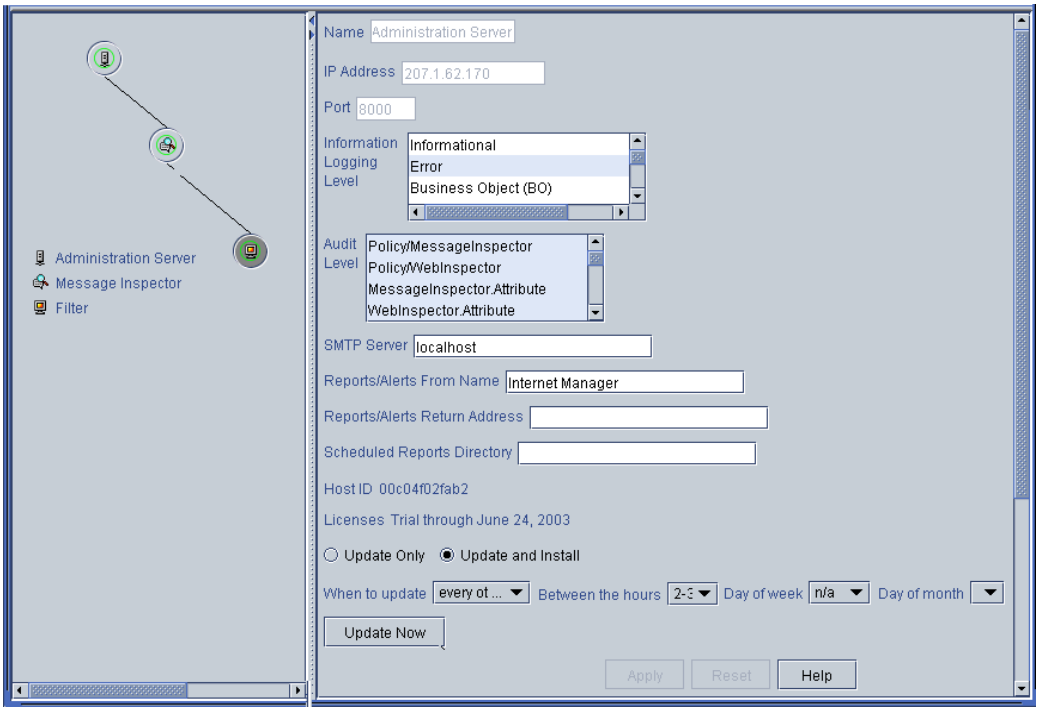
- **Internal Infected Executable** — Quarantines infected .exe files already within the organization
- **Outbound Infected Executable** — Deletes infected .exe files leaving the organization
- **Inbound Infected Executable** — Quarantines infected .exe files entering the system.
- **Internal Fixable Infected Document—** Applies Fix Virus action
- **Internal Unfixable Infected Document**— Quarantines document for later action
- **Outbound Fixable Infected Document** — Applies Fix Virus action
- **Outbound Unfixable Infected Document** — Deletes the attachment
- **Inbound Fixable Infected Document** — Applies Fix Virus action
- **Inbound Unfixable Infected Document** — Deletes the attachment

System Page

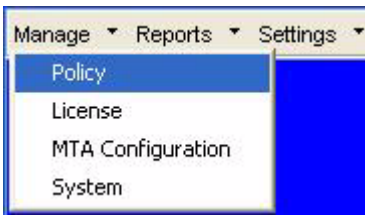
The *System* page, comprising three screens, lets you view and manage configuration parameters for MI administration and operations.

- To access the Administration Server's settings, click the top node icon in the left frame.
- To access MI settings, click the middle node icon.
- To cycle the MI Filter service without leaving the GUI, click the bottom node.

Click on a node to open the screen for the respective level. You can perform most configuration tasks on the right side of the System page: see “Managing Message Inspector” on page 81.



Manage MI



Manage in the main menu is a gateway to a variety of administrative processes.

Use it to:

1. Load or return to the Policy screen.
2. Enter your license keys and keep track of token usage.
3. Manage configuration files without having to log into text files
4. Open the System Administration screens

For details on these tools, see “Managing Message Inspector” on page 81.

Other MI Features

Open the following from the Windows **Start > Programs** menu:

- *Blacklist/Whitelist Manager,* available from the *Custom* setup type in installation, is a personal blacklist/whitelist for individual users. See "Blacklist/Whitelist Manager" on page 69.
- *Quarantine Server (QS),* available from the *Custom* setup type in installation, allows you to take a more detailed look at messages before acting on them. You set up quarantines on the policy screen, act on them from the QS *Reviewer* window and (with appropriate permissions), manage QS from its *Administrator* window. See "Quarantine Server" on page 73.
- *Anti-Virus (AV)* installs with the filter server. It runs scheduled daily scans and scans on boot-up by default. The Anti-Virus GUI is available from the Start menu, and you can customize the AV configuration there to suit your needs.

Using Adobe Acrobat Reader

You can install the free Acrobat Reader from the WI CDs or get the program from the Adobe site at http://www.adobe.com/products/acrobat/readstep.html. Either method will install the Reader and its Web-browser plug-in. Earlier versions may not work with our manuals and other PDF files.

After you install Acrobat, downloading a PDF file will load it in your browser. You can also save a PDF file and open it in the Reader.

Adobe Buttons

Probably the most useful buttons are the binoculars. Click on the left one to search the file for a string. Click the right one to search again for the same string.
Note: *In the browser, use the binoculars instead of the Find function or Ctrl-F. Also the F3 key does not repeat a search in the browser plug-in as it does in the Reader or full product.*

In the Windows convention, click the disk to save the file, or click the printer to send the file to your default printer. If the disk is gray, you can save the file from the browser File menu.

Click to view the file (left to right) full size, fit entirely in window, or fit width in window.

Click the hand to grab a file larger than the window and move it around to view it.

If the hand looks tattooed move your cursor to scroll up or down on the page.

If it displays an index finger you have hit a hot link. Click to go to the word or page under the hand. In many PDF files, the table of contents and index entries and pages are hot, as are many underlined or colored words.

Hold the cursor on the T button to choose between three options (left to right), select text, select a column, or select graphics. Then place the cursor where you want to select something to copy.

After you make a selection, you can click on the icon to the right to copy it to the Windows clipboard.
Note: *The icon to the left displays or hides the navigation panel. This panel may or may not contain navigation links. Whoever made the PDF file determined this. If it has links, click on one to jump to it.*

Hold the cursor on the magnifying glass to choose the plus glass (enlarge) or minus glass (reduce) the file view. Then click on the page.

At the top or bottom of the page, click to go (left to right) to the first page, to the previous page, to the next page, to the last page, and the two arrows on the far right to retrace your steps through the file.

At the bottom of each page, use the arrows to change the file size and move from one page to another. You can also click in either box, type a number and the press Enter to change either.

Note: *You can also use the full version of Adobe Acrobat to view and print our PDFs.*

Adobe Help

The Reader and the full Acrobat have extensive online help — in PDF, of course. Use their Help menus to access this. The plug-in does not offer help except for mouse-over displays on its buttons.

Chapter 4
Creating a Custom Policy

This chapter discusses planning issues to consider and information to gather before starting to construct your electronic-communications policy, followed by a step-by-step description of the procedures for creating components and rules.

Planning Your Policy

Before creating your policy, consider what kinds of rules you need to implement it. The following sections present some considerations and guidelines.

Attributes and Addresses

List the users, companies, and departmental divisions to monitor. Group similar elements together and give the group a name. For example, several competing companies can be put together in an attribute called *Competitors*.

List the most appropriate address for each member of the attribute. For companies, select a domain address like *ourcompany.com*. For a subnet within a company, write down the IP address range. Finally, for individual users who are being referred to independently of any subnet or domain to which they belong, note the user's email address.

Shifts

Examine the pre-defined shifts that come with MI to determine whether there are any shifts you need to create. For each shift you want to create, write down the hours of the day and the days of the week that the shift is to be in effect.

Conditions

After reviewing the pre-defined conditions, decide on what changes to make to: message or attachment size, message content, file type, number of attachments, recipients, or name restrictions.

Filters

Examine MI's pre-defined s and entries and determine whether they can accomplish the task you have in mind. If not, make a list of the filters and entries you need to create to detect your organization-specific content.

Actions

Review the pre-defined actions to determine whether there are any new actions to create. For each action, decide whether to delete the message, deliver it, redirect it, tag it as spam, or supply an x-header. Add one or more notification actions to declare how that message is copied, reported, or stored.

*Disclaimers*s

Your acceptable usage policy may recommend the addition of a disclaimer to incoming or outgoing email. The *Disclaimer* tab lets you review, edit or add disclaimer text. Apply disclaimers with the *Tag* action.

Rules

Sketch out the rules you need in your policy by noting:

- Source and destination attributes necessary to provide relevant address information
- Times during which the rule will be in effect
- The conditions required to trigger the action, including any filters needed
- Policy and notification actions that should result when the rule is triggered

Start by sketching out the general rules of your policy. After you have done this, examine each rule to determine any necessary exceptions. Sketch out rules for these exceptions.

Finally, arrange these rules into a policy by

- Placing the more important rules higher than less important rules and
- Placing general rules lower than the exceptions to the general rules.

Creating a New Rule

The quickest method to create a new rule is to use the default rule components. Although MI's default policy includes a number of pre-defined rules and rule components, you will likely need to modify these rules or create new rules to suit the specific needs of your company. For details on customizing specific rule elements, see "Modifying an Attribute Element" on page 45.

Most rule components can be created or modified in two ways: 1) through the relevant page accessible from the *Policy* menu and, 2) during the creation or modification of a rule. The following sections describe the procedures for configuring rule components through the relevant pages. Creation and modification of rule components during rule configuration is usually very similar. In the description of rule configuration procedures in the Rule Configuration section, we will describe both on-the-fly creation and modification of rule components only when the procedures are different. Otherwise, refer to the relevant description in the component configuration section.

Rules | Attributes | Shifts | Conditions | Actions

New ▾ Edit ▾ Save Help

Name	...	From	To	Shift	Condition	Action		
Report All Email	1	Everyone	Everyone	Never	All Messages	Pass	☑	☑
Infected Executable	2	Everyone	Everyone	24x7	Infected Executable	Delete Infected Attachment	☑	☐
Fixable Infected Document	3	Everyone	Everyone	24x7	Fixable Infected Document	Fix Virus	☑	☐
Unfixable Infected Document	4	Everyone	Everyone	24x7	Unfixable Infected Document	Delete Infected Attachment	☑	☐
Confidential Detection	5	Everyone	Everyone	24x7	Confidential	Pass	☑	☑
Encryption Policy	6	Everyone	Everyone	24x7	Encrypted	Pass	☑	☑
Offensive Material	7	Everyone	Everyone	24x7	Extreme Offensive	Pass	☑	☑
Attachment	8	Everyone	Everyone	24x7	Known Attachment	Pass	☑	☑
Never Spam	9	Not Internal	Internal	24x7	Never Spam	Pass	☑	☐
Always Spam	10	Not Internal	Internal	24x7	Always Spam	Pass	☑	☐
Known Spam	11	Not Internal	Internal	24x7	Known Spam	Pass	☑	☐
Highly Suspected Spam	12	Not Internal	Internal	24x7	Highly Suspected Spam	Pass	☑	☐
Moderately Suspected Spam	13	Not Internal	Internal	24x7	Moderately Suspected Spam	Pass	☑	☐
Spam Expressions	14	Not Internal	Internal	24x7	Spam Expressions	Pass	☑	☐

Creating a Rule From Defaults

1. Click **Manage > Policy** from the main menu.to open the *Rules* tab.
2. Select **New > Rule From Defaults.**
3. Enter a descriptive name for the rule. For example, *Internal Infected Executable.*
4. Click on each of the new rule's fields in turn to select an existing rule component from a drop-down menu. Create negative attributes for *From* and *To* on the fly by selecting **Not** on the pop-up dialog. For example, to define an external source quickly, select **Not**, and **Internal** from the drop-down list.
5. Click **Save** on the menu bar to save the new rule.

Note: *If you cannot open a drop-down menu, drag on the edge of a dialog box to enlarge it. The menu should now open.*

Creating a Rule With the Wizard

The Rule Wizard steps you through creating a new rule. Each rule element that can be customized has a link, both in the software and in this manual, to the section on how to configure that element. To prevent confusion, review the default rule elements before creating a new one.

1. Click **Manage** > **Policy** from the main menu.to open the *Rules* tab.
2. Select **New** > **Rule From Wizard**
3. Enter a descriptive name for the rule in the *Name* field. Give the rule a name that makes it easy to remember its function. For example, *Block Confidential Info***.**
4. Using the slide bar, enter a priority rank. By default, new rules are assigned the highest rank of 1. Adjust this as necessary.

Note: *The default rule,* Report All Email*, is the lowest ranking rule. Because it is designed to catch any email not picked up by the other rules, email rules ranked below it will never be used. Give your new rule a rank higher than* Report All Email.

5. Click **Continue** if you want MI to continue checking the message against other rules. Be aware that the same message can trigger rules with contradictory actions, and that you receive a report for each action. See "Rule Components" on page 28.
6. Click **Reporting** (recommended) if you expect to generate reports concerning this rule. Click **Next.**
7. Select **From** and **To** using the attributes in the drop-down menu. The LDAP domain appears if applicable, and if LDAP is running. If the attribute you need does not appear in the list of available options, click **Modify** and follow the procedures described under "Configuring Attributes" on page 42. Create negative attributes on the fly, based on existing attributes, by selecting **Not**. For example, to define an external source quickly, select **Not**, and **Internal** from the attributes menu.
8. Select the times you would like the rule to be in effect, then click **Next**. Typically, leave the shift at the default of *24x7*.

   If the shift you need does not appear in the list of available shifts, select an existing shift and click **Modify** to edit it, or click **Create** to make a new one. Follow the procedures described under "Viewing the Usage of a Shift" on page 48.Click **Next**.

9. Select the name or names of conditions for the rule to match from the drop-down menu.

   If the name you need does not appear in the list, select an existing condition and click **Modify** to edit it, or **Create** to make a new one. Follow the procedures described under "Configuring Filters" on page 51. Click **Next**.

10. From the list of available actions, select the action that contains the combination of policy and notification actions for the rule to take on any message that matches the previous parameters.

    If the action you need does not appear in the available list, select an existing action and click **Modify**, or **Create** to make a new one. Follow the procedures described under "Creating a New Action" on page 53.

11. Click **Apply.**

Modifying a Rule

Changing an existing rule is as simple as selecting the field you want to modify Double-click a rule's *Name* field or single click any of the other fields. You can edit the *Name* and *Rank* fields directly.

The *From* and *To* fields provide popup dialogs for changes. The *Shift*, *Condition*, and *Action* fields have pull-down menus. On the right, the *Log for reporting* and *Continue* columns have check boxes to toggle their states.

After you change an existing rule, the icon to the left of the rule shows that the rule has unsaved changes. Click **Save** on the menu bar to finish modifying a rule.

Deleting a Rule

Click the icon on the left of the rule you want to delete and select **Mark for Removal**. When you see the scissors icon displayed, select **Save** on the menu bar. The marked rule is now deleted from the policy. Repeat these actions to delete other rules.

To cancel the Delete action, again click on the icon to the left of the message before saving your work and select **Undo Mark for Removal**.

Saving a Rule

Click **Save** to keep the new rule settings. Then to display the current policy, click **Edit** and choose **Reload from Server**.

Creating Custom Rule Elements

The default rule elements cover the most common options. Because each organization is unique, however, you can also choose to design and add your own rule elements.

Source and Destination

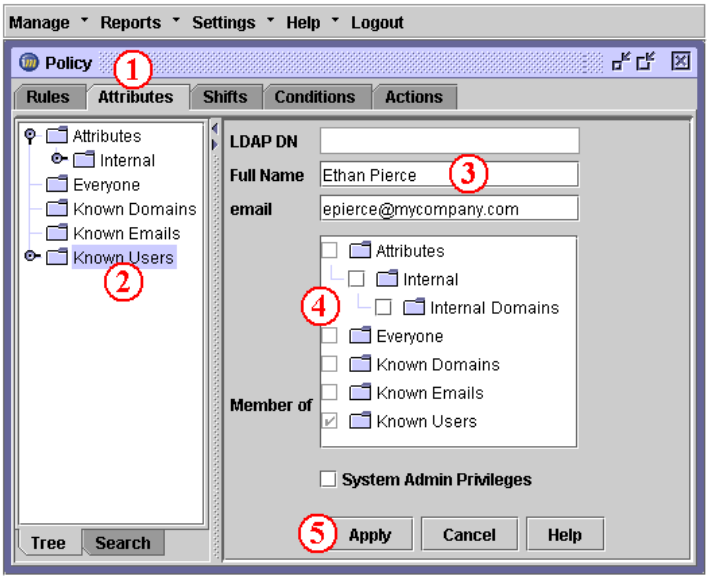
Click the rule elements **From** (source) and **To** (destination) to view the attributes drop-down menu. Make changes to the options on the *Attributes* page, and use **Not** to create negatives of existing attributes.

Configuring Attributes

Attributes are collections of domains or users that make it possible to treat a number of addresses as a single entity. The primary purpose of an attribute is to organize and supply domains, and user email addresses to the source and destination rule components.

Put custom attributes you create in the *Attributes* folder at the top of the tree. The default attributes are:

- *Everyone* — This attribute detects every email message. You cannot delete or modify it.
- *Known Domains* — Populate this attribute with Domains you wish to monitor.
- *Known Emails* — Define messages from known sources you wish to monitor.
- *Known IP Ranges* — Add specific IP address ranges for MI to monitor.
- *Known Users* — Populate this attribute with users to monitor. MI provides one user, *Message Inspector Administrator*, based on your installation data.



Creating an Attribute

First determine which attribute type you need, then do the following:

1. Click **Manage** > **Policy**, then the **Attributes** tab at the top of the Policy window.
2. Right-click *Known Domains, Known Emails* or *Known Users* and select **Add Domain**, **Email** or **User**.
3. In the *Name* field, enter a descriptive name for the new attribute.
4. Review the membership list. The default associations are already checked. If you have created other attributes and want to associate the new one with any of them, check the box next to it.

   Optional: For administrative users, click **System Admin Privileges**, then**:**

   - Add a user name
   - Check off the user's access authority: to policy, reports, or system.
   - If the user has reporting authority, select appropriate reports.
5. Click **Apply**. The new attribute appears on the tree under the appropriate folder.

Note: *LDAP users should add users and domains in LDAP. Non-LDAP users can import large numbers of users from an external file. For steps,* see "Importing Attribute Elements" on page 46.

Domains

The email domain is the part of an address that follows the @ sign: *ourcompany.com* in *jjohnson@ourcompany.com*. The source and destination parameters of a rule may use domain addresses as conditions that must be met to trigger the rule. Domain addresses are useful when you want to cover all the email addresses of a single company. In the future, you can add competitors to the group without changing the finished rule.

Users

When MI detects traffic to or from email addresses that match those in *Known Domains*, it adds these addresses to the *Users* attribute.

In the MI interface:

- You can place users in an attribute to provide a definition for source and destination parameters.
- The source or destination address of a message must be a member of *Known Users*.
- You can assign usernames and passwords to users who administer MI.

Important: *In MI's default configuration, you use the Administrator account to log in the first time. Afterwards, you can assign administrative rights to other user and log in with their names and passwords.*

Provide a name and email address for the administrator on the System page (see"System" on page 82). This "Postmaster" receives MI's automatic alert messages. If you create a rule that sends a notification to an outside source, the administrator's name and address will be seen outside your company.

Linux Administrative Users

If you are using the MI Linux version, you can add administrative users with a script that we supply. This brings over the username and password hash.

To use this script:

1. Create the user with the Administrative Console
2. In a Linux shell window, run the following commands, substituting the appropriate user and password:

   cd /usr/local/im

   ./bin/impasswd -a -u new-admin-username -p new-password

Searching for Elements

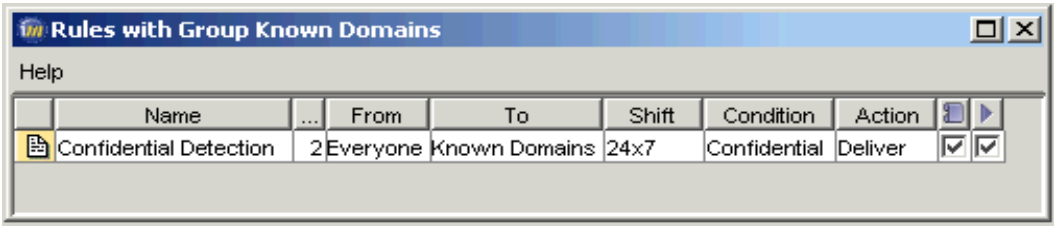
To search a large list of attribute elements:

1. Click on the **Attributes** tab under the main menu, then the **Search** tab in the lower left window.
2. Choose the attribute type you wish to search.
3. Select a search type, then enter a search string in the box.
4. Choose the number of returns to show, and click **Go**.

