CLEARSWIFT
MIMEsweeper™
Simplifying content security

MIMEsweeper™ for SMTP

5.3

Reference

Revision 4.2

Revision 4.2, June 2008
Published by Clearswift Ltd.

Information in this document may contain references to fictional persons, companies, products and events for illustrative purposes. Any similarities to real persons, companies, products and events are coincidental and Clearswift shall not be liable for any loss suffered as a result of such similarities.

Users should ensure that they comply with all national legislation regarding the export, import, and use of cryptography.

Clearswift reserves the right to change any part of this document at any time.

CLEARSWIFT
MIMEsweeper™
Simplifying content security

AMERICA

United States
Clearswift Corporation
100 Marine Parkway
Suite 550
Redwood City
CA 94065
Tel: +1 800 982 6109
Fax: +1 888 888 6884

Clearswift Corporation
1715 114th Avenue SE
Suite 115
Bellevue
Washington, 98004
Tel: +1 425 460 6000
Fax: +1 425 460 6185

Clearswift Corporation
One Penn Plaza Center
250 West 34th Street
36th Floor
New York, NY 10119
Tel: +1 212 835 1595
Fax: +1 212 835 1596

EUROPE

United Kingdom
Clearswift Limited
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire, RG7 4SA
Tel: +44 (0) 118 903 8903
Fax: +44 (0) 118 903 9000

Germany
Clearswift GmbH
Amsinckstrasse 67
20097 Hamburg
Tel: +49 40 23 999-0
Fax: +49 40 23 999-100

Spain
Clearswift Espana S.L.
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcon
Madrid
Tel: +34 91 790 1219 / +34 91 790 1220
Fax: +34 91 790 1112

ASIA PACIFIC & JAPAN

Australia
Clearswift
Level 5, Suite 504
165 Walker Street
North Sydney
New South Wales, 2060
Tel: +61 2 9424 1200
Fax: +61 2 9424 1201

Japan
Clearswift Hanai Bldg. 7F
1-2-9
Shiba Kouen Minato-ku
Tokyo-to, 105-0011
Tel: +81 (3) 5777 2248
Fax: +81 (3) 5777 2249

www.clearswift.com

Contents

PREFACE

CHAPTER 1 Introduction

Part I
MIMEsweeper Policy Editor

CHAPTER 2 Content Security Policy Definition

CHAPTER 3 Classifications

CHAPTER 5 References

CHAPTER 6 Mail Routing and Relay

Part II
MIMEsweeper Manager

CHAPTER 7 MIMEsweeper Manager Web Browser Application

CHAPTER 8 Systems Center

CHAPTER 9 Message Center

CHAPTER 10 Personal Message Manager

CHAPTER 11 Report Center

CHAPTER 12 Security Center

Part III
Appendices

APPENDIX A Auto-responders

APPENDIX B Data Types

APPENDIX C File Formats

APPENDIX D IMAGEmanager

APPENDIX E Housekeeping

APPENDIX F MIMEsweeper for SMTP Folders

APPENDIX G Message Processing

APPENDIX H Testing

APPENDIX I Tokens

APPENDIX J Valid Names

Part IV
Glossary

GLOSSARY

INDEX

Preface

MIMEsweeper™ for SMTP is a content security solution that is deployed in an email network and enables businesses to implement content security policies for email entering and leaving the organization. This Reference describes the functionality and operation of each component of MIMEsweeper for SMTP.

About the Reference

The Reference provides reference information for all aspects of MIMEsweeper for SMTP not covered in the Getting Started Guide, including content security policy definition, system management and monitoring.

The information in the Reference supplements that contained in the help (for further information, see *Related documentation* on page -xi).

Readership

The Reference is intended primarily for system administrators. It assumes system administrators have a working knowledge of:

- Network topology and routing
- Windows
- The Microsoft Management Console (MMC)

The Reference may also be useful to other individuals in your organization who are responsible for:

- Defining your organization’s policies.
- Configuring the MIMEsweeper for SMTP system.
- Configuring your organization’s policies in MIMEsweeper for SMTP.
- Managing email policies for the organization as a whole or for individual groups or departments.
- Managing the MIMEsweeper for SMTP system.

Structure

The Table of Contents provides you with enough information to allow you to decide which chapter to read initially. Under each chapter heading, subheadings provide you with information about the material covered in the chapter.

The information in the Reference is organized as follows:

- **Part 1 - MIMEsweeper Policy Editor**

  Chapters 2 to 6 describe the function and operation of each element of the MIMEsweeper Policy Editor user interface.

  Chapters are in the order that the described topic appears on the user interface.

- **Part 2 - MIMEsweeper Manager**

  Chapters 7 to12 describe the function and operation of the MIMEsweeper Manager user interface.

  Each MIMEsweeper Manager center is described in its own chapter.

- **Part 3 - Appendices**

  The appendices A to K contain guidance on testing and maintaining your system, descriptions of tokens used in different system components, and supplementary information not essential for using the system.

  Appendices are in alphabetical order by title.

- **Part 4 - Glossary**

  The Glossary defines the acronyms, concepts, and terms used in MIMEsweeper for SMTP.

Each chapter and appendix in the Reference observes the following structure:

- A brief abstract describing the function of the topic covered in the chapter.
- A chapter table of contents, which contains a more complete outline of the chapter than is shown in the book Table of Contents.
- A brief overview of the material covered in the chapter, providing an expanded description of the topic, including its purpose and features.
- Detailed descriptions of the feature/functionality covered in the chapter.

Some chapters may contain additional sections, which give detailed information on any properties and special features and restrictions for a specific element.

Where appropriate, descriptions include cross-references to other chapters or appendices with additional or related information and to the help.

Conventions

This guide uses the following conventions:

Convention	Indicates
Bold type	Menus, names, and options displayed on screens, or terms in a definition list.
`This type`	Path names, file names, and extensions; commands or text to be entered in files or dialog boxes; text displayed by the system; or extracts of program code.
Underline	A URL for a site on the World Wide Web.
`<variable>`	A value you must supply, for example, in a command line.
`[<variable>]`	An optional value you can supply, for example, in a command line.
ℹ	A note giving information that emphasizes or supplements important points in the text or information that may apply only in special cases.
⚠	A caution alerting you to actions that could result in the loss of data.

The descriptions in the Reference assume the left mouse button to be the primary button and the right mouse button to be secondary. Be aware of this if you have customized your mouse buttons.

Related documentation

Use the Reference in conjunction with:

- **Getting Started Guide**

  Getting Started introduces the main features of MIMEsweeper for SMTP and provides the information you need to:

  – Plan your initial deployment and install MIMEsweeper for SMTP

  – Create your initial content security policy using the Initial Policy Wizard

  – Get to know the MIMEsweeper Policy Editor user interface

  The information in Getting Started supplements that contained in the Reference and the help.

- **Release documents**

  This document set provides important information on new features, prerequisites, configuration and known problems. You should read these documents before installing and configuring MIMEsweeper for SMTP.

  The documents are supplied as `*.htm` files, on the MIMEsweeper for SMTP CD-ROM.

- **Online help**

  The online help introduces overview and conceptual information on key features of MIMEsweeper for SMTP and provides step-by-step procedures for using the functions, describing their properties and settings. Help is provided for the following MIMEsweeper elements:

  - MIMEsweeper Policy Editor

    Context-sensitive help accessed from the MIMEsweeper Policy Editor standard toolbar **Help** button.

  - MIMEsweeper Manager

    Context-sensitive help accessed from the **Help** hypertext link provided on every MIMEsweeper Manager page.

  - Personal Message Manager

    Help for the Personal Message Manager (PMM) accessed from the **Help** hypertext link provided on the user interface.

- **Tech notes**

  Tech Notes provide supplementary information on various features and functionality of MIMEsweeper for SMTP.

  Tech Notes are available from our website at http://www.clearswift.com.

Accessibility

In describing how to use MIMEsweeper for SMTP, the help describes the use of menus in conjunction with a mouse. However, the software uses standard Microsoft controls that enable you to complete most of the tasks through the use of keyboard controls, for more details see help topic *Using Keyboard Shortcuts*.

CHAPTER 1

Introduction

This chapter outlines how to use MIMEsweeper for SMTP to implement your organization’s email policies and identifies the main features of the system.

Overview

MIMEsweeper for SMTP is a content security solution that integrates with an existing email network and enables businesses to implement content security policies for email entering and leaving the organization.

MIMEsweeper for SMTP provides two primary functions in an SMTP email network:

- **SMTP mail routing and relay**

  MIMEsweeper for SMTP routes and relays email messages based on the routing and relay policy you define.

- **Content security**

  MIMEsweeper for SMTP processes email messages passing through your domain based on the content security policies you define.

This chapter describes the criteria you need to consider to develop a routing and relay policy and a content security policy. It also describes criteria for developing a deployment policy for determining where best to deploy MIMEsweeper for SMTP in your email network.

This chapter also describes the key components of MIMEsweeper for SMTP and how they work to implement the email policies you define.

Each section in this chapter provides cross-references to other chapters in this Reference that contain more detailed information.

Policy types

MIMEsweeper for SMTP routes, relays, and processes email messages according to the email policies you define. You implement the following types of email policy in MIMEsweeper for SMTP:

- Deployment policy
- Routing and relay policy
- Content security policy

One consideration that will have a bearing on all of your email policies, is the number of individuals in your organization who will be responsible for:

- Defining your organization’s policies.
- Installing and configuring the MIMEsweeper system.
- Configuring your organization’s policies in MIMEsweeper.
- Managing email policies for the organization as a whole or for individual groups or departments.
- Managing the MIMEsweeper system.

Deployment policy

A deployment policy defines the way you want to implement MIMEsweeper for SMTP in your email network.

A deployment policy covers criteria for:

- Network architecture.
- Internet connection method.
- The number of people responsible for configuring policies and managing the system.
- Message throughput.
- System resilience.

For further information about	See
Planning a deployment:	Chapter 2 of the *Getting Started Guide*.
Installing MIMEsweeper for SMTP:	Chapter 3 of the *Getting Started Guide*

Routing and relay policy

A routing and relay policy defines the SMTP security rules you want MIMEsweeper for SMTP to enforce.

A routing and relay policy covers criteria for:

- SMTP hosts MIMEsweeper is allowed to accept email from.
- SMTP hosts allowed to connect to and relay email through MIMEsweeper.
- Specific hosts or email addresses from which to reject mail.
- The number of recipients permitted.
- The size of email messages permitted.
- The number of email messages that MIMEsweeper can simultaneously receive.

Based on these criteria, you determine which SMTP security and relay features to implement in MIMEsweeper.

For further information about	See
Configuring routing and relay features in the MIMEsweeper Policy Editor	Chapter 6
Testing configured routes	Appendix H

Content security policy

A content security policy defines the email processing rules you want MIMEsweeper for SMTP to enforce.

An email processing policy covers criteria for:

- **Policy routing**
  - Who can send or receive email messages.
  - Where email messages can be sent or received.
- **Email processing**
  - What types of email messages to detect.
  - What type of text and objects to analyze in a detected message.
  - What type of actions to perform on the analyzed objects.
  - Who to notify about the detected message.
- **Auditing and reporting**
  - What type of system performance information to track.
  - What type of message processing data to track.
  - What type of content analysis and detected content to track.

These areas are described more fully in the following sections. Based on these criteria, you determine which content security features to implement in MIMEsweeper, for example:

- Address lists to specify individuals and groups.
- Scenario folders to manage policies by individuals and groups.
- Scenarios to specify the type of email to which a policy applies.
- Classifications to specify one or more actions, which specify what to do with items and who to notify when a message of a specified type is detected.
- Management reports to display system information recorded in either an audit database, or a message tracking database.

For further information about	See
Configuring content security policies with the MIMEsweeper Policy Editor	Chapter 2
Configuring reporting elements of content security policies with the Report Center	Chapter 11
Housekeeping tasks	Appendix E
Testing content security policy elements	Appendix H

Policy routing

You can define policies that are specific to individual senders and recipients, and those that apply to groups of senders or recipients. Groups can be based on:

- Department (for example, Sales)
- Role (for example, Managers)
- Organization (for example, all competitor companies, or all partner companies)

You configure address lists and scenario folders to manage policies by individuals or groups.

Email processing

You can define policies to determine how MIMEsweeper for SMTP processes email messages passing through your domain. MIMEsweeper email processing includes three key stages:

- **Policy identification**

  MIMEsweeper recognizes the policy rules you have configured by:

  - Determining the scenario folder to apply to an email message based on its sender / recipient routes.
  - Applying the appropriate scenarios from the determined scenario folder.

- **Content analysis**

  MIMEsweeper scans and analyzes text and objects in email messages according to the scenarios you define to:

  - Analyze text within a document or message.
  - Analyze characteristics of email messages.
  - Analyze file types.
  - Add text to messages - in the form of annotations.
  - Archive messages.
  - Remove threats from messages.
  - Allow the administrator to override other classifications.
- **Classification**

  MIMEsweeper selects the actions to perform for email messages detected by a defined scenario by:

  - Determining how to classify an email message.
  - Performing the actions specified in the classification.
  - Notifying appropriate individuals as specified in the classification.

Auditing and reporting

You can define policies to determine what information MIMEsweeper for SMTP records on the way it processes email messages and which of this audited information to display in a management report.

You can configure the following types of auditing:

- Record audit data in a database.
- Writing to the Microsoft Windows event log.
- Generate SMTP Relay transport logging information.

You can also record data in a message tracking database, and generate point-to-point summary reports between two email addresses.

You can configure the following types of reports:

- Top Senders
- Top Recipients
- Top Threats
- Top Format Types
- Top Classifications
- Message Profiles

- Traffic Analysis
- Transaction Reports
- Message Tracking Reports

Developing policies

If your organization does not already have an email policy defined, follow this recommended policy development cycle:

1. Plan your policy on paper.
2. Implement your policy in MIMEsweeper.
3. Test your policy on MIMEsweeper.

Creating a policy plan helps you to clearly identify what you are trying to achieve and provides a useful maintenance record for future changes or additions.

If your organization does already have a defined email policy, you need only follow steps 2-3 of the recommended policy development cycle.

This policy development cycle is an iterative cycle, which you should repeat each time you create or change a configuration in MIMEsweeper. This will enable you to quickly isolate the probable cause of any problems and correct it before moving your test system to a live machine.

Key components

The key components in MIMEsweeper for SMTP are:

- MIMEsweeper Policy Editor
- MIMEsweeper Manager
- MIMEsweeper Edge Servers (optional)
- MIMEsweeper services
- MIMEsweeper folders
- MIMEsweeper message areas
- Scenarios
- Personal Message Manager (PMM)

The following sections provide a brief introduction to the role of these components in configuring your email policies, managing the MIMEsweeper system and processing messages.

MIMEsweeper Policy Editor user interface

The MIMEsweeper Policy Editor user interface enables you to create and maintain your organization’s email policies.

The user interface is based on a Microsoft Management Console (MMC) snap-in called the MIMEsweeper Policy Editor. This snap-in provides facilities to manage licenses and to configure the way MIMEsweeper for SMTP implements your email policies. The settings you specify in the MIMEsweeper Policy Editor are held in the Operations database.

MIMEsweeper Manager user interface

The MIMEsweeper for SMTP Manager web application enables you to access and manage the Message Center, Systems Center, Report Center, and Security Center in a web browser window.

For further information about	See
The MIMEsweeper Policy Editor user interface	See Chapter 6 of the *Getting Started Guide*
The MIMEsweeper Manager user interface	Chapter 7
Configuring content security policies	Chapter 2
Configuring routing and relay policies	Chapter 6

MIMEsweeper Edge Servers

The Edge server is a complete Linux-based Email MTA that you can deploy in front of your Policy Servers to provide hygiene services such as spam and virus protection. One or more MIMEsweeper Edge Servers can operate as an email firewall for your MIMEsweeper for SMTP installation, to handle spam and/or virus and threat detection.

See the *MIMEsweeper Edge Server Deployment Guide* for information on installing and configuring an Edge Server.

Edge Servers and MIMEsweeper for SMTP

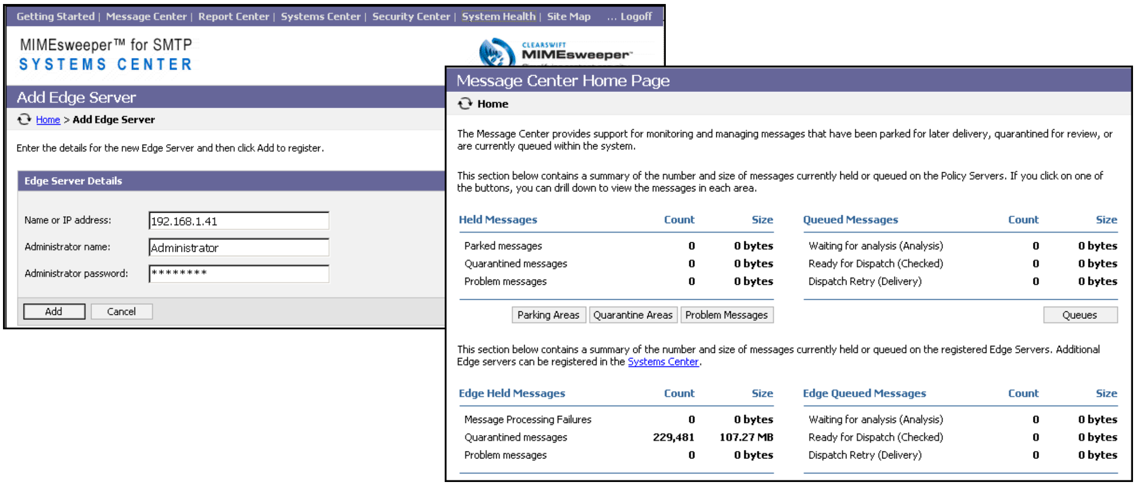
Edge Servers operate in conjunction with your MIMEsweeper for SMTP installation, for example:

- You can use an Edge server or servers to detect unwanted messages, spam messages, and messages that contain threats.
- You can use MIMEsweeper for SMTP to apply your organization's content security policies, for example Attachment Manager and Text Analyzer.

MIMEsweeper for SMTP displays limited information on installed MIMEsweeper Edge Servers—for example:

- The System Center Home Page displays Edge Server information on Edge Server operation status.

- The Message Center Home Page displays limited information on messages quarantined and queued on Edge Servers.
- The System Health page displays information on any installed Edge Servers.


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map ... Logoff
MIMEsweeper™ for SMTP
SYSTEMS CENTER
CLEARSWIFT
MIMEsweeper

Add Edge Server

Home > Add Edge Server

Enter the details for the new Edge Server and then click Add to register.

Edge Server Details

Name or IP address: 192.168.1.41

Administrator name: Administrator

Administrator password: ********

Message Center Home Page

Home

The Message Center provides support for monitoring and managing messages that have been parked for later delivery, quarantined for review, or are currently queued within the system.

This section below contains a summary of the number and size of messages currently held or queued on the Policy Servers. If you click on one of the buttons, you can drill down to view the messages in each area.

Held Messages	Count	Size	Queued Messages	Count	Size
Parked messages	0	0 bytes	Waiting for analysis (Analysis)	0	0 bytes
Quarantined messages	0	0 bytes	Ready for Dispatch (Checked)	0	0 bytes
Problem messages	0	0 bytes	Dispatch Retry (Delivery)	0	0 bytes

This section below contains a summary of the number and size of messages currently held or queued on the registered Edge Servers. Additional Edge servers can be registered in the Systems Center.

Edge Held Messages	Count	Size	Edge Queued Messages	Count	Size
Message Processing Failures	0	0 bytes	Waiting for analysis (Analysis)	0	0 bytes
Quarantined messages	229,481	107.27 MB	Ready for Dispatch (Checked)	0	0 bytes
Problem messages	0	0 bytes	Dispatch Retry (Delivery)	0	0 bytes

Figure 1-1: Edge Server details

Handling detected messages

There are two options that you can use to manage messages that a MIMEsweeper Edge Server detects:

- You can configure MIMEsweeper Edge Server to add X-header information to detected messages, then pass them to MIMEsweeper for SMTP for processing. In MIMEsweeper for SMTP, you can configure a scenario to detect and deal with these messages.

  This is suitable for spam messages. It enables you to use MIMEsweeper for SMTP's PMM functionality to manage spam messages.

- You can quarantine messages on the MIMEsweeper Edge Server.

  This is suitable for messages containing threats such as viruses, as it ensures that these threats do not enter your system.

MIMEsweeper services

These MIMEsweeper services are responsible for processing email messages:

- **Receiver service**

  Validates connections for incoming mail based on your routing policy, receives email messages, and passes them to the Security service for processing.

- **Security service**

  Checks the content of email messages against your configured security policies.

- **Delivery service**

  Delivers email messages to the next host machine on the route to their intended recipients.

- **Infrastructure service**

  Carries out all monitoring, configuration and control tasks that are not specifically carried out by other services.

- **Audit Consolidator service**

  Responsible for processing audit data and sending it to the audit disposer.

- **Audit Disposer service**

  Writes the audit data to the database.

- **Tracking service**

  Responsible for either collating tracking data and writing it to the message tracking database, or for processing tracking data and sending it to the Hive Server, depending upon which machine the services are running.

Figure 1-2 illustrates how these MIMEsweeper services process messages coming through the Internet and local domains (for further details, see Appendix G).

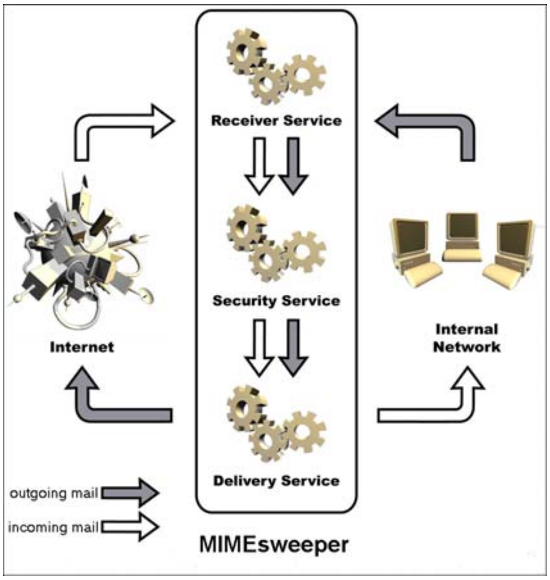


Figure 1-2: MIMEsweeper services

For further information about	See
Starting and stopping the MIMEsweeper services	Chapter 8
How the MIMEsweeper services process messages	Appendix G

MIMEsweeper folders

During different stages of message processing, MIMEsweeper places email in a number of MIMEsweeper folders on your hard disk.

For further information about	See
How MIMEsweeper uses these folders during message processing	Appendix G
The location and contents of MIMEsweeper folders	Appendix F

Message areas

If your content security policy specifies that a certain type of email should not be delivered immediately or automatically, MIMEsweeper for SMTP places the email in a temporary storage area. You specify this storage area, called a message area, when you define a classification (for further information, see *Classifications* on page 1-13).

Emails in message areas are held until they are:

- Reviewed, changed, and manually released or deleted by the individuals in your organization responsible for content security policy, or by the individual system users accessing their Personal Message Manager (PMM) area.

  or

- Automatically released for delivery during a configured release period.

  or

- Automatically deleted after a configured period of time.

MIMEsweeper for SMTP includes a number of default message areas, and you can create your own to meet your policy needs.

For further information about	**See**
Configuring message areas	Chapter 2
How MIMEsweeper uses message areas	Appendix G
The location message area folder on the hard disk	Appendix F

Scenarios

You define scenarios to specify the security operations MIMEsweeper for SMTP performs on types of email message and attachments for a particular content security policy.

For example, nearly all organizations have policies that aim to prevent absolute threats such as viruses. You can define a scenario to scan all mail coming into or going out from the organization for viruses. Any mail found to contain a virus would then be blocked from delivery.

Other policies define circumstances whereby an email constitutes a threat only under particular circumstances. For example, while it may be perfectly legitimate for a member of the accounts department to send a financial report to the company's auditors, sending the same report to the company's main competitors is likely to constitute a threat.

Policies do not necessarily deal just with potential threats. They can also enhance business processes, for example, by specifying that email messages sent to customer support have an automatic reply sent immediately, pending follow-up by an individual.

Policies are liable to change over time, and some have a shorter validity than others. For example, an organization may have a long-standing policy to control the flow of information such as financial reports and design specifications, but may need to define specific policies to deal with events such as impending company mergers or stock issues.

MIMEsweeper for SMTP includes a number of scenario types from which you can create your own scenarios to meet your policy needs, with third-party DLL anti-virus tools.

You can group scenarios in folders to create departmental or organizational security policies, for example, Sales Outgoing Messages. You can arrange these scenario folders in a hierarchy and specify whether scenarios in higher-level folders are inherited or overridden at lower levels.

For further information about	See
MIMEsweeper scenario types	Chapter 4
References for text analysis scenario types	Chapter 5

Classifications

You define classifications to specify the actions MIMEsweeper for SMTP takes and who it notifies when it detects a message of a type specified in the associated scenario.

MIMEsweeper for SMTP includes a number of default classifications and actions, and you can create your own to meet your policy needs.

For further information about	See
MIMEsweeper classification and action types	Chapter 3
Tokens that can be used with actions	Appendix I

Personal Message Manager

To help cope with the increasing amount of junk mail and spam which has to be handled by email systems Personal Message Manager (PMM) can be configured on your system. PMM allows email system users to manage their own messages which have been captured by the system, and therefore reduce the amount of MIMEsweeper administration required from the system administrator.

Messages which are passed to an individual's PMM area include those which are, after processing by MIMEsweeper, not regarded as posing a serious threat, but which require being looked at to determine if they are junk mail or spam and can be disposed of. Each user who has access to PMM receives a digest message from the MIMEsweeper system notifying them that a message has been put into their PMM area and that they should deal with it.

For further information about	See
Configuring Personal Message Manager	Chapter 10
Using Personal Message Manager	Chapter 10

Support for Multiple Languages

The MIMEsweeper for SMTP user interface supports multiple languages. At the time of publication, the supported languages are English and Japanese. Additional languages are available for PMM, including French, German, Italian and Spanish. This feature allows different users to view MIMEsweeper for SMTP in different languages on the same MIMEsweeper system.

The MIMEsweeper for SMTP user interface can be displayed in English or Japanese. Table 1-1 lists the factors that determine the language displayed.

Table 1-1 : Factors determining the displayed language

MIMEsweeper item	Factor determining displayed language
MIMEsweeper for SMTP product CD-ROM	The preferred language setting of the user's web browser. If this is other than English or Japanese, the user interface is rendered in English by default. The method of configuring a web browser's default language varies depending upon the web browser being used.
MIMEsweeper for SMTP product installer	The user interface locale setting of the machine on which the item is running. If this is other than English or Japanese, the user interface uses English by default. The machine's user interface locale settings also determine the format of items such as dates and times. For example, English (United States) option displays in English and uses standard US English date and time formats. The method of configuring the default language on a machine's locale settings varies depending upon the operating system installed on the machine.
Initial Policy Wizard	
MIMEsweeper Policy Editor	
System Maintenance Utility	
Audit Migration Utility	

Table 1-1 : Factors determining the displayed language

MIMEsweeper item	Factor determining displayed language
MIMEsweeper Manager	The preferred language setting of the user's web browser. If this is other than English or Japanese, the user interface is rendered in English by default. The web browser's preferred language setting also determines the format of items such as dates and times.
Personal Message Manager. User interface and notification messages.	The initial displayed language depends on how the PMM account is created. PMM account created by user If the user creates the PMM account (using the **Get One Now** option on the PMM Sign In page), PMM uses the language the user selects on the **Create Account** dialog. PMM users can change the language setting for their own PMM accounts in the Options page, which is accessed from PMM's main navigation bar. PMM account created automatically If no PMM account exists for the user on the first occasion that MIMEsweeper withholds a message for the user in a PMM-managed quarantine area, MIMEsweeper creates the account automatically. In this case, PMM uses the default PMM language for the user's domain. The Administrator sets this default language in the **Configure PMM** pages of the MIMEsweeper Manager. For details about changing languages in PMM, see Chapter 10.

Network authentication

MIMEsweeper for SMTP maintains operation, message tracking, and auditing records on databases running on database servers. In order to write to these databases, MIMEsweeper for SMTP must have sufficient access rights to the database.

Two types of authentication are available for providing MIMEsweeper for SMTP access:

- SQL server authentication, where you supply a database administrator username and password to authenticate the database access.
- Windows Authentication, where the system uses the Windows logon details, along with an Application Server account, to authenticate database access.

An Applications Server account is a Windows user account that you create, with the required access rights to login to the database server or servers, and to access the required databases. You configure this account's details when installing MIMEsweeper for SMTP, and the installation uses this account for all database operations.

See the Getting Started Guide for details.

Part I

MIMEsweeper Policy Editor

CHAPTER 2

Content Security Policy Definition

This chapter describes how to use the MIMEsweeper for SMTP Policy Editor snap-in to configure your email policies.

Overview

You use the MIMEsweeper Policy Editor snap-in to configure the way MIMEsweeper for SMTP implements your email policies.

The MIMEsweeper Policy Editor snap-in is contained in the default Microsoft Management Console (MMC) on the secure MIMEsweeper host machine. For information about installing the MIMEsweeper Policy Editor snap-in see Chapter 3 of the *Getting Started Guide*.

You provide configuration details when you create a new item under the MIMEsweeper Policy Editor snap-in, and you can change configuration properties in the properties page for an existing item. For information on creating new items or editing existing properties, see the MIMEsweeper Policy Editor help and Chapter 6 of the *Getting Started Guide*.

Always ensure you have adequate disk space before saving configuration edits. If disk space is less than the minimum, edits may not save, and you may not get a warning that they have not saved. For details of disk space requirements, see the *Prerequisites* document.

As described in Chapter 1, policies generally include elements of route, type, and action. Route information is a key element of policy implementation, so the third section in this overview, *Specifying addresses* on page 2-3, describes basic concepts you need to understand to effectively specify addresses for route information.

The remaining sections in this chapter describe the properties you can configure to define and implement the elements of your policies.

This chapter also describes configuration settings for the way messages are processed and tracked and where messages are stored. The sections are listed in the order that the configuration areas appear in the MIMEsweeper Policy Editor snap-in of the MMC. For details about the console, see the MIMEsweeper Policy Editor help and Chapter 6 of the *Getting Started Guide*.

Specifying addresses

Some configuration options require you to specify addresses for email senders and recipients. You can specify either individual email addresses or address lists containing a number of email addresses.

In general, you are recommended to use address lists, which provide the following advantages:

- You can refer to an entire list of email addresses by specifying a single label.
- You can edit or remove individual addresses from the list without having to check every configuration option where you might have specified the address.

Email addresses are in the format `username@location`. You can specify email addresses for senders and recipients in the following ways:

- **Explicit**

  This address contains both the full user name and full location.

- **Partially wildcarded**

  This address has the full user name replaced with a wildcard (*) character and one or more, but not all, domain elements of the location replaced with a wildcard (*) character.

- **Fully wildcarded**

  This address has the full user name and the full location both replaced with a wildcard character (*).

When you use wildcard characters in addresses, observe these rules:

- Use only one wildcard character for each element of the address.
- Do not replace part of an element with a wildcard character; for example, do not specify `acc*@inside-yourcompany.com`.

See the MIMEsweeper Policy Editor help for examples of each type of address specification.

The way you specify an address affects the way MIMEsweeper for SMTP prioritizes messages for processing. For information, see *Multiple scenario folder matches and route priority* on page 2-26.

Licenses

You create, view or delete licenses for your MIMEsweeper for SMTP product under the **Licenses** folder in the Policy Editor snap-in. You view the details for each MIMEsweeper for SMTP license in the **License** tab of the MIMEsweeper for SMTP **License Properties** page.

To ensure that you remain compliant with the terms of the license, you should refer to the license agreement before first installing the software and before you make any changes to your installation.

In the **License** tab, you can view license configuration information: company, license key, serial number, product, expiry date, number of users, and functionality options.

You can use this tab to set the Support and Maintenance Agreement password for your license if it is not already configured.

You require a Support and Maintenance Agreement in place in order that your installation can maintain current versions of Clearswift Managed List references. This ensures that your defences protect against current threats.

For example, a Support and Maintenance Agreement ensures that your system uses the latest version of the SpamLogic Signatures list, to ensure that your spam detection keeps up with current trends. See *Configuring managed downloads* on page 5-4 and *SpamLogic* on page 4-39 for more information.

Please ensure that your deployment option conforms with the requirements of the license agreement.

For more information about adding a license, see the MIMEsweeper Policy Editor help.

MIMEsweeper for SMTP 5.3 requires a new license. If you are using a license from an earlier version of MIMEsweeper for SMTP, you must update your license to use the current version. Certain areas of the MIMEsweeper Manager will only be available if using an advanced license.

Separate licenses are required for different language versions of MIMEsweeper for SMTP.

MIMEsweeper for SMTP

The MIMEsweeper for SMTP folder under the MIMEsweeper for SMTP Policy snap-in is referred to as the MIMEsweeper Policy Editor. You use the MIMEsweeper Policy Editor to access the MIMEsweeper Task Pad and also to configure these aspects of your email policies:

- MIMEsweeper for SMTP Properties
- Address Lists
- Policies
- Message Areas
- Alerters
- References
- SMTP Relay
- Servers

MIMEsweeper for SMTP properties

You configure the way MIMEsweeper for SMTP processes email messages and tracks this processing by setting options for the MIMEsweeper for SMTP folder in the MIMEsweeper Policy Editor snap-in. For details on changing options in the properties page for this folder, see the MIMEsweeper Policy Editor help.

You can specify options on the following tabs in the MIMEsweeper for SMTP **Properties** page:

- Addresses
- Monitor

These are described in the following sections.

Addresses

You configure the email addresses for the **MIMEsweeper Service** and for the **MIMEsweeper Administrator** in the **Addresses** tab on the MIMEsweeper for SMTP **Properties** page. These default email addresses are created when you install MIMEsweeper for SMTP.

In the **Addresses** tab, you can change the following default email addresses:

- **MIMEsweeper Service**

  `MIMEsweeper@your-companyname-here.com`

  This is MIMEsweeper's own email address.

- **MIMEsweeper Administrator**

  `postmaster@your-companyname-here.com`

  This is the email address to be used by the individual responsible for administering MIMEsweeper.

For information about the default MIMEsweeper addresses, see the MIMEsweeper Policy Editor help.

Monitor

You can configure the way MIMEsweeper Policy Editor monitors the processing of email messages by setting options in the **Monitor** tab on the MIMEsweeper for SMTP **Properties** page.

In the **Monitor** tab, you can specify the following checks on message processing:

- **Number of suspect messages before sending an alert**

  The number of suspect messages that can be left to continue processing before the monitor sends an alert to the administrator suggesting that they restart the service. A suspect message is one that takes more than 30 minutes to be processed. The default is 10 suspect messages.

- **Number of exceptions before sending an alert**

  The number of exceptions allowed before the monitor sends an alert to the administrator suggesting that they restart the service. An exception is a failure in message processing. The default is 10 exceptions.

- **Check for exceptions every <duration> minute(s)**

  The interval in minutes after which the monitor checks for exceptions in message processing. The default is 60 minutes.

- **Resend alerts every <duration> minute(s)**

  The interval in minutes after which the monitor resends an alert to the administrator about a suspect message or an exception. The monitor continues to resend the alert at the specified interval until the administrator restarts the service. The default is 180 minutes.

For information on how MIMEsweeper Policy Editor monitors message processing, see the MIMEsweeper Policy Editor help.

Task pad

You can quickly get started with using MIMEsweeper Policy Editor by using the Getting Started Task Pad. The Task Pad is displayed in the Details pane when you select the MIMEsweeper for SMTP folder under the Policy Editor snap-in.

From the Task Pad you can:

- Start wizards to create policy components.
- Access the MIMEsweeper Policy Editor help system.
- Obtain information on the MIMEsweeper system.

For details on using the task pad, wizards, and the MIMEsweeper Policy Editor, see the MIMEsweeper Policy Editor help and Chapter 6 of the *Getting Started Guide*.

Address lists

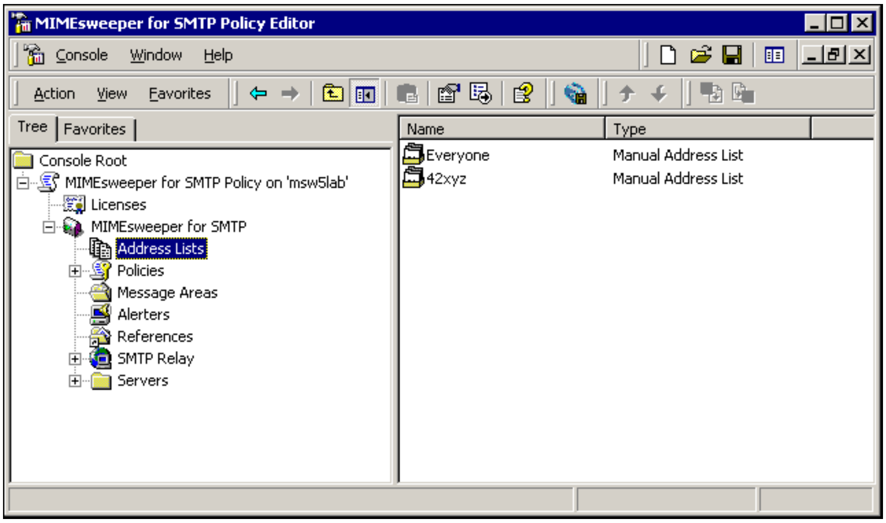
You create address lists, which group together the email addresses of users who share a common task, under the **Address Lists** folder in the MIMEsweeper for SMTP folder. MIMEsweeper Policy Editor uses address lists to provide routing and policy selection information.

You can create the address lists using either of the following methods:

- Manual address lists
- LDAP address lists

These methods are described in the following sections.

The address lists you create are listed in the Details pane of the MIMEsweeper Policy Editor as shown in Figure 2-1.



Name	Type
Everyone	Manual Address List
42xyz	Manual Address List

Figure 2-1: Address lists

If you change details in an address list, you must click **Save** to implement your changes.

You should test your route details before your MIMEsweeper system goes live. This will enable you to correct any potential problems caused by inaccurate route details. For example, if you omit domain names or users from your address lists, policy execution is unpredictable. For more information about testing address lists, see Appendix H.

Manual address lists

You create manual address lists from either local or remote addresses. You must check each list yourself when you add new users or move existing users to another group. This can present a maintenance burden if you have a large number of users or groups to manage.

This section briefly describes the properties of a manual address list. Full details on using manual address lists are provided in the MIMEsweeper Policy Editor help.

In the **Address List** tab of the properties page for an address list, you specify one or more email addresses. For example, you could create address lists for users based in the same organization or for groups of partner organizations.

You specify each email address on a separate line, using any of the following types of email address specification:

- Explicit address
- Partially wildcarded address
- Fully wildcarded address

For more information about these types of address specification, see *Specifying addresses* on page 2-3.

The **Usage** tab displays a list of scenarios currently associated with the manual address list. Each entry shows the scenario name and its location in the scenario folder hierarchy.

PCS LDAP address lists

The contents of a PCS LDAP address list are obtained by querying an LDAP server using a user defined set of search criteria including the organizational units (OUs) to search, the objects to look for, and the attributes whose values should be included in the PCS LDAP address list.

PCS LDAP address list functionality supports the following LDAP servers:

- Microsoft Active Directory
- Lotus Domino
- Sun One Directory Server

PCS LDAP address list data is stored in LDAP digest files. The PCS Infrastructure service replicates LDAP digest file changes to the Policy Servers, as it does for any other part of the configuration. On the Policy Servers, the Receiver service and / or the Security service read the content of the digest files directly. Periodic querying of the LDAP server to reload LDAP digest files can be carried out by the PCS without impacting message processing. New LDAP digest files will only be replicated to the Policy Servers via the PCS, if the LDAP data has changed.

With these technology enhancements the differences between PCS LDAP address lists and LDAP address lists are as follows:

- A PCS LDAP address list is the only type of LDAP-based address list that you can use to configure relay targets.
- A multiple machine deployment using a PCS LDAP address list does not require each Policy Server to have access to the LDAP server, because only the PCS needs access. Thus, a MIMEsweeper system that uses PCS LDAP address lists can be deployed more securely, with both the PCS and the LDAP server located in the internal network. An LDAP address list must give each Policy Server access to the LDAP server, so that the Security service can query the necessary LDAP data.
- Services that use a PCS LDAP address list will restart more quickly than those using a LDAP address list that contains the same amount of data, with less chance of failure.
- Service start-up is not dependent upon the current health of the LDAP server.
- Demand on the LDAP server is not increased by the number of Policy Servers.
- Periodic querying of the LDAP server to reload LDAP digest files can be carried out by the PCS without impacting message processing.
- New LDAP digest files will only be replicated to the Policy Servers if the LDAP data has changed. Consequently the Receiver and Security services will only reload LDAP data if it has changed.
- You can enable and control recursive searching through LDAP groups when you create a PCS LDAP address list, or when you edit the properties of an existing PCS LDAP address list.
- You can specify the paging size to be used when the Infrastructure service on the PCS queries the LDAP server.
- When you use the Identify Policy dialog, it is much quicker for the process to interrogate a PCS LDAP address list than a LDAP address list.

This section briefly describes the properties of an PCS LDAP address list. Full details on using PCS LDAP address lists are provided in the MIMEsweeper Policy Editor help.

In the **Connection** tab you configure how the LDAP server is accessed. You specify the server name, port, connection timeout and the authentication credentials to use. The connection timeout determines how long the LDAP server will be given to return the results from queries or other operations. The authentication credentials do not need to be specified if your LDAP server allows anonymous access.

In the **Address list** tab you configure the LDAP queries used to populate the PCS LDAP address list. For each query you configure the distinguished name (DN) of the LDAP object, a filter of the types of objects to search and the set of attributes to retrieve SMTP email addresses from. You may specify multiple queries, and you can use the Add, Edit, and Delete options to manage the list of queries.

In the **Trigger Times** tab you specify the times when the Infrastructure service on the PCS will query the LDAP server for updates. The PCS Infrastructure service checks the Trigger Times schedule hourly to see whether an update is due. Typically, there is an interval of 15 or 20 minutes before changes are sent to the Policy Servers. However, the interval will depend upon the amount of data that matches the queries in the LDAP server.

On the Policy Server, if the Receiver service and / or the Security service are configured to use PCS LDAP address lists they will check the corresponding digest file for changes every five minutes. If the service finds the digest file has changed, it reloads the LDAP data while continuing to process mail.

It is possible for a digest file to be updated while the Receiver or Security service is in the process of reading the file and reloading the LDAP data in the address list. To avoid errors, the Receiver or Security service checks the timestamp of the digest file again after loading data. If the timestamp has changed during the load, the data is discarded. The service tries again to reload the LDAP data five minutes later.

As well as checking the timestamp after data loading, MIMEsweeper for SMTP has a number of other safeguards built in to avoid replacing valid data with incorrect or incomplete data when the system may be unattended. No reload will take place in either of the following circumstances:

- There are no addresses in a digest file that previously contained one or more addresses.
- There were 100 or more addresses in the last digest file and the refreshed digest file contains less than 80% of the number of addresses there were previously.

You must restart the MIMEsweeper services, if either of these two conditions apply and you want the new digest file data to be used.

In the **Recursion and Paging** tab you can specify how MIMEsweeper will recursively search LDAP directories for the entries to be added to the address list. You specify which attributes should be used for recursive searches and the maximum depth of the search. The paging size is used to prevent the LDAP server abandoning the search if it finds too many results.

In the **Usage** tab you can view the list of scenario folders currently associated with the PCS LDAP address list. If the address list is used by the Receiver service as a relay target, the Usage list includes the entry Anti-relay. The **Show** option displays the folder contents for both options in the Details pane.

LDAP address lists

The contents of an LDAP address list are obtained by searching an LDAP server using the specified queries. This provides automatic access to user information stored and managed in a central directory. LDAP address lists provide a simple mechanism for specifying, for example, an organizational group. Using this option you can only configure routes on scenario folders, unlike PCS LDAP you cannot specify Relay Targets. This is the older style of LDAP address lists used in MIMEsweeper for SMTP, and we recommend that, if possible, you use the PCS LDAP address list option instead.

LDAP address list functionality supports the following LDAP servers:

- Microsoft Exchange 5.5
- Microsoft Active Directory
- Lotus Domino

LDAP address list functionality includes both anonymous and authenticated access on a variety of LDAP servers, such as Microsoft Exchange and Microsoft Active Directory. This enables you to take full advantage of the benefits of using LDAP address lists based on user details stored in LDAP directories. Whether you use anonymous or authenticated access depends upon the requirements of your LDAP server.

This section briefly describes the properties of an LDAP address list. Full details on using LDAP address lists are provided in the MIMEsweeper Policy Editor help.

In the **Connection** tab, you configure details about the LDAP server on which the LDAP directory is stored. You specify the server name, the port to use, the refresh period for updating the address list, and log on details if required for authenticated access to the LDAP server.

To maximize efficiency, MIMEsweeper builds a cache of the members of the LDAP address list when the Security service is started. The contents of this cache are refreshed at the interval you specify. This refresh period should reflect the frequency with which changes are made to the contents of the LDAP directory.

In the **Address List** tab you can configure details on how MIMEsweeper should build your LDAP address list. You identify the level of the LDAP directory to use and the filter for retrieving addresses from the LDAP directory. Email addresses can be built from any level in the LDAP directory hierarchy.

The **Usage** tab displays a list of scenarios currently associated with the LDAP address list. Each entry shows the scenario name and its location in the scenario folder hierarchy.

If MIMEsweeper Policy Editor is dynamically building a large LDAP address list, it may take the Security service longer than the default wait time to start up. By default, if the service has not started within 30 seconds, MIMEsweeper displays a message indicating that the start-up request has failed. For large LDAP address lists, you may need to increase the Security service start-up wait period. For details, see the *Advanced Configuration* release document.

Policies

You configure your email policies and how MIMEsweeper Policy Editor implements them by configuring details in the following areas under the **Policies** folder under the MIMEsweeper for SMTP folder in the Policy Editor snap-in:

- Policies properties
- Classifications
- Scenarios

These areas are briefly described in the following sections. For full details on configuring these areas, see the MIMEsweeper Policy Editor help. Examples of how to configure a policy to automatically respond to incoming messages are provided in Appendix A.

Policies properties

You configure the way MIMEsweeper Policy Editor controls message processing by setting properties in the **Policies** folder under the Policy Editor.

You can specify message processing options in the following tabs in the **Policies Properties**:

- SMTP Options
- Text Options
- Policy Options
- Engine

These tabs in the **Policies Properties** page are briefly described in the following sections.

SMTP options

In the **SMTP Options** tab, you configure which SMTP message header fields MIMEsweeper for SMTP exports. This makes the contents of the specified header available for checking by MIMEsweeper's content security engine. For example, if the **Subject** header field is exported, MIMEsweeper can perform text analysis on the contents of the Subject field.

You can also specify whether to add an empty message body to email messages that do not have a message body.

For further information on configuring SMTP message header fields to export, see the MIMEsweeper Policy Editor help.

Text options

In the **Text Options** tab, you configure how MIMEsweeper Policy Editor determines whether an attachment without a character set specified in its header is a text file.

You can specify the character sets that MIMEsweeper scans for in text files that do not have a character set specified in their header. You also can specify the level of characters in the file that do not conform to the character set that MIMEsweeper accepts before determining that the file is not in that character set.

For further information on configuring the character sets to be accepted in text files, see the MIMEsweeper Policy Editor help.

Policy options

In the **Policy Options** tab, you configure whether MIMEsweeper Policy Editor gives more priority to the sender address or equal priority to both the sender and recipient addresses when determining the policies to apply to an email message.

When processing email messages, MIMEsweeper Policy Editor compares the sender / recipient pair in the message to the routes specified in scenario folders. If the sender / recipient pair in the message matches the route in more than one scenario folder with equal priority, by default MIMEsweeper gives more weighting to the sender address than to the recipient address and selects the scenario folder whose route more explicitly matches the sender's address.

If the standard MIMEsweeper scenario folder hierarchy is used (see *Default scenario folders* on page 2-20), when email messages are sent between users in the same domain, both the sender and recipient addresses will always match at least the default **Incoming** folder (for example, `*@*` to `*@your-companyname-here.com`) and the **Outgoing** folder (for example, `*@your-companyname-here.com` to `*@*`). With more weighting given to the sender address, MIMEsweeper matches the appropriate scenario folder under the **Outgoing** folder.

Because email policies typically are more concerned with the delivery and receipt of email messages passing through the external gateway rather than email messages going through the internal email network, it is usually appropriate for MIMEsweeper to apply policies under either the **Incoming** or **Outgoing** folder and to ignore policies under the other folder.

However, this method of processing can mean that only some policies ever get applied while other policies that also should be applied to the message get ignored. This can be a problem if the same MIMEsweeper for SMTP system is used by:

- Different parts of an organization that have completely independent email policies, for example, different departments or offices in different locations.
- Different domains or subdomains.

To ensure that MIMEsweeper always applies the appropriate policies to internal mail sent between different parts of an organization or to mail sent between different domains hosted on the same system, MIMEsweeper for SMTP needs to give equal weighting to both the sender and the recipient address. To do this MIMEsweeper must be able to process mail twice.

The following example illustrates the difference in how MIMEsweeper for SMTP matches the same message with and without the **Process using sender's policy and recipient's policy** option selected. In this example, a central MIMEsweeper for SMTP system processes the email for company offices in different locations as shown in Figure 2-2.

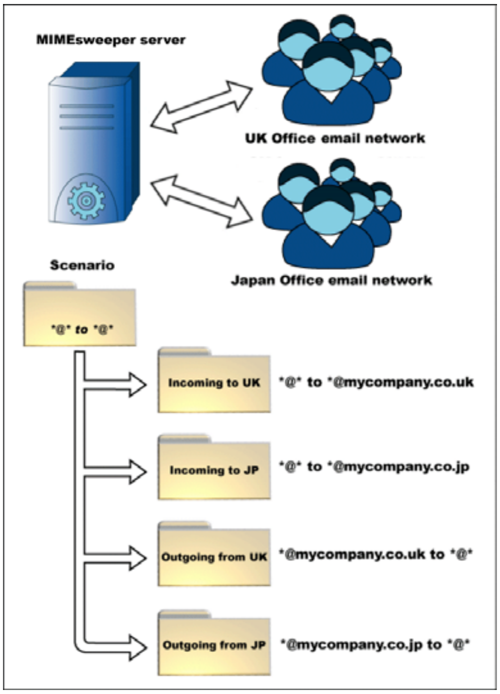


Figure 2-2: Sender/recipient processing

Each office has its own email policies, so there are no shared **Incoming** and **Outgoing** folders. Rather, the central MIMEsweeper system has separate incoming folders for mail coming into the UK office and into the Japan office, and separate outgoing folders for mail going out of each office.

Pat in the UK office sends a message to Tomoko in the Japan office. When it starts processing the email message, MIMEsweeper determines that the sender/recipient pair in the message (`pat@your-companyname-here.co.uk/tomoko@your-companyname-here.co.jp`) matches the route for the **Outgoing from UK** scenario folder for mail going out of the UK office and the route in the **Incoming to JP** scenario folder for mail coming into the Japan office with the same priority:

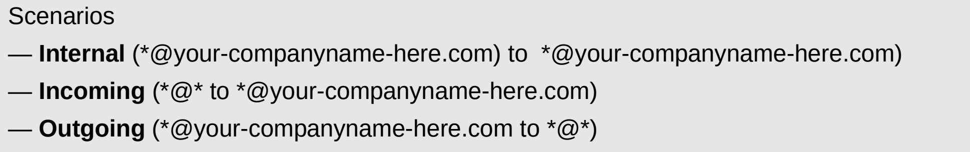
- With the **Process using sender's policy and recipient's policy** check box cleared, MIMEsweeper gives more weighting to the sender address (`pat@your-companyname-here.co.uk`) and determines that the **Outgoing from UK** scenario folder (`*@your-companyname-here.co.uk to *@*`) is the closest match. It applies the policies in that folder before routing the message to Tomoko.

Since MIMEsweeper did not consider the **Incoming to JP** scenario folder the closest match, it does not apply the policies in that folder before delivering the message to Tomoko.

- With the **Process using sender's policy and recipient's policy** check box selected, MIMEsweeper gives more weighting first to the sender address (`pat@your-companyname-here.co.uk`) and determines that the **Outgoing from UK** scenario folder (`*@your-companyname-here.co.uk to *@*`) is the closest match. It applies the policies in that folder when Pat sends the message.

  MIMEsweeper then processes the message again, this time giving more weighting to the recipient address (`tomoko@your-companyname-here.co.jp`) and determines that the **Incoming to JP** scenario folder (`*@* to *@your-companyname-here.co.jp`) is the closest match. It applies the policies in that folder before delivering message to Tomoko.

This option has no effect on scenario folders hierarchies that use a separate folder with a more explicit route at the same level as the default **Incoming** and **Outgoing** folders as shown in Figure 2-3.



Scenarios

— **Internal** (*@your-companyname-here.com) to *@your-companyname-here.com)

— **Incoming** (*@* to *@your-companyname-here.com)

— **Outgoing** (*@your-companyname-here.com to *@*)

Figure 2-3: Sender/recipient processing—separate internal mail folder

Under this scenario folder hierarchy, whether or not the **Process using sender's policy and recipient's policy** check box is selected, the sender / recipient pairs in email messages between individuals at `your-companyname-here.com` will always most closely match the route in the **Internal** folder: the **Incoming** and **Outgoing** folders will never match more closely.

For further details on using the **Policy Options** tab to configure the address to be used for email message processing, see the MIMEsweeper Policy Editor help.

Engine

In the **Engine** tab, you configure the recursion depth to which MIMEsweeper for SMTP decomposes complex data formats, set a memory limit for message processing, and set a timeout limit for message processing.

- **Recursion Depth**

  Recursive disassembly is the process whereby the Content Engine decomposes an email message into its component parts, no matter how many times an object or file may have been compressed or embedded in an email message. This ensures that all of the data is analyzed.

  The Content Engine:

  - Disassembles email messages and attachments into their component parts. For example, text files, bitmaps, binary files, and application executable files.

  - Checks policy actions.
  - Applies defined policies.
  - Reassembles the email message for delivery.

  For further information on configuring the depth of recursive disassembly, see the MIMEsweeper Policy Editor help.

- **Memory Limit**

  A Memory Limit to be used during the processing of each message can be specified. The amount of disk space to be used if this memory limit is exceeded during processing can also be specified.

- **Timeout Limit**

  The length of time that the system will spend processing a message can be specified here in seconds.

Classifications

You configure how MIMEsweeper Policy Editor deals with messages and whom it notifies about them by creating classifications under the **Classifications** folder under the **Policies** folder in the MIMEsweeper Policy Editor. You associate a classification with a scenario when you configure the scenario. For details on scenarios, see Chapter 4.

A number of default classifications are created when you install MIMEsweeper Policy Editor. You can change the default classifications and add your own classifications. For information, see Chapter 3.

The position of a classification in the **Classifications** folder determines its priority. The classification type affects its position in the list, and thus its priority. These concepts are described in *Classification type* and *Classification priority* on page 2-17.

Classifications define actions, which specify how MIMEsweeper should dispose of email messages processed by a scenario. The role of actions is described in *Actions* on page 2-18. The position of an action in a classification determines its priority. For details, see *Action priority* on page 2-18. For details on classifications and the actions you can define in them, see Chapter 3.

Full details on classification and action properties, as well as procedures for working with them, such as creating new classifications, changing the properties of existing actions and changing the type or priority of a classification, are provided in the MIMEsweeper Policy Editor help.

Classification type

Each classification is one of the following types:

- **Exclusive**

  An exclusive classification defines the primary action or actions to be applied to an email message that matches the criteria specified for the scenario associated with the classification. Only one exclusive classification can be applied to a single message.

MIMEsweeper Policy Editor creates a number of default exclusive classifications. You can also create your own.

MIMEsweeper Policy Editor also creates a number of default system classifications: Clean, Encrypted, and Undetermined. These system classifications are a special subtype of the exclusive classification. You cannot change the type of a system classification, nor can you create your own.

- **Inclusive**

  An inclusive classification defines any supplemental actions to be applied to an email message in addition to those defined in an exclusive or system classification. Any number of inclusive classifications can be applied to a single message.

  You must create any inclusive classifications you need; MIMEsweeper does not create any default inclusive classifications.

  The distinction between inclusive and exclusive classifications is different from that between inclusive and exclusive scenarios. For further information, see Chapter 4.

For further details on the default classifications, see Chapter 3. For information on creating classifications, changing their properties, or viewing and changing the classification type, see the MIMEsweeper Policy Editor help.

Classification priority

The priority of a classification is determined by its position in the list in the **Classifications** folder under the **Policies** folder in the Policy Editor. The higher the classification is in the list, the higher the priority it has.

The classification type affects a classification's position in the list, and thus its priority. Exclusive classifications are listed in order of priority, with the classifications at the top of the list taking precedence over those lower down the list. Any number of inclusive classifications can be applied to a message, so their position in the list is not significant. Therefore, exclusive classifications are listed above inclusive classifications. For details on exclusive and inclusive classifications, see *Classification type* on page 2-16.

The position of exclusive classifications in the list is significant because even if a message matches more than one scenario, only one exclusive classification can be applied to the message. MIMEsweeper applies the exclusive classification with the highest priority, which is the one that appears higher up the list.

You can change a classification’s priority by promoting it or demoting it in the list. For details on changing the priority of a classification, see the MIMEsweeper Policy Editor help.

If a message does not match any exclusive classification, MIMEsweeper applies the **Clean** classification and delivers the message normally.

⚠ If you remove the **Deliver** action from the **Clean** classification, MIMEsweeper for SMTP does not deliver your messages. If no other actions are defined, then the message is deleted.

Actions

For each classification, you can define one or more actions, which specify what you want MIMEsweeper to do with the items that match the criteria specified in the associated scenarios and how to record and disseminate information about the detected items.

After MIMEsweeper matches a message to a scenario and applies the associated classification, it performs the actions specified for that classification.

You could, for example, define an **Inform** action in the **Dirty Out** classification to have MIMEsweeper send to a message sender an email containing a note that a message was blocked. To this note, you also could add:

- A copy of the email message.
- An HTML link to your organization’s email policy.
- An HTML summary of the results of a text analysis scenario.

You can add to or change the actions defined for default classifications, though you are not recommended to do so. For information about the actions you can define for classifications in MIMEsweeper Policy Editor, see Chapter 3. For details on changing options in the properties page for actions, see the MIMEsweeper Policy Editor help.

⚠ If you do not define an action for a classification, MIMEsweeper Policy Editor deletes the email message.

Action priority

The priority of an action is determined by its position in the list of actions defined for a classification. Actions are applied in the order they appear in the list from top to bottom. Therefore, when more than one action is defined for a classification, ensure that they are listed in the logical order in which they should be applied.

When you define a new action, it appears below any previously defined actions defined for that classification.

Scenarios

You configure the way MIMEsweeper Policy Editor implements the policies you have defined by configuring routes in the **Scenarios** folder under the **Policies** folder in the MIMEsweeper for SMTP folder. In scenario folders, you define scenarios to implement a range of policies that cover both content and work-flow management, and you specify the individuals and groups of users to whom the policies apply.

You create scenarios within scenario folders, which specify the sender / recipient routes to which the policy is to apply. You define these routes by specifying sender and recipient address combinations. For the sender and for the recipient, you can specify either an individual address or an address list. For information, see *Specifying addresses* on page 2-3.

A number of default scenario folders are created when you install MIMEsweeper Policy Editor. You can change these default scenario folders and add your own scenario folders. For information, see *Default scenario folders* on page 2-20.

Scenario folders are arranged in a hierarchy, which enables you to refine how your policies are applied to email messages. For information, see *Scenario folder hierarchy* on page 2-21.

A lower-level scenario folder located beneath a higher-level scenario folder in the hierarchy automatically inherits the scenarios from its higher-level scenario folder. For information, see *Scenario folder inheritance* on page 2-22. You can control this automatic inheritance by changing the state of an inherited scenario. For information, see *Scenario state* on page 2-23. The effect of changing the state of a scenario may depend on the scenario type. For information, see *Scenario type* on page 2-23.

MIMEsweeper checks the route defined in all of the scenario folders for matches with the route specified in the email. It determines which scenario folder to apply to the sender / recipient pairs in the email message based on whether there were single or multiple matches. For information, see *Scenario folder matching* on page 2-24.

When the route in an email matches the route specified in the scenario folder, the scenarios within that folder are applied to the email. For information about available scenarios, see Chapter 4.

Full details on scenario properties, as well as procedures for working with scenarios, for example, creating new scenarios, changing the properties of existing scenarios, and moving and copying scenarios, are provided in the MIMEsweeper Policy Editor help.

Default scenario folders

MIMEsweeper creates three default scenario folders. Each of the default scenario folders, except for the top-level **Scenarios** folder, references the default address lists `Everyone` (defined as `*@*`) and `<company_domain_name>`.

The default scenario folders are:

- **Scenarios**

  This is the root of the scenario folder tree. This top-level folder processes all mail by matching the sender `*@*` with recipient `*@*`.

- **Incoming**

  This subfolder processes incoming mail by matching the sender `*@*` with recipient `*@<company_domain_name>`.

- **Outgoing**

  This subfolder processes outgoing mail by matching the sender `*@<company_domain_name>` with recipient `*@*`.

You cannot change the route information for the default **Scenarios** folder. You can change the route information for the default **Incoming** and **Outgoing** scenario folders. You can create scenarios directly in any of these default folders, or below these folders, you can create hierarchies that are simple to trace and manage. For information on creating scenario folders, see the MIMEsweeper Policy Editor help.

If you have synonyms defined for your domain, you must add these synonym domains to the scenario folders or to the address lists used by the scenario folders. For details on synonyms, see Chapter 6.

Scenario folder hierarchy

Scenario folders are presented as a hierarchy as shown in Figure 2-4.

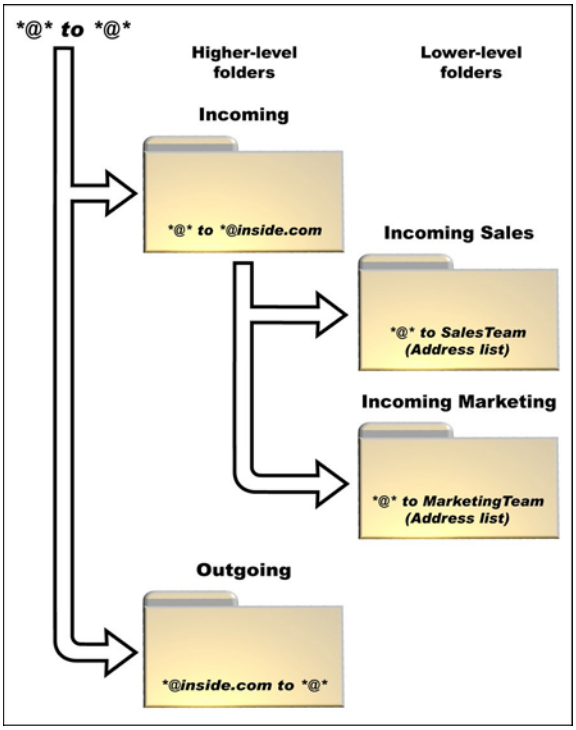


Figure 2-4: Scenario folder hierarchy

The position of scenario folders within the hierarchy affects how MIMEsweeper Policy Editor matches routes in order to determine which policies to apply to an object.

MIMEsweeper Policy Editor evaluates the folders in the hierarchy as follows:

1. MIMEsweeper first checks each of the higher-level folders in the hierarchy to find the folder whose route is the most specific match for the route in an email message. If more than one of the higher-level scenario folders has an equally specific matching route, then MIMEsweeper gives precedence to the folder that appears highest up in the list of scenario folders.
2. MIMEsweeper next checks each of the lower-level folders beneath the matched higher-level folder to find the folder whose route is the most specific match for the route in an email message. If more than one of these lower-level scenario folders has an equally specific matching route, then MIMEsweeper gives precedence to the folder that appears highest up in the list of scenario folders.

3. MIMEsweeper repeats this process for any subfolders beneath the matched lower-level folder to find a folder whose route is the most specific match for the route in an email message. When no subfolders beneath the last matched folder has a more specific match for the route, MIMEsweeper stops searching the hierarchy and uses the last matched folder.

Understanding this evaluation order will help you to make effective use of the scenario hierarchy and provide you with greater control over the design of your policies.

Folders at higher levels in the hierarchy define general routes, for example all messages entering your organization's domain. Folders at lower levels define more specific routes. For example:

- The default top-level **Scenarios** folder specifies the global route for all messages passing through your organization's domain (`*@*` to `*@*`).
- The default second-level **Incoming** scenario folder specifies the general route for any messages destined for your domain (`*@*` to `*@<your domain>`), and the default **Outgoing** scenario folder specifies the general route for any messages leaving your domain (`*@<your domain> to *@*`).
- Lower-level subfolders further refine the route by specifying routes for specific groups of users or for exceptions to global routes. For example, a subfolder under the **Incoming** scenario folder specifies a more specific route for mail incoming to users in the Sales Team. Similarly, an **Incoming to Marketing** folder would specify a specific route for users in Marketing, and this folder could contain a scenario to allow members of Marketing to receive video files even if a scenario in a higher-level folder blocked such attachments.
- If you have more than one folder at a given level, place the most important ones in the list above less important ones.

You can see which scenario folder will match a specific message by using the **Identify Policy** dialog box from the **Policies** folder in the MIMEsweeper for SMTP folder. For information, see the MIMEsweeper Policy Editor help.

If you have specified a large LDAP address list, there may be a delay before the **Identify Policy** dialog box is displayed. The cursor changes to a Busy pointer while MIMEsweeper dynamically creates the LDAP address list and checks the route. For details on LDAP address lists, see *LDAP address lists* on page 2-11.

Scenario folder inheritance

A subfolder in the hierarchy automatically inherits the scenarios contained in the folder immediately above it in the hierarchy. This inheritance enables you to create global policies by placing scenarios in a folder at the highest level of the hierarchy you want the scenario applied to.

If you want a scenario to be active throughout a folder and its subfolders, place it at the top of the hierarchy. This scenario is then inherited by the folder's subfolders. For example, if you define a Virus Manager scenario in the **Incoming** folder, the scenario is applied to any subfolders of the **Incoming** folder.

For further details on how to use the scenario folder hierarchy to define policy, see the MIMEsweeper Policy Editor help.

Scenario state

For special cases or exceptions, you may not want a global policy scenario to apply to a specific user or group. For example, you can have MIMEsweeper block delivery of all large video files to everyone in your organization except those in the Marketing department.