   For example, to search for the user Michael Grant, choose **User**, choose **Contains** or **Starts With**, type **Michael** in the box, accept the default of 100 returns.

Viewing Element Usage

Before modifying a User or Domain, you may want to see what attributes use that element. To view the usage of a attribute element, right-click its icon on the left of the *Tree* tab and click **Show Usage**. The right pane lists all its attributes.



A pop-up window displays rules using the selected element.

Modifying an Attribute Element

1. Click on the *Known Domain*, *Email* or *Users* folder.
2. From the available list, click the item you want to change.
3. Click the field you want to modify and type in the desired changes.
4. Click **Apply**.

Deleting an Attribute Element

1. Open the folder of User or Domain you want to delete.
2. Right-click the element an select **Delete from System**.
3. Click **Yes** at the prompt.

Importing Attribute Elements

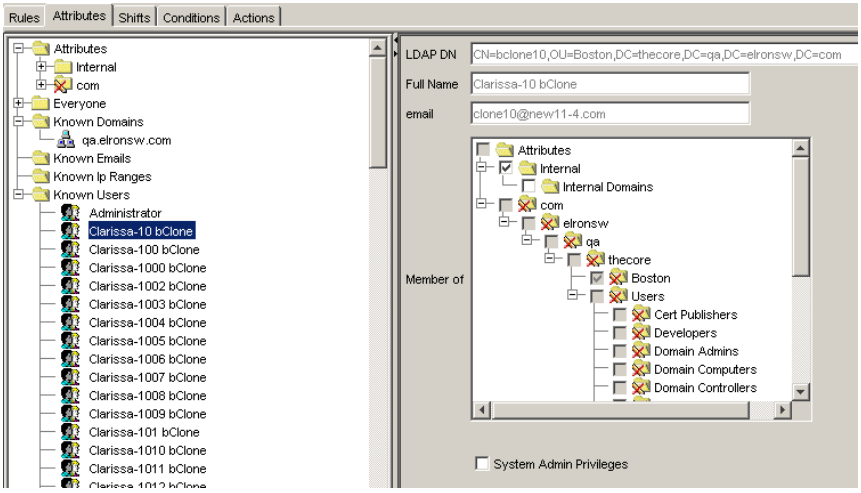
1. Attributes with LDAP

- If you have LDAP installed, users and domains import from LDAP with each update. When LDAP is running, the read-only LDAP DN displays in the right panel of the *Attributes* window. The tree below has clear boxes for attributes you can choose and gray ones for those you cannot. The LDAP groups have red checks over them, indicating that they are set you LDAP and you cannot change them.

Note: *The* LDAP DN *field appears only for users imported from LDAP.*

- You can add Groups, then add LDAP users to them.
  - Select the user or users you want to place in a group
  - Check the new group in *Member of* in the right panel.

2. Attributes Without LDAP



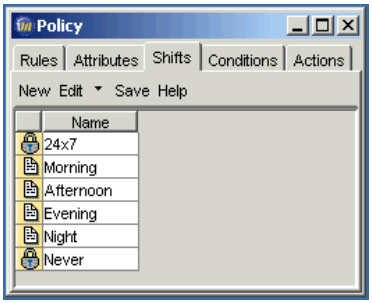
If you do not have LDAP, you can add attributes one at a time on the Attributes screen. When large numbers of users or domains are involved, you should import them from a file. For details, see “Importing Data” on page 101.

Configuring Shifts

A shift determines the hours of the day and the days of the week that a rule will be in effect. For example, the pre-defined shift “Morning” specifies the time between 06:01 and 12:00, seven days a week.

A rule contains only one shift. If you need a particular rule to operate during more than one shift, create an identical rule and assign it a different shift.

You define a shift once, and then can use it any number of rules. You cannot modify the shift *24x7*, which provides for 24 hour operation 7 days a week, or the shift *Never*, which disables a policy without deleting it. You can modify the other shifts as m shift necessary to suit your needs, or create and use custom shifts.



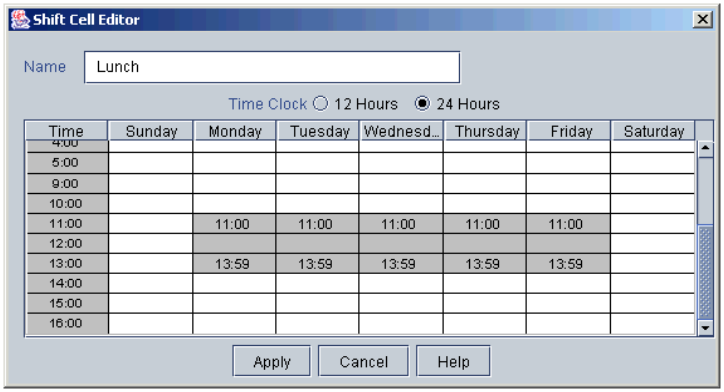
Creating a Shift

To define a shift from defaults when creating a rule, do the following:

1. Click the **Shifts** tab under the main menu.
2. Click **New**.
3. Type a descriptive name for the new shift in the *Name* field.
4. Choose a day and click the *Start Time* field of the new shift. Right-click the field to change the starting minute. You can also drag to carry the same time period over several days.

Note: *Keep the default 24-hour notation: For example, type 23:00 indicates 11 p.m.*

5. Click the *End Time* field of the new shift. Right-click the field to change the ending minute.
6. Click **Apply**.



Viewing the Usage of a Shift

Before modifying or deleting a shift, you may want to see what rules use that shift. To view the usage of a shift, click the icon to its left and select **Show Usage**.

Editing a Shift

On the *Shifts* page, click the field you want to modify. The change mode for that field activates. Procedures are the same as "Creating a Shift" .

Deleting a Shift

1. Click the icon to the left of the shift you want to delete and select **Mark for Removal**.

Note: *To cancel the Delete action, again click on the icon to the left of the shift and select* ***Undo Mark for Removal****. You cannot delete the* 24X7 *or* Never *shifts.*

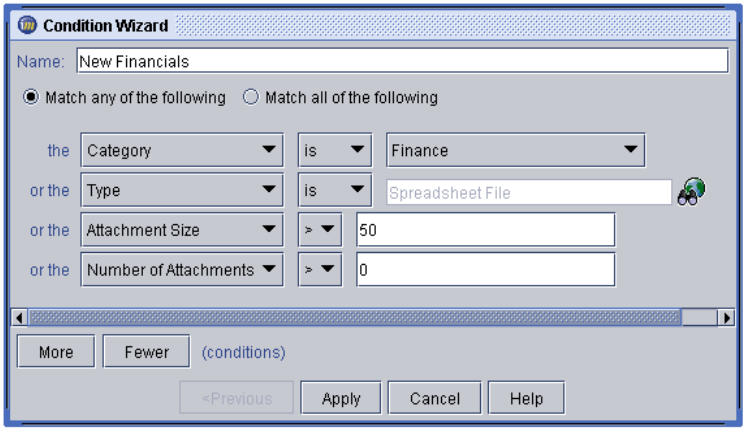
2. When you see the scissors icon displayed, select **Save** on the menu bar. The marked shift is now deleted from the policy. Repeat to delete other shifts.

Configuring Conditions

The *Condition* field sets the file name, size, type, and content required to trigger the rule. For example, you can create a condition called *Financial Data* set to detect spreadsheets over 500K in size that match the confidential filter.

Pre-defined Conditions include:

- All Documents
- All Messages
- Confidential
- Confirmed Spam
- Encrypted
- Executables
- Extreme Offensive
- Fixable Infected Document
- Fixable Virus
- Graphics and Multimedia
- Has Attachments
- Highly Suspected Spam
- Infected Executable
- Known Attachment
- Moderately Suspected Spam
- Offensive
- Unfixable Infected Document
- Unfixable Virus
- Unknown



MI also comes with a complete set of pre-defined categories and parameters that allow you to define a wide variety of conditions.

Creating a Condition

Create and manage conditions and entries on the Conditions page.

To access the Conditions page:

1. Click the **Conditions** tab.
2. Click **New** to open the Wizard.
3. Enter a descriptive name for the new condition in the *Name* box.
4. If all elements must be true to trigger the rule, keep the default, **Match all of the following**. If any single element should trigger the rule, select **Match any of the following**.
5. Select one of the following in the first frame:

- *Category* — Select one of the existing filters from the right-hand drop-down list, or any custom filters you have created. If the filter contains sub-filters, you may choose a lower level. For example, selecting **Extreme** under the *Offensive* filter will check for extremely offensive words only.

- *Type* — Select a file or message type from the menu. The examples and explanations below are a minimal list. The full list of files types supported is in "File Types" on page 113.

Archive File	Compressed files (ZIP, LZH, or TAR)
Database File	Database files (Access, Dbase, Paradox)
Email/News Body Text	Body of Email messages in text format
Executable File	Programs (EXE or DLL)
Graphics File	Pictures (BMP, JPG, or GIF)
Multimedia File	Sounds and movies (MP3 or WAV) **Note:***MI recognizes these files only by extension.*
Password Protected File	Password protected UUENCODE, WinZip, GZIP, or tar archive file. Note: MI treats archived files that are not password protected just like any other file.
PGP Encrypted Email	Email messages encrypted using the PGP protocol
Presentation File	Presentation and slide shows (PPT, PRE, PR4)
Application/no longer convertible	
S/MIME Signed Email	Email messages signed using the S/MIME protocol
Spreadsheet File	Spreadsheets (XLS, 123, Quattro)
Unsupported Format	Messages not covered by the other file types
Word Processor/Text File	Word Processor and text (MS Word, Word Perfect, HTML)

- *Attachment Name* — Enter a keyword to search for in the message. For example, enter **Offer** to track a message with that word in the subject, or **Offer*** for any combination such as "offering" or "offers".
- *Message Size* — Enter the size of message to trigger the rule, in kilobytes.
- *Attachment Size* — Enter the size of the attachment that triggers the rule, in kilobytes.
- *Number of Attachments* — Choose greater than, less than, or equals (>, <, =) and enter a number.

- *Number of Recipients* — Choose greater than, less than, or equals (>, <, =) and enter a number.

6. To add an additional element to the condition, click **More**. Click **Fewer** to eliminate an element.
7. Click **Apply**.

Viewing the Usage of a Condition

Before modifying or deleting a condition, you may want to see what rules use that condition. To view the usage of a condition, click the icon to its left and select **Show Usage**.

Editing a Condition

On the *Conditions* page, click the field you want to modify. The Conditions Cell Editor screen appears. The procedure is the same as that shown under "Creating a Condition" on page 49.

Deleting a Condition

1. Click the icon to the left of the condition you want to delete and select **Mark for Removal**.

Note: *To cancel the Delete action, again click on the icon to the left of the condition and select* ***Undo Mark for Removal****.*

2. When you see the scissors icon displayed, select **Save** on the menu bar. The marked condition is now deleted from the policy. Repeat these actions to delete other conditions.

Important: *You can modify, but not delete, default conditions except for* All Messages, *which is locked.*

Configuring Filters

A filter specifies the type of content a rule is designed to identify, such as *sports* or *offensive langua*ge. Filters consist of entries that contain the keywords MI's filtering engine uses to scan messages. A filter may also include sub-filters. For instance, the *Confidential* filter contains the sub-filters *Code Names* and *Finance*. The sub-filter *Code Names* contains entries like *restricted* and *do not forward this email*.

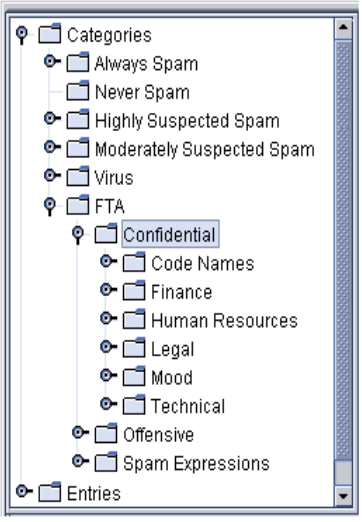
Entries provide the words MI uses to classify the message content. Generally, several entries are needed to cover a particular filter. The filter groups those entries together, either as individual words or words used in combination.

MI provides pre-defined filters to recognize confidential content, offensive content and spam. Each of these contains a number of popular sub-filters. MI also provides a tutorial designed let you create effective filters to protect your company's confidential information.

Create and manage filters on the Filters page. To access it:

1. Click the **Conditions** tab under the *Policy* menu.
2. Select the **Filters** folder in the tree.

The *Filters* page displays a directory tree that shows the hierarchical arrangement of all of MI's filters



Creating a Filter

To create a new filter, do the following:

1.Right-click **Categories** at the top of the tree, then select **Add Filter**.

2.To create a sub-filter of an existing filter, right-click the parent, then select **Add New/Filter**.

3.Type in a descriptive name for the new filter.

4.Click **Apply**. You now have an empty filter and are ready to create a few entries.

Modifying a Filter Name

1.Click the filter, erase the existing name and type in a new name.

2.Click **Apply**.

Deleting a Filter

1. Right-click the filter.
2. Select **Delete from System**.

Note: *You cannot delete default filters.*

For information on creating entries and customizing FTA queries, see "Customizing the FTA Engine" on page 57 and "Constructing Entries" on page 60.

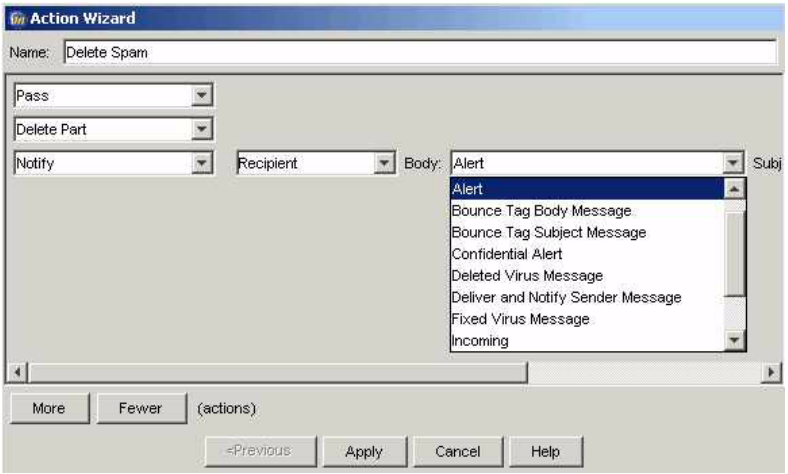
Configuring Actions

When a message matches a certain service, source, destination, shift, and condition, the action runs on that message. There are two types of action: *Policy* action, which affects where the original message goes, and *Notification* action, which affects how that message is copied, reported, or stored.

Creating a New Action

To access the *Actions* page, click the **Actions** tab on the *Policy* menu. The Actions page displays all the default actions. Details on each Action element follow.

1. On the *Actions* page, click **New** on the **Items** tab.



2. In the *Actions* wizard, fill in the *Name* field. We recommend the exact action.
3. The first drop-down menu contains the Policy action. Select one of the following:
   - **Block** — Prevent the message from reaching the recipient.
   - **Pass** — Allow the message through.
   - **Quarantine** — Send the message to the Quarantine Server for further review. See "Adding Reviewers" on page 78. Choose the duration of the quarantine and the disposition at the end of the period.
4. Click **More** to add a notification action:
   - **Redirect** — Return (bounce) the message to the sender or send it to any other email address (enter the address)
   - **BCC** — Send an alert to another user.

- **Notify** — Send an alert to the sender, recipient or other user (enter the address). Select a disclaimer or select **Add New Sys Msg** to create one.
- **Tag** — Allow the message through: add a subject, indicate a location within the message, and choose a disclaimer.
- **Fix Virus** — Repair a detected virus.
- **Delete Part** — Remove any message part (subject, body, in-line attachments, non-archive attachment ,a file in an archive attachment, or similar components of attached emails) that has generated a hit in Category, Type, Attachment Name or Size.

Note: *If multiple parts of an email or the whole email triggers the rule, MI deletes each part that matches, even the whole message.*

- **Dump to Path** — Direct a message to a particular file. You must indicate the path when selecting this option.
- **Auto global white listing**— Send to global *Blacklist/Whitelist* spam list.
- **Auto personal white listing** — Send to user's *Blacklist/Whitelist* spam list. Do not send confirming email.
- **Add X-header** — Add custom *(X-*) header content. Any email with the designated x-header applied will be acted on without judging it spam or non-spam. Give the x-header a name (no spaces) and enter an ASCII text header value (no slashes preferred). MI automatically supplies the *X-* header prefix.

5. Click **Apply**.

Viewing the Usage of an Action

To view the rules currently using that action, click the icon to the left of the action and select **Show Usage**.

Modifying an Action

1. On the Actions page, click the action you want to modify.
2. Modify action elements as if you were creating a new Action, by using the drop-down menus as described in "Creating a New Action" on page 53.

Note: *You cannot modify or delete locked default actions.*

3. Click **Apply**.

Important: *When you modify an action, this affects all rules that use this action. For such cases, we suggest creating a new action and applying it to one rule.*

Important: *Messages affected by Pass and Alert actions may lock in the MTA due to an address discrepancy. To modify such actions,* see "Troubleshooting" on page 97.

Deleting an Action

1. On the Actions page, click the icon to the left of the action. Then select **Mark for Removal**. When the scissors icon displays, select **Save** on the menu bar. The marked action is now deleted from the policy. Repeat to delete other actions.
2. Click **Save** on the menu bar to complete the deletion.

Disclaimers

You can add a disclaimer to any incoming or outgoing email in order to make the recipients aware of your organization's usage policy.

The pre-defined disclaimers are designed to be examples, not legal advice for your organization. Please enter the text as described in your Acceptable Usage Policy, or consult legal counsel.

Creating a Disclaimer

1. On the *Policy* screen, click on **Actions > Disclaimers**. Select **New** on the menu bar.
2. Type a descriptive name for the new disclaimer in the *Name* field.
3. Double-click the *Text* field, then type the text of the disclaimer.
4. Click **Save** on the menu bar to complete the disclaimer.

To create a disclaimer from the Actions window:

1. In the Message menu, select **Add New Sys Msg**.
2. Type a descriptive name for the new disclaimer in the *Name* field.
3. Enter the disclaimer text in the box.
4. Click **Save**.

Variables in Disclaimers

In a disclaimer, you can specify one or more strings to add. For example, if you choose **Tag Subject** and use *$Disposition$* variable, MI will append how it handled the message ("blocked," for example).

The variables, their formats, and what information they provide appear below:

Variable	Format String	Description
Date	$Date$	Date from the email header.
Sender	$Sender$	The Sender's mailbox address.
Recipients	$Recipients$	A comma-separated list of recipient addresses from the original email, before bcc or redrect actions.
Subject	$Subject$	The original email subject line, before tagging actions.
Message ID	$MessageID$	The ID from the email header.
Zix Unique ID	$ZixUID$	The unique ID generated by MI.
Virus Summary	$VirusSummary$	A mini-report summarizing virus status (which attachments had a virus, the name of the virus, whether it was cleaned, and whether MI deleted the attachment.
Disposition	$Disposition$	This will be either "passed," "quarantined, or "blocked."

Modifying a Disclaimer

1. On the *Policy* screen, click on **Actions/Disclaimers** and double-click in the name or text field.
2. Enter your changes.
3. When you are satisfied with your changes, click **Save** on the menu bar.

Deleting a Disclaimer

1. On the *Disclaimers* page, right-click the icon to the left of the message you want to delete and select **Mark for Removal**.

Note: *To cancel the Delete action, again right-click the message icon and select* ***Undo Mark for Removal****.*

2. When you see the scissors icon displayed, select **Save** on the menu bar. The marked disclaimer is now deleted from the policy. Repeat to delete other disclaimers.

Chapter 5
Planning a Policy

MI includes several built-in filters to help you understand and control your organization's messages. This chapter explains the purpose of each existing filter and provides a guideline for creating your own customized filters.

Full Text Analysis

The English language's high degree of ambiguity means that any system of language recognition based on string matching will produce a large number of false hits, making such a system highly unreliable.

MI starts with *content analysis,* based both on word frequency and the relative position of words within a sentence. Content analysis operates on the meaning of the messages.

Full Text Analysis (FTA) goes beyond the conventional keyword approaches of address recognition and string matching by applying a suite of technologies designed to use context and previous experiences to overcome ambiguity. FTA incorporates state-of-the-art techniques from computational linguistics, information retrieval, text mining, and lexicography to complement the content analysis step. It integrates all these techniques and technologies into a unified solution. Forming the core of the product are MI's three proprietary, patented, and patent-pending technologies: Automatic Collocation Identification, Automatic Statistics-based Spam Detection, and Statistical Dynamic Ranking.