In such cases, you can create specific policies for particular users by placing scenarios in lower-level subfolders or by changing the state of an inherited scenario in its origin folder and in different subfolders:

- **Enabled**

  The current state of a scenario is displayed in the Details pane in the **Enabled** column, which is marked **Yes** if the scenario is currently turned on in the specified folder, or **No** if the scenario is currently turned off in the specified folder. If set to **No** in the scenario's origin folder and all of its subfolders, the scenario can only be enabled again in the origin folder.

- **Overridable**

  The current state of a scenario is displayed in the Details pane in the **Overridable** column, which is marked **Yes** if the scenario can be turned off in the subfolder, or **No** if the scenario can not be turned off in the subfolder. In the latter case, you can turn the scenario off only in the origin folder, that is, the folder in which the scenario was created.

The effect of changing the scenario state may depend on the scenario type. For procedures for changing the state of scenarios, see the MIMEsweeper Policy Editor help.

Scenario type

Each scenario is one of the following types:

- **Exclusive**

  Only one instance of this scenario type can be enabled in a scenario folder or subfolder at any one time.

- **Inclusive**

  Multiple instances of this scenario type can be enabled in a scenario folder or subfolder at any one time.

> The distinction between inclusive and exclusive scenarios is different from that between inclusive and exclusive classifications. For further information, see Chapter 3.

The effect of changing the scenario state may depend on the scenario type. If you enable an instance of an exclusive scenario, other instances of that scenario type are automatically disabled in the current folder and in either its subfolder or its immediate higher-level folder in the hierarchy. For further information, see the MIMEsweeper Policy Editor help.

Scenario folder matching

When MIMEsweeper Policy Editor processes an email message, it first categorizes the route information by pairing the sender of the email with each recipient to create:

- A single sender / recipient pair
- Multiple sender / recipient pairs

MIMEsweeper Policy Editor then compares each of these sender / recipient pairs to the sender / recipient pair specified in the route for each scenario folder to determine which folder's route best matches.

MIMEsweeper Policy Editor attempts to match the sender / recipient pairs from an email message to the route in a higher-level folder in the hierarchy. When it finds a match, it then attempts to match the lower-level folders beneath only that higher-level folder in the hierarchy. It continues in this way until it cannot find a better match at a lower level beneath the last level matched. This means that MIMEsweeper does not check every folder in the hierarchy.

When it determines which folder is the best match, MIMEsweeper applies the active scenarios in that folder to the message. If there is not a match to a scenario folder with a more specific route, then the top-level **Scenarios** folder is considered the best match and its scenarios are applied to the message. The **Scenarios** folder normally has a route defined as all senders (`*@*`) to all recipients (`*@*`).

The following scenario folder matches are possible:

- All sender / recipient pairs from the message match only one scenario folder.

  MIMEsweeper applies all active scenarios in that scenario folder to the message. For details, see *Single scenario folder matches* on page 2-25.

- All sender / recipient pairs from the message match more than one scenario folder.

  MIMEsweeper uses folder priority and positioning to determine which one scenario folder to apply. For details, see *Multiple scenario folder matches and route priority* on page 2-26 and *Multiple scenario folder matches and positioning* on page 2-28.

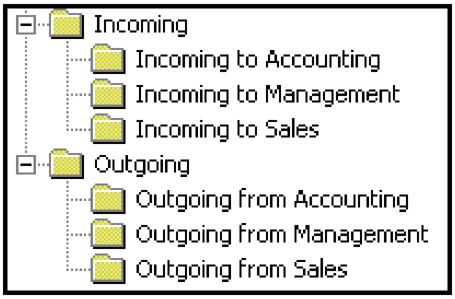
- Different sender / recipient pairs from the message match different scenario folders.

  MIMEsweeper uses folder priority and positioning to determine which scenario folder to apply to which sender / recipient pairs and then splits the original message into as many separate messages as are required to apply each matched scenario. For details, see *Multiple scenario folder matches and route priority* on page 2-26, *Multiple scenario folder matches and positioning* on page 2-28, and *Multiple scenario folder matches and message splitting* on page 2-29.

Single scenario folder matches

If the sender / recipient pairs in an email match only one scenario folder MIMEsweeper applies the scenarios in that folder to the message.

This is illustrated by an example scenario folder hierarchy with a number of new folders added below the default **Incoming** and **Outgoing** folders as shown in Figure 2-5.



Incoming
Incoming to Accounting
Incoming to Management
Incoming to Sales
Outgoing
Outgoing from Accounting
Outgoing from Management
Outgoing from Sales

Figure 2-5: Scenario folder matches

MIMEsweeper looks in these scenario folders for a route that best matches the sender / recipient pairs in the message in the following order:

1. Checks the **Scenarios** folder.
2. Checks the **Incoming** and **Outgoing** folders.
3. If the **Incoming** folder has the closest match, MIMEsweeper then checks its subfolders for a closer match:

   a. **Incoming to Accounting**

   b. **Incoming to Management**

   c. **Incoming to Sales**

   Alternatively, if the **Outgoing** folder has the closest match, MIMEsweeper checks its subfolders for a closer match:

   a. **Outgoing from Accounting**

   b. **Outgoing from Management**

   c. **Outgoing from Sales**

Once MIMEsweeper has identified the folder with the closest match to the sender / recipient pairs in the message, it applies the scenarios defined in that scenario folder as follows:

1. The default route in the **Scenarios** folder was the best match for all of the sender / recipient pairs in an email message. MIMEsweeper applies the scenarios defined in the **Scenarios** folder. These are global policies to be applied to all email users in the organization’s domain.
2. All of the sender / recipient pairs in an email message most closely match the route in the **Incoming** scenario folder.

Table 2-1: Incoming scenario folder

Route	Address list	Address specification
Sender	Everyone	`*@*`
Recipient	Your Company Name	`*@your-companyname-here.com`

MIMEsweeper applies the scenarios defined in the **Incoming** scenario folder. These are general scenarios defined for all incoming mail.

3. All of the sender / recipient pairs in an email message most closely match the route in one of the subfolders under the **Incoming** scenario folder (**Incoming to Accounting**, **Incoming to Management**, and **Incoming to Sales**), for example, the **Incoming to Accounting** subfolder.

Table 2-2: Incoming to Sales scenario folder

Route	Address list	Address specification
Sender	Everyone	`*@*`

Recipient	Accounts	`amy@your-companyname-here.com`
		`debbie@your-companyname-here.com`
		`philip@your-companyname-here.com`

MIMEsweeper applies the scenarios defined in the **Incoming to Accounting** subfolder. This includes both scenarios inherited from the **Incoming** scenario folder and more specific scenarios defined for the members of the Accounts group.

4. All of the sender / recipient pairs in an email message most closely match the route in the **Outgoing** scenario folder. MIMEsweeper applies the scenarios defined in the **Outgoing** scenario folder. These are general scenarios defined for all outgoing mail.
5. All of the sender / recipient pairs in an email message most closely match the route in one of the subfolders under the **Outgoing** scenario folder (**Outgoing from Accounting**, **Outgoing from Management**, and **Outgoing from Sales**). MIMEsweeper applies the scenarios defined in the matched subfolder. These includes both scenarios inherited from the **Outgoing** scenario folder and more specific scenarios defined for the members of the users in the matched route.

Multiple scenario folder matches and route priority

If sender / recipient pairs from an email message match more than one scenario folder, MIMEsweeper applies the folder with the higher priority.

The priority of scenario folders is based on how the sender and recipient addresses have been specified in the scenario folder routes. For information on explicit, fully wildcarded, and partially wildcarded addresses, see *Specifying addresses* on page 2-3. MIMEsweeper identifies the position and number of wildcard characters used in the address or address list specification, where a fully wildcarded route (`*@*` to `*@*`) is the most general, and an explicit user name and location route (`user@domain1` to `user@domain2`) is the most specific.

Sender and recipient addresses obtained from an LDAP address list always contain explicit user names and locations, so MIMEsweeper treats them as fully qualified manual addresses. Therefore, if different scenario folders contain the same LDAP addresses, MIMEsweeper assigns the folders the same priority. For details on LDAP address lists, see *LDAP Address Lists* on page 9-16.

Manually specified addresses are prioritized from highest to lowest depending on the specification of the user name and location elements as follows:

- An explicit user name and location
- An explicit user name and a partially wildcarded location
- A fully wildcarded user name and an explicit location
- A fully wildcarded user name and a partially wildcarded location
- A fully wildcarded user name and a fully wildcarded location

For details on manual address lists, see *Manual address lists* on page 9-15.

If the sender/recipient pair in an email message matches the route information in two scenario folders with equal priority, MIMEsweeper selects the first of these folders in the hierarchy.

Take, for example, the route information for two scenario folders shown in Table 2-3.

Table 2-3: Scenario folder route information

Scenario folder	Sender	Recipient
Sales to Marketing	`*@sales.your-companyname-here.com`	`*@marketing.your-companyname-here.com`
Ali to Marketing	`ali@sales.your-companyname-here.com`	`*@marketing.your-companyname-here.com`

Both folders have identical recipient information, but the sender address in the **Ali to Marketing** scenario folder is explicit, so it has a higher priority than the partially wildcarded sender address in the **Sales to Marketing** scenario folder. An email sent from `ali@sales.inside-yourcompany.com` to `andy@marketing.inside-yourcompany.com` matches both scenario folders, so MIMEsweeper applies the scenario folder with the higher priority, **Ali to Marketing**, to this email.

Multiple scenario folder matches and positioning

If sender / recipient pairs from an email message match more than one scenario subfolder beneath the folder matched at a higher-level, MIMEsweeper applies the scenario subfolder that appears higher in the list of scenario folders immediately beneath the higher-level matched folder.

Thus, the relative position of the scenario subfolders in the list of scenario folders is significant, particularly when you want to define different policies for members of different departments. Typically, organizations have policies specifying that there are types of email that members of one department can receive and send that members of the other department cannot. This can cause conflicts between email policies when an individual is a member of two departments and so is on two address lists.

For example, as shown in Table 2-4, `catherine@your-companyname-here.com` is a member of both the Management and the Sales address lists.

Table 2-4: Address lists

Management address list	Sales address list
andy@your-companyname-here.com	catherine@your-companyname-here.com
catherine@your-companyname-here.com	dieter@your-companyname-here.com
	pat@your-companyname-here.com
	simon@your-companyname-here.com

Figure 2-6 shows that the **Incoming to Sales** scenario folder is located on the list above the **Incoming to Management** scenario folder at the same level of the hierarchy.

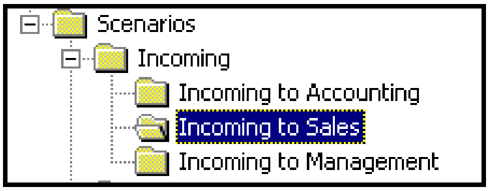


Figure 2-6: Incoming to Sales scenario folder

Therefore, MIMEsweeper applies scenarios in the **Incoming to Sales** scenario folder to email messages containing a recipient of `catherine@inside-yourcompany.com`. This could mean that Catherine could be restricted from receiving messages that she needs as a member of the Management team.

This can be resolved by moving the **Incoming to Management** scenario folder to a position higher in the list of folders at the same level in the hierarchy as shown in Figure 2-7.

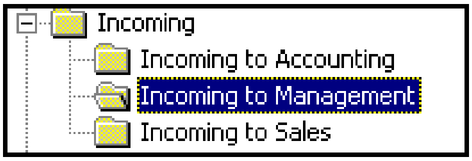


Figure 2-7: Incoming to Management scenario folder

With the scenario folder in this position, MIMEsweeper applies scenarios defined for members of the Management team to `catherine@inside-yourcompany.com` rather than scenarios defined for members of Sales.

Multiple scenario folder matches and message splitting

If different sender / recipient pairs from the message match different scenario folders, MIMEsweeper makes a copy of the message for each matched folder. Note that the number of copies it creates is based on the number of scenario folders matched and not the number of different sender / recipient pairs in the original email message.

This process of creating copies of email messages is known as message splitting. For example, Figure 2-8 shows an email message that is sent from an outside organization to three different recipients based in the Sales, Accounting, and Marketing departments.

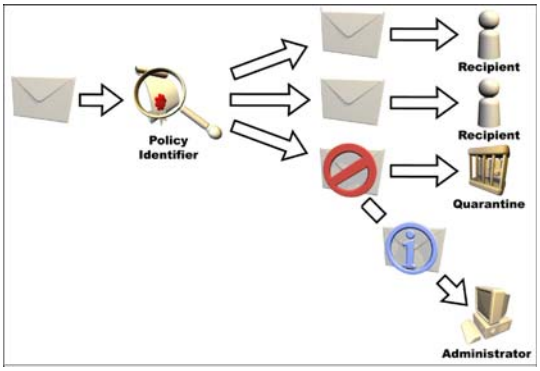


Figure 2-8: Message splitting

There are different scenario folders for Incoming to Sales, Incoming to Accounting, and Incoming to Marketing, so MIMEsweeper processes this message as follows:

1. It splits the message to create three separate messages, one for each scenario folder.
2. For each new message, it applies the scenarios in the matched scenario folder.

Many email messages contain information that is confidential to your organization. A number of these messages are for genuine business purposes, so to block delivery solely according to the content of the message would be counter-productive. Message splitting enables you to block delivery to specific individuals or groups rather than to everyone in your organization.

Message areas

You configure where MIMEsweeper Policy Editor places email messages flagged by a policy by configuring message areas listed in the Details pane for the **Message Areas** folder in the MIMEsweeper for SMTP folder. MIMEsweeper uses message areas, for example, to place email messages whose delivery it has blocked. For details on changing message area properties, see the MIMEsweeper Policy Editor help.

There are two types of message area:

- **Quarantine**

  A storage area for messages that require operator intervention, such as messages containing viruses or prohibited data.

- **Parking**

  A storage area for messages whose delivery is to be delayed. For example, it is useful to delay the delivery of large email messages until outside normal working hours.

You can change the default message areas or add your own message areas. You can have a maximum of 64 message areas. For details on creating quarantine and parking areas, see the MIMEsweeper Policy Editor help.

You specify configuration options in the following tabs of the message area properties:

- Folder
- Management (quarantine areas only)
- Release (parking areas only)
- Usage
- Notes

These configuration details are briefly described in the following sections. For full details on configuring these properties, see the MIMEsweeper Policy Editor help.

Folder

In the **Folder** tab, you specify the name of the folder to contain the email messages assigned to the quarantine or parking area. MIMEsweeper for SMTP creates the new message area folder on the Policy Server. In deployments with more than one Policy Server, MIMEsweeper for SMTP creates the new message area folder on each Policy Server in your deployment.

When creating new message areas, either in distributed deployments or single machine installations, do not attempt to create these message area folders on any of your remote machines. This is not supported by the MIMEsweeper for SMTP software.

You can reference quarantine areas when you create quarantine actions.You can reference parking areas when you create park actions. For more information about quarantine and park actions, see Chapter 3. For further information on specifying the location of a message area, see the MIMEsweeper Policy Editor help.

Management (quarantine areas only)

In the **Management** tab, you specify if the area is to be managed by Personal Message Manager (PMM).

You can also allow messages which are released from this area to be used for spam training by selecting the appropriate check box. Using released messages in this way will result in a reduction in the number of false positives classified by the system.

Checking **Automatically delete messages** causes the system to delete messages when they have been held for the period specified.

For information on setting or changing the schedule for deleting messages held in a quarantine area, see the MIMEsweeper Policy Editor help.

For further details on viewing message areas and folders, and PMM management, see Chapter 10.

Release (parking areas only)

In the **Release** tab, you configure when parked messages are to be released. This is done by selecting a release period by clicking and dragging on the timescale to select the period required. Each division on the scale represents 30 minutes, and is red to show when messages will be held, and green to show the periods when they will be released.

You also specify the maximum number of messages to be released by the system in each of the 30 minute periods. The default is one message.

Usage

In the **Usage** tab, a list of the classification actions that the message area is used by is given. Highlighting a classification, and clicking the **Show** button shows the classification details in the Policy Editor.

Alerters

You configure whether MIMEsweeper Policy Editor generates notification messages to specified users or computers and the address it sends them to by creating an alerter under the **Alerters** folder in the MIMEsweeper for SMTP folder. For details on changing options in the properties page for an alerter, see the MIMEsweeper Policy Editor help.

An alerter is responsible for routing notifications of errors and significant events to a specified destination, such as an SNMP Manager. For example, when a message is moved to the MIMEsweeper Recovery folder, an event is recorded in the Windows Application Log, causing MIMEsweeper for SMTP to issues an alert if one is configured.

MIMEsweeper for SMTP can be configured to use any of the following types of alerter:

- Administrative Alerter
- SMTP Alerter
- SNMP Alerter

You can create only one instance of each type of alerter. These are briefly described in the following sections. For further information on creating alerters, see the MIMEsweeper Policy Editor help.

Administrative Alerter

The MIMEsweeper Administrative Alerter uses the Windows alerts service, which notifies selected users and computers of administrative alerts that occur on a computer. An administrative alert relates to server and resource use, such as problems with security, access, and user sessions. The messenger service sends and receives the Messages transmitted by the Alerter service.

Alerts can be generated by MIMEsweeper based system events, or they can be configured by a user in an Alert action defined in a classification.

In order for alerts to be sent, the Administrative Alerter and Messenger services must be running on all Policy Servers. For alerts to be received, the Windows Messenger service must be running on the machine configured to receive alerts.

SMTP alerter

The MIMEsweeper SMTP Alerter sends email alert messages from a specified SMTP email server to one or more specified recipients. The email alert message relates to the health of a server or service.

Alerts can be generated by MIMEsweeper based system events, or they can be configured by a user in an Alert action defined in a classification.

SNMP alerter

The MIMEsweeper SNMP Alerter interfaces to the Simple Network Management Protocol (SNMP) service, which supports computers running the TCP/IP protocol. In SNMP, agents monitor the activity in the various devices on the network and send an SNMP trap to an SNMP management system when they detect that a certain event type has occurred locally on the managed host. MIMEsweeper sends alerts as SNMP traps.

Alerts can be generated by MIMEsweeper based on system events, or they can be configured by a user in an Alert action defined in a classification.

Before you can configure an SNMP Alerter, you must first install and configure the Microsoft SNMP service on each Policy Server.

References

You configure common text and language details to be used by a number of scenarios that perform text analysis by setting options for the **References** folder in the MIMEsweeper for SMTP folder. You can create References for Text Analyzer and Commercial Disclaimer scenarios to scan the content of email messages for specified words or phrases.

The following types of reference are available, in both Managed and User Defined form, within MIMEsweeper for SMTP:

- **Script list**

  A list of script expressions that MIMEsweeper Policy Editor uses to identify text strings within messages.

- **Expression list**

  A list of keywords and phrases that MIMEsweeper Policy Editor is to detect during text analysis.

- **Checksum list**

  A list of checksums that MIMEsweeper Policy Editor is to detect during message analysis. Each checksum consists of a string of 40 alphanumeric characters.

For further information on references, see Chapter 5.

Servers

To view the **Properties** page for the **Servers** folder, select the folder, and then select **Properties** from the **Action** menu. The following tab will be displayed:

Audit disposer

The Audit Disposer writes audit information to the database.

Choose the Audit Disposer you require from the drop-down list. More than one can be installed on the system, but only the one chosen here is active.

The option of choosing **No active disposer** is also available from the drop-down list.

To view the **Properties** page for an individual server, open the **Servers** folder, select the server required, and then select **Properties** from the **Action** menu. The following tabs will be displayed:

Logging

In the **Logging** tab, you configure what transport logging information MIMEsweeper Policy Editor is to generate by selecting or clearing the following:

- **Log events**

  Log events performed by the Receiver and Delivery services to the Windows Event Log.

- **Log errors**

  Log errors detected by the Receiver and Delivery service to the Windows Event Log.

- **Log basic trace information**

  Log basic trace information on SMTP connections, SMTP commands, and recipient information.

- **Log detailed trace information**

  Log more detailed information on the content of each processed message.

Folders

In the **Folders** tab, you specify the location on the file server for the following folders:

- **Checked messages**

  This folder contains email messages MIMEsweeper considers safe for the Delivery service to attempt to deliver to the recipient addresses.

- **Spool**

  This folder contains the other working folders in which MIMEsweeper for SMTP places all the email messages it handles.

- **Recovery**

  This folder contains messages MIMEsweeper for SMTP is unable to process.

- **Working Folder**

  This folder is used to hold messages while they are analyzed by the system.

- **LDAP Address List cache**

  This folder is used to store the cached LDAP address lists.

Base Folders

In the **Base Folders** tab, you specify the location on the file server for the following MIMEsweeper base folders:

- **Message area base folder**

  This folder is the top level folder for all message area folders.

- **Content Analysis Queue base folder**

  This folder is the top level folder for all Content Analysis Queue folders.

- **Save action base folder**

  This folder is the top level folder for all Save action folders.

- **Archive action base folder**

  This folder is the top level folder for all Archive action folders.

For the Archive and Save actions base folders you are recommended to specify a folder on a different drive from that on which your MIMEsweeper system is installed. This is because these folders may use a large amount of disk space, and a shortage of disk space causes MIMEsweeper performance problems.

Advanced Paths

Advanced Paths provides overrides for the minimal setup of MIMEsweeper, and displays the following two columns:

- **Advanced Path**

  Shows the path originally used in the Policy Editor.

- **New Path**

  Shows the path where it is now pointed to.

These paths can be modified with the buttons provided at the bottom of the screen:

- **Add**

  Opens the **Add Advanced Path** dialog box. From the **Advanced path** field access a drop-down list from which the path requiring modification can be chosen.

  The selected path appears in the **Advanced path** field. Enter the path that is to become the new advanced path into the **New path** field and click **Add**. The details now appear in the list in the **Advanced Paths** tab.

- **Edit**

  Selecting a path from the list and click **Edit** to open the **Edit Advanced Path** dialog box, allowing you to modify the entry as required.

- **Delete**

  Select a path from the list and click **Delete** to remove the selected entry.

⚠ No confirmation message is shown for the delete operation, chosen entries are removed instantly. Ensure that you have chosen correctly before clicking **Delete**.

Routing

In the properties page for Routing you can restrict the maximum number of delivery connections to the chosen server. This controls the traffic which has to be handled, and prevents swamping the server.

- **Connection**

  Select the **Maximum number of delivery connections to any server** check box, then enter the required number in the field provided. The maximum number of connections allowed is 500. Click **Apply** to implement the changes.

CHAPTER 3

Classifications

This chapter provides more detailed information on classifications, describing each of the actions that you can define in a classification in MIMEsweeper for SMTP. It supplements the information on classifications in Chapter 2.

Overview

A classification defines one or more actions, which specify what to do with items that match the criteria specified in the associated scenarios and how to record and disseminate information about the items.

You associate one or more classifications with a scenario. After performing the content analysis specified in the scenario on an email message, MIMEsweeper takes the actions defined in the associated classification.

MIMEsweeper Policy Editor creates a number of default classifications during installation. These are described in the second section of this overview, *System classifications* on page 3-4.

You determine what MIMEsweeper does with email messages detected by a scenario by defining actions for classifications in the **Classifications** folder under the **Policies** folder in the MIMEsweeper Policy Editor. Actions are displayed in the details pane for the associated classification. This is described in the third section in this overview, *Action properties* on page 3-4.

The remaining sections in this chapter provide reference information on each action that is available in the MIMEsweeper Policy Editor. The action reference pages are presented in alphabetical order. Each reference page provides a summary of the action properties you can configure and provides notes on any special features and restrictions you should be aware of when configuring the action.

Full details on classification and action properties, as well as procedures for working with them (for example, creating new classifications, changing the properties of existing actions, changing the type or priority of a classification) are provided in the MIMEsweeper Policy Editor help.

System classifications

MIMEsweeper Policy Editor creates a number of system classifications during installation. Table 3-1 lists the system classifications in their default priority order, identifying the actions defined in them and their type.

Table 3-1: System classifications

Classification	Associated Action	Type
Encrypted	Quarantine	System exclusive
Undetermined	Quarantine	System exclusive
Clean	Deliver	System exclusive

You can use these system classifications, and you can create additional classifications of your own. You must create any inclusive classifications you need; MIMEsweeper does not create any default inclusive classifications. For further details on classifications, see the MIMEsweeper Policy Editor help.

The **Clean** classification is a special type of exclusive classification, and is always the lowest-priority exclusive classification. When an email matches no other exclusive classification, the **Clean** classification is applied, and the email is delivered normally.

If you change a classification that is linked to a scenario, you must Save and Apply your changes. The system will then automatically stop and start the MIMEsweeper for SMTP Security service to action the changes.

If you remove the Deliver action from the **Clean** classification, MIMEsweeper Policy Editor does not deliver processed messages but deletes them.

Action properties

You can create new actions using wizards. You can change the properties of an existing action by configuring options in the tabs of its properties page. For details on how to create or change actions, see the MIMEsweeper Policy Editor help.

The options you can configure for each action are described in the action reference pages later in this chapter. All action properties pages contain the following tabs:

- **General**

  The details of the item, including the item type and a summary of the properties of the item.

- **Notes**

  Any user-specified text describing the item, for example, details of how the item or its configuration forms part of a policy.

Descriptions of these two generic tabs are not included in the scenario reference pages.

List of actions

This list shows the actions you can define in classifications in MIMEsweeper for SMTP:

- **Add Header**, see *Add Header* **on page 3-6**.
- **Alert**, see *Alert* on page 3-7.
- **Copy to Archive Account**, see *Copy to Archive Account* on page 3-8.
- **Copy to Archive Folder**, see *Copy to Archive Folder* on page 3-9.
- **Deliver**, see *Deliver* on page 3-10.
- **Forward**, see *Forward* on page 3-11
- **Inform**, see *Inform* on page 3-13.
- **Log**, see *Log* on page 3-15.
- **Non-Delivery Report**, see *Non-Delivery Report* on page 3-16.
- **Park**, see *Park* on page 3-17.
- **Quarantine**, see *Quarantine* on page 3-18.
- **Relay To**, see *Relay To* **on page 3-19**.
- **Reply**, see *Reply* on page 3-20.
- **Save**, see *Save* on page 3-22.

These actions are described in the following sections, for more details refer to the MIMEsweeper Policy Editor help.

Add Header

The Add Header action is used to add a header to a message. For example, it can add an X-header to a message before delivery which precedes a Deliver action. If configured correctly, this could indicate to the email client that the message has a high probability of being spam.

Properties

The properties of the Add Header action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor Help.

Header Details

The name of the message header to add, and the value it should take.

Action Name

The name for the new Add Header action.

ℹ If the message is to be Quarantined or Parked the message header will not be present, unless the Quarantine or Park action is set up to store any messages in modified format by MIMEsweeper for SMTP.

Alert

The Alert action sends a broadcast message to specified users and computers, using a configured Alerter.

An example of the use of this action would be to advise email system administrators or users of a possible email security threat. This method ensures that users who are logged onto their computer receive urgent messages even if they are not currently logged on to the email system.

Properties

The properties of the Alert action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Message

The text to appear in the Alert messages.

The text can include MIMEsweeper tokens that identify properties of the mail message generating the alert. For example, you can include the **%SENDER%** token to identify the sender of the message.

Tokens available here are:

- %ADMIN%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %REMOVEDNAMES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

For further information about these tokens, see Appendix I.

Special features and restrictions

Before the Alert action can issue a message, you must configure at least one of the available MIMEsweeper for SMTP Alerters:

- Administrative Alerter
- SMTP Alerter
- SNMP Alerter

When an alert action is triggered, the alert message is generated by all of the alerters that are configured in your MIMEsweeper for SMTP system.

Copy to Archive Account

The Copy to Archive Account action adds a Bcc recipient to email messages so that the messages are sent to an archive account in addition to the original recipients.

An example of the use of this action is to send copies of email messages processed by MIMEsweeper for SMTP to a central email account that is used to archive the messages according to your organization's email archiving policy.

Properties

The properties of the Copy to Archive Account action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Recipient

The email address of the archive account to send copies of email messages. This address is added to the email message as a Bcc address, so it cannot be seen by the other email message recipients.

Options

The form in which to archive the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment. You can also specify whether to include the results from any specified text analysis as an HTML attachment to the archived message.

If you choose to archive a message in its original form, rather than as modified by MIMEsweeper, be aware that an email message that poses a threat could enter your organization's email system.

Special features and restrictions

If your organization uses a folder for archiving rather than an email account, use the Copy to Archive Folder action instead.

Archived email messages contain the email address of the original sender. If a user viewing the archived message in an email client uses the Reply function, the reply message is sent to the original sender and not to the archive account email address.

Copy to Archive Folder

The Copy to Archive Folder action adds an archive index (`.idx`) file to a copy of the email message and places the copy in a specified folder for archiving. Archive index files contain information about their associated email messages and provide the means of archiving the messages in a suitable fashion.

An example of the use of this action is to store email messages processed by MIMEsweeper for SMTP in a specified local folder, which is used to archive the messages according to your organization's email archiving policy.

Properties

The properties of the Copy to Archive Folder action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Folder

The relative path to the folder to use to archive messages. The base folder for this operation is set in the **Base Folders** tab of the server's **Properties** page.

Options

The form in which to archive the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment. You can also specify whether to include the results from any specified text analysis as an HTML attachment to the archived message.

If you choose to archive a message in its original form, rather than as modified by MIMEsweeper, be aware that an email message that poses a threat could enter your organization's email system.

Special features and restrictions

If your organization uses an email account for archiving rather than a folder, use the Copy to Archive Account action instead.

Deliver

The Deliver action places email messages in the delivery queue for normal delivery to the intended recipient or recipients.

Properties

There are no properties for the Deliver action other than the generic **General** and **Notes** tab (for details, see *Action properties* on page 3-4). For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Special features and restrictions

The **Clean** classification by default contains a Deliver action. If you remove the Deliver action from the **Clean** classification, MIMEsweeper for SMTP does not deliver processed messages but deletes them.

Forward

The Forward action forwards an email message to specified addresses along with a message informing the recipient of the actions taken during MIMEsweeper message processing.

An example of the use of this action is to direct email messages sent to a utility account to a specific individual. Another example of its use is to send email to a system administrator who is responsible for monitoring possible contraventions of your content security policy.

Properties

The properties of the Forward action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Sender

The email account from which MIMEsweeper is to send messages. This can be the MIMEsweeper administrator email account, the MIMEsweeper Service email account, or any other email account in your organization's domain.

The email addresses for the MIMEsweeper administrator and the MIMEsweeper service accounts are specified in the **Addresses** tab of the MIMEsweeper for SMTP **Properties** page.

Recipients

The email accounts to receive forwarded messages sent by MIMEsweeper. You can specify whether the address is added to the email message as a To, Cc, or Bcc recipient.

Subject and Body

The content of the message MIMEsweeper is to send, including the text to appear in the Subject line of the email message and the text to appear in the body of the email message. The text can include MIMEsweeper tokens. For example, you can use the %SUBJECT% token to include the subject of the original email.

Tokens available for the message **Subject** are:

- %ADMIN%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %REMOVEDNAMES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

Tokens available for the message **Body** are:

- %ADMIN%
- %DETECTED%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %MODIFIED%
- %RCPTS%
- %RECOGNISED%
- %REMOVEDNAMES%
- %RESPONSES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

For further information about these tokens, see Appendix I.

You can also specify an alternative character set for MIMEsweeper to use for generating forward messages if your specified subject or body text contains characters that cannot be displayed by the US-ASCII character set. To access this feature, click the **Advanced** button.

Options

The form in which to forward the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment. You can also specify whether to include the results from any specified text analysis as an HTML attachment to the archived message.

If you choose to forward a message in its original form, rather than as modified by MIMEsweeper, be aware that an email message that poses a threat could enter your organization's email system.

Special features and restrictions

None.

Inform

The Inform action sends a notification message to specified recipients to notify them of the actions taken during MIMEsweeper message processing.

An example of the use of this action is to notify an individual that a threat, such as a virus, was detected in the email message.

Properties

The properties of the Inform action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Sender

The email account from which MIMEsweeper is to send messages. This can be the MIMEsweeper administrator email account, the MIMEsweeper Service email account, or any other email account in your organization's domain.

The email addresses for the MIMEsweeper administrator and the MIMEsweeper service accounts are specified in the **Addresses** tab of the MIMEsweeper for SMTP **Properties** page.

Recipients

The email accounts to receive forwarded messages sent by MIMEsweeper. You can specify whether the address is added to the email message as a To, Cc, or Bcc recipient.

Subject and Body

The content of the message MIMEsweeper is to send, including the text to appear in the Subject line of the email message and the text to appear in the body of the email message. The text can include MIMEsweeper tokens. For example, you can use the %SUBJECT% token to include the subject of the original email.

Tokens available for the message **Subject** are:

- %ADMIN%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %REMOVEDNAMES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

Tokens available for the message **Body** are:

- %ADMIN%
- %DETECTED%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %MODIFIED%
- %RCPTS%
- %RECOGNISED%
- %REMOVEDNAMES%
- %RESPONSES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

For further information about these tokens, see Appendix I.

You can also specify an alternative character set for MIMEsweeper to use for generating forward messages if your specified subject or body text contains characters that cannot be displayed by the US-ASCII character set. To access this feature, click the **Advanced** button.

Options

The form in which to send the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment. You can also specify whether to include the results from any specified text analysis as an HTML attachment to the archived message.

If you choose to attach a message in its original form, rather than as modified by MIMEsweeper, be aware that an email message that poses a threat could enter your organization's email system.

Special features and restrictions

None.

Log

The Log action adds an entry to the MIMEsweeper Log in the Microsoft Windows Event Log. You can view log entries using the MIMEsweeper Manager Systems Center. You can also configure some applications to take action in response to the addition of an entry to the Event Log.

An example of the use of this action is to configure the Microsoft Windows System Management Server (SMS) to send pager messages to specified recipients when MIMEsweeper adds an Event Log entry. This method ensures that users receive urgent messages even if they are not currently logged on to either the email system or the computer. It also provides an audit trail of MIMEsweeper application events.

Properties

The properties of the Log actions are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Message

The text of the entry that will be added to the Microsoft Windows Event Log. The text can include MIMEsweeper tokens.

Tokens available for the Message are:

- %ADMIN%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %REMOVEDNAMES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

For further information about these tokens, see Appendix I.

Special features and restrictions

The Microsoft Windows Event Log does not automatically delete and purge old entries. For information on clearing the contents of the Microsoft Windows Event Log, see the Microsoft Windows documentation.

Non-Delivery Report

The Non-Delivery Report action causes a forced delivery failure of the email messages. The non-deliver action generates a new message to the sender of the original message, stating that their message has not reached one or more of the specified recipients. The message to the sender includes the first 1024 characters of the original message.

An example of its use would be where messages arrive in your system for a recipient who is not on your address list, such as someone who has left the company.

Non-Delivery Report could then be used to return the email message to the sender.

Properties

The properties of the Non-Delivery Report action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Message

The text to appear in the subject of the report. The text can include MIMEsweeper tokens.

Tokens available here are:

- %SENDER%
- %SUBJECT%

For further information about these tokens, see Appendix I.

An optional message can be entered which will be returned to the sender along with the original message to explain why the message was not delivered.

Special features and restrictions

None.

Park

The Park action places email messages in a parking area for later delivery.

An example of the use of this action is to defer the delivery of large email messages until outside of normal working hours.

Properties

The properties of the Park action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Message Area

The parking area in which email messages are to be placed.

Options

The form in which to park the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment.

If you choose to attach a message in its original form, rather than as modified by MIMEsweeper, be aware that an email message that poses a threat could enter your organization's email system.

Special features and restrictions

Users who have access permissions to the parking area can use the MIMEsweeper Manager to force the immediate delivery of email messages held in the parking area outside of the scheduled release time.

Quarantine

The Quarantine action places email messages that are inappropriate for delivery in a quarantine area.

An example of the use of this action is to place messages that have triggered a content check performed by a scenario (such as messages containing viruses or prohibited data) in a secure area where a MIMEsweeper system administrator can examine the messages before deciding whether to process or delete them.

Properties

The properties of the Quarantine action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Message Area

The quarantine area in which email messages are to be placed.

Options

The form in which to quarantine the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment.

Special features and restrictions

Users who have access permissions to the quarantine area can use the MIMEsweeper Manager to view messages held in the quarantine area and process or delete them. You can configure quarantine areas to automatically delete quarantined email messages after a specified time.

Relay To

The Relay To action uses SMTP to relay a copy of a message to a specified host on a specified port. You can use this action, for example, to archive messages on another server, or to relay S/MIME encrypted messages to a separate server for decryption by a third-party tool.

Properties

The properties of the Relay To action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Server

Information about the SMTP server to which messages will be relayed, including the server name and the port assigned to the server. By default, port 25 is assigned.

Special features and restrictions

None.

Reply

The Reply action sends an automatic reply to the sender of a message to inform them of actions taken during MIMEsweeper message processing.

An example of the use of this action is to inform the message sender that MIMEsweeper identified a threat, such as a virus, in the email message that was sent.

Properties

The properties of the Reply action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Sender

The email account from which MIMEsweeper is to send messages. This can be the MIMEsweeper administrator email account, the MIMEsweeper Service email account, or any other email account in your organization's domain.

The email addresses for the MIMEsweeper administrator and the MIMEsweeper service accounts are specified in the **Addresses** tab of the MIMEsweeper for SMTP **Properties** page.

Subject and Body

The content of the message MIMEsweeper is to send, including the text to appear in the Subject line of the email message and the text to appear in the body of the email message. The text can include MIMEsweeper tokens. For example, you can use the %SUBJECT% token to include the subject of the original email.

Tokens available for the message **Subject** are:

- %ADMIN%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %REMOVEDNAMES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

Tokens available for the message **Body** are:

- %ADMIN%
- %DETECTED%
- %UNIQUEID%
- %AREANAME%
- %DATE%
- %MODIFIED%
- %RCPTS%
- %RECOGNISED%
- %REMOVEDNAMES%
- %RESPONSES%
- %POLICY%
- %SENDER%
- %SERVER%
- %SUBJECT%

You can also specify an alternative character set for MIMEsweeper to use for generating forward messages if your specified subject or body text contains characters that cannot be displayed by the US-ASCII character set. To access this feature, click the **Advanced** button.

Options

The form in which to send the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment. You can also specify whether to include the results from any specified text analysis as an HTML attachment to the archived message.

If you choose to attach a message in its original form, rather than as modified by MIMEsweeper, be aware that an email message that poses a threat could enter your organization's email system.

Special features and restrictions

None.

Save

The Save action places email messages in a specified folder on your computer.

An example of the use of this action is to save email messages to a location where they can be accessed by an SMTP email system other than MIMEsweeper.

Properties

The properties of the Save action are briefly described in the following sections. For full details on configuring the action, see the MIMEsweeper Policy Editor help.

Folder

The relative path to the folder to be used to save messages. The base folder for this operation is set in the **Base Folders** tab of the server's **Properties** page. For further details see Chapter 6.

Options

The form in which to send the email message: either in its original form or as modified by MIMEsweeper. For example, MIMEsweeper may have added an annotation or removed an attachment. You can also specify whether to include the results from any specified text analysis as an HTML attachment to the archived message.

Special features and restrictions

MIMEsweeper saves email messages in SMTP format as `.rcp` and `.msg` files. For further details on the use of these files in MIMEsweeper message processing, see Appendix F.

Users who have access to the folder where email messages are saved can open the messages in an email system other than MIMEsweeper for SMTP. This is not desirable if the messages contain security threats or offensive material.

MIMEsweeper does not automatically delete copies of messages in the Save folder.

CHAPTER 4

Scenarios

This chapter provides more detailed information on scenarios, describing each of the scenarios that are supplied with MIMEsweeper for SMTP. It supplements the information on scenarios in Chapter 2.

Overview

Each scenario is configured to implement a particular aspect of your organization's email policy. A scenario implements email policy by modifying or checking message contents for particular characteristics.

Scenarios are stored in scenario folders, which identify the routes to which the scenarios apply. Scenario folders are presented as a hierarchy, and the position of scenario folders within the hierarchy affects how MIMEsweeper Policy Editor determines which scenarios to apply to an email message. For more information about scenario folders, see Chapter 6 of the *Getting Started Guide* and the MIMEsweeper Policy Editor help.

You can create scenarios based on the supplied types of scenarios. Details of the types of content analysis scenarios can provide are described in the second section of this overview, *Scenario categories* on page 4-6.

You determine the way MIMEsweeper Policy Editor implements your content security policy by configuring properties for scenarios listed in the details pane for the **Scenarios** folder under the **Policies** folder under the MIMEsweeper Policy Editor. This is described in the third section in this overview, *Scenario properties* on page 4-8.

The remaining sections in this chapter provide reference information on each scenario that is available in MIMEsweeper Policy Editor. The scenario reference pages are presented in alphabetical order. Each reference page provides a summary of the scenario properties you can configure and notes any special features or restrictions you should be aware of when configuring the scenario.

Full details on scenario properties, as well as procedures for working with scenarios (for example, creating new scenarios, changing the properties of existing scenarios, and moving and copying scenarios) are provided in the help.

Scenario categories

A scenario specifies the type of content analysis to be performed on specific types of email messages. The following categories of scenario are available with MIMEsweeper Policy Editor (scenarios may be listed in more than one category, as they may be suitable for different types of policy; for more information, see the help):

- **Content recognition scenarios**
  - *Attachment Limiter* on page 4-10
  - *Attachment Manager* on page 4-11
  - *Checksum Matcher* on page 4-14
  - *Data Type Manager* on page 4-19
  - *HTML Manager* on page 4-29
  - *IMAGEmanager* on page 4-31
  - *Signature Detect* on page 4-37

  - *Size Manager* on page 4-38
  - *SpamLogic* on page 4-39
  - *Spoof Notifier* on page 4-43
  - *Text Analyzer* on page 4-46
- **Custom text attachment scenarios**
  - *Commercial Disclaimer* on page 4-16
  - *Legal Disclaimer* on page 4-32
- **Data type recognition scenarios**
  - *Attachment Manager* on page 4-11
  - *Checksum Matcher* on page 4-14
  - *Content Scanner* on page 4-17
  - *Data Type Manager* on page 4-19
  - *Executable* on page 4-22
  - *IMAGEmanager* on page 4-31
  - *Reclassifier* on page 4-34
  - *Virus Manager* on page 4-48
- **File type analysis scenarios**
  - *File Detector* on page 4-27
  - *Checksum Matcher* on page 4-14
  - *Pattern Matcher* on page 4-33
- **Mail management scenarios**
  - *Archiver* on page 4-9
  - *Body Manager* on page 4-13
  - *Classifier* on page 4-15
  - *Edge Message Classifier* on page 4-21
  - *Reclassifier* on page 4-34
  - *Subject Labels Manager* on page 4-44
- **Text analysis scenarios**
  - *Commercial Disclaimer* on page 4-16
  - *Text Analyzer* on page 4-46
- **Virus scanning scenarios**
  - *Content Scanner* on page 4-17
  - *Virus Manager* on page 4-48

Scenario properties

You create new scenarios using wizards. You change the properties of existing scenarios by configuring options in the tabs of a scenario's **Properties** page. For details on how to create or change scenarios, see the MIMEsweeper Policy Editor help.

The options you configure for each scenario are described in the scenario reference pages later in this chapter. All scenario properties pages contain the following tabs:

- **General**

  The details of the item, including the item type and a summary of the properties of the item.

- **Notes**

  Any user-specified text describing the item, for example, details of how the item or its configuration forms part of a policy.

Descriptions of these two generic tabs are not included in the scenario reference pages.

Archiver

The Archiver is an inclusive scenario that classifies all email messages that match the route to which the scenario applies.

An example of the use of the Archiver scenario is to archive email messages by associating a classification that contains either a Copy to Archive Account or Copy to Archive Folder action.

Because the Archiver scenario uses an inclusive classification, there is a risk that virus-infected items are archived in addition to being placed in a quarantine area. If such an item is subsequently retrieved from the archive, it can infect the retrieving client.

Properties

The properties of the Archiver scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **In all cases**

  The inclusive classification to apply in addition to the highest-priority exclusive classification that matches the email.

  To archive messages, specify an inclusive classification that has either a Copy to Archive Account or Copy to Archive Folder action, depending on how archiving is implemented in your MIMEsweeper system.

Special features and restrictions

The Archiver scenario does not filter or archive email messages itself. You must associate the scenario with a classification that contains an archive action. That way, when an email message matches the route specified in the scenario folder in which the Archiver scenario is contained, MIMEsweeper applies the specified classification and takes the defined archive action.

Attachment Limiter

The Attachment Limiter is an exclusive scenario that restricts the number of attachments an email message can have.

An example of the use of this scenario is to park email messages with a large number of attachments for delivery outside of office hours, when network traffic is light.

Properties

The properties of the Attachment Limiter scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Attachment limit

The number of attachments that a message is allowed to contain. You can specify whether the scenario is to detect any messages that contain attachments or just those messages that contain more than a specified number of attachments.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **On limit exceeded**

  The exclusive classification to apply when an email message contains more than the number of attachments specified in the **Attachment Limit** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

  Alternatively to delay the delivery of detected messages until a specified time (for example, when network traffic is light), specify a classification that has a Park action.

Attachment Manager

The Attachment Manager is an inclusive scenario that enables attachments to be removed from an email message based on attachment type and size. If attachments are removed or compressed, the email message can be modified with an optional piece of text.

An example of the use of this scenario is to remove attachments containing large sound files from being sent or delivered, while allowing the email message itself to be processed and adding an annotation indicating that the attachment has been removed or compressed.

Properties

The properties of the Attachment Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in email attachments and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

Options

The choice of stripping or compressing all attachments, or defining the size thresholds the scenario is to apply when detecting the data types specified in the **Data Types** tab. You can specify whether the scenario is to strip or compress all attachments of the specified type or just those that are the specified size or larger.

The option is also given to define a size of attachment to be stripped, while compressing all attachments below this size.

Annotation

The text the scenario is to add to an email message that contains attachments of the type specified in the **Data Types** tab, and of the size threshold specified in the **Size** tab.

You might specify an annotation, for example, to advise recipients that a detected attachment has been stripped from the email message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

There are separate annotations available depending on whether strip or compress has been selected.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On message modified**

  The exclusive classification to apply when the scenario strips or compresses attachments of the type specified in the **Data Types** tab and of the size threshold specified in the **Size** tab.

  To deliver detected messages, specify a classification that has a Deliver action.

- **On modification unsuccessful**

  The exclusive classification to apply when the scenario cannot strip or compress attachments of the type specified in the **Data Types** tab and of the size threshold specified in the **Size** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

The Attachment Manager scenario removes or compresses entire attachments, not individual components of an attachment. For example, if a document file attached to an email message contains an image in a format specified for removal, then MIMEsweeper removes the whole document (not just the image) from the message.

When creating a new instance of an Attachment Manager scenario, you are recommended to assign an exclusive classification that quarantines the original version of the messages with attachments in the formats you intend to have removed. This will prevent any accidental loss of data while you are assessing a configuration suitable for your email policies.

Body Manager

The Body Manager is an exclusive scenario which allows the removal of parts of the body of a message on detection of particular body types.

Properties

The properties of the Body Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Body Removal Options

- **Messages with a plain text body and another type of body**

  The non-plain text body can be removed, leaving the potentially safer plain text message to be processed further by the system.

- **Messages with HTML bodies**

  All images can be removed, leaving the remainder of the HTML message to be processed further by the system.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On no plain text body detected**

  The exclusive classification to apply when the scenario detects that the message does not have a plain text body, and there is a strong likelihood that the message is spam.

- **On mixed bodies detected**

  The exclusive classification to apply when the scenario detects that a message has both a plain text body and another type of body, for example, HTML or RTF.

- **On body or image stripped**

  The exclusive classification to apply when the scenario has removed a non-plain text body or images from the message being processed.

- **On strip unsuccessful**

  The exclusive classification to apply when the scenario has been unable to remove the specified item, possibly due to the format of the item detected.

To block the delivery of detected messages, specify a classification that has a Quarantine action.

Checksum Matcher

The Checksum Matcher is an inclusive scenario that detects file checksums and compares them to those held in a specified list. The checksum of a file provides an almost unique identifier of that file.

An example of the use of this scenario would be keeping a known threat out of your Email system, or ensuring that a confidential image is never sent out.

Properties

The properties of the Checksum Matcher scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help

Checksum List

An existing checksum list can be chosen from the list displayed, or a new checksum list added by clicking **New.**

When a new checksum list is added you are given the choice of using a Managed Checksum List, which is updated regularly from the Clearswift server, or a User-defined Checksum List which you add checksums to as required.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of the scenario:

- **On Checksum Matched**

  The classification to apply when a file checksum matches that held in the specified list.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Classifier

The Classifier is an exclusive scenario that assigns items to a specified classification.

An example of the use of this scenario is to detect all messages that match a particular sender/recipient route and block those messages from delivery.

Properties

The properties of the Classifier scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **In all cases**

  The exclusive classification to apply when an email message matches the sender/recipient route in the scenario folder that contains the Classifier scenario.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

The Classifier does not analyze email content, but classifies all email messages that match the route to which the scenario applies.

Commercial Disclaimer

The Commercial Disclaimer is an inclusive scenario that detects specific words and phrases in email messages and adds specified text to detected messages.

An example of the use of this scenario is to add a commercial disclaimer to email messages that give advice to clients, or to enhance email messages with additional information that the recipient may find useful. After adding the disclaimer text, MIMEsweeper continues to process the message.

Properties

The properties of the Commercial Disclaimer scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Expression list

The expression list that contains the words or phrases the scenario is to detect in email messages.

Thresholds

The details of how the score is calculated for an email message when expressions specified in the expression list that is referenced in the **Expression List** tab are detected during text analysis. You can specify options to determine:

- How the text analysis score that causes an email message to be treated as suspect is calculated.
- Whether or not to add to the search threshold value the weighting for detected expressions.
- Whether to aggregate the values across all items in the message.

Scan Areas

The areas of the email message that MIMEsweeper is to scan for words or phrases specified in the expression list referenced in the **Expression List** tab. You can specify whether to search SMTP headers, the message body, attachments, or all areas.

Annotation

The text the scenario is to add to an email message that contains words and phrases specified in the **Expression List** tab.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Special features and restrictions

Like the Text Analyzer scenario, the Commercial Disclaimer scenario uses text analysis to identify email content. To ensure that you get the expected results when searching for multiple occurrences of an expression, it is important to understand how text analysis works. For a detailed explanation, see the MIMEsweeper Policy Editor help.

Content Scanner

The Content Scanner is an inclusive scenario that runs third-party scanning software, such as an anti-virus tool. It scans data in the email message. If the third-party anti-virus tool supports cleaning, you can configure the Content Scanner scenario to clean infected email messages. The scenario can optionally add specified text to messages from which detected items have been removed.

An example of the use of this scenario is to run a third-party anti-virus tool written to support the MIMEsweeper interface.

Properties

The properties of the Content Scanner scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in the body of an email message and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

Application details

The third-party content scanner that the scenario is to use to detect data of the type specified in the **Data Types** tab.

You can specify options to have the content scanner attempt to clean a detected item or to remove infected files from the email message, if the content scanner supports cleaning or stripping. You can specify options to add an annotation to messages from which detected items have been cleaned or stripped.

Cleaned annotation

The text the scenario is to add to an email message from which a detected virus has been cleaned.

You might specify an annotation, for example, to advise recipients that a infected item has been cleaned from the email message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Stripped annotation

The details of the text to be added to an email message from which a detected item has been stripped.

You might specify an annotation, for example, to advise recipients that a detected item has been stripped from the email message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On detected**

  The exclusive classification to apply when the scenario detects items of the type specified in the **Data Types** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

- **On detected items cleaned**

  The exclusive classification to apply when the scenario cleans items of the type specified in the **Data Types** tab.

  To deliver cleaned messages, specify a classification that has a Deliver action.

- **On detected items stripped**

  The exclusive classification to apply when the scenario strips items of the type specified in the **Data Types** tab.

  To deliver stripped messages, specify a classification that has a Deliver action.

- **On threat cannot be removed**

  The exclusive classification to apply when the scenario cannot clean or strip items of the type specified in the **Data Types** tab.

  To block the delivery of messages where the threat cannot be removed, specify a classification that has a Quarantine action.

Special features and restrictions

You must have the appropriate content scanning software installed on your MIMEsweeper machine before you can create instances of the Content Scanner scenario. This can be any third-party content scanner that is based on the Component Object Model (COM) interface. After installation, the content scanner must be listed in the Windows registry in order for MIMEsweeper to locate the software.

Data Type Manager

The Data Type Manager is an inclusive scenario that detects items of a specific file type and, optionally, of a specified size or larger.

An example of the use of this scenario is to prevent the delivery of large video files.

Properties

The properties of the Data Type Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in email messages and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

The scenario includes entries for the **SMTP message** type in the **Container** category and the **Text file** type in the **Document** category. As far as the Data Type Manager scenario is concerned, these two types are the same. That is:

- If you configure the scenario to detect the **Text file** data type, the scenario also detects the **SMTP message** data type.
- If you configure the scenario to detect the **SMTP message** data type, the scenario also detects the **Text file** data type.

Size

The size thresholds the scenario is to apply when detecting the data types specified in the **Data Types** tab. You can specify whether the scenario is to detect all instances of the specified data types or just those that are the specified size or larger.

When checking the size of an email message to use with the Size threshold, the Data Type Manager scenario uses the Internet message format (7-bit ASCII) size. This can result in a size up to 30% larger than the original desktop format (8-bit binary) size of the email message. You may need to take this into account when setting size thresholds.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **On files detected**

  The exclusive classification to apply when the scenario detects data of the type specified in the **Data Types** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

When checking the size of an email message, the Data Type Manager uses the Internet message format (7-bit ASCII) size. This can be up to 30% larger than the original desktop format (8-bit binary) size of the email message.

This scenario does not detect files based on file extensions. The File Detector scenario must be used for that.

Edge Message Classifier

The Edge Message Classifier is an inclusive scenario that detects messages that have been preclassified by a MIMEsweeper Edge Server. These are the messages that a MIMEsweeper Edge Server has been configured to add X-header information to. See *MIMEsweeper Edge Servers* on page 1-8 for more information.

Properties

The properties of the Edge Message Classifier scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Pre classification types

The pre classification types and subtypes that the scenario detects in email messages and the options for processing them. These types and subtypes relate to:

- Messages containing viruses.
- Messages containing dangerous file types.
- Spam messages.

For spam messages, you can specify whether to apply the scenario to all spam detection types and subtypes, or to selected spam detection types and subtypes only.

Classifications

A classification to determine what to do with email messages that match the scenario's outcome:

- **On classified by Edge**

  The exclusive classification to apply when the scenario detects data of the type specified in the **Preclassification Types** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

  To use MIMEsweeper for SMTP's PMM functionality, specify a classification with a message area that is enabled for PMM management, for example the default **Personal Messages** message area.

Special features and restrictions

With a MIMEsweeper Edge Server, it is a good idea to quarantine messages with threats and viruses on the Edge server rather than adding an X-header and allowing MIMEsweeper for SMTP to process the message.

This ensures that messages with threats are dealt with by the Edge server and never enter your MIMEsweeper for SMTP and internal mail system.

Executable

The Executable is an inclusive scenario that enables MIMEsweeper Policy Editor to run a third-party executable program (for example, `.exe`, `.com`, or `.bat` application). The executable program can be any application that is beneficial to the user and increases the functionality of MIMEsweeper.

You might use a third-party executable program, for example, to:

- Perform processing on a file type that MIMEsweeper Policy Editor does not support by default.
- Perform additional processing on a component of an email message that MIMEsweeper has recursively disassembled.

There are a number of preliminary procedures that you must perform before you can create an Executable scenario. For details of these procedures and an example of how to configure an Executable scenario, see *Special features and restrictions* on page 4-9.

Properties

The properties of the Executable scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in email messages and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

Application details

- The details of the executable program that MIMEsweeper is to run. You specify the filename, application type and any command-line parameters for the third-party executable program.

MIMEsweeper expects to find the specified application on the system path of each of your configured servers, or on an advanced path. For further details about setting up advanced paths, see Chapter 6.

You can use one or both of the `%FILENAME%` and `%LOGNAME%` tokens as command-line parameters. If you specify the `%LOGNAME%` token as a command-line parameter, you can use the `%LOGTEXT%` token in the **Description** field on the **Return Codes** tab.

You also can specify any advanced options such as the working folder, timeout period, file extension and mutex name details for the executable program.

Return codes

The details for mapping the numerical return codes of the third-party executable program to MIMEsweeper using the status field. You must use the return codes assigned by the third-party executable program. For details about the appropriate return code values, see the documentation for the third-party executable program. The MIMEsweeper status types that return codes can be mapped to are NONE, NOT_CHECKED, DETECTED, and MODIFIED.

You must enter at least one return code for the NONE status. You must enter at least one return code for either the DETECTED or MODIFIED status. You can specify the `%LOGTEXT%` token in the **Description** field for the DETECTED or MODIFIED status. If you specify the DETECTED status, in the **Classification** tab you must associate an exclusive classification for the **On detected** classification type. If you specify the MODIFIED status, in the **Classification** tab you must associate an exclusive classification for the **On modified** classification type.

Log details

The portion of the log file generated by the third-party executable program from which MIMEsweeper is to extract text. You can specify options to use the complete log file or just a portion of the log file. If you use a portion of the log file and you have specified the `%LOGTEXT%` token in the **Return Codes** tab, MIMEsweeper replaces that token with the text extracted from the generated log file.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On detected**

  The exclusive classification to apply when a DETECTED status is specified on the **Return Codes** tab and the scenario modifies items of the type specified in the **Data Types** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

- **On modified**

  The exclusive classification to apply when a MODIFIED status is specified on the **Return Codes** tab and the scenario detects data of the type specified in the **Data Types** tab.

  To deliver detected messages, specify a classification that has a Deliver action.

Special features and restrictions

This section describes the preliminary procedures that you must perform before you create an Executable scenario. It also provides an example of how to configure an Executable scenario.

Preliminary procedures

Before you create an Executable scenario, you are advised to run preliminary tests to check the following options:

1. Examine the documentation for the third-party executable program to determine which command-line parameters to specify for the executable program.
2. Run the executable program independently of MIMEsweeper for SMTP to ensure the program is problem free.
3. You also should monitor the processing time as MIMEsweeper could run the executable multiple times for each message. If the executable program takes a long time to process, it could seriously decrease the performance of MIMEsweeper. If the processing time is high, see the third-party executable documentation and specify different command-line parameters.
4. Verify the return codes for the executable program. For more information about return codes, see the documentation for the third-party executable program.
5. Examine the log file generated by the third-party executable program to determine which, if any, information might be useful to view in the MIMEsweeper Manager.
6. Ensure that the executable is installed on every Policy Server in your installation.

Example executable scenario

This section provides an example of how to configure an Executable scenario to automatically run an executable program.

This example is based on a company that has a policy to provide copyright protection for its images in digital format using a digital watermark. (A digital watermark is a pattern of bits inserted into a digital image, audio, or video file to identify the file’s copyright information.)

The company, ‘Your Company’, currently uses a command-line program they have written to identify the presence of their digital watermark in an image file, and to insert the digital watermark if it is not there. The program generates a log file listing actions that occur while the program is running based on its return codes:

0 The corporate watermark is already contained in the image <`filename.ext`>.

1 The corporate watermark cannot be added to the image <`filename.ext`>.

2 The corporate watermark has been added to the image <`filename.ext`>.

The company now wants to have MIMEsweeper automatically run this command-line program to check all outgoing email messages containing images and to extract from the log file information that they can view in the MIMEsweeper Manager after outgoing email messages have been processed.

To do this, Your Company creates an Executable scenario:

1. From the **Scenarios** folder, select the **Outgoing** scenario folder.

2. From the **Action** menu, select **New**, then click **Executable** from the menu.
3. On the **Initial Scenario State** page, leave the **Enabled** and **Overridable** check boxes selected.
4. On the **Data Types** page:
   a. Select the **Image** check box to select all image subtypes and clear the other data type check boxes.

   b. Click **Include selected data types** then **Next.**
5. On the **Application Details** page:
   a. In **Application location**, enter the full path and file name of the executable program or use the **Browse** button to navigate to its location.

   b. In **Command line**, enter the command line to run the executable program, and specify the following tokens:

   `%FILENAME%` to represent the name of any file processed according to this Executable scenario.

   `%LOGNAME%` to specify that the executable program should generate a log file.

   c. In **Application Type**, select DOS.
6. On the **Return Codes** page, enter the return code details for the application, associate a MIMEsweeper status, and enter a description for return codes with a status of `DETECTED` or `MODIFIED`, using the `%LOGTEXT%` token where you want MIMEsweeper to extract text from the log file for the image file processed:

0	NONE	
1	DETECTED	The Your Company digital watermark %LOGTEXT%.
2	MODIFIED	The Your Company digital watermark %LOGTEXT%.

7. On the **Log Details** page, select **Use partial log file** and identify the text that appears in the log file before and after the text you want MIMEsweeper to replace the `%LOGTEXT%` token with:

   Enter the text that precedes the information to be extracted

   `The corporate watermark`

   Enter the text that follows the information to be extracted.

   `.\r\n`

   (`\r\n` specifies a carriage return / line feed, so the following text is displayed on a new line.)
8. On the **Classifications** page, assign an appropriate exclusive classification for each possible outcome:
   - **On detected**

     For example, associate the **Dirty Out** classification.

- **On modified**

  For example, associate the **Cleaned** classification.

9. On the **Scenario Name** page, enter a meaningful name for the Executable scenario (for example, “Your Company Digital Watermark”) and a description (for example, “Ensure the Your Company digital watermark is present on outgoing mail containing images”).

When MIMEsweeper processes an outgoing email message containing an image file that does not contain the corporate digital watermark (`logo.jpeg`) using this Executable scenario:

1. MIMEsweeper runs the executable program.
2. The executable program determines that `logo.jpeg` does not contain the Your Company digital watermark and inserts the watermark in the image.
3. The executable program passes to MIMEsweeper a return code of 2 and a log file containing the entry:

   ```
   The corporate watermark has been added to the image logo.jpeg.
   ```
4. MIMEsweeper interprets the return code of 2 as its MODIFIED status and extracts from the executable program’s log file the text between the specified preceding and following text:

   ```
   has been added to the image logo.jpeg
   ```
5. MIMEsweeper replaces the `%LOGTEXT%` token with this extracted text, which appears behind the text specified in the **Description** field for the MODIFIED status:

   ```
   The Your Company digital watermark
   ```
6. MIMEsweeper Manager displays in the dialog box for the processed message the following text:

   ```
   The Your Company digital watermark has been added to the image logo.jpeg.
   ```
7. MIMEsweeper delivers the modified email message containing `logo.jpeg` as specified in the **Cleaned** classification.

File Detector

The File Detector is an inclusive scenario that detects files with specified file names or extensions.

An example of the use of this scenario is to configure a quick, temporary search that stops a specific file extension being sent from or received by an organization.

Properties

The properties of the File Detector scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

File mask

The details of the file or files the scenario is to detect. You specify the names of files the scenario is to block. You can use wildcard characters to specify a range of files.

You can also specify whether or not MIMEsweeper is to strip detected files from the email message. You can specify an option to add an annotation to messages from which detected files have been stripped.

Stripped annotation

The text the scenario is to add to an email message that contains file names or extensions specified in the **File Mask** tab.

You might specify an annotation, for example, to advise recipients that a detected file has been stripped from the email message.

You can specify whether the annotation text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On detected files stripped**

  The exclusive classification to apply when the scenario strips files specified in the **File Mask** tab.

  To deliver detected messages, specify a classification that has a Deliver action.

- **On strip unsuccessful**

  The exclusive classification to apply when the scenario cannot strip files specified in the **File Mask** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

The File Detector scenario does not use a numerical signature. If you require additional security, use the Pattern Matcher scenario on page 4-33, which does use a numerical signature.

Consider using the Data Type Manager scenario in addition to the File Detector to block files even if their extension has been changed to disguise their type.

HTML Manager

The HTML Manager is an exclusive scenario that detects—and optionally removes—HTML items.

An example of the use of this scenario is to block potentially malicious JavaScript or VBScript contained in email messages.

Properties

The properties of the HTML Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

HTML

The HTML items to detect in, and optionally remove from, email messages. You can specify options for:

- **Shortcuts**

  Internet shortcuts reference programs and commands that a web browser can execute.

- **Automatic mailtos**

  Automatic mailing addresses take the form of the HTML `mailto` command. They can reveal mail accounts, domains, and organizations.

- **Scripts**

  Internet shortcuts reference programs and commands that a web browser can execute.

Annotation

The text the scenario is to add to an email message that contains HTML items of the type specified in the **HTML** tab.

You might specify an annotation, for example, to advise recipients that a detected HTML item has been stripped from the email message.

- You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

If you have chosen to annotate the subject line of the message be aware that only the first line of the text you enter will be used.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On HTML items detected**

  The exclusive classification to apply when the scenario detects items of the type specified in the **HTML** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

- **On HTML items removed**

  The exclusive classification to apply when the scenario cleans items of the type specified in the **HTML** tab.

  To deliver detected messages from which specified items have been removed, specify a classification that has a Deliver action.

Special features and restrictions

The HTML Manager scenario can be used to block potentially malicious script.

IMAGEmanager

The IMAGEmanager is an inclusive scenario which analyzes messages against the current settings for the scenario and also detects specified image types and compares them to a database of preclassified images.

An example of the use of this scenario would be to block delivery of email messages containing unacceptable images.

For further information on IMAGEmanager, see Appendix D.

Properties

The properties of the IMAGEmanager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Image Types

The format of the image to be detected.

Classifications

The classification to determine what to do with email messages that match the outcome of the scenario and contain unacceptable images.

For details of the preclassified image database, see Chapter 9.

Special features and restrictions

You can only place an image in the pre-classified image database that is smaller than 4MB. If you place an image larger than 4MB, you may experience problems.

If you try to import images from a zip file, the file size is limited to 4 MB. This is due to the **MaxRequestLength** attribute which is a default set by Microsoft in the machine configuration file, and indicates the maximum file upload size supported by ASP.NET. The specified limit can be used to prevent denial of service attacks caused by users posting large files to the server. The size specified is in kilobytes. The default is 4069 KB (4 MB).

For more information about adding images to the pre-classified image database, see the MIMEsweeper Manager help.

Legal Disclaimer

The Legal Disclaimer is an inclusive scenario that adds specified text to the body of email messages. The scenario can search the body or subject of email messages for specified words or phrases that prevent the disclaimer text from being added. This is useful for preventing legal disclaimers from being added to personal email messages or to email messages that already contain the disclaimer text.

An example of the use of this scenario is to add a statement limiting your organization's legal liability for the contents of the message.

Properties

The properties of the Legal Disclaimer scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Annotation

The text the scenario is to add to an email message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Bypass

The conditions under which users can prevent the disclaimer text specified in the **Annotation** tab from being added to outgoing email messages. You can specify options to enable message senders to bypass the addition of the specified disclaimer text and specify the phrase they must use to bypass it.

Prevent multiple disclaimers

The options for controlling the number of disclaimers added to each email message MIMEsweeper processes. You can specify options to prevent MIMEsweeper from adding the disclaimer text specified in the **Annotation** tab to a previously processed email message that already contains the disclaimer.