Customizing the FTA Engine

Training/Calibrating the System

Training is the process of exposing an engine to known examples of the category it is filtering, to enable it to recognize and act upon new instances.

The FTA is a text filtering engine based on search technology similar to that used in most Internet search engines. The FTA can determine that:

- An entry is similar to a query for a search engine, by specifying a search criterion that incoming documents should match.
- A document is an ASCII converted document, for example an email or attachment.

A filtering engine works like a search engine in reverse: instead of searching for a query in a set of relevant documents, it searches within a document for a set of relevant entries.

When scoring relevance, a filtering engine scores an entry to a document as compared to other documents already seen or potentially seen, while a search engine ranks all the documents retrieved by decreasing order of relevance to a given query.

Although the FTA ships with predefined language, the Filters page allows you to add Filter entries (see "Constructing Entries" below) to the default set, and relax and constrain the Boolean expressions of the default entries.

Building Boolean Expressions

Writing a good filter entry is a challenge, and the result is very often complex but imperfect, because even the most sophisticated entry may have some false positive and false negative rates. Boolean logic, used to write MI filters, is both powerful and very difficult to master. Experienced users usually define their queries using stepwise refinement techniques. That is, they write the query and then try to add or remove constraints depending on the results obtained. These advanced users have specific techniques for refining queries that involve relaxation and constraining tools.

Relaxation tools include:

- Changing AND to OR
- Removing one word from an AND OR expression.
- Adding one word to an OR expression.

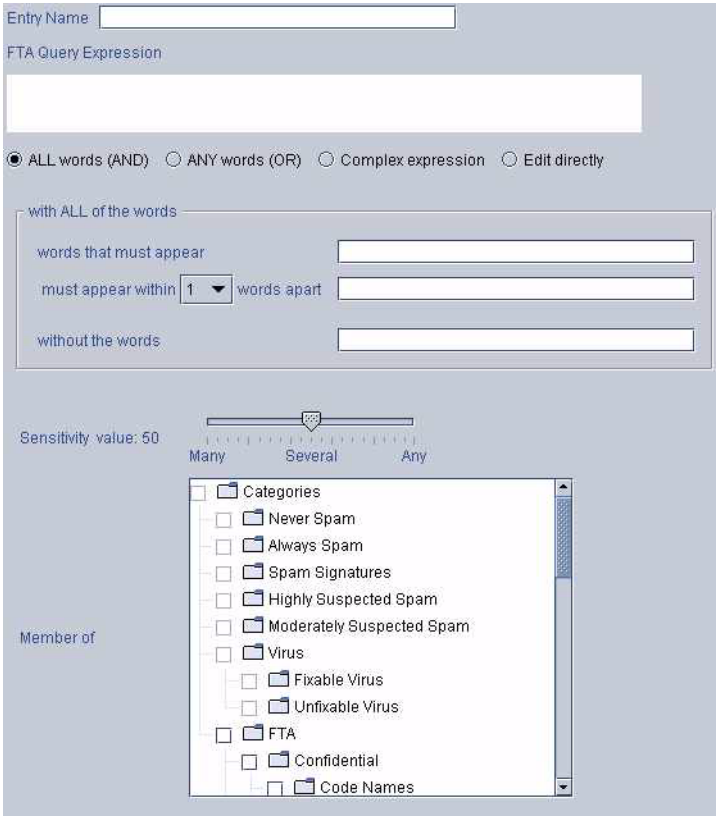
Constraining tools include:

- Changing OR to AND
- Removing one word from OR expression
- Adding one word to an AND OR expression.

MI provides an additional tool for refining entries: The ability to select only the most relevant documents using the sensitivity slider.

Constructing Entries

1. Select **Conditions/Filters**.
2. On the Filters page, right-click a filter and select **Add /Entry**.
3. In the main window, type a descriptive name for the new entry in the *Entry Name* field.



4. If any one of these words should trigger the rule, select **Any.** If all of the words must appear for the rule to trigger, select **All.**

   To make both options available at once, broadening your options, choose **Complex Expression**. If you wish to work on the Boolean expression in text, select **Edit Directly**.

Important: *If you are not experienced with building Boolean expressions, you should use the built-in query expressions.*

5. In the *Words* field, enter words that should trigger the rule. If you need an exact match for a word or expression, put it in quotation marks. Indicate how close words or expressions should appear, one to ten words apart.

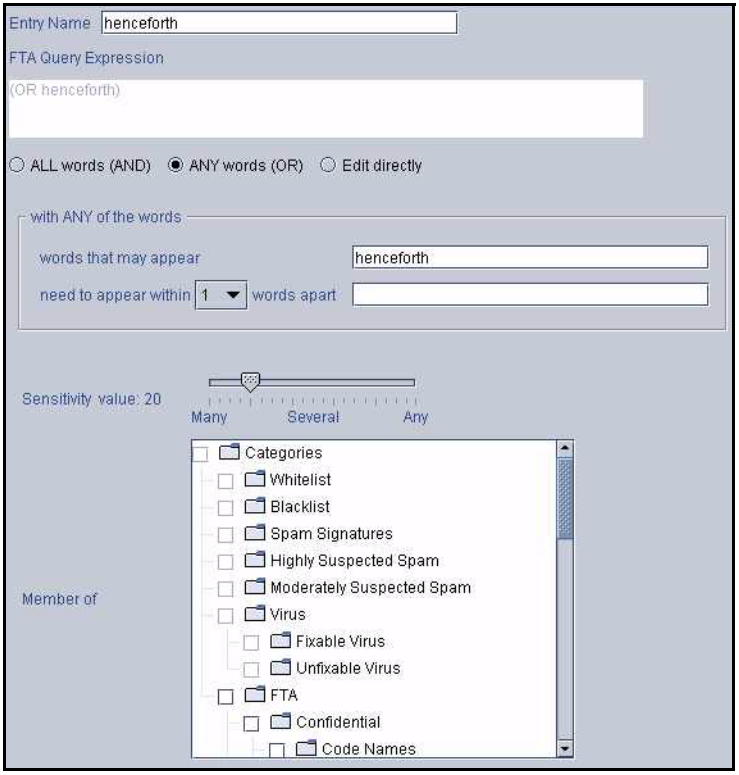
   You can include the following numerical values in your expressions, entered as shown with parentheses and capital letters:

   - (DATE)
   - (SSN)
   - (CREDIT_CARD_NUMBER)
6. Set the *sensitivity value*, ranging from *Many* occurrences (1 percent) to *Any* (100 percent).

   To set the sensitivity level, estimate how unique the entry's keywords are to the content you want to identify. Ask yourself how likely is it that you would find the keywords in messages that are not consistent with the target. If every occurrence of a keyword is likely to indicate the content you are trying to identify, set the sensitivity slider to **Any**. If the keywords are fairly common and you want the slider to detect only strong matches, set it to **Many**.
7. In *Member Of,* the filter you first selected is checked. Select any other relevant entries.
8. When you are done, click **Apply**. The FTA Boolean query expression corresponding to your entry appears in the window near the top of the screen. An icon for it appears under *Entries* in the left frame.
9. Repeat steps 1-8 until you have entered enough entries to reliably identify the confidential content you want to protect.

Editing Entries

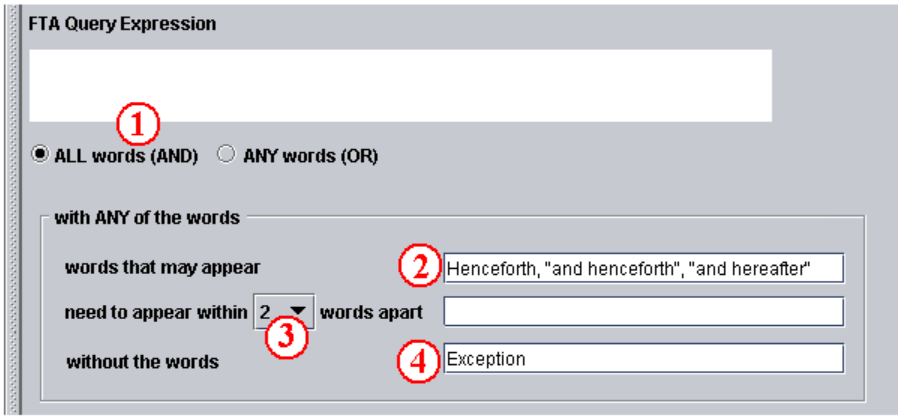
Open **Filters > Confidential > Legal > Contracts**. Select the entry **Henceforth**. The editing panel opens to the right.



- The default setting is *Any Words*, which defines the Boolean operator as OR.
- The only term searched is *henceforth*
- For one word, the default setting of one word apart remains
- The sensitivity is set at 20. It will take many occurrences of the term in the expression to trigger the filter.

The *FTA Query Expression* box shows the Boolean expression *(OR Henceforth)* resulting from the default settings.

To see how the tools affect the expression, make the following changes.



1. Select **All Words**, then click **Yes** at the prompt. Changing the expression clears the settings.
2. Restore *Henceforth*, then add the expressions "*and henceforth"* and *"and hereafter"*. Place them in quotation marks to indicate a single expression.
3. To expand your collocation, increase to two words apart.
4. To exclude a particular word or expression — use *"Exception"* for the example —using the Boolean operator NOT, enter it in *without the words*.
5. For this example, leave the sensitivity setting at 20.
6. Click **Apply**.

The FTA Query Expression window shows your new Boolean expression: *(AND Henceforth, (SEQ and henceforth), (SEQ and hereafter) (NOT Exception))*.

Including Spam Management In Your Policy

Spam is junk email. MI identifies up to 2500 spam-like characteristics, enabling you to control it more effectively. In addition, MI provides a default policy action (Spam Tag) that marks suspected spam, making it easy for end users to spot in their inbox.

MI's default spam rule delivers spam messages to their intended recipients and creates a record of the event in the database. The spam rule should inspect *only* incoming messages from the Internet. MI uses specific header parameter information that is missing or incomplete on outgoing or internal email. Naturally too, you do not need a spam engine to tell you if the email you send is spam or not.

Blocking or Tagging Spam

By default, MI reports spam, but does not block or alter it. You have the option to permit users to receive tagged spam or block it entirely.

Note: *Use the tag option for a short period when you first implement the spam engine. This makes it easy to add the source address of messages accidentally tagged as spam to the global or personal* Never Spam *list, and to confirm suspect email as spam, then add it to the global or personal* Always Spam *list.*

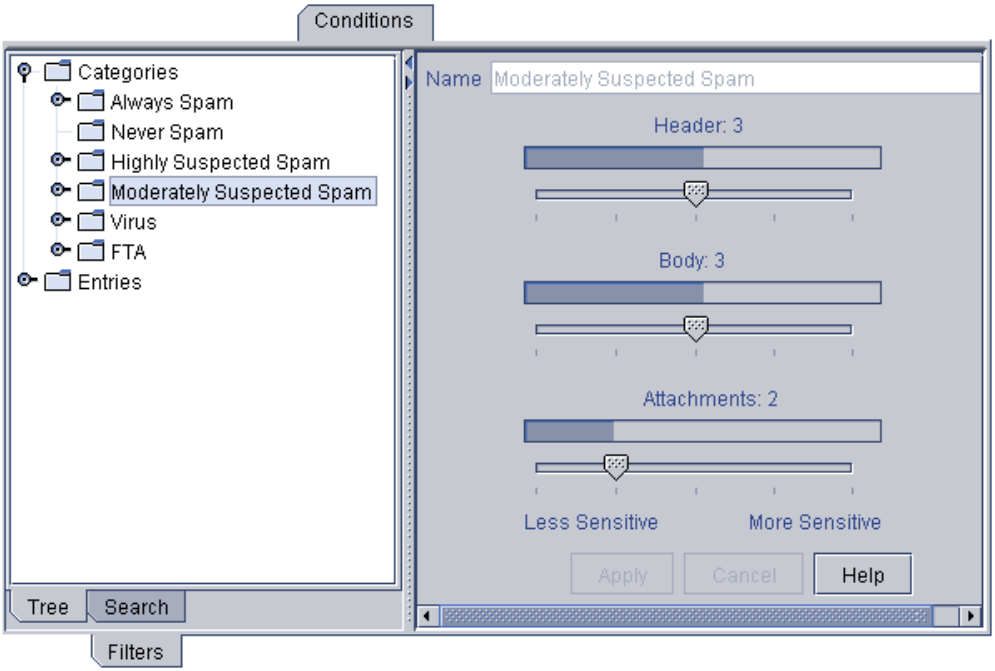
1. If a message meets the *From*, *To* and *Shift* parameters of a rule, MI applies the rule.
2. If you have set up Blacklist/Whitelist Rules, MI checks the sender email address against the global and local blacklists and whitelists. If the address is in either, it will act on the message automatically and not scan it. See "Blacklist/Whitelist Manager" on page 69.
3. If there is no sender address match, the Body engine will check the email for Body-like characteristics against the built-in parameters. If the email meets a threshold, MI will act on it.

To change the default spam rule to block or tag instead of deliver, refer to "Modifying a Rule" on page 41.

Modifying the Spam Engine

The default spam rule labels a matching message as *Always Spam*. You can modify a matching entry with the spam categories *Highly Suspected* or *Moderately Suspected*.

1. Select the category.
2. In the right frame, choose filter sensitivity for the message header, body, and attachments.



If you move the slider all the way to *Less Sensitive (1)*, the spam engine will ignore that portion of the message entirely. If you move it all the way to *More Sensitive (5)* almost any discrepancy triggers the spam engine. Less sensitive settings reduce false positives but miss more spam. More sensitive settings miss few spam messages but are more likely to generate false positives. See “Spam Slider Guidelines” on page 66.

3. Click **Apply**.

We suggest monitoring spam performance and tweaking these settings to suit your network and traffic. As your company policies change and particularly as spammers alter their tactics, you can fine-tune the spam engine’s performance.

Spam Slider Guidelines

You can customize the MI spam engine to your network and traffic as described above. There is a bit of an art to using the sliders.

Header Slider. A sub-engine of the spam engine analyzes email headers for typical spam expressions and anomalies as determined by our lexicographers. It calculates a score, with the most likely spam having the highest totals. With the slider all the way to the right, MI will identify nearly any header as spam. With it all the way to the left, MI will have almost no false positives of legitimate mail, but has a greater chance of missing spam.

Body Slider. another sub-engine analyzes both email bodies and attachments. It looks for specific strings, patterns, and expressions. Set all the way to the right, MI will identify nearly all email as spam. All the way to the left, the slider setting allows nearly all mail through. Again, the false-positive rate would be very low, but the false-negative rate so high that many spam messages would pass.

Attachment Slider. This follows the same settings and operations as the body slider's. In most cases, you will want the attachment slider at a lower setting (more to the left) than the body slider.

Monitoring and Controlling Offensive Content

MI filters identify sexually oriented, abusive, and inappropriate content limiting legal liability from offensive messages. These filters are based on words and phrases from dictionaries, newsgroups, and the Web.

Our lexicographers at have categorized these words and phrases into three types: sexually oriented, abusive, and inappropriate; and three degrees, mild, moderate, and extreme.

Sexually Oriented			
Abusive	**Mild**	**Moderate**	**Extreme**
Inappropriate			

Because the categories are divided in this fashion, your rules can be as flexible as your Acceptable Usage Policy. Review the words under each dictionary to decide what level of offensive content is permissible. Determining this level is a highly subjective task.

MI's offensive content filters are designed to identify content that is not suitable for formal business communication. In everyday practice, not every message requires maximum filtering. The decision depends on the identity of the sender, the recipient, and the context. Consider these issues when designing your policy.

Chapter 6
Blacklist/Whitelist Manager

The Blacklist/Whitelist Manager, an option available from the *Custom* setup type in installation, is a personal block-or-pass list system for individual users.

Note: *MI does not include the Blacklist/Whitelist Manager by default in its* Typical *installation. If you did not choose this, restart installation and select* Custom *to add this component. Doing so does not affect the existing MI.*

Blacklist/Whitelist Manager forces MI to apply the Blacklist or Whitelist rules on mail from specified email addresses or domains. If the Whitelist rule is to pass messages, those in the whilelist will pass. Likewise, if the Blacklist rule is to block messages, MI applies this to all address and domains in the blacklists.

MI has a global whitelist that the administrator manages. This affects messages for all users. If the administrator installs the personal blacklist/whitelist component and enables it, each user can specify addresses and domains to either list. Users who know which messages are acceptable make the decision to whitelist them. This eases one administrative burden. The Blacklist/Whitelist Manager also lets individual users expand on MI's default lists, for example singling out spam that may be useful for their work.

Using the Personal Blacklist/Whitelist Manager

Before you direct email, we recommend your changing actions on the default spam rules to *Spam Tag* (see "Blocking or Tagging Spam" on page 64). Leave these actions in place for a short period to evaluate your traffic.

Directing Messages to the Blacklist/Whitelist Manager

1. Build an action with a policy action of *Deliver* and a notification action of *Personal Blacklist/Whitelist* (see "Creating a New Action" on page 53).
2. Edit the default rule *Moderately Suspected Spam* as follows:
   - **To:** Known Users
   - **Condition**: Moderately Suspected Spam.
   - **Action:** Your new action (see **1**, above)

Important: *DISABLE* Continue. *MI should stop searching for matches when this rule triggers.*

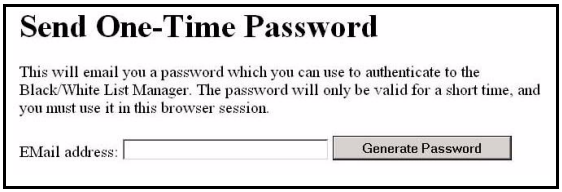
3. Save the rule.

Messages from the protected sources now go to the Address Management screen of users' personal blacklists and whitelists for management.

Using the Address Management Screen

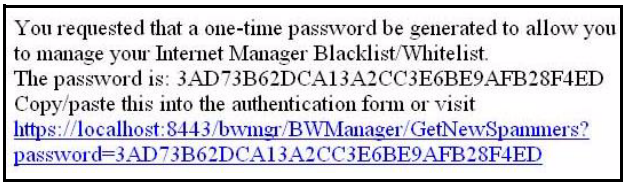
MI sends users email each night when there has been new activity affecting their blacklists or whitelists.

1. Follow the link from the message to open the Blacklist/Whitelist Manager, or open **Start > Programs > Message Inspector > Blacklist/ Whitelist Manager**.



2. To obtain a one-time password, enter the email address of a known user from MI Attributes. Click **Generate Password**.

   The resulting email provides a temporary password. The recipient cuts and pastes the email into browser box. Alternately, clicking on the blue link at the bottom of the email performs the same function. This link includes the URL of the Blacklist/Whitelist Manager and the password.

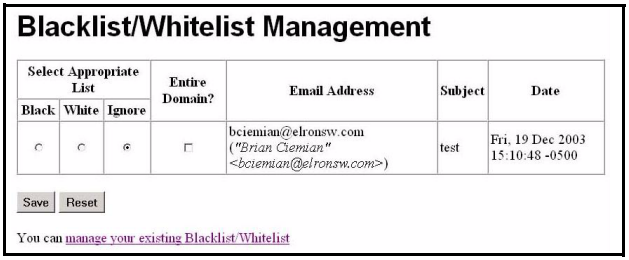


Important: *The password is valid for ten minutes (600 seconds).*

3. Cut and paste the password into the box and click **Authenticate** to open the address-management screen.

This opens the *Blacklist/ Whitelist Management* screen, with the new suspected spam addresses. Here you can:

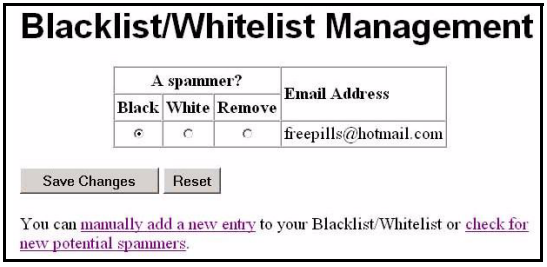
1. Review the summary information on the messages.



2. Under the *Select Appropriate List* column, click **Black**, **White**, or **Ignore**.
3. To act on the entire domain, check **Entire Domain.**
4. Click **Save** to keep your settings or click **Reset** to clear them and start over. When you save, a *New Entries Processed* confirmation screen displays.
5. Click the link to open the management screen (below).
6. Log out.