Special features and restrictions

After adding the disclaimer text, MIMEsweeper continues to process the message and apply any other scenarios as appropriate.

Pattern Matcher

The Pattern Matcher is an inclusive scenario that checks file signatures to detect types that are not supported via the Data Type Manager. A signature is a pattern of bytes that identifies the data type of a file.

An example of the use of this scenario is to detect an in-house data format that must not be copied from your internal network to an outside organization.

Properties

The properties of the Pattern Matcher scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

File signature

The sequence of bytes (byte pattern) that identifies the data type of a file to be detected. You enter the byte pattern in decimal format, that is a number in the range of 0 to 255. The byte pattern is a signature that consists of a sequence of bytes at a particular location in the file. You can select:

- The search direction, that is whether to begin the search at the beginning or at the end of the file.
- The search offset, or the number of bytes from the beginning or the end of the file to start the search.

You can specify byte pattern details, or you can import a byte pattern from either a local file or the MIMEsweeper website. You also can export an existing byte pattern to a local file.

Size

The size thresholds the scenario is to apply when detecting the data types specified in the **File Signature** tab. You can specify whether the scenario is to detect all instances of the specified data types or just those that are the specified size or larger.

This size is the size of the entire message, including control information.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **On files found**

  The exclusive classification to apply when the scenario detects data of the type specified in the **File Signature** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

  To deliver detected messages, specify a classification that has a Deliver action.

Reclassifier

The Reclassifier is an inclusive scenario that assigns to specified classifications other than the system-defined classifications items that contain encrypted data or data that could not be fully identified because it is corrupt or because of a system failure.

An example of the use of this scenario is to allow the delivery of email messages containing encrypted data, such as PGP or S/MIME-encrypted items or password-protected zip files, which by default would automatically be blocked.

Properties

The properties of the Reclassifier scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in email messages and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On corrupt items detected**

  The exclusive classification to apply when the scenario cannot fully identify an item because it is corrupt.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

- **On system failure**

  The exclusive classification to apply when the scenario cannot fully identify an item because of a system failure (for example, message processing was interrupted).

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

- **On encrypted items detected**

  The exclusive classification to apply when the scenario detects a message that contains encrypted data.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

To treat different types of data in different ways, create separate Reclassifier scenarios for each type of data that is to be detected.

By default, MIMEsweeper automatically places email messages containing encrypted data in the **Encrypted Messages** quarantine area. To allow such email messages to be delivered, create a Reclassifier scenario that detects encrypted data only, and associate the scenario with a classification that has a Deliver action.

By default, MIMEsweeper automatically places items containing data that cannot be identified in the **Undetermined** message area.

When a message matches more than one exclusive classification, the priority of the classifications determines which gets applied. To ensure that the classification specified in the Reclassifier scenario is applied, you must position this classification higher in the list than the **Encrypted** or **Undetermined** classification which would by default be applied. To avoid affecting other policy elements, you are recommended to create a new classification to associate with your Reclassifier scenario.

Script Manager

The Script Manager is an inclusive scenario which detects combinations of words and phrases which are characteristic of scripts, and compares them to those held in a specified list.

An example of this would be to detect VB or Java scripts.

Properties

The properties of the Script Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in email messages and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

Script List

An existing script list can be chosen from the list displayed, or a new script list added by clicking **New.**

When **New** is clicked you are given the choice of using a Managed Script List, which is updated regularly from the Clearswift server, or a User-defined Script List which you add script expressions to as required.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **On scripts detected**

  The classification to apply when the scenario detects a script that matches an entry in the specified list.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Signature Detect

The Signature Detect is an exclusive scenario that detects PGP or S / MIME email messages that have been digitally signed. The scenario can search the body or subject of email messages for specified words or phrases that enable digitally signed email messages to bypass the classification.

An example of the use of this scenario is to prevent the delivery of personally signed email messages from individual users.

Properties

The properties of the Signature Detect scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Bypass

The conditions under which users can prevent an outgoing email message that contains a digital signature from being classified as a signed email message and blocked from delivery. You can specify options to enable message senders to bypass the scenario.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **On signature detected**

  The exclusive classification to apply when the scenario detects a digitally signed message that does not contain the phrase specified in the **Bypass** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

To avoid affecting other policy elements, you are recommended to create a new quarantine area specifically for digitally signed email messages and associate your scenario with a classification that includes a Quarantine action to place messages in this new quarantine area.

Size Manager

The Size Manager is an exclusive scenario that detects messages that are above a specified size or are within a size band.

An example of the use of this scenario is to place messages that exceed a specified size threshold into a parking area for delivery during a specified period, and to place messages that exceed a higher threshold into a quarantine area.

Properties

The properties of the Size Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Scheduled threshold

The size thresholds the scenario is to apply when processing email messages at the specified times of day. You specify the times of day when the scenario is to check for email messages and the largest size message that will be allowed to be processed during those times.

Fixed threshold

A second, optional, size threshold that MIMEsweeper applies to all processed email messages regardless of the schedule specified in the **Scheduled threshold** tab. You specify the largest size message that will be allowed to be processed before the scenario is applied.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On scheduled threshold exceeded**

  The exclusive classification to apply when the scenario detects an email message that exceeds the size specified in the **Scheduled threshold** tab during the times of day specified in that tab.

  To delay the delivery of detected messages until a specified time (for example, when network traffic is light), specify a classification that has a Park action.

- **On fixed threshold exceeded**

  The exclusive classification to apply when the scenario detects an email message that exceeds the size specified in the **Fixed threshold** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

When checking the size of an email message, the Size Manager scenario uses the Internet message format (7-bit ASCII) size. This could be up to 30% bigger than the original desktop format (8-bit binary) size of the message.

SpamLogic

The SpamLogic scenario is an exclusive scenario that detects spam messages using a combination of four techniques.

SpamLogic detection techniques

The SpamLogic detection techniques are:

- URL detection
- Bayesian content detection
- SpamLogic Signatures content detection
- Anti-spam Engine detection

To supplement the SpamLogic scenario, you can also create and use Checksum and Expression list references, and use these in Text Analyzer scenarios.

ℹ If you use a MIMEsweeper Edge Server to detect spam messages, you do not need to use the SpamLogic scenario.

URL detection

SpamLogic URL analysis uses a URL database lookup service named SURBL (http://www.surbl.org) to detect domains whose inclusion in a message identifies the message as spam. You can extend the URL analysis capabilities of the SpamLogic scenario in the following ways:

By configuring a list of additional URL database look-up services to be checked if a URL domain is not found in SURBL.

By configuring your own Whitelist and Blacklist of URL domains. Detection of the listed domains within a URL in a message determines whether the message is treated as spam. A URL identified by either list is not checked against SURBL or additional URL databases that you may have configured.

ℹ To block messages based on the originating domain, rather than the domains contained inside the message, you use the Policy Editor **Anti-spam Properties** dialog box. See *Anti-spam properties* on page 6-15 for more information.

Bayesian content detection

Bayesian content detection is a type of statistical analysis used to detect the likelihood that messages are spam. The statistical analysis process uses the results of URL detection as part of its analysis. Because of this, URL detection must be enabled before you can use Bayesian content detection.

SpamLogic Signatures content detection

SpamLogic Signatures checks message for unique properties or signatures that identify spam messages. To do this, SpamLogic derives each message's signature, and searches the signatures database for a match.

A SpamLogic Signatures database is installed during product installation. To maintain an updated version of this database, to protect against current trends in spam messages, you require a Support and Maintenance agreement in place for the installation, and the password for this agreement to be registered on the Clearswift website.

You can configure the installation’s password when you install MIMEsweeper for SMTP, or you can add the password later. See *Configuring managed downloads* on page 5-4 for details.

If you do not have a current Support and Maintenance license, the SpamLogic Signatures data remains unchanged since installation. The quality of your installation’s spam detection degrades over time as spam evolves and changes.

See the MIMEsweeper Manager help for information on checking if your Support and Maintenance license is current. See your normal support provider for information on obtaining or renewing a Support and Maintenance contract.

Anti-spam Engine detection

Anti-spam Engine detection uses message characteristics such as the content and the way that the message is constructed to identify spam messages. SpamLogic determines each message's characteristics, and compares these to the SpamLogic Definition List reference.

A SpamLogic Definition List reference is installed during product installation. To maintain an updated version of this reference, as with SpamLogic Signatures, you require a Support and Maintenance agreement in place for the installation, and the password for this agreement to be registered on the Clearswift website.

If you do not have a current Support and Maintenance license, the SpamLogic Definition List reference remains unchanged since installation. The quality of your installation’s spam detection degrades over time.

SpamLogic properties

The properties of the SpamLogic scenario are briefly described in the following sections. For more details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Size

You can specify the size threshold from the **Scan all messages** or **Scan messages smaller than or equal to** options. Messages that exceed the threshold are treated as **not** spam and are not subjected to any further anti-spam analysis.

Detection types

Use this property to re-configure the options selected when you created the scenario. The available options are:

- URL detection
- Bayesian content detection
- SpamLogic Signatures content detection
- Anti-spam Engine detection

URL

Use this property to specify the host names of URL database lookup services to be checked, in addition to SURBL. MIMEsweeper for SMTP checks the databases in the order in which they are listed.

In the **Advanced** property area you can specify URL Whitelist and Blacklist domains:

- Messages originating from Whitelist domains are not checked for spam, and allowed.
- Messages originating from Blacklist domains are blocked and classed as spam by default.

With the **URL** property, you can use the **Resilience** option to improve the resilience of the SpamLogic installation. You do this by configuring SpamLogic to suspend URL lookups at times when there is a high level of URL lookups, and a high proportion of these lookups fail.

Content

Allows you to enable or disable the following two options:

- **Record detailed results**: Enables or disables the inclusion of Bayesian analysis results in the **Spam Analysis** tab on the **View Message** page in the Message Center.
- **Enable auto-training**: Enables or disables SpamLogic automatic self-training, based on SURBL results. This option is enabled by default.

It is recommended that you do not disable the SpamLogic **Enable auto-training** option, unless you are advised to do so by your MIMEsweeper for SMTP support provider.

Tagging

You can specify tagging options to add text to the subject line of a message identified as spam.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of the scenario:

- **On spam URL detection**

  The classification to apply when URL analysis indicates a high probability of spam.

- **On spam content detection**

  The classification to apply when Bayesian content detection, SpamLogic Signatures content detection, or spam engine detection indicates a high probability of spam.

Spoof Notifier

The Spoof Notifier is an exclusive scenario that detects email messages that may have originated from a source other than the apparent sender. The scenario can optionally add specified text to messages MIMEsweeper identifies as spoofed.

An example of the use of this scenario is to prevent the delivery of spoofed messages that distribute inappropriate material or attempt to acquire information by underhand methods.

Properties

The properties of the Spoof Notifier scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Spoof detection level

The detection level MIMEsweeper must reach before reporting a message as being spoofed, that is, sent from a source other than the apparent sender. You can specify a detection level between high and low. If you specify a high detection level, MIMEsweeper is more likely to detect spoofed messages; however, this may also increase the number of false positives beyond an acceptable level. If you specify a low detection level, MIMEsweeper is less likely to detect spoofed messages; however, this is likely to keep false positives to a minimum. You are recommended to leave the spoof threshold set at the default detection level.

The Spoof Notifier scenario analyzes email message headers for evidence of spoofing and calculates a spoof index based on the amount of evidence detected. When the value of the spoof index reaches the specified detection level, the scenario reports the message as being spoofed.

Annotation

The text the scenario is to add to an email message that meets or exceeds the level specified in the **Spoof Detection Level** tab.

You might specify an annotation, for example, to warn recipients of the likelihood that the email message has been spoofed and recommend that they contact the system administrator, who can attempt to identify the actual sender of the message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Subject Labels Manager

The Subject Labels Manager scenario is an exclusive scenario that enables you to classify a message if one or more categories of label (a word or phrase) are present in, or absent from, the message subject line.

You can define up to three categories of label to look for. You can associate each category with a different classification, and specify a classification if no label is detected. You can also specify where to search for the category label within the subject line.

For example, you could create a scenario defining two categories of label, one category comprising the labels ‘Confidential’ and ‘Restricted’; and the second category comprising the label ‘Unrestricted’. You could then use this scenario to:

- classify as clean all messages labelled ‘Unrestricted’
- route all messages labelled ‘Confidential’ or ‘Restricted’ to a particular message area.
- quarantine all messages that do not have a label
- quarantine all messages that do not have a label in the specified part of the subject line.

Properties

The properties of the Subject Labels Manager are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Category 1

The category labels that the scenario is to match in the subject line of the message. This category is enabled by default, and you must add a category label before you can continue.

Category 2

A second, optional, list of category labels to be matched in the subject line of the message. You must enable this category before you can add a category label.

> You can only specify which classifications to use for Category 2 labels if Category 2 is enabled.

Category 3

A third, optional, list of category labels to be matched in the subject line of the message. You must enable this category before you can add a category label.

> This category can only be used if you have enabled Category 2.
>
> You can only specify which classifications to use for Category 3 labels if Category 3 is enabled.

Options

The location of the category label in the subject line that a Subject Labels Manager scenario is to scan for in email messages. You can specify whether the label should be searched for at the beginning of the subject line, at the end, or anywhere within the subject line.

You can also select to remove the label from message, for example, if you do not wish them to be visible to the email message recipient.

Classifications

One or more classifications to determine what to do with email messages that match each unique outcome of a scenario:

- **On category 1 label(s) detected**

  The classification to apply when the scenario detects any of the category labels specified in the **Category 1** tab.

  To block the delivery of messages matching the subject labels associated with category 1, specify a classification that has a Quarantine action with no Delivery action.

- **On category 2 label(s) detected**

  The classification to apply when the scenario detects any of the category labels specified in the **Category 2** tab.

  To block the delivery of messages matching the subject labels associated with category 2, specify a classification that has a Quarantine action with no Delivery action.

  This classification item is only displayed if category 2 is enabled.

- **On category 3 label(s) detected**

  The classification to apply when the scenario detects any of the category labels specified in the **Category 3** tab.

  To block the delivery of messages matching the subject labels associated with category 3, specify a classification that has a Quarantine action with no Delivery action.

  This classification item is only displayed if category 3 is enabled.

- **On no category label detected**

  To block the delivery of messages matching the subject labels associated with the category, specify a classification that has a Quarantine action with no Delivery action.

  ℹ If you only wish to release the email messages that do not have subject labels, you must specify the Clean default system classification.

Text Analyzer

The Text Analyzer is an inclusive scenario that detects in email messages specific words and phrases specified in a referenced expression list.

An example of the use of this scenario is to block delivery of email messages containing offensive material.

Properties

The properties of the Text Analyzer scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data Types

The data types that will be processed, or excluded from processing, by the scenario.

Expression list

The expression list that contains the words or phrases the scenario is to detect in email messages.

Thresholds

The details of how the score is calculated for an email message when expressions specified in the expression list that is referenced in the **Expression List** tab are detected during text analysis. You can specify options to determine:

- How the text analysis score that causes an email message to be treated as suspect is calculated.
- Whether or not to add to the search threshold value the weighting for detected expressions.
- Whether to aggregate the values across all items in the message.

Scan areas

The areas of the email message that MIMEsweeper is to scan for words or phrases specified in the expression list referenced in the **Expression List** tab. You can specify whether to search SMTP headers, the message body, attachments, or all areas.

For Adobe PDF, Microsoft Office document attachments, and Open Office document attachments, you can select to scan the document body, the header and footer and the document properties.

Size

The size thresholds the scenario is to apply when determining messages to scan. You can apply a size limitation on messages that the the scenario is to scan:

- **Scan all messages**: Scans all messages regardless of size.
- **Scan message items smaller than or equal to**: Within each message, scans message items, for example attached Word documents, smaller than or equal to a specified size.

- **Scan messages smaller than or equal to**: Scans messages smaller than or equal to a specified size. This size includes message attachments and control information .

> Message control information can add to a message's size. When you plan to detect messages of a specific size, you need to allow for this control information.

Classifications

A classification to determine what to do with email messages that match each unique outcome of a scenario:

- **On threshold exceeded**

  The exclusive classification to apply when the scenario detects an email message that generates a text analysis score that exceeds the limits specified in the **Thresholds** tab.

  To block the delivery of detected messages, specify a classification that has a Quarantine action.

Special features and restrictions

Like the Commercial Disclaimer scenario, the Text Analyzer scenario, uses text analysis to identify email content. To ensure that you get the expected results when searching for multiple occurrences of an expression, it is important to understand how text analysis works. For a detailed explanation, see the MIMEsweeper Policy Editor help.

Virus Manager

The Virus Manager is an inclusive scenario that runs a supported virus-checking executable program on items. If the virus-checking program supports cleaning, you can configure the Virus Manager scenario to clean infected email messages. The scenario can optionally add specified text to messages from which detected items have been cleaned or stripped.

An example of the use of this scenario is to prevent the delivery of virus-infected email messages.

Properties

The properties of the Virus Manager scenario are briefly described in the following sections. For full details on configuring the scenario, see the MIMEsweeper Policy Editor help.

Data types

The data types and subtypes that the scenario detects in email messages and the options for processing them. You can specify whether to apply the scenario to all data types and subtypes, only selected data types and subtypes, or to all except selected data types and subtypes.

Application details

The anti-virus tool that the scenario is to use to detect data of the type specified in the **Data Types** tab.

You can specify options to have the anti-virus tool attempt to clean a detected item or to remove infected files from the email message, if the anti-virus tool supports cleaning or stripping. You can specify options to add an annotation to messages from which detected items have been cleaned or stripped.

Cleaned annotation

The text the scenario is to add to an email message from which a detected virus has been cleaned.

You might specify an annotation, for example, to advise recipients that a detected virus has been cleaned from the email message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

Stripped annotation

The text the scenario is to add to an email message from which a detected virus has been stripped.

You might specify an annotation, for example, to advise recipients that a detected virus has been stripped from the email message.

You can specify whether the text is to be added at the start of, or at the end of, the email message or at the start of, or at the end of, the message subject.

CHAPTER 5

References

This chapter provides more detailed information on References, describing the types of References you can associate with specific scenarios in MIMEsweeper for SMTP. This chapter supplements the information on References in Chapter 2.

Overview

A MIMEsweeper for SMTP Reference is a configuration item containing a list of expressions, checksums or script details that are used during text and content analysis. These lists, or References, are used by scenarios to detect certain types of message content, for example, profanity. References provide a resource for use by scenarios.

About reference types

There are three primary reference types, and each of these types can be either managed, or user-defined:

- **Expression lists** are referenced in a Commercial Disclaimer or a Text Analyzer scenario to identify the words or phrases that the scenario is to detect.
- **Checksum lists** are used in the Checksum Matcher scenario. This is an inclusive scenario that detects file checksums and compares them to checksums of known files held in the checksum list.
- **Script lists** are used in Script Manager scenarios which detect the presence of script expressions in a file.

For information on these scenarios, see Chapter 4.

In addition to these three reference types, the SpamLogic Definition List reference maintains details of characteristics which indicate that a message is spam. The SpamLogic scenario’s Anti-spam Engine detection functionality uses this reference to detect spam messages.

About managed references and user-defined references

References can be either managed or user-defined. Managed or user-defined references are identified by an icon that appears next to each Reference in the list:

- Managed references icon:
- User-defined references icon:

About managed references

A copy of each available managed reference is installed when you install MIMEsweeper for SMTP. Managed references are automatically updated on a regular basis, to protect against threats as they change and evolve.

For this update process to occur, a current Support and Maintenance agreement must be in place for your installation. If your Support and Maintenance contract is not current, automatic updates do not occur, and protection against threats degrades over time.

For example, the PDF Image Spam managed checksum list includes checksums of PDF images as they appear in common spam messages. This list is updated regularly to include checksums of the PDF images that appear in most recent spam messages.

About user-defined references

A user-defined reference is one that you create and define. For example, you can create a user-defined expression list that can be used to detect words and phrases tailored to your environment. User-defined references are not updated automatically—you must maintain them manually.

Configuring managed downloads

To ensure that your managed references are updated regularly and automatically:

- A current Support and Maintenance agreement must be in place for your installation.
- Your license must be registered on the Clearswift Threatlab website, and a managed downloads password configured for the license.

  You can register your license and set the password at installation time, or after installation.

If you do not have a current Support and Maintenance agreement in place, this registration process fails.

For more information on the Support and Maintenance agreement, contact your normal support provider.

To register your managed downloads password

As a MIMEsweeper for SMTP user you will receive a license key for both product activation and activation of the managed services. The license key and its associated serial number are in the format:

License Key: xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xx

Serial Number: nnnn-nnnn-nnnn-nnnn

To register your MIMEsweeper for SMTP Support and Maintenance password on the Clearswift website to enable Managed Downloads:

1. Connect to the Clearswift website:

   `https://www.clearswift.com/download/produpdates/register.aspx`

2. Login using your Membership Center login

   You will already be registered if you are an existing customer, or have previously downloaded any of Clearswift’s products for evaluation. If you are not already registered, you can create a member account by following the on-screen instructions.

3. Enter your license details:
   - Company Name
   - License Key
   - Serial Number
4. Enter a password. The password you specify here must be used to authorize all downloads from the Clearswift website.

   When you complete the process, a message appears, confirming that your password is registered.
5. In the MIMEsweeper Policy Editor, configure the password with your license key in the **MIMEsweeper for SMTP License Properties** page as follows:
   a. Open the **MIMEsweeper Policy Editor**.
   b. Select **Licenses** in the console tree and access the license properties from the Details pane.
   c. Select the **License** tab and enter the password in the **Password (optional):** field.
   d. **Save** and **Apply** the changes in the MIMEsweeper Policy Editor.

   Your MIMEsweeper for SMTP server is now ready to authenticate with Clearswift's website to receive managed services.

> ℹ You can reset the password at any time by changing the password in the License Registration screen. You must also reset the password in the MIMEsweeper for SMTP License Properties page.

Configuring a reference

To configure expression lists, checksum lists and script lists, access the **References** folder in the MIMEsweeper Policy Editor console tree. See *Reference properties* on page 5-5 for details.

The following sections in this chapter provide information on the different Reference types. Each Reference page provides a summary of the properties you can configure and provides notes on any special features and restrictions you should be aware of when configuring the Reference.

For details about References, as well as procedures for working with them see the MIMEsweeper Policy Editor help.

Reference properties

You can create new References using wizards and you can change the properties of existing References by configuring the options in a Reference's properties page. To configure a Reference, access properties from the Reference item in the Details pane of the MIMEsweeper Policy Editor.

There are some common Reference properties that are accessed from the Reference folder in the console tree.

These are:

- **General**

  The details of the item, including the name and type of the item.

- **Proxy**

  If you are using a Proxy server in your deployment you must enter the server details in this tab including server name, port number, user name and password. This facilitates the maintenance of your managed lists; the downloads are delivered from the Clearswift server via this proxy server. Further information about Managed lists is provided in the descriptions of Reference properties in the following sections.

- **Notes**

  Any user-specified text describing the item, for example, details of how the item or its configuration forms part of a policy.

All Reference properties pages contain the **General** and **Notes** tabs.

Expression list

Expression lists contain words and phrases that MIMEsweeper for SMTP is to detect during text analysis. The relative value of each expression is returned when detected.

⚠ The Profanity expression list, whether managed or user-defined, may contain certain words and phrases that could cause offense to some people. If you feel that you may be offended by the contents of these expression lists, do not view them. However, using this expression list can help to stop the circulation of profanity to and from your organization and should only be used in this context—it is not intended for circulation.

A phrase can be a simple phrase containing a string of words, or a compound phrase containing multiple words and phrases, connected by expression operators. For more information, see *Expression operators* on page 5-9.

There are two types of expression list Reference:

- **Managed expression list**

  Dynamic lists managed by Clearswift. Managed lists are imported from the Clearswift server by the managed list wizard. Your managed expression lists are automatically refreshed every time the list is updated by Clearswift. Managed expression lists cannot be edited. Setting up managed lists is described in the following Properties sections in this chapter.

- **User-defined expression list**

  Static lists that you create in MIMEsweeper Policy Editor using the user-defined list wizard to create a new list of manually entered expressions. Using the property pages you can edit user-defined lists. You can also import expression lists from the Clearswift server, or other locations, which you then edit in the wizard or the Properties dialog. Expression lists imported using the user-defined wizard, will not be automatically updated.

Expression list Properties

The properties of an expression list are briefly described in the following sections. These sections contain reference information that you can use when configuring expression lists. For full details on configuring expression lists, see the MIMEsweeper Policy Editor help.

General

The **General** property page displays the title given to the expression list and its type, for example, Managed Expression List.

Managed List - managed expression lists only

The **Managed List** tab details the available managed lists that you can use. Select one or more lists for the reference to use.

Management - managed expression lists only

The commands on the **Management** tab allow you to specify when the expression list is updated.

You can set an interval in which the Managed expression list is automatically updated from the Clearswift server, or you can perform an immediate update.

Each time the update interval is reached, MIMEsweeper for SMTP checks for a new definition file. A download will not take place if the current file being used is the latest available.

The **Management** tab also incorporates a log file window which lists log entries recording the number of successful updates to the Managed expression lists.

For information on registering your MIMEsweeper for SMTP license on the Clearswift website to enable Managed Downloads, see *Configuring managed downloads* on page 5-4.

Expressions

The list of keywords and phrases that are to be detected during text analysis. You can specify phrases in the following ways:

- **Clearswift Standard Patterns**: You can configure these to detect the following standard patterns:
    - Credit card number.
    - UK National Insurance Number.
    - US Social Security Number.
- **Regular Expression (PERL/POSIX)**: Multiple words and phrases connected by expression operators.

- **Simple or Regular Expression (MIMEsweeper)**: these can be simple word or phrase lists. With these types, you can also use the syntax available with previous versions of MIMEsweeper for SMTP to configure regular expressions.

  If you are upgrading from a previous version of MIMEsweeper for SMTP, you may need to update your regular expressions, if you have defined any, to ensure that they are compatible with the new release. See the Policy Editor online help for details on how to upgrade your previous expression lists for use with MIMEsweeper 5.3.

For each keyword or phrase, you specify a weighting that identifies the relative importance of the specified expression when it is detected during text analysis. The weighting score is compared to the search threshold specified in the **Thresholds** tab of the reference’s Properties page. If the total calculated score for a scan area exceeds the specified search threshold, the message is considered suspect and is processed according to the options specified in the scenarios.

You also can specify whether the capitalization of the specified keyword or phrase must match in order for it to be detected.

To import expression lists from the Clearswift server or from your local PC, use the **Import** command. For more information, see *Importing references* on page 5-27.

When importing a list there are three import options:

- **Clear existing list**

  Clears all expressions listed on the property page, and imports the new list.

- **Merge with existing list and overwrite existing entries**

  Merges imported expressions with those listed on the property page and overwrites expressions that are duplicated. When overwritten, an expression assumes the weighting and case settings of the imported expression.

- **Merge with existing list but do not overwrite existing entries**

  Merges imported expressions with those listed on the property page. Duplicated expressions are not overwritten and keep their existing weighting and case settings.

When viewing the properties of a managed expression list, the property page displays the expressions in read only format.

Usage

A list of the scenarios currently associated with the expression list. Each entry shows the scenario name and its location in the scenario folder hierarchy. You can navigate to a Scenario item by highlighting a Scenario from the list and clicking the **Show** button.

Configuring expressions

The following sections provide reference information on how to specify compound phrases.

See the Policy Editor online help for more information, and examples.

Glossary of terms

The following table defines the terminology used in this section.

Table 5-1: Glossary of terms used with expressions

Term	Meaning
Atom	A single character or an expression surrounded by ‘()’, or ‘[]’. These can be wholly affected by repeating metacharacters such as ‘*’ and by bounds ‘{}’.
Expression	A simple keyword, an ordered list of words within a phrase or a regular expression.
Normal	Alphanumeric characters (A-Z, a-z, 0-9).
Punctuation	Any characters other than those classified as normal or whitespace. This class includes the hyphen and underscore characters.
Whitespace	Space, tab, linefeed or carriage return characters.
Word	A string of alphanumeric characters delimited by whitespace or punctuation (or the beginning or end of the string). This leads to words containing punctuation being split into multiple ‘Lex words’.

Expression operators

You list keywords or phrases to be detected during text analysis in the **Expressions** tab of the Properties page for expression lists. A phrase can be a simple phrase containing a string of keywords, or a compound phrase containing multiple keywords and phrases, connected by expression operators.

Expression operators are used to connect multiple keywords or phrases to specify a compound phrase in the list. Compound phrases created with expression operators are treated as a single expression, which is counted once for the purposes of weighting.

Table 5-2 describes the available expression operators. Full details and examples are provided in the MIMEsweeper Policy Editor help.

Table 5-2: Expression operators

Operator	Description
.AND.	Both keywords or phrases must be present.

Table 5-2: Expression operators

Operator	Description
.ANDNOT.	The keyword or phrase that precedes the operator must be present, and the keyword or phrase that follows the operator must not be present.
.NEAR.	Both keywords or phrases must be present, and they must be within a specified number of words of one another. The number is specified in the proximity threshold setting of the Text Analyzer or Commercial Disclaimer scenario properties.
.OR.	One or the other keyword or phrase must be present.
.XOR.	One or the other keyword or phrase must be present but not both.
.BEFORE.	Both keywords or phrases must be present and the keyword or phrase that precedes the operator must occur before the keyword or phrase that follows the operator.
.AFTER.	Both keywords or phrases must be present and the keyword or phrase that precedes the operator must occur after the keyword or phrase that follows the operator.
.FOLLOWEDBY=x.	Both keywords or phrases must be present and the keyword or phrase that follows the operator must be within x words of the one that precedes the operator.
.REGEXP.	A regular expression that contains metacharacters or wildcard characters to identify character strings that can be substituted in order to search for variations of the specified keyword.

Configuring Regular (PERL/POSIX) expressions

PERL / POSIX regular expressions allow you to configure complex patterns to be matched. This section provides reference information for configuring PERL / POSIX) expressions.

Regular Expression Syntax

The table below provides information on the syntax to use in PERL / POSIX) expressions.

Table 5-3: Regular Expression Syntax

Character	Description
.	Any single character.
^	Anchor character, matches the start of a line.
$	Anchor character, matches the end of a line.
()	Sub-expression. Separates the expression within the brackets allowing it to be subjected to the repeating metacharacters or referenced with the back reference function. See below for details of these functions.
|	Or operator. Matches either the expression preceding or succeeding the operator. For example, “a|b” matches either “a” or “b”.

Table 5-3: Regular Expression Syntax

Character	Description
*	Zero or more occurrences of the preceding atom. For example, "ab*c" matches "ac", "abc", "abbbbbbbbc" etc... "(he)*" matches "he", "hehehehehehe" etc...
+	One or more occurrences of the preceding atom.
?	Zero or one occurrences of the preceding atom.
{x}	Bounded repeat. Matches exactly 'x' occurrences of the preceding atom.
{x,y}	Matches between 'x' and 'y' (inclusive) occurrences of the preceding atom.
{x,}	Matches 'x' or more (inclusive) occurrences of the preceding atom.
x?	Non greedy repeat of repeating metacharacter 'x'. The repeating functions above attempt to match as much as possible (they are greedy). Following any of the repeating metacharacters with a "?" causes the repeat to be non greedy. That is, the match is as short as possible. For example, in the string "It went on and on and on.", "went.{2,}on" matches "went on and on and on" whereas "went.{2,}?on" only matches "went on and on".
\n	Back reference. Matches the string that was matched by sub-expression 'n'. Where 'n' is a number from 1 to 9. For example, "(.*)-\1" matches "abc-abc" and "1234-1234" but not "abc-1234".
\x	Where 'x' is a metacharacter this syntax indicates that 'x' is to be treated literally and not as a metacharacter. For example, '\$' matches '$'. '\\' matches '\'. Where 'x' is a predefined escape sequence character (or sequence of characters) match the character or character class defined by that escape sequence. For more information about escape sequences, see the table below.
[]	Character set. Matches any one character from the list. For example, "[abc]" matches either "a" or "b" or "c". The whole character set may be subjected to the repeating metacharacters. For example, '[abc]*' matches 'aabcac' but not 'abcdcba'.
[^]	Negated character set. Matches any one character which is not in the character set. For example, "[^bc]" matches "a" and "d" but not "b" or "c".
[x-y]	Character range. Matches one character in the range 'x' to 'y'. For example, "[a-c]" matches "a", "b" or "c". The range endpoints must be in the correct order. That is, the first endpoint must precede the second endpoint in the Unicode codepoint sequence. To include a literal '-' character in a character set enter it as the first or last character.