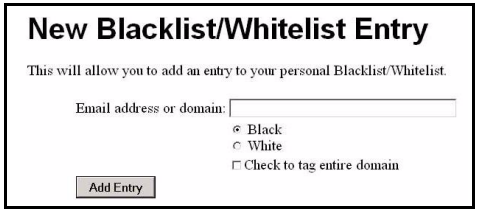
Spam Address Management

All address entries appear on the management screen with the lists initially assigned them. You can:



1. Change the selection from *Black* to *White* or vice versa, by clicking the appropriate radio button, or select **Remove** to delete the entry from the list.
2. Click **Save Changes** to confirm any changes to the list, or **Reset** to restore the previous settings.
3. Click the link to add a new entry manually.
4. Log out.

Adding New Entries Manually



You may learn of a new spam source or other unwanted mail, or of a new address to protect, before email from it shows up in your mailbox. In such cases, click the option to **manually add a new entry** on the *Blacklist/Whitelist Management* screen. Then:

1. Enter the email address for the list to act on.
2. Select either **Always** or **Never**, or check the box to tag the entire domain.
3. Click **Add Entry**. The screen refreshes to show which entry has been added and in which category.
4. Log out.

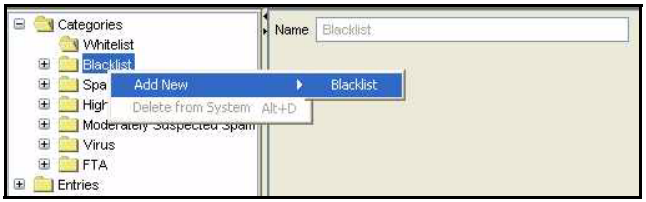
Managing Global Blacklist/Whitelist Entries

MI populates the global Blacklist/Whitelist lists according to your rules. You can also add entries or remove them manually.

Adding Addresses and Domains

MI populates the global lists according to your rules. You can add email addresses and domains to protect or classify as always spam. To do this:

1. In the Administrative Console, choose **Manage/Policy/Conditions**.
2. Click the **Filters** tab at the bottom of the screen.



3. In the tree on the left, right click on the **Blacklist** or **Whitelist** category.
4. Choose **Add New** and the category name.
5. In the right window, enter the address or domain.
6. Click **Apply**.

Removing Addresses and Domains

You can delete individual or multiple addresses or domains from either blacklist or whitelist category. To do this:

1. In the tree on the left, choose the entry or use the Shift-click and Ctrl-click combinations to select multiple entries.
2. Right click on the selection and choose Remove from System or Delete from this Filter. Remove eliminates it from the database and Delete leaves it available if you search for it. Deletion is immediate.

Note: *If there are too many entries to display in the category list, you can click the Search tab for the entry and manage it on that screen.*

Chapter 7
Quarantine Server

Quarantine Server (QS) lets you take a more detailed look at messages before delivering or acting on them.

Set up Quarantine in Policy, with a Quarantine Action designating a reviewer, the time to hold a message affected by this rule, and the default disposition of the message. Most reviewers can open only those messages pertinent to rules they are monitoring.

Quarantine Server comes with two default windows, which you access separately from the Windows Start menu:

1. *Administrator*: the Quarantine Server administrator. They can add reviewers or super reviewers and can perform any review function.
2. *Super Reviewer:* a super reviewer can review all quarantined messages regardless of type and subject, and evaluate decisions of reviewers with limited rights.

Enabling Reviewers

You can allow any known user to review quarantines email. You must do this in your policy rules and on the QS. To do this in the QS, see "Adding Reviewers" on page 78.

For reviewers to be able to access the quarantines email, the rules must include them. The following example shows such a rule.

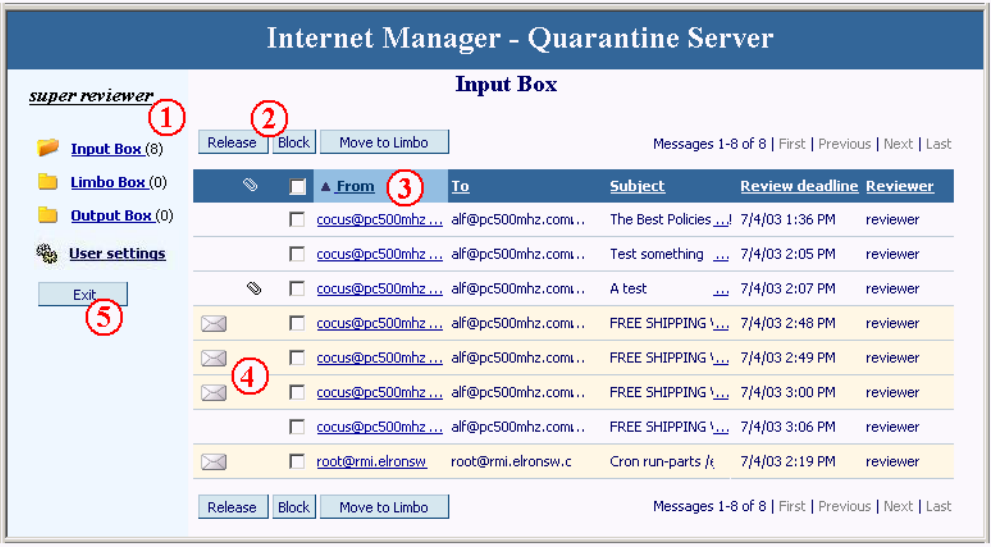
1. Verify that known user *Rex Solomon* is available. If he is not already a reviewer, add him on the QS side before applying him to the types of quarantined email he should review. See "Adding Reviewers" on page 78.
2. Create a new Action named **Rex Solomon Review**. Select **Quarantine** from the drop-down list, type in **Rex Solomon** in the *Reviewer* box, and click **Apply**.
3. On the *Rules* tab, change one or more of the *Action* boxes that quarantine email to use *Rex Solomon Review.*

Now in the QS, messages that triggered the rules and arrived there will be available to Rex to review. Any super-reviewers can also act on those messages.

Using QS Reviewer

1. If QS is loaded locally, go to **Start > Programs > Message Inspector > Quarantine Server**, and choose **Reviewer**.
2. If you are accessing QS remotely, open a Web browser and type in the address: *http://[IP address]:8080/qs/reviewer/login*
3. Log in. The default user name and password are *super reviewer/super reviewer* (case sensitive). You should change the default settings as soon as possible. See "Modifying Reviewers" on page 79.

The Review window has a user setting for choosing how many messages to display per screen and three pages or boxes: *Input*, *Limbo*, and *Output*. Each has similar features:



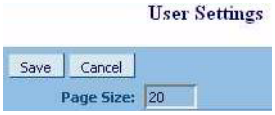
1. A file menu to the left that shows the number of messages at each stage of disposition. The open folder symbol indicates the box visible to the right.
2. Disposition buttons that allow you to release a message you have selected, delete it, or hold it for further consideration.
3. Click on a column header to sort by it. Use the check box at the head of the first column to select all messages at once.

4. Check a message to open it and begin reviewing. The envelope icon indicates a new message. A paper clip indicates an attachment. Use the checkbox in the column header to select all.
5. **Exit** closes QS.

Important: *If you exit the QS, you must close and restart your browser or open a separate browser window to log in again. This security procedure prevents non-authorized users from accessing the QS.*

User Settings

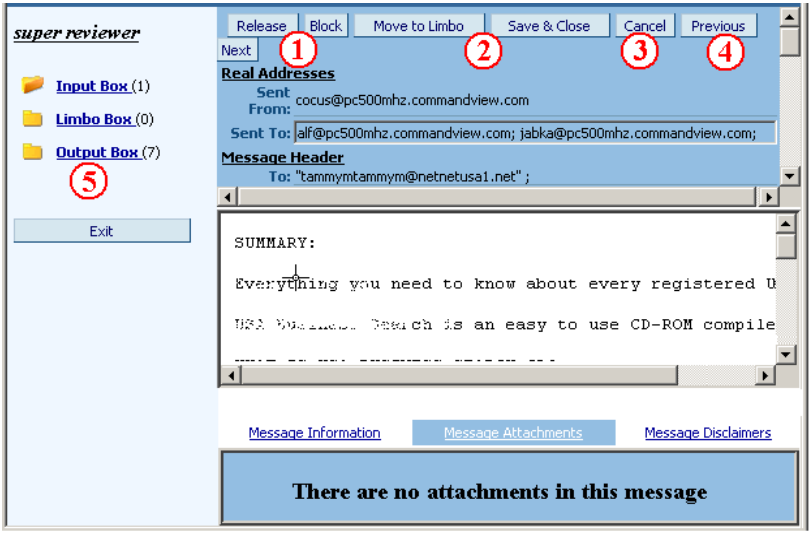
By default, the QS displays 20 messages per page. To change the number of messages that display:



1. Click **User settings**.
2. Change the number to display per page.
3. Click **Save**. The QS automatically returns you to its main screen.

Input Box

Click on the message entry in *Input* to open the message page. It shows the real addresses of the sender and recipient, the header and subject of the message.

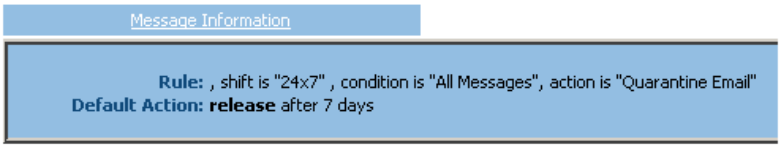


1. You can **Release** or **Block** a message, which sends it to the Output box.

2. If you do not want to make a disposition now, you can:
   - Send the message to Limbo.
   - Click **Save and Close**. The message remains in *Input*, without the envelope.
3. Click **Cancel** to close the message with no action and return to *Input*.
4. Click **Next** to move down, or **Previous** to move up the list of quarantined messages. without returning to the summary screen.
5. As you act on messages, their locations change to reflect your dispositions. For example, if you begin with four new messages, take no action on two, send one to *Limbo* and release one, the message counts change to reflect this.

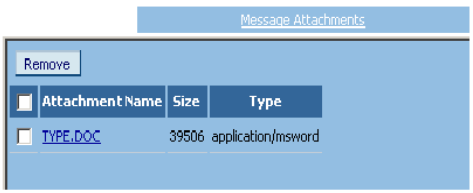
Message Information

Click **Message Information** near the bottom to display a summary of rules, actions and conditions that affect this message, and the message life from the System screen.



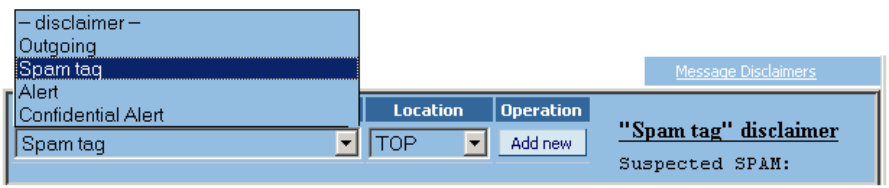
Message Attachments

This option shows a standard summary of message attachment parameters. Check attachments to remove them before releasing the message from QS.



Message Disclaimer

Choose an appropriate disclaimer from your MI options here, without having to leave QS to make the selection.



Limbo Box

Limbo holds messages for further review. You can release or block messages from it, or leave them (no longer marked unread) in the box indefinitely. When you select a message in Limbo for action, act on it as you would a message in Input.

Output Box

Output is the last stop in Quarantine, and displays disposition of messages for a configurable period.

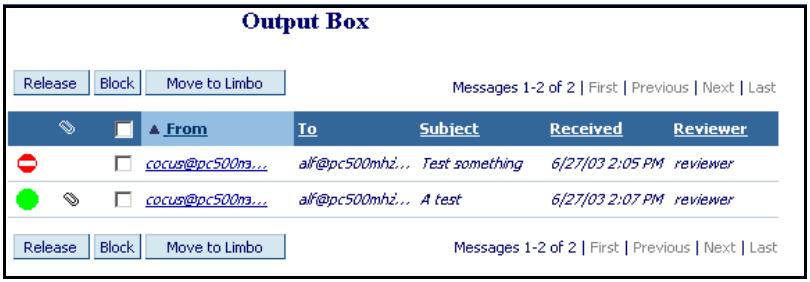
QS marks messages in *Output* as *Released* or *Blocked*.

To act on a message, click the check box, then choose a disposition button. You can

- Select a message and click **Release** to return it to the MI delivery stream. Click the box at the top of the column to release all messages.

Note: *It may take several minutes for the Output Box's contents to be released, particularly under heavy load.*

- Click **Block** to change the message's status.
- Send it back to Limbo for further consideration.



Using QS Administrator

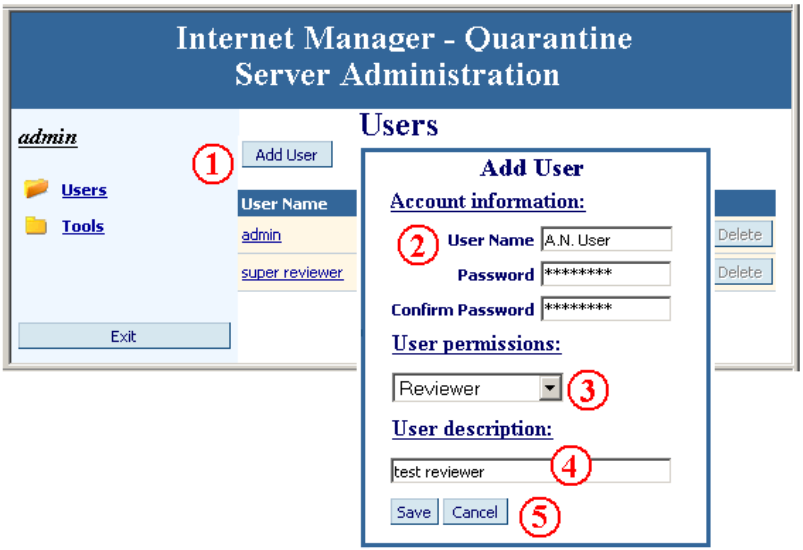
1. If QS is loaded locally, go to **Start > Programs > Message Inspector > Quarantine Server**, and choose **Administrator**.
2. If you are accessing QS remotely, open a Web browser and type in the address: *http://[IP address]:8080/qs/admin/login*
3. Log in: the default user name and password are *admin / admin* (case sensitive). Change the password as soon as possible. See “Modifying Reviewers” on page 79.

The opening window shows the administration screen. There are two available windows in QS: *Users*, and *Tools,* which turns the service *TSAgent* (required for Quarantine Server) on and off.

Adding Reviewers

1. Click **Add User** on the User Admin page, then
2. Enter the user information.
3. Choose permissions: reviewer or super reviewer.
4. Add a description of the user’s function.

5. Click **Save** to return to the Admin screen, or **Cancel** to clear.



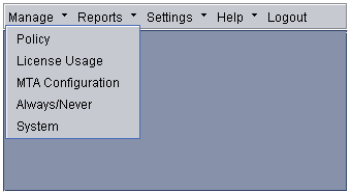
Modifying Reviewers

1. On the Admin screen, click on the user name you wish to modify.
2. Make your changes and click **Save** to return to the Admin screen, or **Cancel** to clear.
3. On the Admin screen, click **Delete** to remove a user.

Note: *You can modify, but not delete, the default users*

Chapter 8
Managing Message Inspector

The Manage Menu



Policy

Policy opens the Rules page. For details on creating and customizing policy rules, see "Creating a Custom Policy" on page 37.

License Usage

The GUI summarizes MI policy elements available under your purchase. For example, if you did not buy AntiVirus, AntiVirus options will not appear. Use the text box to enter the license keys you receive for products you have purchased.

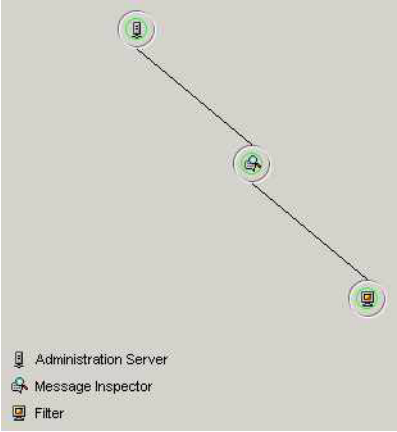
MTA Configuration

1. Click this to open browser-based, editable text boxes for each MTA configuration file, so you do not have to search for and open the following:
   - Mailertable
   - Access
   - Custom Configurations (including MAPS configuration)
   - Aliases
   - Virtual User Table
2. Make your changes and click **Apply**.

Important: *When you make changes in* Aliases*, you must still run* newaliases.cmd*, or the Sendmail MTA will not see them.*

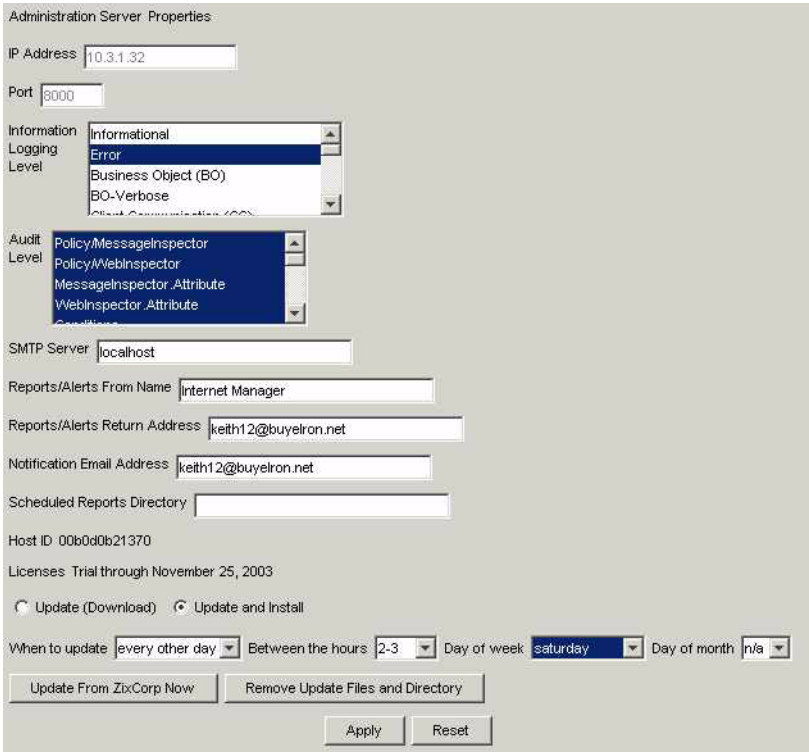
System

The System page displays a hierarchy of Message Inspector components in its left frame and the system settings of each component in its right frame. Click on a component on the left pane to view or modify its settings in the right. MI's System page has three levels:



- The *Administration Server Node*, to configure the Administration Server
- The *MI Product Node*, to maintain basic MI settings
- The *Filter Node,* which allows you cycle the MI Filter service without leaving the GUI.

Note: *You cannot change fields that are grayed out.*



Administration Server

To access the Administration Server's settings, click the top node icon. You can edit:

- *Information Logging Level:* Choose the levels of diagnostic information to be logged. You can Ctrl-click or Shift-click to select a single level or several levels.
- *Audit Level*: Choose one or more data objects for the Server to audit. You can Ctrl-click or Shift-click to select a single object or several objects.
- *SMTP server:* The domain name or IP address of the SMTP server that IM products use to send email reports and alerts.
- *Reports/Alerts From Name*: The name in the From header field in emailed reports and alerts.
- *Reports/Alerts Return Address*: The email address in the *From* header field in emailed reports and alerts.
- *Notification Email Address*: The email address where MI sends the messages that trigger rules with *Notify.*

- *Scheduled Reports Directory*: Location for reports you have scheduled.
- *Update* Options for Anti-Virus. If you have installed Anti-Virus, you can choose to download Anti-Virus files for manual installation or have MI download and install them. Below are the scheduling changes for updates.
- *Update From ZixCorp Now* and *Remove Update Files and Directory*: These buttons let you start an update and installation of new Anti-Virus files and delete the current update files and directory.

Updating LDAP

If you use LDAP and you enabled MI for LDAP at installation, you can see update and scheduling buttons at the bottom of the Administration Server screen, and you can customize automatic updating from LDAP.