Table 5-3: Regular Expression Syntax

Character	Description
[:x:]	Character class. A predefined set of characters—see *Character classes* on page 5-13 for available definitions. Character classes must be used within a character set definition. For example, “[[:digit:]]” matches any numeric character. You can use character classes in conjunction with other characters in a character set definition. For example, “[abc[:digit:]]” matches either “a” or “b” or “c” or any numeric character.
[.x.]	Collating element. A single character or sequence of characters that collates as a single element. Collating elements may only be used within a character set. For example, “[[.ae.]]”. (This assumes that ‘ae’ is a collating element in the current system locale. Collating elements may also be used as a form of escape character as most special characters lose their special significance when used within a character set. For example, to specify a ‘-‘ as a range endpoint, it can be declared as a collating element such as “[!-[.-.]]”. Additionally some characters can be declared in a collating element by referring to the characters symbolic name. See below for a table of available symbolic names.
[=x=]	Equivalence class. A character set of all characters with the same primary sort key as character ‘x’. An equivalence class may only be used within a character set. For example, “[[=e=]]” would match any of the following characters. “eÈÉÊËèéêëEeEeEeEeEe”. Note that this function is locale specific so should be used with caution. Different locales or platforms may result in different behavior.
(?#comment)	Comment. Text between the ‘#’ and the closing ‘)’ are ignored. This can be used to explain how the expression works for future reference. For example, “(?#3 letters)[[:alpha:]]{3}(?#followed by 5 digits)[[:digit:]]{5}”.
(?=pattern)	Positive lookahead. Returns a match if ‘pattern’ matches. The current point of reference is not moved so subsequent expressions match from the same point. This can be used to logically ‘and’ two or more regular expressions. For example, “(?=.*[[:lower:]])(?=.*[[:upper:]])” confirms that there are upper and lower case characters in the string.
(?!pattern)	Negative lookahead. Returns a match if ‘pattern’ does not match. The current point of reference is not moved so subsequent expressions match from the same point.
(?<=pattern)	Positive lookbehind. Returns a match if ‘pattern’ matches immediately before the current point of reference. The current point of reference is not moved so subsequent expressions match from the same point.
(?<!pattern)	Negative lookbehind. Returns a match if ‘pattern’ does not match immediately before the current point of reference. The current point of reference is not moved so subsequent expressions match from the same point.

Table 5-3: Regular Expression Syntax

Character	Description
(?>pattern)	Independent sub-expression. A sub expression that does not allow backtracking into ‘pattern’ in order to try and satisfy the larger expression. This function can be used to achieve significant performance improvements. For example, “([ab}+)[bc]+” matches “abb”. But “(?>[ab}+)[bc]+” does not match “abb”. It does however match “abc”.
(?(condition)true|false)	Conditional expression. If ‘condition’ is true, attempts to match the ‘true’ pattern. If ‘condition’ is false, attempts to match the ‘false’ pattern. The condition may be either a lookahead or the index of a marked sub-expression.
(?(condition)true)	Conditional expression. If ‘condition’ is true, attempts to match the ‘true’ pattern. If ‘condition’ is false the expression returns no match. The condition may be either a lookahead or the index of a marked sub-expression.

Character classes

The table below provides information on the PERL / POSIX) character classes.

Table 5-4: PERL / POSIX) character classes

Character class	Description
[:alnum:]	All alphanumeric characters. Note: This is not restricted to the Latin alphabetic characters.
[:alpha:]	All alphabetic characters. Note: This is not restricted to the Latin alphabetic characters.
[:blank:]	All whitespace characters apart from line separator characters.
[:cntrl:]	All control characters.
[:d:] [:digit:]	All decimal digit characters.
[:graph:]	All graphical characters.
[:l:] [:lower:]	All lower case characters. This character class is not affected by configuring the expression to match case insensitively.
[:print:]	All printable characters.
[:punct:]	All punctuation characters.
[:s:] [:space:]	All whitespace characters.
[:unicode:]	All extended characters with a code point of greater than 255.
[:u:] [:upper:]	All upper case characters. This character class is not affected by configuring the expression to match case insensitively.

Table 5-4: PERL / POSIX) character classes

Character class	Description
[:w:] [:word:]	All alphanumeric characters and the underscore character.
[:xdigit:]	All hexadecimal digit characters.

The above may only be used within a character set.

Escape Sequences

The table below provides information on the PERL / POSIX) escape sequences.

In the list below:

- The escape sequences listed below are case-sensitive.
- All other escape sequences, other than escaped metacharacters, are undefined and may result in unexpected behavior; they should not be used.

Table 5-5: Escape sequences

Sequence	Meaning
\a ’	‘bell’ character.
\e	‘escape’ character.
\f	‘form feed’ character.
\n	‘newline’ character.
\r	‘carriage return’ character.
\t	‘tab’ character.
\v	‘vertical tab’ character.
\b	‘backspace’ character, but only inside a character set declaration.
\cd	An ASCII escape sequence – the character whose code point is d % 32.
\xhh	A hexadecimal escape sequence – the character whose code point is 0xhh.
\x{hhhh}	A hexadecimal escape sequence – the character whose code point is 0xhhhh.

Table 5-5: Escape sequences

Sequence	Meaning
\0ddd (\zero)	An octal escape sequence – the character whose code point is 0ddd.
\N{name}	Matches the single character which has the symbolic name 'name’. (See below for a table of available symbolic names).
\d	Matches any digit character.
\l	Matches any lower case character. This escape sequence is not affected by configuring the expression to match case insensitively.
\s	Matches any whitespace character.
\u	Matches any upper case character. This escape sequence is not affected by configuring the expression to match case insensitively.
\w	Matches any alphanumeric character or underscore character.
\D	Matches any character that is not a digit.
\L	Matches any character that is not lower case. There is a distinction between this and matching any upper case character as some characters do not have case and would therefore match this escape sequence.
\S	Matches any character that is not whitespace.
\U	Matches any character that is not upper case. There is a distinction between this and matching any lower case character as some characters do not have case and would therefore match this escape sequence.
\W	Matches any character that is neither alphanumeric nor an underscore character.
\px	Equivalent to the single character, character class “[[:x:]]”. For example, “\pd” matches any digit character.
\p{name}	Equivalent to the character class “[[:name:]]”. For example, “\p{punct}” matches any punctuation character.
\Px	Equivalent to the negated single character, character class “[[:x:]]”. For example, “\Pd” matches any character that is not a digit.
\P{name}	Equivalent to the character class “[[:name:]]”. For example, “\p{punct}” matches any character that is not punctuation.
\<	Matches the null string at the beginning boundary of a word. Word in this context is in regular expression terms, not Lexical terms. See character classes for details.

Table 5-5: Escape sequences

Sequence	Meaning
\>	Matches the null string at the end boundary of a word. Word in this context is in regular expression terms, not Lexical terms. See character classes for details.
\b	Matches the null string at either the beginning or end boundary of a word. Word in this context is in regular expression terms, not Lexical terms. See character classes for details.
\B	Matches when not at a word boundary. Word in this context is in regular expression terms, not Lexical terms. See character classes for details.
\	`Matches the start of the text being searched. This is slightly different to the '^' anchor which matches the beginning of a line.
\'	Matches the end of the text being searched. This is slightly different to the '$' anchor which matches the end of a line.
\A	Matches the start of the text being searched. This is identical in function to '\`'.
\z	Matches the end of the text being searched. This is identical in function to '\''.
\C	Matches any single code point. This is identical in function to '.'.

Symbolic names

The table below provides information on the PERL / POSIX) symbolic names.

Symbolic names may only be used with a collating element.

Table 5-6: Symbolic names

Name	Character
NUL	\x00
SOH	\x01
STX	\x02
ETX	\x03
EOT	\x04
ENQ	\x05
ACK	\x06

Table 5-6: Symbolic names

Name	Character
alert	\x07
backspace	\x08
tab	\t
newline	\n
vertical-tab	\v
form-feed	\f
carriage-return	\r
SO	\xE
SI	\xF
DLE	\x10
DC1	\x11
DC2	\x12
DC3	\x13
DC4	\x14
NAK	\x15
SYN	\x16
ETB	\x17
CAN	\x18
EM	\x19
SUB	\x1A
ESC	\x1B
IS4	\x1C
IS3	\x1D
IS2	\x1E
IS1	\x1F
space	\x20
exclamation-mark	!
quotation-mark	"
number-sign	#
dollar-sign	$
percent-sign	%

Table 5-6: Symbolic names

Name	Character
ampersand	&
apostrophe	'
left-parenthesis	(
right-parenthesis	)
asterisk	*
plus-sign	+
comma	,
hyphen	-
period	.
slash	/
zero	0
one	1
two	2
three	3
four	4
five	5
six	6
seven	7
eight	8
nine	9
colon	:
semicolon	:
less-than-sign	<
equals-sign	=
greater-than-sign	>
question-mark	?
commercial-at	@
left-square-bracket	[
backslash	\
right-square-bracket	]
circumflex	~

Table 5-6: Symbolic names

Name	Character
underscore	_
grave-accent	`
left-curly-bracket	{
vertical-line	|
right-curly-bracket	}
tilde	~
tilde DEL	\x7F

Configuring Simple or Regular Expressions (MIMEsweeper)

A simple expression is an ordered word list. Any punctuation that is not specified in the expression is effectively removed from the text being searched and any whitespace is consolidated into single spaces. For example, the following will all return matches:

Table 5-7: Simple expression, text matches

Expression	Text
Me	Me.
Me	(Me!)
Yes thank you	Yes, thank-you.

Partial Word matches are not reported by simple expressions. For example, the following will not return matches:

Table 5-8: Simple expression, partial word non-matches

Expression	Text
butt	butter.
swear	menswear
pig	spigot

Punctuation specified in a simple expression must be present in the text being searched for a match to occur. Conversely, punctuation within the text being searched does not need to be matched by respective punctuation in the expression. However, punctuation does serve to delimit words. For example:

Table 5-9: Simple expression, punctuation matches

Expression	Result	Text
Here and there	Matches	Here and there

Table 5-9: Simple expression, punctuation matches

Expression	Result	Text
Here and there	Matches	Here, and there.
Here and there	Matches	Here-and-there.
don't	Matches	don't
dont	Does not match	don't
don t	Does not match	don't
don't	Matches	dont
don't	Does not match	don t

Configuring MIMEsweeper regular expressions

You can use the .REGEXP. expression operator with a keyword or phrase to indicate a regular expression. Except for some small differences, these expressions are compatible with previous versions of MIMEsweeper for SMTP. See the online help for information on how to check that your expressions created using previous versions of MIMEsweeper are compatible.

See the Policy Editor online help for more information, and examples.

A regular expression uses metacharacters and wildcard characters to identify one or more characters that can be substituted in order to search for variations of the specified keyword or phrase. You can include more than one metacharacter or wildcard in a regular expression. The second metacharacter or wildcard modifies the previous metacharacter or wildcard.

Table 5-10 shows the metacharacters and wildcard characters you can use to create a regular expression. Examples are provided in the MIMEsweeper Policy Editor help.

Table 5-10: Regular expression metacharacters and wildcard characters

Metacharacter	Description
?	Any single character.
*	Zero or more of the preceding character or metacharacter.
+	One or more of the preceding character or metacharacter.
\	An escape sequence that specifies a metacharacter as a literal character. For example, \? indicates the question mark (?) is to be included in the search.
\h{*xxxx*}	An escape sequence that specifies a hexadecimal character code, where xxxx is the hexadecimal character code.
(*literal-expression*){*x*,*y*}	Matches *x* or *y* occurrences of the literal expression.
(abc)	The group of characters “abc”.

Table 5-10: Regular expression metacharacters and wildcard characters

Metacharacter	Description
a|b	One, but not both, of the characters.
(a|b|c)	Any one of the characters.
[abc]	Any one of the enclosed characters.
[a-c]	Any one of the enclosed range of characters. This is equivalent to [c-a].
[0-9]	Any one of the range of numbers.
{x}	Matches exactly x number of the preceding character or metacharacter.
{x,y}	Matches between x and y number inclusively of the preceding character or metacharacter.
{,y}	Matches zero and y number of the preceding character or metacharacter.
{x,}	Matches between x or more of the preceding character or metacharacter.

Regular expressions can have a significant effect on system performance if used excessively. It is recommended to avoid using them if possible.

Checksum list

Checksums lists allow known files, which have been identified as containing potential threats, to be evaluated on their content, and not by their name. The content of a file is defined by a checksum, which is a unique 32 digit hexadecimal value based upon the byte information within the file. This is an MD5 hash value. The checksum uniquely identifies a specific file. MIMEsweeper Policy Editor generates a checksum for each file included in the checksum list.

Checksum lists are used by the Checksum Matcher scenario, which detects files with matching checksums and classifies them accordingly. To be detected, the file must be the exact one identified by its checksum. For information on these scenarios, see Chapter 4.

In addition to identifying files containing threats, a checksum list can be used to identify known files containing information that your organization does not want to transmit. For example photographs or diagrams of a new products.

There are two types of checksum list Reference:

- **Managed checksum list**

  These are dynamic lists managed by Clearswift. Managed lists are imported from the Clearswift server by the managed list wizard. Your managed checksum lists are automatically refreshed every time the list is updated by Clearswift. Managed checksum lists cannot be edited. For details on managed lists, see *Importing references* on page 5-27.

- **User-defined checksum list**

  These are static lists that you create in MIMEsweeper Policy Editor by using the user-defined list wizard and manually adding files. When you browse for a file and add it to the list, MIMEsweeper Policy Editor generates a 32 digit hexadecimal value which is defined by the file content. You can also import checksum lists from the Clearswift server, or from your local PC. Checksum lists imported using the user-defined wizard, will not be automatically updated.

Managed and user-defined checksum lists are configured and maintained in exactly the same way as Expression lists. For details on managed and user-defined lists, see *Expression list* on page 5-6.

Checksum list properties

The properties of a checksum list are briefly described in the following sections. For full details on configuring checksum lists, see the MIMEsweeper Policy Editor help.

General - managed checksum list only

The **General** tab displays the title given to the checksum list and its type.

Management - managed checksum lists only

The commands on the **Management** tab allow you to specify when the checksum list is updated.

You can set an interval in which the Managed checksum list is automatically updated from the Clearswift server, or you can perform an immediate update.

Each time the update interval is reached MIMEsweeper for SMTP checks for a new definition file. A download will not take place if the current file being used is the latest available.

The **Management** tab also incorporates a log file window which lists log entries recording the number of successful updates to the Managed checksum list.

For information on registering your MIMEsweeper for SMTP license on the Clearswift website to enable Managed Downloads, see *Configuring managed downloads* on page 5-4.

Checksums

Displays the list of files and their associated checksums that are currently included in the checksum list. You can create new checksums by entering an MD5 value, browse for existing checksums or delete them from the list. When a file is added to the list a checksum is generated and inserted into the **Checksum** column.

In the **Comment** column, you can add a comment to the checksum or leave the default comment that is the name of the file used to generate the checksum.

To import checksum lists from the Clearswift server or from your local PC, use the **Import** command. For more information, see *Importing references* on page 5-27.

When importing a list there are three import options:

- **Clear existing list**
  Clear all checksums listed on this property page.
- **Merge with existing list and overwrite existing entries**
  Merge imported list with those on this page and overwrite duplicated ones.
- **Merge with existing list but do not overwrite existing entries**
  Merge imported list with those on this page. Duplicated checksums are not overwritten.

When viewing the properties of a managed checksum list, the property page displays the files in read only format.

Usage

A list of the scenarios currently associated with the checksum list. Each entry shows the scenario name and its location in the scenario folder hierarchy. You can navigate to a Scenario item by highlighting a scenario from the list and clicking the **Show** button.

Script list

Script lists contain parts of scripting language (script expressions) that MIMEsweeper for SMTP uses to detect potential source code extracts for malicious activity. Script lists are used in Script Manager scenarios to detect files that contain scripts that are deemed potential threats.

Script lists in scenarios work in a similar way to expression lists, except that a script expression is not allocated a weighting. A script expression is either detected or not detected in a file. If detected by the scenario, the message is classified accordingly. For more information about scenarios, see Chapter 4.

Detecting script expressions in a message is a two-stage process. A script list is made up of two separate lists: a Primary list and Secondary list. For scripts in a message to be detected, one expression in the Primary list must be found, then one expression in the Secondary list must be found. The process is as follows:

Initially, the Primary list is read to detect the presence of scripts in a file.

- Script examples from the Primary list: `<script>`
  - If scripts are detected, the Secondary list is read to determine if any of the scripts contained in the file are deemed to be malicious.
- Script expression example from the Secondary list: `.regcreate`
  - If matching script expressions are found, the scenario will classify the message as specified.

There are two types of script list Reference:

- **Managed Script lists**

  Dynamic lists managed by Clearswift. Managed lists are imported from the Clearswift server by the managed list wizard. Your managed script lists are automatically refreshed every time the list is updated by Clearswift. Managed script lists cannot be edited. Setting up managed lists is described in the following Properties sections in this chapter.

- **User-defined Script lists**

  These are static lists that you create in MIMEsweeper Policy Editor by using the user-defined list wizard and manually adding files. When you browse for a file and add it to the list, MIMEsweeper Policy Editor generates a 32 digit hexadecimal value which is defined by the file content. You can also import script lists from the Clearswift server, or from your local PC. Script lists imported using the user-defined wizard, will not be automatically updated.

Managed and user-defined Script lists are configured and maintained in exactly the same way as Expression lists. For details on managed and user-defined lists, see *Expression list* on page 5-6.

Script list properties

The properties of a script list are briefly described in the following sections. For details about configuring script lists, see the MIMEsweeper Policy Editor help.

General - managed script lists only

- The **General** property page displays the title given to the script list and its type, for example: Managed Script List.

Management - managed script lists only

The commands on the **Management** tab allow you to specify when the script list is updated.

You can set an interval in which the Managed script list is automatically updated from the Clearswift website, or you can perform an immediate update.

Each time the update interval is reached your MIMEsweeper for SMTP server checks for a new definition file. A download will not take place if the current file being used is the latest available.

The **Management** tab also incorporates a log file window that lists log entries recording the number of successful updates to the Managed script list.

For information on registering your MIMEsweeper for SMTP license on the Clearswift website to enable Managed Downloads, see *Configuring managed downloads* on page 5-4.

Primary expressions

The list of keywords that are to be detected during the first stage of detecting scripts.

You can specify phrases in the following ways:

- **Simple keyword**: A string of words.
- **Compound keywords**: Multiple words and phrases connected by expression operators. For details, see *Expression operators* on page 5-9.

Unlike Expression lists, you cannot specify a weighting for a script expression. This column is not configurable and defaults to Detected.

You can specify whether the capitalization of the specified keyword must match in order for it to be detected.

For user-defined expressions, users must only use US ASCII characters when creating script expressions.

Any user-defined script expressions containing non-US ASCII characters created in a release prior to 5.1 will be ignored during script analysis of messages. Users will need to correct any such expressions.

8-bit characters can be entered using \xhh syntax (that is, \x followed by two hexadecimal characters).

To import Script lists from the Clearswift server or from your local PC, use the **Import** command. For more information, see *Importing references* on page 5-27.

The import command can only be executed from the Primary Expressions tab, although both primary and secondary script expressions are imported.

When importing a list there are three import options:

- **Clear script list**

  Clears all script expressions listed on this property page.
- **Merge with existing list and overwrite existing entries**

  Merges imported script expressions with those listed on this property page and overwrites script expressions that are duplicated.
- **Merge with existing list but do not overwrite existing entries**

  Merges imported script expressions with those listed on this property page. Duplicated expressions are not overwritten.

When viewing the properties of a managed script list, the property page displays the expressions in read only format.

Secondary expressions

The list of keywords that are to be detected during the second stage of detecting scripts.

Usage

A list of the scenarios currently associated with the script list. Each entry shows the scenario name and its location in the scenario folder hierarchy. You can navigate to a Scenario item by highlighting a scenario from the list and clicking the **Show** button.

Importing references

When using a Reference wizard to create a user-defined Reference, for example an expression, checksum or script reference, you can import the reference from the Clearswift website, or from a file.

To import a reference, on the screen where you configure the reference, click the **Import** button, and select to import from a file or from the web. If you select to import from the web, a list of the current Clearswift available references is displayed.

Edit existing References by accessing the properties of the Reference item in the Details pane of the MIMEsweeper Policy Editor. The options for importing and editing lists in the properties pages are the same as those available in the wizards. However only user-defined lists can be edited. For details on the difference between managed and user-defined lists for each Reference type, see *Expression list* on page 5-6, *Checksum list* on page 5-22 and *Script list* on page 5-24.

Exporting lists

You can export details to a local list from an existing expression, checksum or script list. For more information about how to import and export lists, see the MIMEsweeper Policy Editor help.

CHAPTER 6

Mail Routing and Relay

This chapter describes the system parameters of MIMEsweeper for SMTP that control the routing and relay of email messages and the security of SMTP relays.

Overview

MIMEsweeper for SMTP is a full SMTP relay, through which you can route email messages for policy implementation. When MIMEsweeper for SMTP receives email messages, it performs any configured message processing, and then forwards messages to the next host for delivery. You can configure relay security options to prevent other mail hosts from forwarding mail through MIMEsweeper for SMTP. Configuration takes place in the MIMEsweeper Policy Editor.

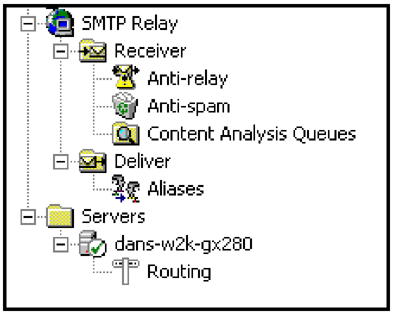


Figure 6-1: SMTP Relay folder structure

Access SMTP Relay properties from the components contained in the SMTP Relay folder. The folder structure is shown in Figure 6-1.

Be aware that items in the console tree, for example the **Servers** folder, can have a different set of properties from the corresponding server item properties accessed from the Details pane.

Selecting the SMTP Relay container opens the Task Pad in the Details pane. This is described in *Task pad* on page 6-5.

Whether you are creating new items by accessing wizards from the Task Pad, or editing existing items by accessing their properties, the configuration options presented are the same. No distinction is made between wizard options or properties in the following descriptions. For details on wizards, see Chapter 6 of the *Getting Started Guide*.

The various aspects of the SMTP Relay configuration, dependent on the selected component, folder or item, are described below:

- **SMTP Relay**

  Configure MIMEsweeper for SMTP routing information and the routes used to deliver mail by configuring synonym domains. This is described in *SMTP Relay* on page 6-6.

- **Receiver**

  Configure the system parameters and relay security. This is described in *Receiver properties* on page 6-7.

- **Anti-relay**

  Configure relay security options to prevent other mail hosts from forwarding mail through MIMEsweeper for SMTP. This is described in *Anti-relay properties* on page 6-12. Note that the Anti-relay folder does not contain items that can be selected in the Details pane.

- **Anti-spam**

  Configure Mail Database lookup sites to block messages from known sources of spam. This is described in *Banned addresses* on page 6-16. Note that the Anti-spam folder does not contain items that can be selected in the Details pane.

- **Content Analysis Queues**

  Configure queues that allow priority mail to be accelerated through the security service. This is described in *Content Analysis Queues* on page 6-17.

- **Deliver**

  Configure delivery authentication and the retry schedule for undelivered messages. This is described in *Deliver properties* on page 6-18.

- **Aliases**

  Configure the way one email address (or group of addresses) is mapped to another by creating aliases. This is described in *Aliases* on page 6-19.

- **Servers**

  Configure properties for the mail processing servers on your system. This is described in *Servers* on page 6-21.

- **Routing**

  Configure the delivery paths the Delivery service uses to direct incoming email messages. This is described in *Routing* on page 6-24.

Task pad

The **SMTP Relay Settings** page is displayed in the Details pane when you select the **SMTP Relay** folder. This page is referred to as the Task Pad.

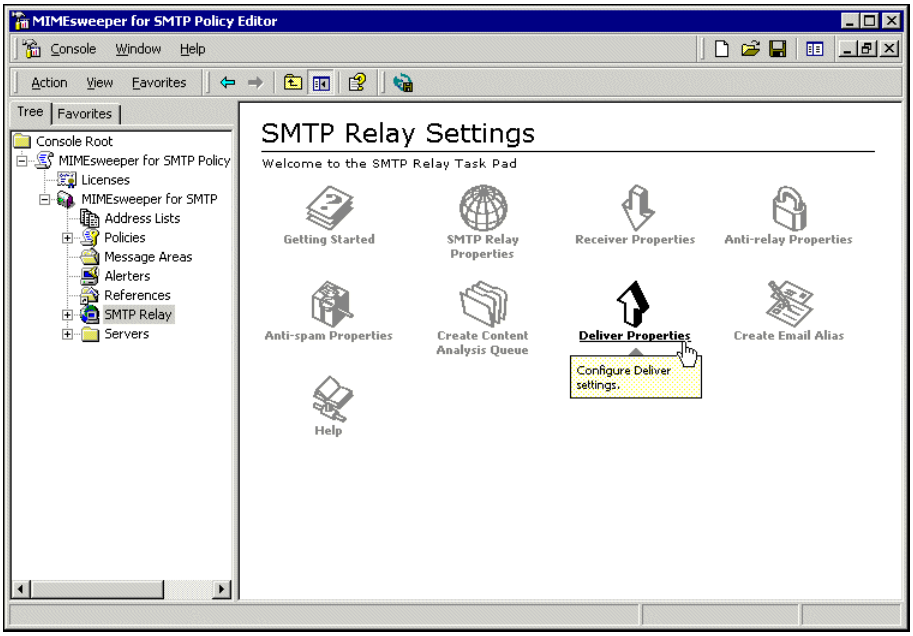


Figure 6-2: SMTP Relay Task Pad

The Task Pad is designed to help new or infrequent users to quickly get started with using the SMTP Relay settings. The Task Pad icons provide a quick and easy way to access the relay wizards and the MIMEsweeper Policy Editor help system. For details on using wizards in MIMEsweeper Policy Editor, see Chapter 6 of the *Getting Started Guide.*

For details about the links available from the Task Pad see the MIMEsweeper Policy Editor help.

SMTP Relay

You configure how the MIMEsweeper Policy Editor controls routing information, as well as the routes used to deliver mail, by configuring synonym domains under the **SMTP Relay** folder. The default domain name for your company is set up after installation using the Initial Policy Wizard. This is the domain used to construct default routes. For details on constructing routes, see *Routing* on page 6-24.

SMTP Relay properties

You can configure the secondary domains that MIMEsweeper Policy Editor uses as local domains in addition to your default domain. This is done by creating synonym domains in the **Domains** tab of the **SMTP Relay** Properties page. A synonym domain is useful, for example, for two companies that have merged and are using a single network or gateway for email users on separate domains.

The default domain is created after installation in the Initial Policy Wizard. You can see the domain details by selecting the **SMTP Relay Properties** icon in the Task Pad. All users at this default domain are represented in the default address list Company Name, which is created during installation.

This section briefly describes the properties of a domain.

Domains

In the **Domain** tab of the properties page for your domain item, you specify a list of domains to which the MIMEsweeper Policy Editor applies the routes and the relay security properties for your default domain. These domains are also used by aliases, auditing, Personal Message Manager (PMM) and Relay Targets.

The domains that you define in this section are available for assigning to MIMEsweeper Manager users. You can restrict MIMEsweeper Manager users so that they can manage messages from specific domains only.

PMM accounts may only be checked for addresses which are part of your primary domain or one of your synonym domains.

PMM Accounts are cleared down if you delete synonym domains.

You must specify synonym domains in policy configuration items such as **Address Lists**. You can then define appropriate email policies for users in different domains.

An alias address which maps from a synonym or local domain must be constructed correctly for it to work. See *Synonym domains in aliases* on page 6-19.

You specify whether delivery failure reports are sent to the postmaster for the listed synonym domains by setting the **Delivery Options** on the **Retry Schedule** of the **Deliver Properties** page. See *Retry schedule* on page 6-18.

You can rename your default domain. However, be aware that the new domain name is not automatically updated in SMTP relay and routing items in the **SMTP Relay Properties** page, the **Policies Properties** page, or in policy configuration items such as **Address Lists**. You must manually update your domain name in these areas. For details about renaming your default domain, see the MIMEsweeper Policy Editor help.

Receiver properties

MIMEsweeper Policy Editor controls routing information and the behavior of the Receiver service according to the options specified in the **Receiver Properties** page.

Security

In the **Security** tab, you configure the security features of the Receiver service.

You specify any checks that MIMEsweeper for SMTP is to perform on connecting SMTP hosts that attempt to relay email messages, including whether or not to perform a reverse address lookup in the DNS when an SMTP host attempts to connect to the MIMEsweeper for SMTP gateway. You also specify whether or not MIMEsweeper for SMTP checks that the domain of the sender's email address is listed in the local DNS.

When **Look up connecting SMTP hosts in DNS** is selected, reverse DNS lookup is enabled. When selected, it affects what you can specify in many other Relay configuration items. Specifically, for the items listed below, you can enter host names as well as IP addresses.

- Relay Hosts
- Banned Hosts
- Receiver Service Authentication

If Reverse DNS lookup is not enabled, host names cannot be used in these configuration items.

You can specify whether MIMEsweeper for SMTP accepts connections from an SMTP host if the reverse lookup fails, and whether or not MIMEsweeper for SMTP accepts the NetBIOS name of a connecting host from a reverse address lookup in the DNS.

NetBIOS addresses have either:

- No dots
- One or more characters that are not alphanumeric, hyphen, underscore or dot

Everything else is counted as a DNS name except IP addresses.

When **Validate HELO/EHLO against the DNS** is activated, this feature requests the Receiver service to validate the SMTP HELO / EHLO parameter against the reverse DNS lookup result and any aliases.

If there is no match then the host is blocked. Connecting hosts whose IP addresses are listed in the Host Safelist are exempt from blocking by this check.

When **Validate sender address in the DNS** is active, this feature validates the domain part of the sender's address in the Domain Name system. You may exempt addresses from this validation by adding them to the Address Safelist. This validation is not applied to outgoing email when sent from a configured Relay Host.

In the **Security** tab, you can also customize the SMTP greeting that the MIMEsweeper for SMTP gateway issues to a connecting host when a connection is confirmed.

When the **Insert IP Address into Received Header for** is activated, you configure the circumstances under which MIMEsweeper for SMTP inserts into the header of a received email message the, IP address of the connecting host that sent an email message.

Throttling

You can specify if the Receiver service performs a selected level of throttling. This function increases the number of messages being processed, and helps to maintain processing throughput of the MIMEsweeper for SMTP system. The two levels of throttling are as follows:

- If the specified lower limit threshold is exceeded the Receiver service will start to slow down the rate at which new messages are accepted from connecting hosts by imposing delays between commands.
- If the specified upper limit threshold is exceeded because mail continues to build up in the Content Analysis Queues, the Receiver service will start rejecting incoming messages. The connecting SMTP hosts will retry these messages at a later time.

Setting upper and lower limits

The lower limit sets the level of processing allowed before MIMEsweeper for SMTP starts throttling messages through the Receiver service. The default is 200 messages.

The upper limit sets the level of throttling allowed before MIMEsweeper for SMTP stops messages being accepted by the Content Analysis Queues. The default is 500 messages.

Host safelist

The Host Safelist is a user-configured list of hosts in IP address form. MIMEsweeper for SMTP Receiver services exempts these IP addresses from certain blocking mechanisms. The hosts specified in the Host Safelist are:

- Not blocked if the Reverse DNS Look-up fails.
- Not blocked if the SMTP HELO/EHLO name does not match the Reverse DNS Look-up name.
- Excluded from the Mail Database Look-up feature. For more information, see *Mail database lookup* on page 6-15.

- Exempt from blocking by the Anti-spoof feature.

Address Safelist

The Address Safelist feature in the MIMEsweeper for SMTP Receiver service exempts sender addresses from certain blocking mechanisms. The Address Safelist is a user-configured list of safe addresses. The addresses specified in the Address Safelist are:

- Exempt from the **Validate sender address in the DNS** command.
- Exempt from blocking by a Banned Address entry. For more information, see *Banned addresses* on page 6-16.
- Exempt from blocking by the Anti-spoof entry. For more information, see *Anti-relay properties* on page 6-12.

The following are examples of how the Safelists can be used:

Example 1:

- Banned Address list item `*. outside-yourcompany.com`. All addresses in this domain are blocked.
- Address safelist item: `Someuser@ outside-yourcompany.com`. Message delivered.

Example 2:

With **Validate sender address in DNS** activated, messages are blocked where a sender address contains a domain element that is not registered in any DNS lists. This works in most circumstances. However, a new supplier cannot get mail through to you because the domain used for their email, `outside-yourcompany.com`, is not listed in the DNS. The system administrator can add all or just specific addresses to the Address safelist:

- `*. outside-yourcompany.com`.
- `chris.sales@ outside-yourcompany.com`.

Receiver Service Authentication

To increase security against email threats such as spoofing, the Receiver service performs server-to-server, domain-based SMTP authentication at the beginning of a connection. This is an Extended SMTP (ESMTP) capability to verify the identity of a mail server before accepting mail. MIMEsweeper for SMTP authentication uses the LOGIN Simple Authentication and Security Layer (SASL) mechanism for identifying and authenticating connecting servers. Servers are identified by their IP address or host name. System Administrators must manually exchange user-configured user name and password information to establish a server-to-server connection and authenticate when sending email, or authenticate the client when receiving email. Use of this feature, therefore, requires a degree of trust and cooperation between the administrators or participating mail servers.

You configure SMTP authentication in the **Authentication** tab of the **Receiver Properties** page.

This section briefly describes the Receiver service authentication settings. For details about authentication see the MIMEsweeper Policy Editor help.

The primary configuration takes place in the upper half of the authentication page titled **Unspecified hosts**. These settings determine the Receiver service configuration which applies to all connecting hosts, except those listed in **Specified hosts**, in the lower half of the page. Specified hosts effectively refine the behavior of the **Unspecified hosts** settings.

The Receiver service processes messages from unspecified hosts in the following ways:

- **Accept unauthenticated (default)**

  Accepts messages from hosts not listed in **Specified hosts**. MIMEsweeper for SMTP does not advertise its authentication mechanism to connecting hosts in response to their EHLO greeting.

- **Reject**

  Rejects messages sent by any host not listed in **Specified hosts**.

- **Accept if authenticated using default authentication**

  MIMEsweeper for SMTP authenticates any connecting host not listed in **Specified hosts**, using the default authentication, entered in the fields below this option.

  The username and password are arbitrary values chosen by the system administrator. They are not Windows Security user names or passwords. The relevant values must be supplied to the systems administrators of client hosts that want to authenticate with your Receiver service.

You can configure specified hosts to refine the authentication behavior of the unspecified hosts configuration. For example, you can define authentication requirements for a specific host, regardless of the requirements for all other unspecified hosts. The configuration overrides that defined in the unspecified hosts section. For details about specified host configuration, see the MIMEsweeper Policy Editor help.

Advanced

You can change the port number on which MIMEsweeper for SMTP accepts SMTP connections. By default, MIMEsweeper for SMTP listens on port 25 for incoming messages.

You can configure the maximum number of Received headers that will be accepted by MIMEsweeper for SMTP. This feature detects and prevents mail loops. By default messages with over 20 Received headers will be rejected.

You can specify any connection limits on the SMTP port, including the maximum number of email messages that the Receiver service accepts from a single connection to the SMTP port, and the maximum number of messages per connection.

You can specify the maximum number of concurrent connections to the SMTP port that the Receiver service accepts, and the maximum number of recipient addresses allowed in an email message that MIMEsweeper for SMTP processes.

Additionally, you can prevent very large messages from being passed through by specifying the maximum size, in megabytes, of messages that MIMEsweeper for SMTP accepts. Before sending a message, the sending SMTP gateway informs the Receiver service of the message size in bytes. If the message is larger than the specified maximum, the Receiver service rejects the connection before the data is transmitted.

Figure 6-3 shows a Receiver service status report generated during an exchange of data with a sending gateway.

```
220 yourcompany.com MAILsweeper ESMTP Receiver Version
5.3.1.19 Ready
ehlo gateway.somecompany.com
250-yourcompany.com
250-SIZE 1048576
250-ETRN
250-ENHANCEDSTATUSCODES
250-DSN
250-URFY
250-AUTH
250 8BITMIME
mail from: <someuser@somecompany.com> size=2048765
552 5.3.4 message exceeds 1048576 bytes
```

Figure 6-3: Receiver service status report

During this exchange of data, the sending SMTP gateway informs MIMEsweeper for SMTP that the message to be sent is 2048765 bytes.

The byte size of the message increases by 30% when the files are converted from desktop format (8-bit binary) to Internet message format (7-bit ASCII). As this exceeds the maximum message size allowed in this example (1048576 bytes, that is, 1MB), the Receiver service rejects the connection.

You can configure timeout intervals (in seconds) for the time that a single connection to the SMTP port is to remain open, and for the time between the SMTP port sending an SMTP command to the Receiver service and the Receiver service closing the SMTP connection.

In the **Advanced** tab, you also can specify if MIMEsweeper for SMTP is to reformat invalid recipient and sender addresses that contain extra dots.

You can insert a custom product name in the received headers instead of the default entry. This prevents the SMTP technology information that you are using from being relayed outside your company. Typically, the product name and version are written in received headers.

Anti-relay properties

You configure relay security options to prevent other mail hosts from forwarding mail through MIMEsweeper for SMTP.

Relay hosts

Configure the connecting SMTP hosts that are allowed to relay email messages through MIMEsweeper for SMTP to domains other than your own in the **Relay Hosts** tab. This configuration is typically used to protect your local domain from being used as a third-party mail relay.

If a connecting host that is not on this list tries to send an email message to recipients outside of your local domain the email message is rejected. The exception is if the email is destined for a domain listed in the **Relay Target** tab. Domains listed in the **Relay Target** tab are not used until this **Relay Hosts** tab has been configured.

If you do not specify any entries in the **Relay Hosts** list, any SMTP host will be allowed to relay messages through your MIMEsweeper for SMTP system. This could result in your organization being listed in a web-based database of hosts that are known to be sources of large amounts of unsolicited email, such as the Realtime Blackhole List (RBL) maintained by the Mail Abuse Prevention System (www.mail-abuse.org) or the abuse.net Contact Database maintained by the Network Abuse Clearinghouse (www.abuse.net).

A host name can be specified as a Fully Qualified Domain Name, an IP address, or a NetBIOS name. Depending on the format in which you specify host names in this **Relay Hosts** tab, you may need to select specific options in the **Connecting Hosts** area of the **Security** tab. For more information about the Relay Hosts settings, see the MIMEsweeper Policy Editor help.

Relay targets

You can use Relay targets to configure the valid recipient addresses for incoming messages, where incoming messages are those from hosts not listed as approved hosts in the **Relay Hosts** tab.

Used to its fullest, the Relay Targets list will define as valid only those addresses that match your internal mail accounts. This will enable the Receiver Service to block all invalid recipients, significantly reducing the number of undesirable messages entering your system. The behavior of the Receiver service when relay hosts exist or do not exist are specified below:

- When one or more relay hosts exist and no relay targets exist, the Receiver service automatically validates recipient addresses of incoming messages as though the home domain and all synonym domains exist in the Target list with addresses in the forms `*@<home_domain>` and `*@<synonym_domain>`.

- When one or more relay hosts exist and one or more relay targets exist, the Receiver service does not automatically treat home and synonym domain addresses as relay targets.

ⓘ It is very important to note the consequence of the rules above. If you have configured one or more relay target entries, the Relay Targets list must describe every recipient address to which external hosts may relay email, including all appropriate addresses for the home domain and any synonym domains.

It is recommended that you use manual address lists or PCS LDAP address lists to include your home domain and synonym domain addresses. If you do not have address lists containing the appropriate information, add an entry with a Target value of an asterisk (*) that uses Combination validation. This relay target allows you to receive mail addressed to any user at your home and synonym domains. Replacing this entry with more specific address lists will reduce the amount of spurious mail accepted by the Receiver service.

- **Target**

  The addresses to which MIMEsweeper for SMTP will relay email messages from external hosts.

  You can disallow a relay target, or specify an exception to an existing relay target, by adding an exclamation point (!) before the disallowed relay target. The Receiver service checks the list from top to bottom, so you must place an exception above the entry it affects. The order of the list can be rearranged.

- **Validation**

  The address validation mode that the Receiver service uses for the relay target. The validation mode can be one of the following:

  - **Simple**

    Simple validation assumes that all relay target addresses (whether entered directly or in a manual address list or a PCS LDAP address list) are in the form `<user_part>@<domain_part>`. The Receiver service simply attempts to match each incoming recipient address against the relay target list entries.

  - **Combination**

    Combination validation assumes that all relay target addresses are at least in the form `<user_part>` and ignores any domain part of the address. If you select combination validation, you need enter only the user part of an email address, but you can also enter a relay target address in the form `<user_part>@<domain_part>`.

    Combination validation combines the user part of the address with the home domain and any synonym domains to define a number of valid address combinations.

ⓘ **Relay Target** settings are not used until the **Relay Hosts** tab has been configured with at least one entry. For more information about the Relay Target settings, see the MIMEsweeper Policy Editor Help.

⚠ Take care when configuring your relay targets to prevent MIMEsweeper for SMTP from acting as an open SMTP host, that is, one which allows unauthorized users to send email messages. An incorrectly configured relay target could allow anyone to route messages through your site. This could result in your organization being listed in a web-based database of hosts known to be sources of unsolicited email, such as the Realtime Blackhole List (RBL) maintained by the Mail Abuse Prevention System (www.mail-abuse.org) or the abuse.net Contact Database maintained by the Network Abuse Clearinghouse (www.abuse.net).

Banned hosts

In the **Banned Host** tab, you configure the SMTP hosts from which the Receiver service is to reject email messages. This is typically used to block spam from known hosts.

You specify the host machines from which no email messages are accepted. Messages from a specified host machine which are routed through your local domain, are rejected.

⚠ A host name can be specified as a Fully Qualified Domain Name (FQDN), an IP address, or a NetBIOS name. Depending on the format in which you specify host names in the **Banned Hosts** tab, you may need to select specific options in the **Connecting Hosts** area of the **Security** tab.

If a NetBIOS or FQDN is specified, it must match what is returned from the DNS system for a reverse lookup. An IP address is not dependent on reverse lookup.

Host names are only permitted if **Look up connecting SMTP hosts in DNS** is enabled. For details, see *Security* on page 6-7.

Incoming

In the **Incoming** tab, you configure behavior for incoming connections, those from any host that is not on the Relay Hosts list.

You configure the Anti-spoof settings to make the Receiver service block spoofed sender addresses and / or record spoofing activity. An address is considered to be spoofed if it originates from an external host and the domain part matches your home domain or any synonym domain. If you choose to record spoofing activity each submission of a spoofed address create an Event Log entry that states the spoofed address and either the supplying host or its IP address.

You configure Directory Harvesting Detection to counteract attempts to discover the addresses of your internal mailboxes. You can configure a number of invalid recipients and a number of RSET commands issued per SMTP connection that you regard to be symptomatic of directory harvesting. When directory harvesting is detected you can make the Receiver service close the SMTP connection and / or record details of the connecting host and the detection criteria that was triggered.

Advanced

You can specify whether or not the Receiver service blocks recipient addresses that have a blank domain part.

You also can specify whether or not the Receiver service blocks a sender address that has a blank domain part. Blank addresses are not blocked by these options.

You can specify how the Receiver service interprets addresses containing an extra `@` or `!` when comparing the addresses against the Relay Targets list.

Anti-spam properties

You configure Anti-spam options to block messages from matched hosts and reject email messages from banned addresses.

Mail database lookup

You can configure MIMEsweeper Policy Editor to check if the IP address of an external mail host has been recorded in one or more databases of hosts that are known to be sources of large amounts of unsolicited email. Specifying multiple databases provides a higher level of coverage, not least because databases often have different criteria for listing a host.

To block messages based on the domains contained inside the message rather than the originating domain, you configure the SpamLogic scenario's **URL properties**. See *SpamLogic* on page 4-39 for more information.

You can configure the Mail Database lookup to:

- Search multiple sites
- Check connecting hosts and / or IP addresses in received headers
- Block messages from matched hosts
- Accept messages irrespective of the lookup results and annotate them with an X-header
- Fully explain the reason for rejection in the SMTP response
- Cache lookup results
- Record an entry in the Windows Application Log when it rejects a message from a mail host listed in the specified database

Third-party organizations may require a subscription and IP address registration to use their web-based database. Check the website of the relevant organization for details before setting this option.

Mail database lookup exemptions and overrides

Mail database lookups are not carried out on any of the hosts that appear in the following list:

- The Relay Hosts list

- The Banned Hosts list
- The Host Safelist.

If a connecting host fails the Reverse DNS Lookup, but appears in the **Host Safelist**, it is exempt from blocking.

If you want to prevent a specific host from being exposed to this validation, you should add its IP address to the Host Safelist.

Annotate mail from matched hosts

Add custom headers to messages that originate from hosts matched by a Mail Database lookup. This option is only available if the **Reject mail from hosts matched in a Mail Database** option is not activated.

You can specify a custom header property name and value. The value can include the token "`%MAILDATABASE%`" which inserts the website that matched the message's sending host.

If you use the default value for the x-header property name and you filter messages that contain this header property, you may detect messages that have been annotated with the same property name by another company's mail system. To avoid this, enter a value that is unlikely to be chosen by anyone else.

Lookup results cache

Each configured lookup site creates an additional delay in receiving messages. You can configure the Receiver service to maintain a cache of Mail Database lookup results for positive (matched) and negative (not matched) IP addresses to reduce processing time.

The performance benefits gained can vary between systems, depending upon many factors. It is recommended that the results cache is disabled, unless you are certain that Mail Database lookups are causing unacceptable delays in message receipt. If you do enable the results cache, neither positive nor negative effects will be apparent until after the Receiver service is restarted and the cache has built up. You are advised to monitor your system for several hours after enabling it.

The results cache is a run-time cache, therefore when the Receiver service is stopped the cache is lost. The cache is given a default lifetime of four hours and a default entry limit of 5000 entries. These parameters are designed to ensure that the time taken to search the list is optimized.

Banned addresses

Configure details of senders from which MIMEsweeper for SMTP is to reject email messages in the **Banned Address** tab. This configuration is typically used to block junk mail from known sources.

You specify the email addresses of senders from whom no email messages are to be accepted. If an email message is received from a specified address, the email message is rejected.

Content Analysis Queues

Content Analysis Queues (CAQs) enable you to prioritize message processing by sender address. This feature is typically used to enable important mail to be accelerated through the Security service.

To configure CAQs:

- Create folders (CAQs) for the Receiver service to deposit mail into.
- Create a list of sender addresses for each CAQ to determine which one a specific sender's mail is sent to. The Receiver service checks the address lists on all CAQs and places each message on the queue with the best match of sender address.
- Give each CAQ a priority number. A folder's priority is relative to its number - a higher number has a higher priority. The priority number sets the maximum number of messages the Security service will process from that queue before checking for messages on other queues.

Default folders

A default CAQ folder is created during installation. The default is used if a message's sender address does not match any other CAQ address list. The default CAQ cannot be deleted.

All non-default CAQs must have a sender address list containing at least one address, and the address must be in a valid format:

- `someuser@outside-yourcompany.com`
- `*.@outside-yourcompany.com`.

The default CAQ does not normally need a sender address list and one would only be useful where its settings override that of another CAQ, for example:

Low priority message - `*@outside-yourcompany.com`.

Default - `someuser@outside-yourcompany.com`.

For more information, see *Sender addresses* on page 6-18.

Properties

Configure CAQs in the following property pages.

Details

Enter the folder name and priority for that folder in the **Details** tab of the properties page. The folder name is the base folder for holding messages for that particular CAQ. You can view the location of the folder in the **Base folders** tab of the **Server Properties** page. For more information, see *Server properties* on page 6-21.

Sender addresses

Enter the addresses that the Receiver service is to allocate mail to for that particular CAQ in the **Address** tab.

The Receiver service looks in all CAQ address lists for a full address match even if it has already found a partial address match. If you have a CAQ with a wildcard address, such as:
`*@outside-yourcompany.com`
, you can create a further CAQ with a more specific address:
`someuser@outside-yourcompany.com`.

Recommendations

We recommend the following when setting up CAQs:

- Set up your CAQ location and folder names immediately after installation. If possible, leave the folder names unchanged. Changing folder names may require unprocessed mail in old folders to be manually moved to new folders, otherwise they will not be picked up by the Security service.

  Changes to other properties of CAQs do not have this effect.

- If possible, do not configure more than five CAQs.
- Only use the valid address formats

  A special address value of “<>” can be configured to match blank “<>” sender addresses. This enables users to lower the priority of emails with no sender address, for example, non-delivery reports.

Deliver properties

MIMEsweeper for SMTP controls routing information and the behavior of the Delivery service according to the options specified in the **Deliver Properties** page. You configure delivery authentication and the retry schedule for undelivered messages.

Retry schedule

Configure how the Delivery service handles an email message that it has problems trying to deliver in the **Retry Schedule** tab.

You specify the schedule the Delivery service should follow when trying again to deliver an email message that it has previously not been able to deliver. You also define what the Delivery service should do about messages it continues to have problems delivering.

Delivery Service Authentication

This section briefly describes the Delivery service authentication settings. For information about authentication, see the MIMEsweeper Policy Editor help.

The authentication properties of the Delivery service are identical to those described in the Receiver Properties section, see *Receiver Service Authentication* on page 6-9. However important information specific to the Delivery service authentication is included here. Alternatively, you can configure a default username and password that should be used when delivering to unspecified hosts.

You configure how the Delivery service authenticates itself to unspecified hosts. By default the Delivery service attempts to deliver to unspecified hosts without authentication.

You can configure the Delivery service to not deliver to unspecified hosts. It treats the messages as though delivery failed and does not try again, but creates a non-delivery report. For details about the non-delivery action, see Chapter 4.

You specify a list of known hosts that the Delivery service connects to, and the username and password to use for each one.

Use the **Do not deliver to unspecified hosts** option with great caution. If you specify this option, messages are delivered only to specified hosts. To avoid blocking messages that MIMEsweeper for SMTP should deliver, see the MIMEsweeper Policy Editor help, which provides a full list of recommendations.

Aliases

Configure the way MIMEsweeper for SMTP maps one email address, or group of addresses, to another by creating aliases in the **Aliases** folder under the **Delivery** folder.

You use aliases to change the recipient addresses of email messages by mapping an address from one domain name to another name. Aliases are applied by the Delivery service not the Receiver service. For example, your organization may choose to alias its external email address into an address format that is used internally. When an email address that is specified in an alias appears as a recipient in an incoming email message, MIMEsweeper for SMTP delivers the message to the email address specified in the alias.

Synonym domains in aliases

To alias from an address whose domain part is the main domain or a synonym domain, you must only specify the user part of the address. The alias will then match any of the synonyms plus the main domain. To alias from any other address you must specify the domain part of the address as well.

If you include the domain part in the alias, and it is the main domain or a synonym domain, the alias will not work.

Alias properties

This section briefly describes the properties of an alias. For details about alias properties, as well as procedures for working with aliases (for example, creating new aliases, changing the properties of existing aliases, and importing and exporting aliases, see the MIMEsweeper Policy Editor help.

Alias

Specify the source email address to map from and the target email address to map to in the **Alias** tab of the **Alias Properties** page.

Below are some examples of how you can specify addresses in an alias to re-route email messages to a different email address:

- To route incoming email messages for Bob to the mail host on gateway1

Map from	Map to
boris@inside-yourcompany.com	boris@gateway1.inside-yourcompany.com

- To route incoming email messages for Fred to the mail host on gateway2.

Map from	Map to
fred@inside-yourcompany.com	fred@gateway2.inside-yourcompany.com

- To route all incoming email messages to the mail host on gateway

Map from	Map to
*@inside-yourcompany.com	*@gateway.inside-yourcompany.com

- To route all incoming email messages for Mary Edward to Mary Philip

Map from	Map to
mary.edward@inside-yourcompany.com	mary.philip@inside-yourcompany.com

- To route all incoming email messages for a user on a synonym domain or the main domain.

Map from	Map to
Simon	Simon@synonym-yourcompany.com

Alias priority

Aliases are scanned in the order that they appear in the list from top to bottom. You can change the order of the list by selecting an alias in the Details pane and promoting it up the list or demoting it down the list. The first alias email address matched by MIMEsweeper for SMTP is applied.

Servers

The Policy Servers currently configured are contained in the **Servers** folder of the MIMEsweeper Policy Editor. You configure the delivery paths the Delivery service uses (routes) for each server configured. For details about delivery paths, see *Routing* on page 6-24.

A large MIMEsweeper for SMTP deployment can include up to eight enabled Policy Servers. You can configure more than eight Policy Servers if required but a maximum of eight can be enabled at any one time. The **Servers** folder shows all configured Policy Servers in the deployment. To view a newly installed Policy Server, you must close then re-open the MIMEsweeper Policy Editor.

Policy Servers can be enabled or disabled individually by accessing the context menu of the server icon and selecting **Enabled** or **Disabled** as required.

Icon overlays show a server's current status: ✓ Enabled, ☒ Disabled.

Disabling a Policy Server in the MIMEsweeper Policy Editor does not stop the services. However, the Policy Server will not process mail while disabled.

Enabling a server will cause any stopped services to be restarted.

For details on starting, stopping and monitoring services in the Systems Center, see Chapter 8.

Servers folder properties

The Servers folder properties are accessed from the **Servers** folder in the console tree.

Audit Disposer Server

The Audit Server hosts the Audit Disposer service which commits consolidated audit data to the Audit database. To select a server from your deployment to act as the Audit Disposer server, access the properties of the Servers folder in the console tree. Select from the list of active servers that are listed in the **Audit Disposer** tab.

Server properties

Server properties for an individual server are accessed from the **Server** icon in the Details pane.

Editing the properties of a **Server** icon in the Details pane changes the configuration of the selected server only.

To apply configured changes to the content security policy, you must execute a save command using the **Save** toolbar button, and then select the **Yes** option to apply the changes to your Policy Servers.

Logging Properties

Configure what transport logging information SMTP Relay is to generate in the **Logging** tab.

You specify whether to log to the Windows Application Log events performed by the Receiver and Delivery services and errors detected by the Receiver and Delivery services. You can also specify whether to log only basic trace information on SMTP connections, SMTP commands, and recipient information in a MIMEsweeper for SMTP system log file. Alternatively you can specify whether to append to the basic trace information more detailed information on the content of each processed message.

Folders

The **Folders** tab displays the configuration paths for various system folders.

Base folders

The **Base Folders** tab specifies the default location of various Base folders. For instance, the Base folder for all MIMEsweeper message areas.

Base folders are those in which other folders are created. For example when creating a CAQ, the folder name you enter in the **Details** tab of the **Content Analysis Queues Properties** page is created as a sub-folder of the base folder for the CAQs. All CAQs folders are created in this base location.

You can override a Base folder locations in the **Advanced Paths** tab.

Advanced paths

The **Advanced Paths** tab lists any new paths that you have specified. Advanced paths provide two separate functions, these are:

- To override the default locations of configuration items such as message areas.
- To map to the location of third-party executables.

Override default locations

The default paths for base folders are defined in the **Base Folders** tab. Advanced paths are used to change a specific path from its default location. For instance, if a particular message area becomes too large, you may want to move it to another disk separate from the other message areas.

For example, by default message areas are created in:

```
C:\Program Files\Clearswift\MIMEsweeper for SMTP\Mail\MessageAreas
```

Configuring a new message area in the MIMEsweeper Policy Editor, for example ‘Image Messages’, will create:

```
C:\Program Files\Clearswift\MIMEsweeper for SMTP\Mail\MessageAreas\Image Messages
```

You may then want to create an new path to a separate drive for the Image Messages message area. This means that messages added to this message area by your policy are stored in the location you have defined, For example:

```
E:\Messages\Image Messages.
```

To create a new path:

Select **Add** in the **Advanced Paths** tab to open the **Add Advanced Path** dialog box.

The **Advanced Path** drop-down list displays the items for which you can create new paths. Select the required item.

Enter the new location in the **New Path** field and select **Add**. The item and its new path are entered in **Advanced Paths** tab.

> In a multiple machine deployment, the new path only applies to the server whose properties you are editing.

Map to third-party executables

The ability to be able to create multiple servers in a MIMEsweeper for SMTP deployment, means that servers need to be aware of the location of certain configurable items such as:

- Anti-virus tool which are specified in Virus Manager scenarios
- Executable programs which are run in Executable scenarios

You may need to configure an advanced path for these items.

On installation of third-party software, some executables become added to the system path. This is a system environment variable used by Windows. An executable included in the system path does not need to have an advanced path defined for it as the server machines will already be able to locate it.

To find out if an executable is included in the system path:

- From the **Start** menu select **Run**
- Enter the name of the executable in the **Open** field and select **OK**. Do not enter the path.

  If the executable is included in the system path it will be located by the **Run** utility.

If the executable is not included in the system path, you can either:

- Edit the system path to include the executable

  For information about changing environmental variables, see Windows help.

- Create an advanced path

  Installed third-party software is listed in the **Advanced Path** drop-down list in the **Add Advanced Path** dialog. Select the required item from the list and then enter its location in the **New Path** field.

Routing

You configure the delivery paths that the Delivery service uses to direct incoming email messages for your domain received from the Internet, and where it is to direct outgoing email messages for other domains forwarded from an internal SMTP gateway, by creating manual routes in the **Routing** folder under the **Server** folder in the MIMEsweeper Policy Editor.

After installing MIMEsweeper for SMTP, you specify your company name and domain name. This information is used to create your default domain and initial routes and relay host properties. You can also specify the host machine to be used for incoming mail and the host machine to be used for outgoing mail. When you enter these details, MIMEsweeper for SMTP is automatically configured to forward incoming mail and outgoing mail to these machines. You must also configure incoming and outgoing mail routes to enable MIMEsweeper to successfully receive and deliver mail.

Domain and routing configuration is done in the Initial Policy Wizard, which runs the first time you open the MIMEsweeper Policy Editor. For details on using the wizard, see Chapter 6 of the *Getting Started Guide*.

After installation you can use the MIMEsweeper Policy Editor to:

- Change the details you entered in the Initial Policy Wizard.
- Add another domain. Your organization may have more than one domain (you must create a manual route for each additional domain that MIMEsweeper Policy Editor uses to process email messages).
- Configure routes in the **Routing** tab of a route’s Properties page.

Routing properties

This section briefly describes the properties of a route. For details about route properties, as well as procedures for working with routes (for example, creating new routes, changing the properties of existing routes, and importing and exporting routes) see the MIMEsweeper Policy Editor help.

Access the properties of the **Routing** folder in the console tree, or the **Route** icon in the Details pane.

Connection

You can specify the maximum number of connections that the Delivery service will make to any single remote server. Use of such a limit can prevent a remote server from being overwhelmed by excessive connections.

Routing

Specify the name of the domain to which the manual route applies. This is configured in the **Routing** tab of properties page, accessed from the **Route** icon in the Details pane.

You also configure the manual route details, including the host name or IP address of the host machine for the domain, the TCP/IP port to be used for SMTP connections to the specified host machine, and the MX preference level for this host machine on the domain. By default, TCP/IP port

25 is allocated. If you have another SMTP connection assigned to port 25, change this default to an available TCP / IP port. If a domain has multiple hosts, MIMEsweeper for SMTP tries to deliver mail first to the route with the lowest MX preference level.

By default, the Delivery service automatically uses the DNS to direct mail straight to the destination. However, you can create different types of manual routes to override or complement Mail eXchange (MX) records in the DNS:

- Additional
- Default
- Forced

The route type determines how the route is to be used in relation to the route information returned by the DNS server. These route types are explained in the following sections.

You can create one or more of each type of route. If you do, the priority of a route is determined by its position in the list of routes in the **Routing** folder.

When the Delivery service attempts to deliver an email message, it checks the domain element of the recipient's address against the routes in the list, reading from top to bottom. It delivers the mail to the first route with a matching domain.

Additional route

When the DNS returns multiple hosts for the domain, MIMEsweeper Policy Editor merges the route information in the additional route with that returned by the DNS. The Delivery service then delivers the email message to the host with the lowest MX preference value.

Use an additional route to assign a preference value to a particular host, so that you can determine the order in which the Delivery service tries to deliver mail to the host.

For example, Table 6-1 shows that the DNS server has returned the names and MX preference values for two host machines for the `outside-yourcompany.com` domain name.

Table 6-1: Route details returned by DNS

Domain name	Host name	MX Preference
`outside-yourcompany.com`	Host A	5
`outside-yourcompany.com`	Host B	7

You have created an additional route with the details shown in Table 6-2.

Table 6-2: Additional route

Domain name	Host name	MX Preference
`outside-yourcompany.com`	Host C	6

The Delivery service tries to deliver the email message as follows:

1. It tries to deliver the message to Host A, having the lowest MX preference value (5).
2. If it is not able to deliver the message to Host A, the Delivery service then tries to deliver the message to Host C, which has the next lowest MX preference value (6).
3. If it is not able to deliver the message to Host C, the Delivery service then tries to deliver the message to Host B, which has the highest MX preference value (7).

Forced route

When an email message is received from the domain specified in a forced route, the Delivery service always delivers the message using the information in the forced route instead of querying the DNS. The forced route is the common route type for routing email messages through MIMEsweeper for SMTP.

Use a forced route:

- When a DNS server is not available.
- When a DNS server query is inappropriate. For example, for delivering internal mail.
- To send email messages to a specified gateway at your ISP.
- To prevent the loop that occurs when MIMEsweeper for SMTP receives a message for your local domain address, queries the DNS for a host for your domain, and then has its own name returned by the DNS.

You can specify a partially wildcarded domain address in a forced route to have the Delivery service deliver all email messages to a particular host in your domain.

Default route

When an attempt to query the DNS server fails for any reason, the Delivery service delivers the email message using the route information in the default route.

Part II

MIMEsweeper Manager

CHAPTER 7

MIMEsweeper Manager Web Browser Application

This chapter describes how to access the MIMEsweeper Manager and the information available from the various Centers accessed from the Getting Started page.

Overview

MIMEsweeper Manager provides the user interface which allows you to access the areas of MIMEsweeper where you can configure, control and monitor your system.

MIMEsweeper Manager consists of the following areas:

- **Message Center**

  The Message Center provides information for monitoring messages. You can use the Message Center to identify how the system is managing processed messages and how messages are tracked and managed by the content security policy. This enables you to determine if your configuration meets your content security policy requirements and to identify any adjustments you might need to make to ensure that MIMEsweeper is processing messages as expected. From the Message Center you can also access the message tracking database, the Pre-Classified Image Database, and the configuration tools for the Personal Message Manager (PMM).

  The Message Center provides limited information on messages held on any installed MIMEsweeper Edge servers in your deployment. See *MIMEsweeper Edge Servers* on page 1-8 for more information on MIMEsweeper Edge Servers.

- **Systems Center**

  The Systems Center provides support for monitoring MIMEsweeper servers and managing their associated services. It also monitors system performance.

  You can use the System Center to configure MIMEsweeper Edge servers in your deployment, and to access an Edge Server's user interface.

- **Report Center**

  The Report Center allows you to generate and view reports based on audit information collected from your MIMEsweeper system.

  The Report Center contains a list of available views from which you access the reports available for that view. The available reports are categorized in a number of report groups. For details about the types of report available, see Chapter 11.

- **Security Center**

  The Security Center provides facilities to control user's access, define roles assigned to users and control access to the various features of the MIMEsweeper Manager application using permissions.

- **System Health**

  The System Health window gathers data from various parts of the MIMEsweeper for SMTP system to provide an overview of the health of the system. The System Health window displays limited information on the status of configured MIMEsweeper Edger Servers. The System Health window is described in this chapter. See *System Health* on page 7-6.

How to access MIMEsweeper Manager

You access MIMEsweeper Manager by logging on to the application from a web browser. You must supply the name and password of a MIMEsweeper user account that has been assigned permissions to access MIMEsweeper Manager.

MIMEsweeper Manager authenticates the user name and password before providing access to the application containing the Message, Systems, Report and Security Centers. For details on user names and passwords, and for details about assigning access permissions to user accounts, see Chapter 9.

To access MIMEsweeper Manager from a web browser:

1. Enter the URL for the MIMEsweeper Manager application.

   The MIMEsweeper Manager Getting Started page is displayed.

2. Select a center (Message, Systems, Report or Security) from either the site navigation bar, or from within one of the areas on the Getting Started page. The Getting Started page is shown in Figure 7-1.

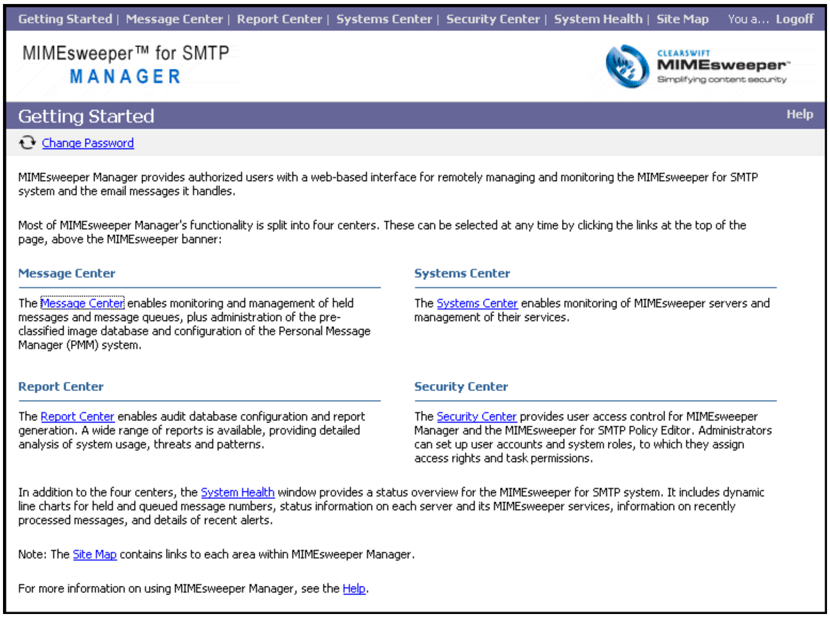
   The MIMEsweeper Manager Logon page is displayed.

3. On the Logon page, enter the username and password for a MIMEsweeper user account that has permissions to access the required MIMEsweeper Manager application.
4. Click **Logon**.

   If the logon is successful the MIMEsweeper Manager Home page for the center you selected is displayed.

Once logged on, users can view only those areas of the MIMEsweeper Manager that they have been assigned access permissions for. For details, see Chapter 9.

MIMEsweeper Manager Getting Started page


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map
You a... Logoff
MIMEsweeper™ for SMTP
MANAGER
CLEARSWIFT
MIMEsweeper™
Simplifying content security
Getting Started
Help
Change Password

MIMEsweeper Manager provides authorized users with a web-based interface for remotely managing and monitoring the MIMEsweeper for SMTP system and the email messages it handles.

Most of MIMEsweeper Manager's functionality is split into four centers. These can be selected at any time by clicking the links at the top of the page, above the MIMEsweeper banner:

Message Center

The Message Center enables monitoring and management of held messages and message queues, plus administration of the pre-classified image database and configuration of the Personal Message Manager (PMM) system.

Report Center

The Report Center enables audit database configuration and report generation. A wide range of reports is available, providing detailed analysis of system usage, threats and patterns.

Systems Center

The Systems Center enables monitoring of MIMEsweeper servers and management of their services.

Security Center

The Security Center provides user access control for MIMEsweeper Manager and the MIMEsweeper for SMTP Policy Editor. Administrators can set up user accounts and system roles, to which they assign access rights and task permissions.

In addition to the four centers, the System Health window provides a status overview for the MIMEsweeper for SMTP system. It includes dynamic line charts for held and queued message numbers, status information on each server and its MIMEsweeper services, information on recently processed messages, and details of recent alerts.

Note: The Site Map contains links to each area within MIMEsweeper Manager.