Important: *Before updating from LDAP, verify that the administration server and LDAP server systems clocks are in sync. Otherwise the administration server may not see updates from LDAP.*

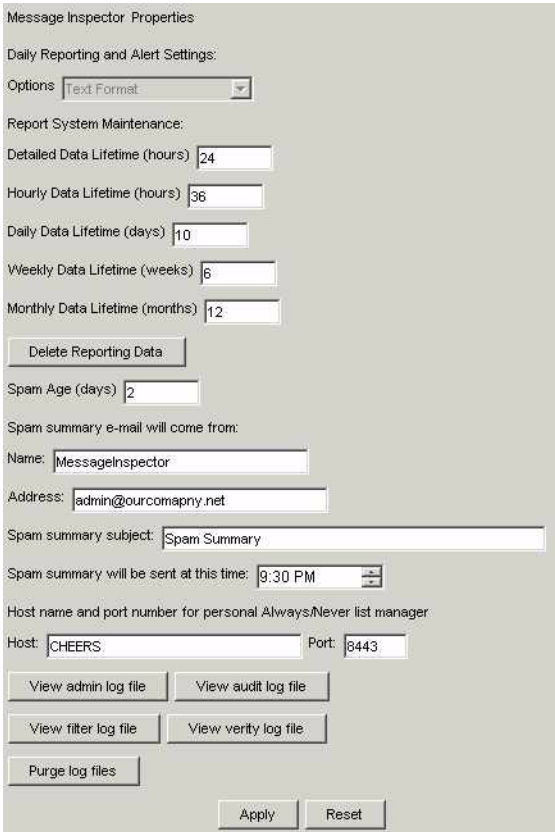
In the right frame of the Administration Server node, scroll down to the LDAP buttons. Here, you can re-synchronize LDAP users and groups, overwrite them from the LDAP server, view the last LDAP update date, or schedule daily automatic LDAP updates.

Here you can:

1. Click Update from LDAP to get the changes since the last time the servers synchronized. You will typically do this when you have added new users or new groups. This happens immediately after you click the button. Depending on the size and complexity of the LDAP tree, this may take a few minutes or even hours.
2. Click Replace All from LDAP to reload the users and attributed from the LDAP server. This removes the administration server's current LDAP users and groups, replacing them with the latest LDAP ones. You will typically do this when you have changed your LDAP tree, such as modifying or deleting users or groups.
3. View the Last Sync with LDAP time and date below these buttons.
4. Use the Automatic LDAP Update Time dialog to set a daily hour and minute for this to occur. Then click Apply to set the automatic update. With LDAP enabled, MI automatically updates LDAP daily.

MI Product Node

To access MI settings, click the lower icon in the left frame. The right frame displays read-only *Daily Reporting and Alert Settings* and *Report System Maintenance*.



You can change any of the following in this frame:

- Detailed data lifetime (in hours)
- Hourly data lifetime (in hours)
- Daily data lifetime (in days)
- Weekly data lifetime (in weeks)
- Monthly data lifetime (in months)
- Days to age spam
- Sender of the periodic spam summary (typically, administrator) with an email address
- Subject line of spam summary
- Time the daily spam summary is sent.

The MI node contains view buttons enabling you to access log files for the following without leaving the GUI:

- Admin
- filter
- audit log
- Verity

Buttons on the MI node allows you to delete all reporting data and to purge all log files.

Click **Apply** when you complete editing to save the changes, or **Reset** to begin new changes. MI prompts you to save your changes when you leave the screen.

Blacklist/Whitelist Manager Options

If you have installed the Blacklist/Whitelist Manager, the Host (server name) and its communications port appear below the spam-summary section of this frame. You can change these here.

Important: *Important: Do not change the host name or port unless the Blacklist/Whitelist manager is installed on that server and port, and its services are running.*

The Blacklist/Whitelist Manager is an optional component that does not come with the Typical MI install. You can add this component at any time without disrupting an existing MI installation. To do, use the CD or downloaded files to start an installation on the server for the Blacklist/Whitelist manager. Choose a Custom installation and pick only Blacklist/Whitelist Manager. Follow the on-screen steps from there.

Important: *Important: Depending on your system load, the number of users and the size of the global and personal Always Spam/Never Spam lists, this server can be computer intensive. We strongly recommend installing this component on a separate server.*

System Logs

System logs record important information about system performance and errors for our technical support team. They should be used only by technical support to identify and correct issues.

Admin Users

By default, only the Administrator has the rights to access the Message Inspector interface. Give additional users administrative rights, or modify existing privileges in the **Policy > Groups > Users** window: see “Creating an Attribute” on page 43.

Stopping and Starting

To stop or start individual IM and MI services, go to **Start > Settings > Control Panel > Administrative Tools > Services**. Infrequently, the IM System Monitor may halt one or more services as well. Use Services to restart a stopped service.

If you are troubleshooting and want to stop one of the services, stop *IM System Monitor* first. Otherwise it will restart any of the others.

Important: *If you stop the MTA or Filter service, this halts all incoming mail until that service restarts and MI can process mail again. If the MTA service remains stopped, mail will eventually route to the next MX record in your DNS server list.*

If you stop only the Administration Server service, you will not be able to access the IM client and the MI interface. However, MI will continue to process mail.

Chapter 9
Reporting

When an email message triggers a policy rule whose actions specify *Report*, MI enters a record of the event into the database. These records show when the message was detected, the source, destination, and message content. The records in the current records database build MI's reports.

Report Types

MI has six report types: *Message Detail, Virus Reports, Quarantine Reports*, *Attributes, Graphs,* and *Statistics*. You can access and adjust all of them from Reports on the main menu. The menus under Reports also let you delete or edit the delivery of scheduled reports.

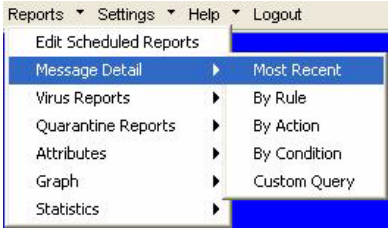
Important: *Virus Reports are available during the MI trial period and remain active if you purchase MI AntiVirus.*

Selecting Reports

Message Detail

Message Detail generates snapshot views of the traffic through MI in the past 24 hours (or other configurable time). You can sort these views by time, sender, or subject.

1. Open **Reports > Message Detail** and select a report.
2. In the next window, enter the hours for the summary to cover (24 is default).
3. Under Most Recent, choose to sort by sender, subject, or time.



4. If you choose **Custom Query**, also choose from:
   - Sender
   - Recipient
   - Sending Host
   - Applicable Rule, Condition or Action by name.
   - Group
5. Click **OK**. Your Web browser opens to display the report you chose. Use the **Schedule** button to configure delivery. For details on "Scheduling Text Reports", see page 94.

Virus Reports

With *Virus Reports* (available with MI AntiVirus) you can detail viruses by disposition (fixed, unfixed, deleted, or quarantined) or by quantity (top number of viruses or senders).

1. Open **Reports > Virus Reports** and select a report.
2. Enter the hours to cover and choose the sort order.
3. If you select the reports **Top N Viruses** or **Top N Senders**, choose the value of N or accept the default, 10, instead of a sort order.
4. Click **OK**. Your Web browser opens to display the report you chose.

Quarantine Reports

Choosing **Reports > Quarantine Reports > Summary** is similar to a most-recent message-detail report. It lets you choose the time period and displays a summary of each quarantined message by review, time and action.

You can drill down by clicking on the QS message ID link. This let you see what rules it triggered and even the words or phrases involved.

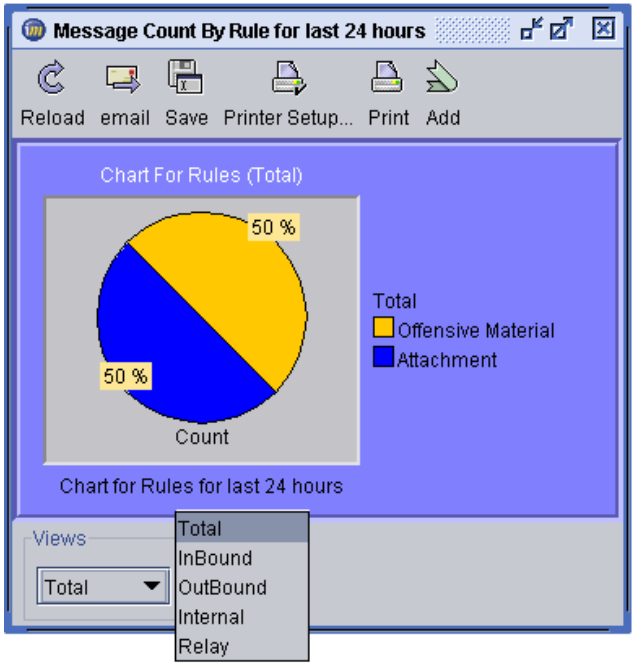
Attributes

These reports deliver message counts showing the particular user, groups or known email, total messages, and inbound, outbound, internal or relay traffic.

1. Open **Reports > Attributes** and select a report.
2. Enter the hours to cover.
3. Click **OK** and review your report in the browser.

Graphs

Using charts and graphs, you can evaluate the performance and effectiveness of your policy at a glance.



The graphs show you the top returns triggered for each of the following measurements over a configurable period (default is 24 hours).

- *Rule*
- *Action*
- *Condition*
- *Users*
- *Groups*
- *Viruses*
- *Virus Senders*

Each graph has five available, color-coded views:

- Total messages
- Inbound messages
- Outbound messages
- Internal messages
- Relay messages

Important: *If you have not set up internal users or domains (see "Creating Custom Rule Elements" on page 25) results appear only in the Total and Relay views.*

Creating a Graph

1. Open **Reports >Graph** and select a graph type.
2. Choose **Bar Chart** or **Pie Chart** from the drop-down list.
3. Click **OK** on the Options window.
4. The graph appears in the MI window. You can change the view shown on the graph, then use the toolbar to reset, email, save or print the graph. You can also right-click anywhere in the graph to bring up a dialog with the toolbar options.

5. Click **Add** in the toolbar to add the graph to the Favorites list.

Statistics

Statistics reports deliver details about activities ranging from message counts, number of rules, actions or condition triggered, as well as top users and emails.

1. Open **Reports >Statistics** and select a report type.
2. For each element, choose the time interval the report will cover: hour, day, week, or month.
3. On the next screen, accept the default number (for example, 36 hours) or click the number field to replace the number with your own choice.

4. For *Top N Users* and *Top N Known Emails*, choose the top N value and message parameters.
5. Click **OK** to bring up the report in your browser.

Statistics reports show only the rule ID active at the time of the report. Use the detailed reports to see complete information on the rule elements that are triggered. For example:

- A rule has the action *Pass* and two messages are passed.
- You change the action to *Pass and Alert* and send four messages through.
- The detailed report shows two messages as *Pass* and four messages as *Pass and Alert*.
- The statistics reports show all six as *Pass and Alert*.

Schedule

Message Count By Hour (Last 36 hours)

Date/Time	Inbound	Outbound	Internal	Relay	Total
14:00:00 07 May 2003	0	0	0	3	3
15:00:00 07 May 2003	0	0	0	8	8
09:00:00 08 May 2003	0	0	0	1	1

Printer Friendly

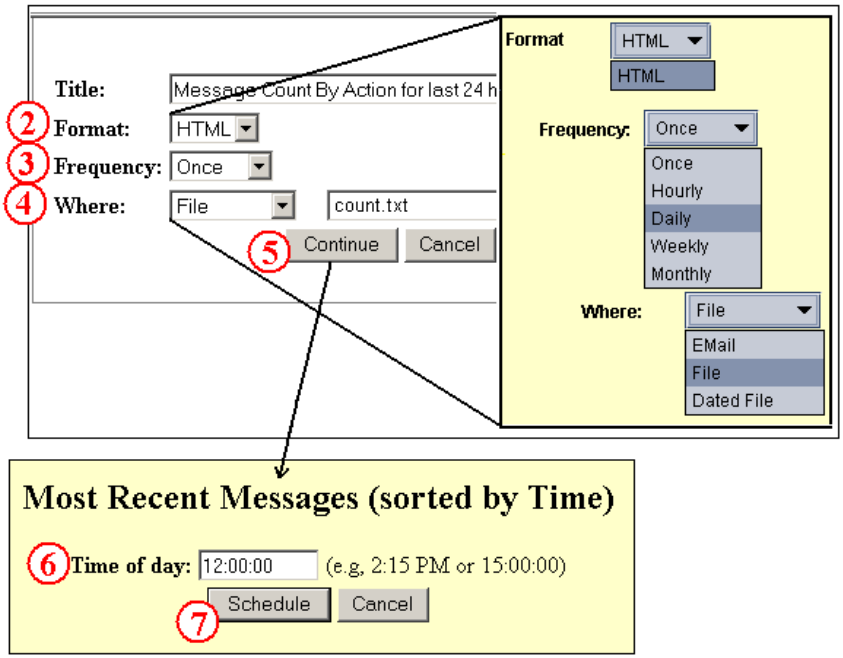
Note: *MI's detailed report tables contain complete information on the rule elements that are triggered. Data for the statistical tables show only the rule ID active at the time of the report. For example:*

- *A rule has the action* Pass *and two messages are passed.*
- *You change the action to* Pass and Alert *and send four messages through.*
- *The detailed report shows two messages as* Pass *and four messages as* Pass and Alert.
- *The summary/count reports shows all six as* Pass and Alert.

Scheduling Text Reports

Important: *If you have chosen the parameter* Continue *for a rule, MI generates two or more reports, and the actions may conflict. When such multiple rule hits appear in reports, last item listed is the final message disposition.* *See "Rule Components" on page 20.*

1. Click **Schedule** at the top of the message summary to set up the scheduling, format and destination of the report.



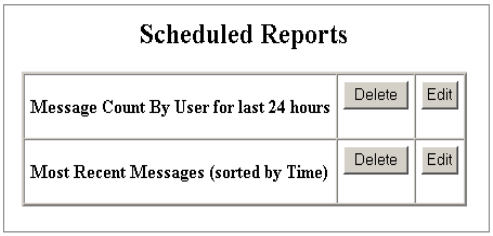
2. Select the report's file format: currently, HTML only.
3. Select report frequency. You can choose to deliver a report once, or at intervals from hourly to monthly.
4. Deliver the report to an email address, a general file or a dated file. If you choose a file option, enter a file name in the box to the right. If you select Email, enter the address in the box.
5. When you have defined the report, click Continue.
6. Enter time of day on the next form (required) as HH/MM (AM/PM), and confirm that the date is correct.

7. Click Schedule.

The completed form shows the date and hour you selected for the report.

Editing Scheduled Reports

After you have scheduled one or more reports, click **Edit Scheduled Report**s in the report menu to reach a browser menu of scheduled reports.



Click **Edit** next to any entry to open the scheduling form and make changes in the process, or click **Delete** to remove it.

Appendix A
Troubleshooting

Uninstalling Older Cygwin Versions

We recommend uninstalling any existing Cygwin before installing MI. Unless there is a perfect Cygwin version match, an installation over an existing Cygwin will fail.

Standard Cygwin Uninstall

1. Stop the ipc-daemon and postmaster services
2. Open a cygwin command prompt and

   remove postmaster:

   cygrunsrv -R PostgreSQL

   remove ipc-daemon:

   ipc-daemon --remove-as-service
3. Delete the cygwin directory
4. Remove the cygnus solutions registry key
   (under HKEY_LOCAL_MACHINE > software)
5. Remove cygwin from System Path under the System Control Panel Applet.
6. Reboot.

If you still have Cygwin conflicts, you may have other related registry keys.

1. Go to **Start > Run > regedit > Find**.
2. Do a search for “cyg”.
3. Delete any cygwin keys revealed.

Starting MI

If an MI login fails with the error message *Unable to establish a connection to Admin Server,* stop the admin service, then start it again. Do not use *Restart*: execute the two separate steps.

Policy

1. Messages affected by Pass and Alert actions may lock in the MTA due to an address discrepancy. To configure alerts successfully, make the following changes:

- Go to **Policy>Actions.**
- Click **Pass and Alert** or **Pass and Confidential Alert**.
- Change the addressee *Administrator* to the email of the person you wish to notify.
- In *filter.ini* change *NotifyFrom* to a valid email for the source of the notification.

2. After updating LDAP on the *System* screen, to ensure that LDAP DNs appear in the *Policy* screen and its wizards, cycle the *System* screen or click **Edit > Reload from Server** on the *Policy* screen. Repeat the cycling if necessary.
3. If spam sensitivity changes do not take effect immediately, cycle the IM Filter.
4. When you create or edit rules, selecting the parameter *Continue* can set up conflicting reports. In such cases, the last report of a series represents the final disposition of the message. See “Scheduling Text Reports” on page 94.
5. A message of type *multipart/alternative* will trigger the FTA twice. Since it is not certain that both parts in such a message are identical, the FTA must scan both and report on both separately.

Quarantine Server

If the Apache Tomcat server for Quarantine Server (QS) crashes, messages are locked and cannot be removed from QSA *Release All* button is under development to avoid this. Use the following workaround until it is deployed:

Open a DOS session and write

psql qsdb [hit Enter]

In the psql prompt write

update qs_messages set lock=NULL where lock is not NULL [hit Enter]

To close psql write

\q

Start Tomcat [hit Enter]

Blacklist/Whitelist List

If addresses you added to a Never Spam list still appear as suspected spam:

1. Have you created a Never Spam rule? For steps to create this rule, see "Using the Personal Blacklist/Whitelist Manager" on page 69.
2. If you have, check its ranking. The rule must rank higher than the spam rules or it will not send messages to the personal list.

Preventing an HTTP Attack on the Admin Server

Take the following steps to lock down your server(s) against this form of attack.

1. Make sure your Intranet is separated from the Internet with a firewall.
2. Configure MI to force the use of SSL. This denies all HTTP connection attempts.
3. Disable all non-essential services on the system(s) running MI.
4. On a UNIX system, use *ipchains*,
   OR
5. On a Windows 2000 system, use *TCP/IP filtering* to allow connections only to legitimate ports for MI services on that computer.
6. Protect the following services to defend incoming or outgoing data.

Service	Direction	Default Port
MP Adapter	in	6500
	out	vendor-dependent
Sendmail	in	5000
	out	5000
Admin Server—clients	in	8002
	out	8001
Admin Server—GUI	in	8000
	out	8000

If you are not using default ports, review your configuration files to determine what ports to lock down. Review your system documentation if your need help using the firewall tools.

Appendix B
Importing Data

If you do not use LDAP, you can still add users and domains by importing them from an external file, using either comma-delimited (*.csv*) or tab-delimited (*.tsv*) files. We recommend doing this when there are a large number of additions, making manual changes impractical.

There are two steps to importing data:

1. Create the import file,
2. Import the file into the appropriate attribute

Importing Users

1. Open a new file in an ASCII text editor such as Notepad.
2. Save the file with the extension .csv or .tsv, depending on whether you plan to use commas (*.csv*) or tabs (*.tsv*) to delimit the data.
3. Starting on the first line, type in the data in the format shown below. The examples show comma-delimited data.

   Imported users contain the following fields: FullName, EmailAddress.

Important: *Both the user name and the email address must be unique.The import of duplicates fail and return errors.*

Note: *MI imports only these two fields, not passwords or other user data.*

4. When you finish entering the data, save the file.
5. On the *Attributes* page, right-click **All Users > Import**.
6. Select the import file, then click **Open**.
7. You can now place imported users in groups on the *Attributes* page.

If there is any irregularity in the display of the data, go to the *Rules* page, click **Reset** on the menu bar, then select **Reload From Server**. All displays are refreshed with the most current data in the database.

Follow the same steps to import *.csv* or *.tsv* files to any Attributes folder.

Importing Domains

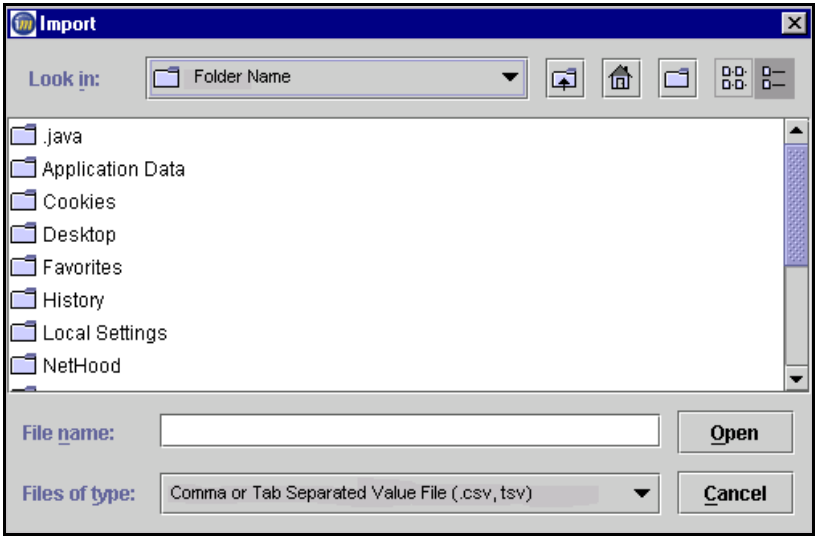
Imported domains contain only one field, *Domain*. For example, the first three lines of a Domain import file:

ourcompany.com
subsidiaryone.com
subsidiarytwo.com

When you finish entering the data, save the file.

Importing a File

1. Click **Policy > Attributes > Domains**
2. In the tree, right-click **Known Domains** and select **Import.**
3. Select the import file, then click **Open**.



4. The elements are now imported and ready to be placed on the *Attributes* tab. For details on how to incorporate your imported information, see "Attributes and Addresses" on page 37.

If there is any irregularity in the display of the data, go to the *Rules* page, click **Reset** on the menu bar, then select **Reload From Server**. All displays are refreshed with the most current data in the database.

Appendix C
Archiving and Restoring the MI Policy Database

You can archive and restore your MI policy using shell scripts we provide as part of the installation. These files are in the *Message Inspector/bin* directory on the drive where the program is installed.

Archiving

You can backup your policy database for MI or MI/AV with the *43dump_partial.sh* script. To do this:

1. Create the directory where you want to store the archives.
2. Copy *43dump_partial.sh* to this directory.
3. Double click the Cygwin icon on the desktop to open the shell.
4. Navigate to the archive directory.
5. Run the script by typing:

   ./43dump_partial.sh

   and pressing Enter.

Important: *This script overwrites any other database archive in the directory.*

Note: *This backs up your policy for MI or MI and AV. It does not save reporting data.*

Running the script stops MI services, dumps the database into the directory, and restarts the services.

Restoring

You can restore your archived policy database for MI or MI/AV with the *43restore_partial.sh* script. To do this:

1. Copy *43restore_partial.sh* to the archive directory you created.

2. Double click the Cygwin icon on the desktop to open the shell.
3. Navigate to the archive directory.
4. Run the script by typing:

   ./43restore_partial.sh

   and pressing Enter.

Running the script stops MI services, restores the archived files into the database, and restarts the services.

Appendix D
Backing Up Your Windows 2000 Configuration

Before performing any of the installation tasks, you may want to back up your current configuration. Message Inspector installation includes new services and a device driver, modifying the system. If you need to go back to your original configuration, you can choose it during a reboot if you follow the steps below:

Saving a Copy of Your Original System Configuration

1. Open **Settings > Control Panel** and double-click the **System** icon.
2. Select the **Hardware** tab and click **Hardware Profiles**
3. If you have only one configuration for your computer, *Profile 1 (Current)* will appear in the *Available Hardware Profiles* box.
4. Click **Copy**. Windows 2000 gives the copy the default name of *Profile 2*. Accept it or type in a new name. Click **OK** twice.
5. Now follow the installation steps in Chapter 2, *Installing Message Inspector,* on page 9.
6. When you are done and the service has loaded, go back into the *Control Panel*, and double-click the **Services** icon.
7. Scroll down until you see the *IM MTA* and highlight it.
8. Click the **HWProfiles...** button.
9. Highlight the **Original Configuration** and click **Disable**.
10. Repeat steps 7 through 9 for each of the Internet Manager services.
11. Highlight the other configuration (*Internet Manager*, in the example above), and click **Enable**. Click **OK**.

Now, when you reboot the computer, you can choose to load your original configuration without the Internet Manager services or the one you created with Message Inspector enabled.

Appendix E
Microsoft Exchange

AV can protect against viruses in internal Microsoft Exchange email. If you want to do that, read this chapter *before* following the instructions in "Installing Message Inspector" on page 9.

Important: *Do not install AV on the same server as Exchange.*

- Log into the same NT domain as the Exchange server, using an account with Administrator rights on both the Exchange server and the AV server. This requires that the AV server belong to the same NT domain as the Exchange server.
- Record the name and password used by the Exchange service. The account running the Exchange service must have administrator privileges on the AV server.
- Install MAPI with Microsoft Exchange Service support before installing AV.

Installing MAPI

Installing Microsoft Outlook (not Outlook Express) also installs MAPI with the Exchange service. The installation procedures depend on the Outlook version.

Outlook 97

Use **Typical install** or **Custom** with **Microsoft Exchange Service Support** selected.

Outlook 98

Use Minimal, Standard, or Full installation. On the *email Service Options* screen, select **Corporate** or **Workgroup**.

Outlook 2000

1. Use any installation. After the install, start Outlook to finish configuring MAPI.
2. At *email Service Options* select **Corporate** or **Workgroup**.
3. Select **Microsoft Exchange Server** information service.
4. After completing the configuration, start Outlook and at the prompt, make Outlook your default mail manager.

Important: *With Outlook 2000, it must be your default mail manager for AV to work with Exchange.*

Troubleshooting

This section covers problems that would cause AV to not monitor internal Exchange mail. Many involve reading the Exchange service log found in *Program Files\Elron Software\Internet Manager\CVBin\Exchange.txt.*

Unable to Locate DLL

Symptom

When the Internet Manager Common Gating Service is started, an *Unable to Locate DLL* dialog pops up referring to MAPI32.DLL.

Cause

MAPI is not installed.

Solution

- Install Outlook. See “Installing MAPI” on page 107.
- Select **Internet Manager Common Gating Service** from **Control Panel → Services**.
- Click **Stop**. Wait for the service to stop.
- Click **Start**.

The Information Store Could Not Be Opened (Case 1)

Symptom

The Exchange log contains *IMAPISession::OpenMsgStore() returned The Information Store could not be opened. (see MAPI 1.0:646) 0x80040111*.

Cause

The Internet Manager Common Gating Service is not running under the proper account.

Solution

- Select **Internet Manager Common Gating Service** from **Control Panel → Services**.
- Click **Startup**.
- Under *Log On As,* select the **This Account** checkbox.
- Enter the Exchange service account information under *This Account*.

- Click **OK**.
- If this fails with *Error 1057: The account name is invalid or does not exist*, the Internet Manager Server may not belong the Exchange server's NT domain. Add the AV computer to the correct domain and try again.

The Information Store Could Not Be Opened (Case 2)

Symptom

The Exchange log contains *IMAPISession::OpenMsgStore() returned The Information Store could not be opened. (see MAPI 1.0:646) 0x80040111*.

Cause

The Exchange server name is incorrect.

Solution

- Select **Control Panel → Mail** or **Mail and Fax→Show Profiles**.
- Select profile *Elron Internet Manager - Incorrect Exchange Server*.
- Click **Remove** and confirm removal in dialog.
- Close and run **REGEDT32**.
- Select the **HKEY_LOCAL_MACHINE\SOFTWARE\Elron Software\Parameters\ExchangeMP** key.
- Check value of *ServerName1* entry. This should be the NT name of the Exchange server. If not, edit it and close the Registry Editor.
- Select **Internet Manager Common Gating Service** from **Control Panel →Services**.
- Click **Stop**. Wait for the service to stop.
- Click **Start**.

Could Not Find Default Information Store

Symptom

Exchange log contains *Could not find default information store*.

Cause

The Internet Manager MAPI Profile is invalid.

Solution

- Select **Control Panel →Mail** or **Mail and Fax →Show Profiles**.
- Select profile *Elron Internet Manager - Incorrect Exchange Server*.

- Click **Remove** and confirm the removal in dialog.
- Close and run **REGEDT32**.
- Select the **HKEY_LOCAL_MACHINE\SOFTWARE\Elron Software\Parameters\ExchangeMP** key.
- Check value of *ServerName1* entry. This should be a Exchange mailbox with Exchange mailbox Administrator privileges. If not, edit it and close the Registry Editor.
- Select **Internet Manager Common Gating Service** from **Control Panel→Services**.
- Click **Stop**. Wait for the service to stop.
- Click **Start**.

This information Service Is Not Installed on Your Computer

Symptom

The Exchange log contains *Alert - IMsgStoreAdmin::CreateMsgService(): This information Service is not installed on your computer. To install it, use the Mail and Fax icon in the Control Panel. (see MAPI 1.0:1185) 0x004010F.*

Cause

The Microsoft Exchange Message Service was not installed with Outlook 97.

Solution

- Select **Control Panel →Add/Remove Programs**.
- Select **Microsoft Outlook 97** and click **Add/Remove**.
- In *Outlook Setup*, select **Add/Remove**.
- Select **Microsoft Exchange Server Support** and click **Continue**.
- Close *Add/Remove Programs* and open **Mail and Fax**.
- Select **Services → Add**.
- Select **Microsoft Exchange Server** and click **OK**.
- Enter the name of the Exchange Server click **OK**.
- Select **Internet Manager Common Gating Service** from **Control Pane→Services**.
- Click **Stop**. Wait for the service to stop.
- Click **Start**.

IMsgSTore::QueryInterface() returned 0x80004002

Symptom

The Exchange log contains *IMsgSTore::QueryInterface() returned 0x80004002*

Cause

The Microsoft Exchange Message Service was not installed with Outlook 98

Solution

- Select **Internet Manager Common Gating Service** from **Control Panel ➔Services**
- Click **Stop**. Wait for the service to stop.
- Close out of services and click **Add/Remove Programs**
- Select **Microsoft Outlook 98** and click **Add/Remove**
- Select **Add New Components**
- Select **Corporate** or **Workgroup email**
- Click **Next**, then **Install**.

MAPILoginEx() returned 0x80040005

Symptom

When Internet Manager Common Gating Service starts, a dialog with the message *Either there is no default mail client...* appears and the Exchange log contains *MAPILoginEx() returned 0x80040005*.

Cause

Outlook 2000 has not been run for the first time.

Solution

- Run Outlook 2000 and complete the configuration.
- Select **Internet Manager Common Gating Service** from **Control Panel ➔Services**.
- Click **Stop**. Wait for the service to stop.
- Click **Start**.

Could not get name of Exchange Server #1

Symptom

Exchange log contains *Could not get name of Exchange Server #1 (The system cannot find the file specified)*.

Cause

Incorrect value for *NumServers* in the Internet Manager Exchange registry or missing *ServerName#* entry.

Solution

- Run **REGEDT32**.
- Select the **HKEY_LOCAL_MACHINE\SOFTWARE\Elron Software\Parameters\ExchangeMP** key.
- Check value of *ServerName1* entry. There should be entries named *ServerName#* where # is a number between 1 and the value of NumServers. For example, if *NumServers* is 2, there should exist a *ServerName1* entry and a *ServerName2* entry.
- Run Outlook 2000 and complete the configuration.
- Select **Internet Manager Common Gating Service** from **Control Pane→Services**.
- Click **Stop**. Wait for the service to stop.
- Click **Start**.

Appendix F
File Types

MI supports over 250 types of files, categorized into the groups listed below. These files are not merely detected by the file extension, but by signatures in the files themselves.

Archive

- Compactor / Compact Pro Archive
- cpio Archive Format (UNIX/VAX/SUN)
- Disk Doubler Compression format
- GZ Compress Encapsulation
- Microsoft Windows OLE 2 Encapsulation
- PAK/ARC Archive format
- PKZip ZIP archive format PKWARE versions through 2.0g
- PEX Binary Archive (SUN)
- PGP Compressed Data
- Serialized Object Format (SOF) Encapsulation format
- Stuff It Archive (Mac)
- UNIX Compress Encapsulation
- UNIX SHAR Encapsulation
- UNIX TAR Encapsulation
- Wang Office GDL Header Encapsulation
- Windows C++ Object Storage

Database

- Ability DB
- ACT Format
- Comma Separated Values (CSV)
- dBase
- FileMaker (Mac)
- Informix SmartWare II Database
- Microsoft Access
- Microsoft Works Database (Mac)

- Microsoft Works Database (PC)
- Microsoft Works Database (Windows)
- MORE Database Outliner (Mac)
- Paradox (PC) Database
- Reflex Database

Email Body Text

The part of an email hat is not an attachment. This is valid for any type of encoding, including, HTML, multipart, MIME, uuencode, and base 64.

Executable File

- DLL
- EXE
- PC COM
- UNIX/VAX/SUN Executables

Graphics File

- Ability GR
- Adobe DCS
- AMI Pro Draw Graphics (SDW)
- Applix Graphics
- AutoCAD Drawing Exchange format (DXF) R13, R14, and R2000
- AutoCAD Drawing format (DWG) R13, R14, and R2000
- AutoDesk WHIP
- AutoShade Rendering
- Aldus Freehand Mac
- Aldus PageMaker (DOS, Mac)
- Computer Graphics Metafile (CGM)
- Corel CMX
- Corel Draw CDR (TIFF header) 2.x to 9.0
- Device Independent file (DVI)
- Encapsulated PostScript (TIFF header)
- GEM Bit Image
- Graphics Environment Manager (GEM VDI)
- Graphic Interchange Format (GIF)

- Harvard Graphics
- HP Graphics Language (HP-GL)
- JFIF File Interchange Format
- JPEG File Interchange Format
- KW ODA G31D Raster Image (G31)
- KW ODA G4 Raster Image (G4)
- KW ODA Internal G32D Raster Image (G32)
- KW ODA Internal Raw Bitmap (RBM) Raster Image
- Lotus Notes Bitmap
- Lotus Pic (PIC)
- Macintosh PICT (raster content)
- MacPaint (Macintosh) (PNTG)
- Micrografx Designer
- Microsoft Device Independent Bitmap
- Microsoft Office Drawing
- Microsoft Publisher
- Microsoft Windows Bitmap (BMP, RLE, CUR),
- Microsoft Windows Metafile (WMF) 3.0
- NeWS font file (SUN)
- PC PaintBrush (PCX)
- Portable Network Graphics (PNG)
- PostScript File
- Quark Express (Mac)
- Quick Draw Picture Format (PICT)
- QuickDraw 3D Metafile (3DMF)
- RIFF Device Independent Bitmap
- Sun Raster SGI RGB
- Tagged Image File (TIFF)
- Windows/Micrografx Draw (DRW)

Multimedia File

- Ability COM
- Amiga IFF (8SVX) Sound
- Amiga MOD Sound

- Audio Interchange File Format (AIFF) Sound
- AutoDesk Animator FLIC Animation
- Creative Voice (VOC) Sound
- Curses Screen Image (UNIX/VAX/SUN)
- Fax Systems (TIFF, CCITT, DCX) Groups 3 & 4
- ID3 versions 1 and 2
- Informix SmartWare II Communication File
- Keyword COM.FILE (KSIF)
- Lasergraphics Language
- Lotus Screen Cam
- Keyword OSM
- Keyword Viewer Markup Format
- Microsoft Enhanced Window Metafile
- Microsoft Wave Sound File
- Microsoft Works Communication (Mac)
- Microsoft Works Communication (Windows)
- MIDI Sound File
- MPEG Audio
- MPEG Movie
- MP3
- OS/2 PM Metafile Graphics
- QuickTime Movie
- Real Audio
- RIFF MIDI
- RIFF Multimedia Movie
- SGI Image
- SUN Audio Data
- Truevision Targa 2.0 (video, mm)
- Video for Windows
- VRML

Other File Types

- Apple Single/Double
- Decimal Hexadecimal--devel

- Framework
- Framework II
- FTP Session DataHP Printer Control Language (PCL)
- IBM 1403 Line Printer
- Keyword PICL
- KPIF Chart Stream
- MacBinary
- Microsoft Project 98, 2000, 2002
- PC True Type Font
- Plan Perfect
- SUN vfont definition
- Program Information File
- Q & A for DOS/Windows
- Simple Vector format (SVF)
- UNIX/VAX/SUN Link Library
- UNIX/VAX/SUN)Object Module
- Usenet format
- Windows Palette

Password Protected File

Microsoft Office password protected files

PGP Encrypted Email

Email encrypted using a PGP plug-in. PGP plug-in is available only for Netscape, Outlook Express and Eudora Pro.

Presentation Formats

- Adobe Portable Document Format (PDF): 40-bit encryption only.
- Applix Presents 4.3, 4.4
- Corel Presentations 5.x to 8.0
- E Persuasion Presentation
- Lotus Freelance Graphics for Windows 2.x, to Millennium Edition R9
- Macromedia Director (presentation
- Microsoft PowerPoint for Windows 4.x to 2002
- Microsoft Visio

S/MIME Encrypted Email

Email encrypted using the S/MIME standard.

S/MIME Signed Email

Email signed using the S/MIME standard.

Spreadsheet File

- Spreadsheet
- Ability SS
- Applix Spreadsheets 4.2, 4.3, 4.4
- DIF Spreadsheet
- ENABLE Spreadsheet
- Informix SmartWare Spreadsheet
- Lotus 1-2-3 Charts through 5.0
- Lotus 1-2-3 for SmartSuite 96, 97, Millennium Edition R9
- Microsoft Excel Charts 2.x to 7.0
- Microsoft Excel for Macintosh 98
- Microsoft Excel for Windows 3.x to 2002
- Microsoft Works Spreadsheet 1.x to 4.0
- Multiplan Spreadsheet
- PeachCalc Spreadsheet
- Supercalc Spreadsheet
- SYLK Spreadsheet
- Symphony Spreadsheet
- Ultracalc Spreadsheet
- Uniplex Ucalc Spreadsheet
- Quattro Pro for Windows
- Quattro Pro (DOS)

Word Processor/Text File

- Ability WP
- Adobe FrameMaker
- Adobe FrameMaker Markup Language
- Adobe Maker Interchange Format (MIF) 5.5, 7.0

- AES Multiplus Comm Format
- Alis word processor
- Applix Words 4.2, 4.3, 4.4, Asterix
- ANSI Text
- ASCII Text All versions
- COMET TOP Word
- Corel/Novell WordPerfect for Windows through 10.0
- Data Point VISTAWORD
- CPT Communication Format word processor
- DDIF word processor
- DECdx word processor
- DEC WPS PLUS
- DG CEOwrite word processor
- DG Common Data Stream (CDS) word processor
- Display Write 4 &5
- EBCDIC Text
- Enable word processor
- Envoy word processor (EVY)
- Folio Flat File 3.1
- Hewlett-Packard word processor
- Honey Bull DSA101 word processor
- HTML document
- IBM DCA-RFT word processor
- IBM DCF Script word processor
- IBM Display Write 4 word processor
- Informix SmartWare II word processor
- Interleaf word processor
- JustSystems Ichitaro 8.0, 9.0, 10.0, 12.0
- Lotus AMI Pro 2.0, 3.0
- Lotus Word Pro 96, 97, Millennium Edition R9 (Windows only)
- Lyrix word processor
- Lotus Notes CDF word processor
- MacWrite, MacWrite II word processor

- MASS-11 word processor
- Microsoft RTF All versions
- Microsoft Windows Write word processor
- Microsoft Word for Macintosh 4.x, 5.0, 6.0, 98
- Microsoft Word (UNIX) word processor
- Microsoft Word for Windows through 2002
- Microsoft Word Pad All versions
- Microsoft Works word processor through 6.0
- MultiMate 4.0 word processor
- Navy DIF word processor
- NBI Async Archive Format word processor
- NBI Net Archive Format word processor
- NIOS TOP word processor
- Novell WordPerfect for Linux 6.0
- Oasys 7.0
- Office Writer word processor
- ODA/ODIF (FOD 26) word processor
- ODA/ODIF word processor
- OLIDIF word processor
- Philips Script word processor
- PRIMEWORD word processor
- Quadratron Q-One (V1.93J, 2.0) word processor
- SAMNA Word IV word processor
- SGML document
- SMTP document
- Targon Word (V 2.0)
- Text Mail (MIME)
- Unicode Text All versions
- Uniplex (V6.01) word processor
- Volkswriter word processor
- WANG PC word processor
- Wang WITA word processor
- WANG WPS Comm. format word processor

- Word Connection word processor
- WordERA (V 1.0) word processor
- WordMARC word processor
- WordPerfect to 6.1
- WordPerfect General File Format /WPD format
- WordPerfect Graphics (WPG and WPG2) 1.0, 2.0, 7.0
- WordPerfect Mac word processor
- WordStar 2000
- WordStar 6.0
- WordStar word processor
- WriteNow word processor
- Writing Assistant word processor
- Xerox 860 Comm. format word processor
- Xerox Writer word processor
- XyWrite 4.12

Glossary

Action. The MI Action rule component determines what happens to a message. If the rule matches the parameters, the action runs on the message. Each rule specifies a policy action. See also Notification, and Policy Action.

Active Attack. An attack on a system that either injects false information into the system, or corrupts information already present on the system. See also Passive Attack.

ActiveX Controls. Software modules based on Microsoft's Component Object Model (COM) architecture. They can be linked to Web pages and downloaded by an ActiveX-compliant browser to perform like any other program launched from a server. ActiveX controls can have full system access. Most such access is legitimate, but some can be malicious.

Administrator. The user with full rights to the MI software. By default, all automatic reports and alerts go to the Administrator's email account, as specified during installation.

Alert. An automatic email message generated and sent by MI to the Administrator when a message triggers a rule whose Notification parameter specifies that an Alert be sent.

Algorithm. A sequence of steps needed to solve logical or mathematical problems. Certain cryptographic algorithms are used to encrypt or decrypt data files and messages and to sign documents digitally.

Always Spam. An MI option enabling you to automatically delete any message from a given source.

Ambiguity. Quality of having several meanings. In English, ambiguous words are understood only in the context of the full message.

Anti-Anti-Virus Virus. Anti-anti-virus viruses attack, disable or infect specific anti-virus software.

Anti-Virus Software. Program scans memory, drives or email for viruses. If it finds one, it may inform the user, and clean, delete or quarantine affected files, directories or disks.

Anti-Virus Virus. These locate and remove other viruses.

Applet. A miniature application, typically transported over the Internet as an enhancement to a Web page. Java applets are usually only allowed to access specified safe areas of the user's system.

Archive. Long-term storage for recorded statistics. MI uses separate databases for information longer than the time set in Report preferences. By default, records over two weeks old are sent to backup databases.

Armored Virus. An armored virus tries to prevent analysts from examining its code. The virus may use various methods to make tracing, disassembling and reverse engineering its code more difficult.

ASCII Files. Text files consisting of only ASCII characters. With effort, it is possible to write program files consisting only of printable characters (See EICAR Standard Anti-Virus Test File). Windows batch (BAT) files and Visual Basic Script (See Batch (.BAT) Files, and VBS) files are also typically pure text.

Because of the danger macro viruses pose, using ASCII files in email communications may by less risky. ASCII files can contain viruses, but they let you control both content and layout, ensuring email legible to most email programs.

Asymmetric Encryption. Encryption that permits the key used for encryption to be different from the key used for decryption. RSA is the most widely used asymmetric encryption algorithm.

Attack. An attempt to subvert or bypass a system's security. Attacks may be passive or active. Active attacks attempt to alter or destroy data. Passive attacks try to intercept or read data without changing it. See also Active Attack, Brute Force Attack, Denial Of Service (DoS), Hijacking, Password Attacks, and Password Sniffing.

Attribute.

1. Characteristics assigned to all files and directories. Attributes include: Read Only, Archive, Hidden or System.
2. In MI, a collection of domains or users that lets MI treat a number of addresses as a single entity.

Authentication. The process of assuring that data has come from its claimed source, or of corroborating the claimed identity of a communicating party.

Authorization. Determining whether a subject is trusted for a given purpose.

Availability. The prevention of unauthorized withholding of information or resources.

Back Door. An undocumented means of bypassing the normal access control procedures of a computer system. Programmers often build back doors to allow special privileges normally denied to users, for example to fix bugs. This is a security risk when hackers learn one. See also Back Orifice and Trapdoor.

Back Orifice. A remote administration tool with potential for malicious misuse. If surreptitiously installed, it gives system-administrator access over a network or the Internet. It can sniff passwords and other data, and then email them. See also Password Sniffing

Background Scanning. A feature in some anti-virus software to automatically scan files and documents as they are created, opened, closed or executed.

Background Task. A task executed by the system but generally remain invisible to the user. The system usually assigns background tasks a lower priority than foreground tasks. Some malicious software is executed by a system as a background task so the user does not realize unwanted actions are occurring.

Bad Sectors. During formatting of MS-DOS disks, all sectors are checked for usability. Unusable sectors are labelled as ‘bad’ and are not used by DOS. The remaining areas can then still be used. Viruses sometimes label good sectors as bad to store their code outside the reach of the users and the operating system.

Batch (.BAT) Files. Text files with an MS-DOS command on each line. Commands execute sequentially. If present, AUTOEXEC.BAT runs first when a computer boots.

BCC . An MI Notification action that sends an alert to specified user

Bell-LaPadula Model. An access security model couched in terms of subjects and objects. Information cannot not flow to a lesser or non-comparable classification.

Biba Model. An integrity model in which there can be no contamination by a less trusted or non-comparable subject or object.

Bimodal virus. A bimodal virus infects both boot records and files. See also Boot Sector Virus, File Viruses, and Multipartite Virus.

Block Cipher. A cipher that provides encryption and decryption by operating on a specified size of data block, e.g. 64 bits.

Boolean Logic. A system that addresses variables through the basic operators AND, OR, NOT (with others for certain purposes). MI filters use Boolean logic.

Boot Protection. Method used to prevent bypassing security measures installed on a hard disk by booting a computer from a floppy disk.

Boot Record. The program recorded in the boot sector. This record contains information on the characteristics and contents of the disk and information needed to boot the computer. If a user boots a PC with a floppy disk, the system reads the boot record from that disk. See also Boot Sector.

Boot Sector. The first track of a hard drive or floppy disk that contains information to load the rest of the operating system. A virus can infect it and from there spread to other drives when the computer boots. See also Boot Sector Virus and MAPS.

Boot Sector Virus. A type of computer virus that subverts the initial stages of the booting-up process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Brute Force Attack. An attack in which each possible key or password is attempted until the correct one is found. See also Attack.

Cavity Virus. A cavity virus overwrites a part of its host file without increasing the length of the file while also preserving the host's functionality.

CBC. Cipher Block Chaining, a mode of use of a block cipher.

CFB. Cipher Feedback, a mode of use of a block cipher.

Checksum. Calculated value from a file's data. A computer can compare the recorded checksum with the one it calculates to verify that a file has not changed.

Cipher. Encryption algorithm.

Ciphertext. A term used to describe text (or data) that has previously been encrypted. See also Encryption.

Clean. adj. Of a computer, file or disk that is free of viruses. Also, v. To remove a virus or other malicious software from a computer, file or disk. See also Disinfection.

Cluster Virus. Cluster viruses modify the directory table entries so the virus starts before any other program. The virus code only exists in one location, but running any program runs the virus as well. Because they modify the directory, cluster viruses may appear to infect every program on a disk. See also File Viruses.

Collocation. A collocation is group of words that occur together more often than is statistically probable and, therefore, highly indicative of a particular type of content. Collocations are very useful for content recognition.

COM File. In MS-DOS, the executable file's extension. These files cannot be larger than 64K and are typically utilities. Viruses can infect these.

Companion Virus. A virus with the same file name with a different extension as a benign program. Because MS-DOS tries to load .BAT files, then .COM files, and then .EXE files, a virus with a .COM extension can reside in the same directory as a legitimate program. Typically these viruses load from a command-line execution.

Compressed File. See File Compression.

Compromise. To access or disclose information without authorization.

Condition. Condition is an MI rule element containing the file name, size, type, and content required to trigger the rule.

Content Analysis. A language recognition tool that uses word frequency and the relative position of words within a sentence. Content

analysis operates on the meaning of the messages. See also Full Text Analysis (FTA).

Continue. Selecting the MI Rule parameter Continue enables MI to go on reviewing email for rule matches after its first match.

Cookies. Text files placed on a hard disk during Web-site access to identify users to the sites. It They may contain login, registration or shopping-cart information, or user preferences. They can be convenient or insecure depending on what information they store and communicate. Browser preferences can control cookie generation.

CRC. Cyclic Redundancy Check, a mathematical method for verifying the integrity of data. It is a form of checksum, based on the theory of maximum length polynomials. While more secure than a simple checksum, CRCs do not offer true cryptographic security. See also Cryptographic Checksum.

Cryptanalysis. The study of an encryption system, often with the intention of detecting any weakness in the encryption algorithm.

Cryptographic Checksum. A checksum calculated by using a cryptographically based algorithm. It is impossible to engineer changes to a file to leave a cryptographic checksum unchanged.

Deciphering. The same as decrypting. See Decryption.

Decryption. Decryption is the process of transforming ciphertext back into plaintext. It is the reverse of encryption.

Decryption Key. See Key.

Default Password. A password on a system when it is first delivered or installed.

Delete. An MI Policy action that prevents a message from reaching the recipient.

Deliver. An MI Policy action that allows a message through.

Denial Of Service (DoS). An attack to prevent normal functioning of a system and access to it by authorized users. Hackers can cause denial of service attacks by destroying or modifying data or by overloading the system's servers until service to authorized users is delayed or prevented. See Attack.

DES. Data Encryption Standard, an algorithm for encrypting or decrypting 64 bits of data using a 56-bit key.

Destination. In an MI rule, a set of addresses that MI compares with the destination address of a message to determine whether it matches the description provided by the rule.

Digital Signature. A means of protecting a message from denial of origination by the sender, usually involving the use of asymmetric encryption to produce an encrypted message or a cryptographic checkfunction.

Direct Action Virus. A direct action virus works immediately to load itself into memory, infect other files, and then to unload itself.

Disclaimer. Notice that MI can attach to incoming or outgoing messages. Generally, they contain text from an organization's usage policy and minimize legal liability.

Disinfection. Removal of virus by anti-virus software, and if possible, recovery of any affected data.

DNS. Domain Name System or Service, the distributed database used to translate human-readable Internet addresses into IP addresses. See also IP Address.

DOC File. A Microsoft Word or other word processor file with the extension.DOC. These files can have macros, which virus authors can use to infect computers. See also Macro.

Domain. A domain is an Internet domain address, a group of computers on a network. In MI, a domain can be a component of an attribute.

Downloading. A process where data transfer electronically from a host computer to another computer.

Dropper. A file that includes and installs a virus. Typically it is a .COM or .EXE file that does not replicate itself. See also Injector.

ECB. Electronic Code Book, a mode of use of a block cipher.

EICAR. European Institute of Computer Anti-Virus Research. In conjunction with several anti-virus software companies, EICAR has developed a test file for anti-virus software. See also EICAR Standard Anti-Virus Test File.

EICAR Standard Anti-Virus Test File. This text file consists of one line of printable characters. Anti-virus software should see it as a virus, even though it is benign. Saved as EICAR.COM and run, it displays: "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!" It is a safe way to test anti-virus programs.

Electronic Mail (email). Messages exchanged over a computer communications network.

Enciphering. See Encryption.

Encrypted Virus. An encrypted virus's code begins with a decryption algorithm and continues with scrambled or encrypted code for the remainder of the virus. Each time it infects, it automatically encodes itself differently, to try to avoid detection by anti-virus software.

Encryption. Scrambling or disguising information so it becomes difficult for an unauthorized person to unscramble and interpret.

Encryption Key. See Key.

Entry. A filter entry contains the actual content words, phrases, and file type specifications MI uses to identify the content of messages and files transmitted via Mail. Each entry must belong to a filter. See also Filter.

EXE. In MS-DOS, an executable file's extension. The can be larger than 64K, but are similar to .COM files. Viruses can infect these.

Exhaustive Key Search. Finding out which key an encryption system uses by testing all possible keys in turn.

False Hit.

1. In MI, a hit is false is an incorrect identification of message content. These can be false negatives and false positives. False negatives fail to categorize messages that the filter should have caught. A false positive categorizes a message by a filter that does not apply. MI's Full Text Analysis drastically reduces both types of false hits.
2. In AV, a false negative is failure to detect an infected file. A false positive reports a virus where there is none. Keeping AV signature files up to date minimizes false negatives of new virus types. False positives can occur when a string common in a specific virus appears in a benign file.

Fast Infector. When active in memory, these viruses infect both executed programs and those that are merely opened. Using a program, such as anti-virus software, that opens many programs but does not execute them, can result in all programs becoming infected. See also Slow Infector.

FDISK /MBR. In MS-DOS 5.0 or later, the command FDISK /MBR can remove viruses that infect the master boot sector but do not encrypt it. However, this command can cause unrecoverable damage.

File Compression. The compacting of a file through the process of recoding its bit structure into a shorter form. File compression must be reversible. See also ZIP File.

File Encryption. The transformation of a file's contents (in plaintext) into an unintelligible

form by means of some form of cryptographic system or manipulation.

File Integrity. Techniques used to provide safe backup files for recovery purposes in the event that critical files have become contaminated through some accidental or intentional mechanism (e.g. virus attack).

File Labelling. The classifying of the sensitivity level of a file either by external (visible outside marking) or internal (magnetic coding of the header label) coding, or by both.

File Viruses. File viruses usually replace or attach themselves to COM and EXE files. They can also infect files with the extensions SYS, DRV, BIN, OVL and OVY. They may be non-memory-resident, but the most common are TSR viruses. Many non-resident viruses simply infect one or more files whenever an infected file runs.See also Parasitic Virus and TSR.

Filter. A filter is the MI component of a rule that supplies the information needed to make the rule sensitive to a particular type of content and file types. Filters group together all the entries designed to recognize the particular type of content. For example, entries that specify content words and phrases relating to baseball might belong to a *Baseball* filter. Also, a filter may contain sub-filters in addition to entries. See also Entry and Sub-Filter.

Full Text Analysis (FTA). MI's language recognition tool, FTA uses computational linguistics, information retrieval, text mining, and lexicography to complement content analysis. The core of the product is MI's three proprietary, patented or patent-pending technologies: Automatic Collocation Identification, Automatic Statistics-Based Spam Detection, and Statistical Dynamic Ranking. See also Content Analysis.

Good Times. See Virus Hoaxes

Hacker. Someone who breaks into a computer or network, usually with malicious intent. The original meaning was of a computer expert or enthusiast.

Hash Function. A function that maps a set of variable size data into objects of a single size. Widely used for fast searching.

Hashing. The process of calculating a hash function.

Heuristic Analysis. Behavior-based analysis of a computer program by anti-virus software to identify a potential virus. Heuristic scanning can produce false alarms when a clean program behaves as a virus might.

Hijacking. An attack in which an active session is intercepted. Hijacking can occur locally when a logged-in user leaves a computer unprotected. Remote hijacking can occur via the Internet.

Hit. In MI, a word or phrase in a message that matches a content definition keyword or phrase and triggers the rule action.

Hole. Vulnerability in the design of oftware or hardware that allows circumvention of security.

Host. In anti-virus, the file to which a virus attaches itself.

HTTP. Hyper-Text Transport Protocol, built on top of TCP, this protocol is used by Web servers to serve documents to Web browsers.

IDE. The extension given to a file containing a virus identity encoded with Sophos's Virus Description Language (VDL). An IDE appears as an ASCII string.

In The Wild. A virus is in the wild if it is verified as having caused an infection outside a laboratory situation. Most viruses are in the wild and differ only in prevalence. See also In The Wild and Zoo Virus.

Infection. The action a virus carries out when it enters a computer system or storage device.

Injector. See Dropper

Integrity. A security protection aimed at ensuring that data cannot be deleted, modified, duplicated or forged without detection.

IP. Internet Protocol, the base level of the TCP/IP system, is a specification for addressing and data packets. By itself, IP treats each packet separately and does not establish a connection between two computers. It normally combines with TCP for Internet communications. See also TCP.

IP Address. A numeric Internet address, a 32-bit binary number, normally written in dotted-decimal notation, e.g. *192.168.145.1*.

IP Range. This consists of a low and a high IP address and all addresses between. It is a useful way to specify a subnet.

IV. Initialization Variable, a value used to initialize modes of use of certain block ciphers.

JavaScript. A scripting language for interactive Web sites. It can run with an interpreter such as Web browser or server, or the Windows Scripting Host. A Web page with JavaScript runs within a Web browser in much the same way as Java applets and does not have access to host machine resources. An Active Server Page (ASP) or a Windows Scripting Host (WSH) script containing JavaScript is potentially hazardous. These give scripts unrestricted access to resources such as the file system and registry and application objects.

Joke Programs. These are not viruses, but may contain a virus if infected or otherwise altered.

KDC. Key Distribution Centre, a central system for the generation and distribution of encryption keys. A KDC ensures that in cases where a large number of systems need to talk to each other, they do not need to share a unique key between each pair of systems.

KEK. Key Encrypting Key, a key that is used exclusively for the encryption of other encryption keys.

Key.

1. In Windows Registry, a key stores computer or software configuration settings. Viruses can modify these keys and harm the computer.
2. In encryption, the numbers or characters that an algorithm uses to encrypt or decrypt data.

Key Gun. A device for the secure transport of encryption keys from the point of generation to the point of application.

Key Management. The process of securely generating, transporting, storing and destroying encryption keys.

Key Space. All the possible keys that can be used by an encryption algorithm.

Keystream Generator. A system that generates keys continuously.

Keystream Sequence. The output of a keystream generator.

KTC. Key Translation Centre, a central system that can receive an enciphered encryption key, decipher it and re-encipher it under a new key.

LAN. Local Area Network, a data communications network covering a limited area (up to several kilometers in radius) with moderate to high data transmission speeds.

Letter Bomb. A logic bomb contained in electronic mail, which will trigger when the mail is opened. See also Logic Bomb.

Lexicography. The study and practice of building dictionaries.

Lightweight Directory Access Protocol (LDAP). A protocol for accessing online directory services. The directory entry is a collection of attributes with name, type and one or more values.

Limbo. A location in MI's Quarantine Server that holds messages for further review until the default deadline date.

Link Virus. A virus that subverts directory entries to point to the virus code.

Log. A log is a report of system errors. In MI, the log threshold determines the level of detail stored in the logs.

Logic Bomb. A Trojan horse that some date, set of keystrokes or other condition triggers to execute.

Macro. Many software products allow their data files to contain instructions to carry out program commands automatically. These instructions are often called macros, and they generally allow access to a substantial range of functions such as the opening, manipulating and closing of files.

Macro Virus. A virus that uses macros in a file to become active in memory and attach itself to other files. Unlike conventional viruses, macro viruses are easy to write and can also attain a degree of platform independence.

Mailbomb. Excessively large email (typically many thousands of messages) or one large message sent to a user's email account, for the purpose of crashing the system, or preventing genuine messages from being received. Also, a verb, to send a mailbomb.

Malicious Code. A piece of code designed to damage a system or the data it contains, or to prevent the system from being used in its normal manner.

Malware. A generic term used to describe malicious software such as: viruses, trojan horses, malicious active content, etc.

MAPS. Mail Abuse Prevention System, a not-for-profit organization monitoring email abuse. Subscribers use MAPS databases to enhance their email filtering policies.

Master Boot Record. The 340-byte program in the master boot sector. This program reads the partition table, determines what partition to boot and transfers control to the program stored in the first sector of that partition. There is only one master boot record on each physical hard disk. See also Boot Record.

Master Boot Sector. The hard drive's first sector, which loads when a computer boots. Viruses can infect this and interfere with loading the active partition or do other damage. See also MAPS.

Master Boot Sector Virus. Master boot sector viruses infect the master boot sector of hard disks, though they spread through the boot record of floppy disks. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy disk DOS accesses. See also Boot Record.

Meet-in-the-Middle Attack. A cryptographic attack based on an optimized exhaustive search.

Memory-Resident Virus. This remains in a computer's memory after execution. Typically, it will perform its malicious actions when certain conditions occur, such as a specific program loading. See also TSR.

Message Authentication. The process of calculating and then verifying a message authentication code.

Message Digest. Same as hash function.

Message Processing Client. A computer, dependent on the Administration Server, that can see MI traffic. The message processing client uses the same policy as the administration server to handle a specified subset of email messages.

Mirroring.

1. A technique where data are written to two or more disks simultaneously, with the

intention of enabling data retrieval even when one of the disks fails.

2. When a network device, such as a switch, duplicates traffic from a source port on another port.

Mode of Operation. A set of rules that defines a particular way in which an encryption algorithm should be used.

MP3 File. Moving Picture Experts Group Audio Layer 3 File, a highly compressed audio track, very popular on the Internet. MP3 files are not programs, and viruses cannot infect them. This file type has the extension MP3.

Multipartite Virus. These can infect boot sectors, documents and executable files. Typically they start in memory and spread to the boot sector. They may infect the entire hard drive. Repair can be a time-consuming chore of removing a computer from its network, booting from a floppy containing a repair disk, and cleaning both the boot sector and then all infected files.

Mutating Virus. A mutating virus changes, or mutates, as it progresses through its host files making disinfection more difficult. Some experts also include non-intentionally mutating viruses. See also Polymorphic Virus.

Never Spam. An MI option enabling you to automatically deliver any messages from a selected source.

Notification. In MI, this refers to the reports, alerts and messages generated when a message violates the policy. Each rule can contain a notification option.

Notify. An MI Notification action that sends an alert to the sender or recipient.

Not In The Wild. Viruses not in the wild are in the real world but fail to spread successfully. See also In The Wild and Zoo Virus.

OFB. Output Feedback, a mode of use of a block cipher.

On-Access Scanner. A real-time virus scanner that scans disks and files automatically and often in the background. An on-access scanner scans files for viruses as the computer accesses the files.

On-Demand Scanner. A virus scanner the user starts manually. Most on-demand scanners allow the user to set various configurations and to scan specific files, folders or disks.

One-Way Function. A function that can readily be calculated, but whose inverse is very difficult to calculate. The knowledge of the result does not allow anybody to determine the parameters used to produce that result.

Overwriting Virus. This type copies its code over its host file, destroying the original program. Disinfection is possible, but files cannot be recovered. It is usually necessary to delete the original file and replace it with a clean copy.

Parasitic Virus. A computer virus that attaches itself to another computer program, and is activated when that program is executed. A parasitic virus can attach itself to either the beginning or the end of a program, or it can overwrite part of the program.

Passive Attack. An attack on a system that extracts information and makes use of it, but never injects false information or corrupts any information, which would be an active attack.

Password. Sequences of characters that allow users access to a system. Although they are supposed to be unique, experience has shown that most people’s choices are highly insecure. People tend to choose short words such as names, which are easy to guess.

Password Attacks. Attempts to obtain or decrypt a legitimate user's password. Hackers can use password dictionaries, cracking programs, and password sniffers in such attacks. Limited defenses include a password policy with minimum length, unrecognizable words and frequent changes. See also Password Sniffing.

Password Sniffing. The use of a sniffer to capture passwords as they cross a network. The network could be a LAN or the Internet. The sniffer can be hardware or software. Most sniffers are passive and only log passwords which the attacker anlayzes. See also Sniffer.

Payload. Either the effects produced by a virus attack or a virus associated with a dropper or Trojan horse.

Pest Program. A collective term for programs with deleterious and unanticipated side-effects, e.g. Trojan horses, logic bombs, viruses, and malicious worms.

PGP. Pretty Good Privacy, a strong program for encrypting data files and email. PGP includes authentication to verify the sender of a message and non-repudiation to prevent someone denying they sent a message.

Piggyback. Gain unauthorized access to a system via an authorized user's legitimate connection.

Plaintext. Data before it has been enciphered. The opposite of ciphertext.

Polyalphabetic Cipher. An encryption algorithm in which every letter in the plaintext is substituted with a different letter in the ciphertext.

Policy. An MI policy is the set of all rules ranked numerically. It represents a specific treatment of email traffic.

Policy Action. See Action.

Polymorphic Virus. These encrypting viruses try to avoid detection by making varying copies of themselves. From one computer to another, they can appear quite different. Some can mutate and alter their virus code. See also Mutating Virus.

Program Infector. A program infector virus infects other program files when an infected application executes and an activated virus loads into memory.

Proprietary Encryption Algorithm. An encryption algorithm designed to a proprietary, usually secret specification.

Quarantine . In MI, an application that isolates for further review messages that violate a rule.

Rank. The relative importance of an MI rule. Because messages may trigger only one rule, they are checked in rank order, from highest to lowest. MI checks the rule with rank *1* first. See also Continue.

Real-time Scanner. An anti-virus software application that operates as a background task, allowing the computer to continue working at normal speed, with no perceptible slowing. See also On-Access Scanner.

Redirect. The action used by some viruses to point a command to a different location. Often this different location is the address of the virus and not the original file or application.

Rename. The action by which a user or program assigns a new name to a file. Viruses may rename program files and take the name of the file so that running the program inadvertently runs the virus. Anti-virus programs may rename infected files so the are unusable until manually cleaned or deleted.

Replication. The process by which a virus makes copies of itself to carry out subsequent infections. Replication is one of major criteria separating viruses from other programs.

Reportable. An MI rule parameter. Enable *Log for reporting* to generate reports from a rule.

Resident Extension. A resident extension is a memory-resident portion of a program that remains active after the program ends. It essentially becomes an extension to the operating system. Many viruses install themselves as resident extensions.

Resident Virus. A resident virus loads into memory and remains inactive until a trigger event. When the event occurs the virus

activates, either infecting a file or disk, or causing other consequences. All boot viruses are resident viruses and so are the most common file viruses.

Reviewer. In MI, the administrator designates reviewers to perform quarantine functions. See also Super-Reviewer.

Rogue Program. Software intended to damage programs or data or to breach a system's security. This includes Trojan Horses, logic bombs, and viruses.

RSA. An asymmetric encryption algorithm, invented by Rivest, Shamir and Adleman in 1976. Unlike DES, the RSA algorithm can be implemented using any number of bits.

RTF File. Rich Text Format File, an alternative format to the DOC file type. RTF files are ASCII text files with embedded formatting commands. RTF files do not contain macros and cannot be infected with a macro virus. However, some macro viruses attempt to intercept saving a file in RTF and instead save it as a DOC file with an RTF extension. See also DOC File.

Rule. In MI, the basic operational unit of the policy. It specifies conditions on the source and destination address, network service, time, file type, and content of network transmissions. Each rule has a ranked position. A message that matches the conditions set by the rule triggers the rule if the rule has the highest priority of all the rules that it matches. A rule specifies policy and report actions MI takes on the message.

Scrambling. See Encryption.

Scanner. A program that searches for viruses. See Anti-Virus Softwareee, On-Access Scanner, and On-Demand Scanner.

Secret Key. Encryption key that must not be disclosed. If it is revealed, the security offered by the encryption algorithm is compromised. Not all encryption keys have to be kept secret, e.g. public keys in asymmetric encryption.

Sector Viruses. See Boot Sector Virus and Master Boot Sector Virus.

Secure Socket Layer (SSL) . A protocol for managing message -ransmission security. Most Web browsers and servers have SSL. It uses a public/private-key encryption system. Before enabling SSL for MI, you must have a digital certificate and private key pair from a trusted Certificate Authority (CA). See “Enabling SSL for the GUI” on page 20.

Self-Encrypting Virus. Self-encrypting viruses attempt to conceal themselves from anti-virus programs. Most anti-virus programs try to identify signatures unique to each virus. Self-encrypting viruses encrypt these text strings differently with each infection to avoid detection. See also Encrypted Virus and Self-Garbling Viruses.

Self-Extracting Files. These decompress into one or more parts when executed. Some anti-virus products cannot search self-extracting file components. To scan these components, they must first extract the files and then scan them.

Self-Garbling Viruses. A self-garbling virus attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way their code is encoded so that anti-virus software cannot find them. A small portion of the virus decodes the garbled portion when activated. See also Polymorphic Virus and Self-Encrypting Virus.

Sensitivity. In MI, how selective the entry is concerning keywords found in a scanned document. If it is highly sensitive, even a message that does not match very closely is likely to be detected. If it is not very sensitive, a message must closely match the entry to be detected.

Shift. A shift is an MI rule component that defines the hours of the day and the days of the week that the rule is in effect.

Signature. A search pattern, often a simple string of characters or bytes, expected to be found in every instance of a particular virus or spam message. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses. See also Virus Signature.

Slow Infector. Slow infectors are active in memory and only infect new or modified files. See also Fast Infector

SMTP. Simple Mail Transfer Protocol, designed to send email messages between servers. Many Internet email systems use SMTP between servers. Refer to RFC 1123 for full details.

Sniffer. A software program that monitors network traffic. Hackers use sniffers to capture data transmitted via a network.

Source. In an MI rule, source refers to a set of addresses that MI compares with the source address of a message in determining whether it matches the description provided by the rule.

Spoofing. Pretending to be someone or something else (e.g. entering someone else's password).

Spam. Unsolicited, junk email, generally advertising of some sort.

Spam Summary. Daily report emailed to specified administrator address, containing a list of the last 24-hours of spam messages. Configure when MI generates the summary and where it send it on the System screen.

Sparse Infector. A sparse infector viruses use conditions before infecting files. Examples include files infected only on the 10th execution or files that have a maximum size of 128kb. These viruses use the conditions to infect less often and therefore avoid detection.

Stealth Viruses. These trap interrupt and disk-access requests to hide themselves. This can mean that anti-virus software cannot see that file size has changed.

Stream Cipher. A cipher that provides encryption and decryption by operating on a continuous stream of data, without imposing limits on the length of the data.

String. A consecutive series of letters, numbers, and other characters. *afsH(*&@~* is a string, as is *Mad Hatter*. Anti-virus applications often use specific strings (signatures) to detect viruses. See also Signature.

Sub-Filter. A sub-filter is a filter that is included in another filter. See Filter.

Super-Reviewer . A super reviewer can review all quarantine messages regardless of type and subject, and evaluate decisions of reviewers with limited rights. See also Reviewer.

Symmetric Algorithm. An algorithm in which the key used for encryption is identical to the key used for decryption. DES is the best known symmetric encryption algorithm.

SYS. The extension given to system file names in MS-DOS. An example is the file CONFIG.SYS that sets up various configuration parameters for the operating system on power-up.

System Boot Record. See Boot Record.

Tag. A Notification action that allows the message through and adds a descriptive term (such as *Suspected Spam*) to it.

TCP. Transmission Control Protocol, a reliable, connection-oriented service on top of IP. It allows two computers to establish a connection, and then guarantees that data packets arrive and in the order sent. See also IP.

TCP/IP. Transmission Control Protocol/Internet Protocol, the collective name for the standard Internet protocols, even though they contain more than TCP and IP.

Time Bomb. A logic bomb set to trigger at a specific date or time. See also Logic Bomb.

TOM. Top of Memory. A design limit at the 640kb-mark on most PCs. Often the boot record does not completely reach top of memory, thus leaving empty space. Boot sector infectors often try to conceal themselves by hiding around the top of memory. Checking the top of memory value for changes can help detect a virus, though there is also non-viral reasons this value change.

Trapdoor. A hidden flaw in a system mechanism that can be exploited to circumvent the system's security. See also Back Door.

Triggered Event. An action built into a virus set off by a specific condition. Examples include a message displayed on a specific date or reformatting a hard drive after the tenth execution of a program.

Trojan Horse. A malicious program that appears useful or benign. While technically not viruses, Trojans can be destructive.

TSR. Terminate and Stay Resident, of a program that remains in memory after execution. Some TSR viruses are remain to infect programs or files. See also Memory-Resident Virus.

Tunneling. A virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system actions before the OS can execute a virus. Tunneling viruses try to intercept the actions before the anti-virus software can detect the malicious code.

UDP. User Datagram Protocol, essentially IP with port numbers and checksums for data integrity. Used for simple protocols where the overhead of TCP is too great.

Uploading. The process of transferring data from a remote computer to a central host.

URL. Universal Resource Locator, a World Wide Web address.

User. In MI, a name given to an email address. The user name may be a component of an attribute.

Vaccination. A technique of some anti-virus programs to store information about files to notify the user about file changes. Internal vaccines store the information within the file itself, while external vaccines use another file to verify the original for possible changes.

Variant. A modified version of a virus. Usually produced on purpose by the virus author or another person amending the virus code. If changes to the original are small, most anti-virus products will also detect variants. However, if the changes are large, the variant may go undetected by anti-virus software.

VBS. Visual Basic Script, a programming language that can invoke any system function, including starting, using and shutting down applications, without user knowledge. VBS programs can be embedded in HTML files and provide active Web-page content. Users should be careful about changing security settings without understanding the implications. This file type has the extension VBS.

VDL. Virus Description Language, a proprietary Sophos language used to describe virus characteristics algorithmically. It has extensive facilities to cope with polymorphic viruses.

Virus. A program that infects a computer's operating system, files, memory or drives. It usually copies makes copies of itself and has undesirable effects. See also Boot Sector Virus, Companion Virus, File Viruses, Link Virus, Macro Virus, Multipartite Virus, and Parasitic Virus.

Virus Hoaxes. Hoaxes are not viruses, but are usually deliberate or unintentional email warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by massive amounts of unnecessary email. Sometimes hoaxes start out

as viruses and some viruses start as hoaxes. Both should be considered threats.

Virus Identity. An algorithm describing various characteristics of a virus and used for virus recognition. Sophos describe viruses using the proprietary Virus Description Language (VDL).

Virus Mutation. A version of Polymorphic Virus.

Virus Pattern. A sequence of bytes extracted from a virus and used for virus recognition.

Virus Signature. An identifier recognized by the virus as meaning 'this item is already infected, do not reinfect'. It can take different forms such as the text *sURIV* at the beginning of the file, the size of the file divisible by a number, or the number of seconds in the date stamp set to 62. Some viruses do not recognize their signatures correctly.

Web. See World Wide Web (WWW).

Web Browser. The client side of the World Wide Web, the program used to access information on the Web.

Web Server. A computer connected to the Internet that serves Web documents, generally using HTTP.

Windows Scripting. Windows Scripting Host (WSH), a Microsoft integrated module that lets programmers use any scripting language to automate operations throughout the Windows desktop.

World Wide Web (WWW). A distributed hyper-text system for the reading of documents across the Internet. World Wide Web documents are generally written in HTML and served by Web servers using the HTTP protocol.

Worm. Files that do not infect executables but replicate themselves. They can spread throughout a single computer or through a network or the Internet to others. They often transfer by Internet Relay Chat (IRC).

Worm Attack. Interference by a program that is acting beyond normally expected behavior, perhaps exploiting security vulnerabilities or causing denials of service. See also Worm.

X-Header. Custom email header content, marked by the prefix *X-*. In MI, the X-Header Notification action applies an x-header to email, directing that it be acted upon without judging it spam or non-spam.

XOR. An abbreviation of the logical operation known as Exclusive-or. An exclusive-or function is defined as having the value true when either of the input conditions (but not both) is true.

ZIP File. A form of archive. It contains compressed collections of other files. A ZIP file can contain viruses if any of the files packaged in it contain viruses, but by itself is not directly dangerous. Other archive files include RAR, and LHA files. This file type has the extension ZIP.

Zoo. A collection of viruses used for testing by researchers. See also In The Wild.

Zoo Virus. A zoo virus exists in the collections of researchers and has never infected a real world computer system. See also In The Wild.

Index

A

action
- definition 123

actions
- configuring 53
- deleting 55
- description 29
- designing customized 38
- modifying 54
- notification action 41, 53
- policy action 53

add
- global blacklist/whitelist entry 72

address
- add to global blacklist/whitelist 72

administration server
- settings 83

administrator
- definition 123

alert
- definition 123

always spam
- definition 123

ambiguity
- definition 123

Anti-Virus 34

archive
- definition 124

attachments
- selecting for conditions 50

attribute elements
- working with 45

attributes
- configuring 42
- definition 124
- designing customized 37
- domain or user attribute
  - creating 43
- domains 44
- elements
  - deleting 45
  - importing 46, 101
  - modifying 45
- importing
  - importing a file 102
- users 44
- with LDAP 46

AV client
- requirements 10

B

backing up NT 105

bcc
- definition 124

Blacklist 34, 69

blacklist/whitelist 69
- address management 70
- personal 69
- rules 64

blacklist/whitelist manager
- directing messages to 69
- manual entries 71

blacklist/whitelisttroubleshooting 99

blocking spam 64

bold type in guide 7

Boolean logic
- definition 125

C

circled numbers
- in illustrations 7

client
- operating system 10
- requirements 10

collectors
- installing multiple 15

collocation
- definition 125

condition
- definition 125

conditions 29
- creating 49
- deleting 51

designing customized 37
configuration
actions 53
attributes 42
conditions 48
disclaimers 55
domain 44
filters 51
MTA 15
shifts 46
source and destination 42
users 44
content analysis 1
definition 125
continue
definition 126
conventions in guide 7
Creating 52
creating a new rule
from defaults 39
with the wizard 40
custom policy
creating 37
planning rules 37–39

D

daily reporting and alert settings 85
default information store error message 109
default rules
description 31–32
delete
definition 126
global blacklist/whitelist entry 72
deleting
actions 55
disclaimers 56
deliver
definition 126
destination 42
definition 126
disclaimer
definition 126
designing customized 38
disclaimers
configuring 55
creating 55
deleting 56
modifying 56
DLL error message 108
domain
add to global blacklist/whitelist 72
definition 126
domains
importing data from file 102

E

email
addresses in a domain 44
attachment types 50
for individual users 44
encryption 50
entry
definition 127
error message
default information store 109
DLL 108
IMsgSTore 111
information store 108
MAPILoginEx 111
name of Exchange Server 112
error messages
Exchange 108
Exchange
error messages 108
installing MAPI 107
troubleshooting 107, 108

F

false hit
definition 127
file types
definitions 113
in conditions 50
filter
definition 128
filters
creating for confidential content 60
deleting 52
designing customized 37
modifying 52
spam 31, 63
FTA

definition 128
entries
editing with MI 62
see full text analysis
full text analysis
definition 128
engine 1
customizing 57

G

global blacklist/whitelist
managing 72
glossary of terms 123

H

hit
definition 128
false
definition 127
HTTP attack
preventing 99

I

illustrations with circled numbers 7
importing
attributes
elements 101
domains 102
file 102
users 101
importing data
attributes
elements 101
importing domains 102
users 101
IMsgSTore error message 111
information store error message 108
installation
backing up Windows 2000 before installing 105
enabling LDAP after 15
MAPI 107
Message Inspector 9
MI components 10, 13
modifying MI components 24
MTA configuration 15
quarantine server 11
requirements 10
troubleshooting 24
installing
multiple collectors 15
internal email
monitoring 21
IP addresses
installation 15
IP range
definition 129
IP ranges
definition 129

L

LDAP
see lightweight directory access protocol
levels of information reporting 83
lexicography
definition 129
license usage
opening from manage menu 81
Lightweight Directory Access Protocol
definition 129
lightweight directory access protocol 2
enabling MI for 15
updating and reloading from MI 17
limbo
definition 130
log
definition 130
login 25
using the administration client 25
using the web browser 26
logs
system 86
Lotus Domino 2
requirements for tracking 22, 24
setup 22, 24

M

mail
routing 18
mail transfer agent 9
configuring 81
main menu
manage menu

license usage 81
MTA configuration 81
policy 81
system 82
logs 86
manage menu
summary 33
managing
global blacklist/whitelist lists 72
MAPI
installing 107
MAPILOGinEx error message 111
MAPS
definition 130
Message Inspector
blacklist/whitelist manager 69
description of functionality 3
embedded MTA 13
IM and MI services
stopping or starting 86
installing 9, 10, 13
planning 9
requirements 10
interface 25
login 25
managing 81
modifying
uninstalling 24
new features 1
placement 10
quarantine server 34, 73
reporting 89
report types 89
selecting reports 89–93
system management 82
Message Inspector. See also MI
message processing client
definition 130
messages per page
quarantine server 75
Microsoft Exchange 2
error messages 108
installing MAPI 107
troubleshooting 107, 108
modifying
actions 54
monitor and control mode
requirements 12
MTA
configuration 15
see mail transfer agent

N

name 28
name of Exchange Server error message 112
network
placement
monitor and control 12
never spam
definition 131
notification
action 3
definition 131
notification action 41, 53
notify
definition 131
numbers in illustrations 7

O

objects to be audited 83
offensive material
categories 53
how to block 29
rule 31
operating system
client 10
overview
of Message Inspector 1

P

policy
creating custom 37
definition 132
enabling quarantine-server reviewers 73
opening from manage menu 81
operation 3
policy action 3, 53
definition 132

Q

quarantine
definition 132
enabling reviewers 73

quarantine server 2, 34, 73
administration
adding reviewers 78
modifying reviewers 79
administrator window 78
enabling reviewers 73
input message page 75
installing 11
limbo
definition 130
limbo page 77
output box 77
reviewer window 74
user settings 75

R

rank 28
definition 132
report all rule 32
report system maintenance 85
reports/alerts from name 83
reports/alerts return address 83
requirements
AV client 10
requirements for installation 10
reviewer
definition 133
reviewers
enabling 73
routing mail
to the MI/AV server 18
rules
blacklist/whitelist 64
components 28–30
action 29
actions 53
condition 29
conditions 48
continue 30
disclaimers 55
filters 51
sub-filters 51
name 28
rank 28
reportable 30
shift 29
shifts 46
creating
new rule from defaults 39
new rule from the wizard 40
default 31
offensive material 31
report all email 32
definition 133
deleting an existing rule 41
designing customized 38
modifying an existing rule 41
saving changes 41

S

secure socket layer
definition 133
implementing with MI 19
sensitivity
definition 133
server configuration
minimum requirements 10
placement of the Administration Server 10–12
services
IM and MI
stopping and starting 86
settings
administration server 82
shift
definition 134
deleting 48
shifts 29
creating 47
designing customized 37
SMTP
server setting 83
SMTP domain
installation 15
SMTP server
installation 15
Sophos Anti-Virus 34
source 42
definition 134
spam
blacklist/whitelist 2, 64
address management 71
blacklist/whitelistmanager 69

blocking 64
default spam rule
changing 64
definition 134
engine 2
filters 31, 63
individual spam management
blacklist/whitelist manager 69
management 63
never spam 31
planning for in your policy 64
rule 31
tag action 64
tagging 64
SSL
definition 133
see secure socket layer
sub-filter
definition 134
sub-filters 51
super-reviewer
definition 134
super-reviewers
enabling 73
support 24
system
admin users 86
logs 86
requirements 10
system page 82
administration server node 82
administration server settings 82
MI product node 85

T

tag
definition 134
tech support 24
troubleshooting
blacklist/whitelist 99
cygwin
uninstalling older versions 97
Exchange 107, 108
installation 24
MI login fails 97
MI policy 98
type conventions 7

U

Unable to Locate DLL
message 108
uninstalling
adding components
reinstalling 24
user
definition 135
user settings
quarantine server 75
users
admin users 86
importing 101

W

Windows 2000
backing up configuration 105

X

x-header
definition 136