For more information on using MIMEsweeper Manager, see the Help.

Figure 7-1: MIMEsweeper Manager Getting Started Page

Changing your password

You can change the password of the MIMEsweeper user account you are currently logged in with, provided your account has the required permissions.

To change your password:

1. In MIMEsweeper Manager, access **Getting Started** from the navigation bar on any page to display the Getting Started page.
2. Select **Change Password** on the location bar. The Change Password dialog appears.
3. Enter your current password in the **Old Password** field. User account passwords must use only alphanumeric characters: A-Z, a-z, 0-9.
4. Enter a new password in the **Password** field, and enter it again in the **Confirm Password** field. If your user account does not have password change permissions, the Change Password option does not appear on the location bar.

Accessing the areas within MIMEsweeper Manager

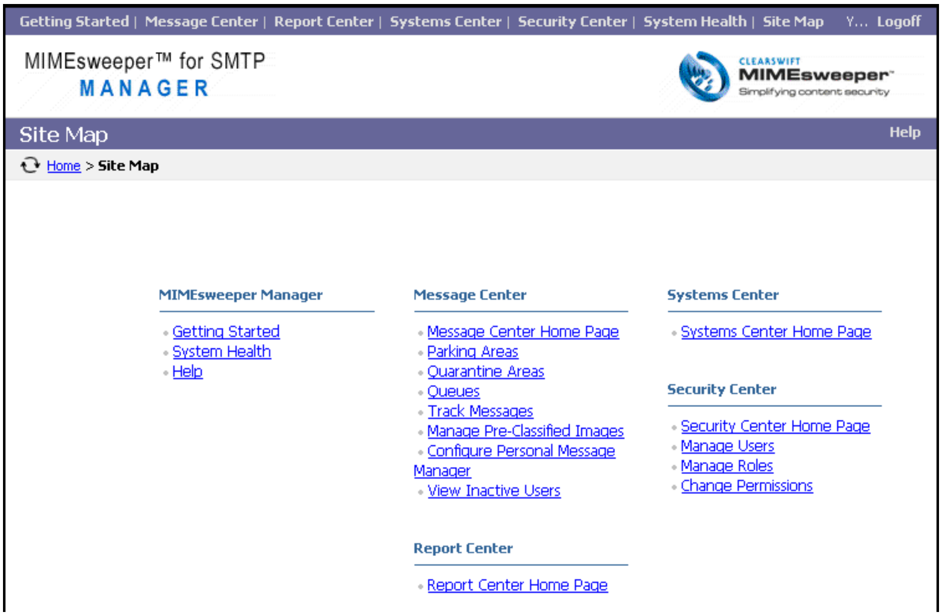
The four centers available within MIMEsweeper Manager are:

- Message Center
- Systems Center
- Report Center
- Security Center

These centers can be selected at any time by clicking on the links on the site navigation bar at the top of the page above the MIMEsweeper banner. They can also be accessed by clicking on the hyperlink in the short description of each center presented on the MIMEsweeper Manager Getting Started page.

Clicking the **System Health** link in the site navigation bar opens the System Health page.

Clicking the **Site Map** link in the site navigation bar opens the site map, allowing access to the areas within the individual centers by using the hyperlinks provided.



Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map Y... Logoff

MIMEsweeper™ for SMTP
MANAGER

CLEARSWIFT MIMEsweeper™ Simplifying content security

Site Map Help

Home > Site Map

MIMEsweeper Manager

- Getting Started
- System Health
- Help

Message Center

- Message Center Home Page
- Parking Areas
- Quarantine Areas
- Queues
- Track Messages
- Manage Pre-Classified Images
- Configure Personal Message Manager
- View Inactive Users

Report Center

- Report Center Home Page

Systems Center

- Systems Center Home Page

Security Center

- Security Center Home Page
- Manage Users
- Manage Roles
- Change Permissions

Figure 7-2: Management Center Site Map

Logging Off from MIMEsweeper Manager

Click **Logoff** in the site navigation bar to log off the current user and return to the MIMEsweeper Manager Logon page.

The **Logoff** button is available from each area in MIMEsweeper Manager.

System Health

The System Health window gathers data from various parts of the MIMEsweeper for SMTP system to provide an overview of the health of the system. Access to the System Health window is provided from the site navigation bar of the MIMEsweeper Manager Getting Started page.

The window is for viewing purposes only and is refreshed every 10 seconds. The following data is provided:

- **Held messages**

  Held messages are messages that MIMEsweeper for SMTP has parked or quarantined, or placed in the problem messages area.

  A graphical display plots a trace for each type of held message. The trace indicates the current volume of held messages.

  Below the plot area the actual number of messages and the disk space occupied by them is displayed. The message numbers provide links to the relevant areas of the message center.

  Icons indicate:

  ✓ System healthy

  ❗ Alert - The **Alerts** pane displays short messages indicating the nature of the alert.

- **Queued messages**

  Queued Messages are those that are awaiting either analysis or delivery by the system. Queued messages are grouped in analysis queues, checked queues or delivery queues.

  A graphical display plots a trace for each type of queued message. The trace indicates the current volume of queued messages.

  Below the plot area the actual number of messages and the disk space occupied by them is displayed. The message numbers provide links to the relevant areas of the message center.

  Icons indicate:

  ✓ System healthy

  ❗ Alert - The **Alerts** pane displays short messages indicating the nature of the alert.

- **Services**

  This pane displays the status of the Receiver, Security and Delivery Services. The data shown applies to the server selected in the drop-down list. The drop-down list provides an option to select all servers.

  - Receiver service
    - **Active connections -** The number of currently active connections in the service. Indicates current service activity.
    - **Messages received -** The number of messages which have been received by the service since it was last restarted.
  - Security service
    - **Checked messages -** The number of messages that the service has checked.
    - **Completed messages -** The number of messages that have been processed by MIMEsweeper for SMTP.
    - **Messages being processed -** The number of messages being processed by MIMEsweeper for SMTP.
  - Deliver service
    - **Active connections -** Outgoing SMTP connections that are currently open.
    - **Messages sent -** The number of messages that have been sent by the service since it was last started.

  The counter values for a specific service are reset to zero every time that service is restarted. If an individual service is restarted, its counter values will be inconsistent with the other services.

- **Servers**

  This pane displays the status of all the active servers in the MIMEsweeper for SMTP deployment in one, two, or three columns. If you add six or more Policy Servers the display is split into two or three columns, as appropriate. If the server information is hidden when the number of Policy Servers is increased, the information can be viewed by moving the mouse pointer over the appropriate icon.

  Services for a specific server are managed on the **Services** page, which is accessed by selecting the server name.

  The icon in the **Status** column indicates the status of a server’s associated services.

  A server’s performance is indicated by graphic displays, which show the percentage of CPU or memory usage. To display a percentage value on a ToolTip, move the mouse pointer over a graphic display.

The alerts area displays significant events regarding the status of the system. These events, if not resolved, may potentially affect the system performance.

⚠ You must monitor your server disk space to ensure that it does not get dangerously low. If you do not you may risk damage to email and operating system data.

- **Edge servers**

  This pane lists any MIMEsweeper Edge Servers that are installed, and whether or not they are active.

- **Recent messages**

  This pane shows summary information for messages recently processed by all the mail servers in your deployment. Messages are sorted by process date and time with the most recent message at the top of the list.

- **Alerts**

  The **Alerts** pane displays system alert messages that are associated with alert icons displayed in other system health panes.

  To clear the **Alerts** pane, select the **clear** command.

CHAPTER 8

Systems Center

This chapter describes the monitoring of MIMEsweeper for SMTP servers and managing their associated services in the Systems Center.

Overview

The Systems Center allows the administrator to monitor the status of the MIMEsweeper services, monitor system performance parameters such as CPU usage, memory and disk space and monitor recent messages.

You also use the Systems Center to add, configure, or remove Edge server or servers installed in your deployment.

Monitoring recent messages provides a means of evaluating recent policy changes. Further systems information is provided by event logs.

The Systems Center is accessed from the Getting Started page of the MIMEsweeper Manager. This is where you can view the servers in your deployment and start or stop their services. However, configuration of servers is done in the MIMEsweeper Policy Editor. Access server properties in the **Servers** folder of the console tree.

The Systems Center consists of the following areas:

- **Systems Center Home page**

  This page displays the status of each active server in the MIMEsweeper for SMTP deployment. Information about each server is provided by graphic indicators that show CPU usage and Memory usage. Free disk space values are also displayed.

  All services are simultaneously started or stopped using the **Start All Services** and **Stop All Services** buttons. These commands only apply to servers that have the check box next to the server name selected.

  For more information, see *The Systems Center Home Page* on page 8-4.

- **Services**

  This page displays the status of each service for a particular server in the MIMEsweeper for SMTP deployment. All services for that server are listed and the status is indicted in a status column.

  You can start or stop one or more selected services.

  For more information, see *Services* on page 8-5.

- **Recent Messages**

  This page displays a summary of the most recently analyzed messages for a particular server in the MIMEsweeper for SMTP deployment.

  Recent message summaries include the subject, size and message classification information, which is useful when monitoring processed messages to evaluate recent policy changes.

  For more information, see *Recent messages* on page 8-7.

- **Logs**

  Event logs allow you to gather information about hardware, software, system problems and security events.

  You can view events for every active server in the MIMEsweeper for SMTP deployment.

  Logs are typically divided into four categories: Application, MIMEsweeper, Security and System.

  For more information, see *Logs* on page 8-8.

How to access the Systems Center

You access the Systems Center in the following ways:

- If you are already logged on to MIMEsweeper Manager

  To display the Systems Center Home Page, select **Systems Center** from the Getting Started page or from the site navigation bar at the top of any MIMEsweeper Manager page.

- If you are not logged on to MIMEsweeper Manager

  When you log on to the MIMEsweeper Manager from a web browser, you must supply the name and password of a MIMEsweeper for SMTP user account that has been assigned permissions to access the MIMEsweeper Manager. The log on credentials are authenticated before access to the MIMEsweeper Manager is provided. For details on user names and passwords, and for details on assigning access permissions to user accounts, see Chapter 4.

To logon and access the Systems Center from the Start menu:

1. From the **Start** menu navigate to **MIMEsweeper for SMTP** in the **Programs** menu and select **MIMEsweeper Manager**.

   The MIMEsweeper Manager Getting Started page is displayed.

2. Click on **Systems Center** or select it from the site navigation bar at the top of the page.

   The MIMEsweeper Manager logon page is displayed.

3. Enter a valid MIMEsweeper for SMTP user name and password and click **Logon**.

   If the logon is successful, the Systems Center Home page is displayed.

To logon and access the Systems Center from a web browser:

1. Enter the URL for the MIMEsweeper Manager.

   ```
   http:/<ServerName>/mswsmtp/
   ```

   Where `<ServerName>` is the name of the server running MIMEsweeper for SMTP.

   The MIMEsweeper Manager Getting Started page is displayed.

2. Click on **Systems Center** or select it from the site navigation bar at the top of the page.

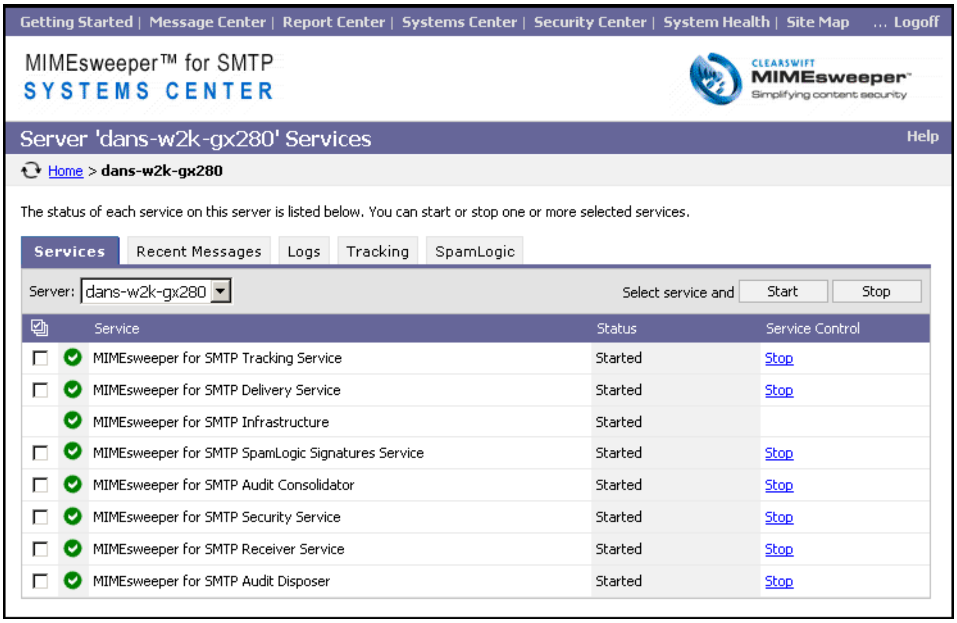
   The MIMEsweeper Manager logon page is displayed.

3. Enter a valid MIMEsweeper for SMTP user name and password and click **Logon**.

   If the logon is successful the Systems Center Home page is displayed.

Once logged on, users can use only those areas of the Systems Center to which they have been assigned access permissions. For further information on access permissions, see Chapter 4.

The Systems Center Home Page


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map ... Logoff
MIMEsweeper™ for SMTP
SYSTEMS CENTER
CLEARSWIFT MIMEsweeper Simplifying content security
Help
Services | Recent Messages | Logs | Tracking | SpamLogic
Start
Stop

Server 'dans-w2k-gx280' Services

Home > dans-w2k-gx280

The status of each service on this server is listed below. You can start or stop one or more selected services.

Server: dans-w2k-gx280 ▼ Select service and Start Stop

		Service	Status	Service Control
□	✓	MIMEsweeper for SMTP Tracking Service	Started	Stop
□	✓	MIMEsweeper for SMTP Delivery Service	Started	Stop
	✓	MIMEsweeper for SMTP Infrastructure	Started	
□	✓	MIMEsweeper for SMTP SpamLogic Signatures Service	Started	Stop
□	✓	MIMEsweeper for SMTP Audit Consolidator	Started	Stop
□	✓	MIMEsweeper for SMTP Security Service	Started	Stop
□	✓	MIMEsweeper for SMTP Receiver Service	Started	Stop
□	✓	MIMEsweeper for SMTP Audit Disposer	Started	Stop

Figure 8-1: Systems Center Home Page

The Systems Center Home Page displays the status of all the active servers in the MIMEsweeper for SMTP deployment, and provides links to further server pages providing more detailed information.

The Systems Center home page includes user interface controls to add, modify and remove MIMEsweeper Edge Servers.

If you have MIMEsweeper Edge Servers installed, this page displays the server name or IP address, and whether or not it is active. You can select the name link to open the Edge Server’s login screen, and log in to configure or manage the Edge Server.

You can select one or more servers by selecting their associated check boxes. Alternatively use the **Select All** button ☑ to select all servers.

The **Start All Services** and **Stop All Services** buttons only affect selected servers. If a server is selected all its services will be started or stopped when the buttons are used.

Services for a specific server are managed on the **Services** page, which is accessed by selecting the server name. For more information, see *Services* on page 8-5.

The icon in the **Status** column and the status message indicate the status of the servers's associated services:

✅ All services are started.

❗ Alert. The status message indicates the status of services. If some of the services have been stopped, they are listed in the status message. A "Not available" messages could indicate a failure in the network or the Infrastructure service for example. The alert icon also indicates whether a deployment update is pending.

Each server's performance is indicated by graphic displays, which show the percentage of CPU and memory usage. To display a ToolTip giving the percentage value, move the mouse pointer over a graphic display.

The server's free disk space values are also displayed in GB.

⚠ You must monitor your server disk space to ensure that it does not get dangerously low. If you do not you may risk damage to email and operating system data.

To display further pages where you can manage services, monitor recent messages and view logs for a specific server, select a server name. These pages are described in the sections that follow.

Services

The **Services** page is accessed by selecting a server name on the Systems Center Home Page. You can monitor the status of each service for a particular server in the MIMEsweeper for SMTP deployment. All the services associated with the selected server are listed individually. The status of each service is indicted in the **Status** column.

You can view further information for the selected server by selecting the **Recent Messages** tab or the **Logs** tab. For more information, see *Recent messages* on page 8-7 and *Logs* on page 8-8.

Managing services

The MIMEsweeper for SMTP services are responsible for processing email messages. You monitor the Delivery, Receiver, Security, Audit and Tracking Services for the server that you have selected from the Systems Center Home Page.

The MIMEsweeper for SMTP administrator can configure which users in your organization have access permissions to monitor and manage the services. For details on service access permissions, see Chapter 5 of the *Getting Started Guide*.

The Infrastructure service is a set of distributed components that manage the various housekeeping tasks essential to the functioning of MIMEsweeper for SMTP. This service cannot be disabled.

When you create or edit policies in the MIMEsweeper Policy Editor, you use the **Save the MIMEsweeper Policy** button in the MIMEsweeper for SMTP toolbar to save draft versions of the policy you are editing, and to apply finished policies to the Policy Servers. When you use the Save button, the Receiver, Delivery and Security services stop and restart automatically. You can see the status of the service change on this page, and view events in the MIMEsweeper log. For details about accessing and viewing logs, see *Logs* on page 8-8.

You can select one or more services by selecting their associated check boxes. The services you select are then controlled using the **Start** and **Stop** buttons.

You can control individual services by selecting their Start or Stop hyperlinks in the **Service Control** column. Controlling services this way is independent of the status of the service's check box. The service status changes regardless of whether it is selected or not.

The **Start** and **Stop** buttons on this page control individual services, or a group of services, for the selected server. The **Start All Services** and **Stop All Services** buttons on the Systems Center Home Page control all services for a selected server or a group of servers.

The icon and the status message in the **Status** column both indicate the status of each service:

✅ Started.

❌ Stopped.

⊗ Disabled.

Services for a Policy Server which has been disabled, cannot be restarted. Policy Servers in the MIMEsweeper for SMTP deployment are enabled and disabled in the MIMEsweeper Policy Editor. Failure of a service to start will be recorded as an error event in the MIMEsweeper log.

From this page you can also select the **Recent Messages, Tracking**, or **Logs** tabs for the current server.

Audit Consolidator and Audit Disposer services

The Audit Consolidator and Audit Disposer services process files for the Audit database, which is used for creating reports. If auditing is switched off in the Report Center, these services will be stopped. For details about the Audit database, see Chapter 11.

Restarting the Audit Disposer service after the database unavailability

If the audit database becomes unavailable to MIMEsweeper, for example because a network connection is lost, the Audit Disposer service may not restart when the database becomes available again. If this occurs you may see the following message:

```
Could not connect to audit database
```

To resume the storage of audit data when the database has become available again, restart the MIMEsweeper Audit Disposer service in the MIMEsweeper Manager. For more information, see *Managing services* on page 8-5.

Tracking Service

The Tracking Service processes message tracking data generated by messages as they pass through the system. The message tracking database maintains this data. Using this data, you can track messages as they pass through the MIMEsweeper system, and create message tracking reports. For more details on the message tracking database, see Chapter 9.

Recent messages

Access the Recent Messages page by selecting the **Recent Messages** tab on the selected server's page.

The **Recent Messages** tab is only available if the selected server is one of your mail processing Policy Servers.

You can monitor the behavior of the MIMEsweeper for SMTP system by viewing the most recently analyzed messages for a specific server during the current session. The **Recent Messages** page shows summary information for each message. Messages are sorted by process time with the most recent message at the top of the list.

The recent messages listed are those processed by the server that is currently being monitored. This is the server selected from the Systems Center Home Page.

The following information is given for each message:

- **From**: The email address of the message sender
- **To**: The email address of the recipient
- **Subject**: The subject line of the message
- **Processed**: The date and time the message was processed by the Security service.
- **Size**: The size of the message in kilobytes
- **Scenario Folder**: The location of the scenario which determined the policy applied to the email message.
- **Classifications**: The classification that has been applied to the message.

For further details about viewing recent messages for servers, see the MIMEsweeper Manager help.

ℹ To view recent messages, the services must be started. For details of starting and stopping services for a server, see *Managing services* on page 8-5.

From this page you can also select the **Services**, **Logs**, and **Tracking** tabs for the current server.

Logs

To access the Logs page select the **Logs** tab on the selected server's page.

Event logs allow you to gather information about hardware, software, system problems and security events for every active server in the MIMEsweeper for SMTP deployment. Events are displayed for the server that is currently being monitored. This is the server selected from the Systems Center Home Page.

You can use the **Server** drop-down list to change the current server in view.

The log categorizes events using the icons shown in Table 8-1:

Table 8-1: Icons

Icon	Event	Description
✖	Error	A significant event, such as a failure of one of the MIMEsweeper for SMTP services or a failed logon attempt, is logged as an error
⚠	Warning	A less significant event that may indicate a possible future problem such as low disk space, is logged as a warning.
ℹ	Information	An event such as the successful start up of a service, is logged as an information event.
🔑	Success Audit	An audited security access attempt that succeeded.
🔒	Failure Audit	An audited security access attempt that failed.

You can select from the logs available from a drop-down list:

- **Application**

  The Application log contains events logged by applications or programs that are running. For example, a database program might record a file error in this log.

- **MIMEsweeper**

  The MIMEsweeper log contains events related to the MIMEsweeper for SMTP. For example the successful start up of the Security service.

- **Security**

  The Security log can record security events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files.

- **System**

  The System log contains events logged by the Windows system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log.

To filter the logged entries select **Only MIMEsweeper entries** from the **Show** drop-down list. This filter applies to all log types.

From this page you can select the **Services** tab or the **Recent Messages** tab for the current server.

Message tracking

From the Policy Editor, you can configure message tracking components, such as the location of the Tracking Server. From MIMEsweeper Manager, you can configure the database, and track messages.

Message tracking components

The Tracking System uses three main components in order to collect and maintain tracking records.

- **Policy servers** collect message tracking data as they process messages, and at regular intervals, submit this data to the Message Tracking Server.
- The **Message Tracking Server** collates this data and sends it to the Tracking Database Server.
- The **Tracking Database Server** buffers the data to temporary storage and at regular intervals of around a minute, ripens the data and makes it available for use with message tracking and reporting functionality.

The MIMEsweeper installation automatically configures the machine that acts as the Message Tracking Server. You can change this machine at a later date. You change the Message Tracking Server from the Policy Editor by configuring the **Servers** properties. In the Policy Editor, right click on the **Servers** option to access the properties page.

The Tracking page

From a server’s page in MIMEsweeper Manager, you can access the Tracking page by selecting the **Tracking** tab on the selected server’s page. The Tracking page displays information on the message tracking system. You use the Tracking page to monitor the message tracking system and in particular the message tracking database operation.

The layout of the tracking page reflects the tracking system architecture:

- The **Submission Statistics** area displays information relating to the selected Policy Server. This area is available when you select a Policy Server.

- The **Disposal Statistics** area displays information relating to the Message Tracking Server. This information is available only when you select the server that is acting as the Message Tracking Server.
- The **Database Statistics** area displays information to the Tracking Database Server. As with Disposal Statistics, this information is available only when you select a server that is acting as the Message Tracking Server.

Submission statistics area

The **Submission Statistics** area provides the following information:

- **Disk space used**: The disk space on the Message Tracking Server occupied by message tracking data
- **Number of successful submissions**: The number of times that data received from the Message Tracking Server has been successfully written to the message tracking database.
- **Last successful submission occurred**: The time that the last successful submission occurred.
- **Number of failed submissions**: The number of times that the write operation has failed.
- **Last submission failure occurred**: The time of the last database write operation

Disposal Statistics area

The **Disposal Statistics** area provides the following information:

- **Number of successful receipts**: The number of times the Message Tracking Server has successfully received tracking data from a Policy Server.
- **Last submission received**: The time of the last successful receipt.
- **Number of failed receipts**: The number of times that receipts from Policy Servers has failed.
- **Last failed receipt occurred**: The time that the last successful receipt occurred.
- **Disk space used**: The amount of disk space on the Tracking Database Server that tracking data occupies.
- **Number of successful disposals**: The number of times that the tracking server has successfully disposed of data to the Tracking Database Server.
- **Last successful disposal occurred**: The time that the last successful disposal occurred.
- **Number of disposal failures**: The number of times that tracking data disposal has failed.
- **Last disposal failure occurred**: The time that the last failure occurred.

Database Statistics area

The **Database Statistics** area provides the following information:

- **Server hosting the database**: The name of the machine hosting the tracking database.
- **Database name**: The tracking database name.
- **Last ripen occurred**: The last time that the data was written from the database buffer to the database.

- **Time taken to ripen**: The time between when the data was written to the buffer and the time that it was written to the database.
- **Last purge occurred**: The last time that the daily task to purge records older than the retention period occurred.
- **Time taken to purge**: The length of time taken to perform the daily purge operation.

For further details about viewing tracking records, see the MIMEsweeper Manager help.

From this page you can also select the **Services**, **Recent Messages** or **Logs** tabs for the current server.

CHAPTER 9

Message Center

This chapter describes how to monitor and manage email messages that have been parked, retained for review, or queued for processing by an SMTP Mail Policy Server in the Message Center under MIMEsweeper Manager. It also describes how to maintain message tracking records in a message tracking database, manage pre-classified images in an image database and configure the Personal Message Manager (PMM) features.

Overview

The Message Center provides support for monitoring and managing messages that have been parked for later delivery, quarantined for review, or are currently queued within the system. These services are accessed from the Message Center Home Page.

The Message Center Home Page contains a summary of the number and size of messages currently in the system. Click on one of the buttons for a message area to view the messages in each area.

The page also provides access to the message tracking database, the Pre-Classified Image Database, and to the management area for Personal Message Manager (PMM).

The Message Center Home Page is divided into five areas: **Held Messages**, **Queued Messages**, **Track Messages**, **Pre-Classified Image Database** and **Personal Message Manager.** If your installation uses a MIMEsweeper Edge Server or servers, two additional areas, **Edge Held Messages**, and **Edge Queued Messages** are added. See *MIMEsweeper Edge Servers* on page 1-8 for more information.

The following buttons are provided:

- **Parking Areas**

  Contain copies of processed email messages that have been blocked and will be delivered later according to the release policy. For details on parking areas, see *Views onto Parking, Quarantine and Problem Message areas* on page 9-9.

- **Quarantine Areas**

  Contain processed email messages that have been prevented from being delivered and are available for review by the administrator or by users using Personal Message Manager. For details on quarantine areas, see *Views onto Parking, Quarantine and Problem Message areas* on page 9-9.

- **Problem Messages**

  Contains messages which the system has encountered problems with while trying to process them and that have caused an internal failure during content analysis. These can include messages that have been deliberately malformed for use in a denial-of-service attack. For details on problem messages, see *Views onto Parking, Quarantine and Problem Message areas* on page 9-9.

- **Queues**

  Contain messages that are waiting to be analyzed or delivered by the MIMEsweeper for SMTP system. For details on queues, see *Views onto message queues* on page 9-17.

- **Track Messages**

  Allows you to search for message records in the message tracking database by defining various criteria to be used in the search. For details on finding messages, see *Configuring Message Tracking* on page 9-20 and *Tracking Messages* on page 9-23.

- **Manage Pre-Classified Images**

  Provides facilities to add and manage images in the image database. For details on managing pre-classified images, see *Manage pre-classified images* on page 9-32.

- **Configure**

  Allows configuration of Personal Message Manager (PMM) settings to enable individual end users to manage their own messages which have been processed by the system and placed in quarantine areas that have PMM enabled.

- **View Inactive Users**

  Provides a list of inactive users of the PMM system. An inactive user is one who has received emails into their PMM area within the last month, but has not deleted or released any of the messages using the PMM system.

Why use the Message Center?

The Message Center Home Page provides information for monitoring messages in the system. You can use the Message Center to identify how the system is managing processed messages and how messages are tracked and managed by the content security policy. This enables you to determine if your configuration meets your content security policy requirements and to identify any adjustments you might need to make to ensure that MIMEsweeper for SMTP is processing messages as expected.

The other areas of the Message Center enable you to track the passage of email messages through MIMEsweeper for SMTP. You can view and manage messages that have been parked or quarantined for review by the system administrator, as well as those that are currently queued for processing.

From the Home page you can access the contents of the following Message Center areas:

- Parking areas
- Quarantine areas
- Problem Messages
- Queues
- Message tracking database
- Pre-classified Image Database
- Personal Message Manager

ℹ To manage messages held on a MIMEsweeper Edge Server, you need to log on to the Edge Server.

Each of the message areas contain a list of default views. A view shows the output of a filter applied to specify which messages are displayed together. You can create custom views to meet your organization's requirements. For details about creating views, see *Add View* on page 9-9. For details about the contents of views for message areas, review areas, and queues, see *Views onto Parking, Quarantine and Problem Message areas* on page 9-9 and *Views onto message queues* on page 9-17. For details about working with views, see the MIMEsweeper Manager help.

User access to the various areas in the Message Center is dependent on the permissions assigned to the individual user. The MIMEsweeper for SMTP Security Center enables you to assign permissions for individual roles and users to specific areas of the Message Center. This provides control over who can access an area and what actions they may perform on messages in that area. For details about setting roles and user permissions see Chapter 5 of the *Getting Started Guide.*

How to access the Message Center

You access the Message Center from MIMEsweeper Manager which accesses message data held on the MIMEsweeper Manager Operational Database on the Primary Configuration Server (PCS).

If you are already logged on to MIMEsweeper Manager

To display the Message Center Home Page, select Message Center from the Getting Started page or from the site navigation bar at the top of any MIMEsweeper Manager page.

If you are not logged on to MIMEsweeper Manager

When a user logs on to MIMEsweeper Manager from a web browser, they must supply the name and password of a MIMEsweeper user account that has been assigned permissions to access the Manager application. The MIMEsweeper application authenticates these log on credentials before providing access to the Manager application containing the Message Center. For details about user names and passwords, and for details about assigning access permissions to user accounts, see Chapter 5 of the *Getting Started Guide.*

To logon and access the Message Center from the Start menu:

1. Click **Start**.
2. Select **Programs**.
3. Select **MIMEsweeper for SMTP**.
4. Click **MIMEsweeper Manager.**

   The MIMEsweeper Manager Getting Started page is displayed.

5. Click on **Message Center** or select it from the site navigation bar at the top of the page

   The MIMEsweeper Manager logon page is displayed.

6. Enter a valid MIMEsweeper user name and password and click **Logon.**

   If the logon is successful the Message Center Home page is displayed.

To logon and access the Message Center from a web browser:

1. Enter the URL for the MIMEsweeper Manager application. (`http:/<ServerName>/mswsmtp/` where `<ServerName>` is replaced with the name of the server running MIMEsweeper web applications.)

   The MIMEsweeper Manager Getting Started page is displayed

2. Click on **Message Center** or select it from the site navigation bar at the top of the page

   The MIMEsweeper Manager logon page is displayed.

3. Enter a valid MIMEsweeper username and password and click **Logon.**

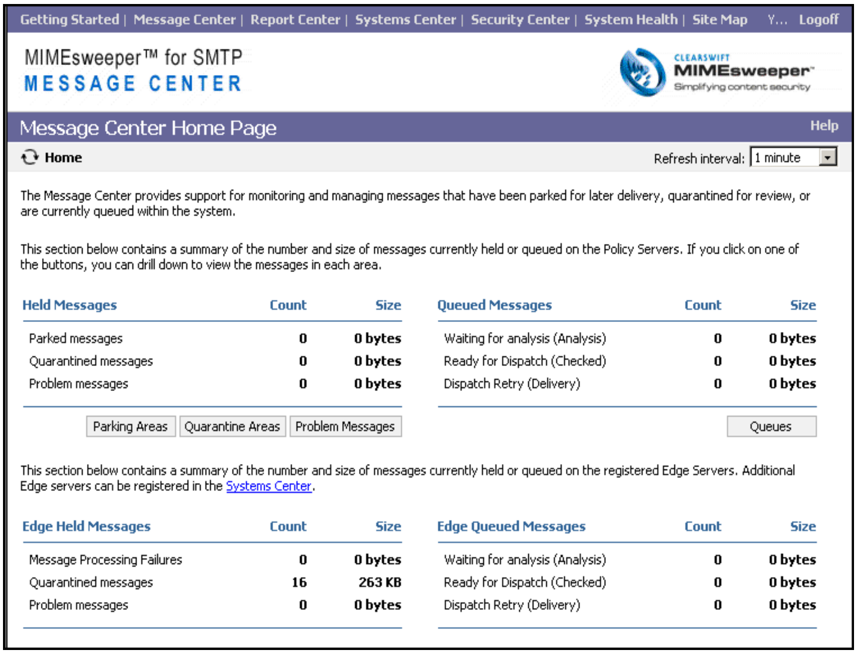
   If the logon is successful the Message Center Home page is displayed.

ⓘ Once logged on, users can only use those areas of the Message Center that they have been assigned access permissions in the Message Center itself. For details, see Chapter 5 of the *Getting Started Guide*.

Message Center Home Page

The Message Center Home Page displays the status of email messages in MIMEsweeper for SMTP and system statistics. It also provides links to other Message Center areas that enable you to monitor and manage email messages that have been parked, quarantined, or queued for processing, together with managing the message tracking database, the image database and the user's Personal Message Manager areas. You can control user access to these Message Center areas, if you have permission to do so, using the Security Center.

For details about controlling user access see Chapter 5 of the *Getting Started Guide*.


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map Y... Logoff
MIMEsweeper™ for SMTP
MESSAGE CENTER
CLEARSWIFT MIMEsweeper Simplifying content security
Message Center Home Page
Help
Home
Refresh interval: 1 minute
Parking Areas
Quarantine Areas
Problem Messages
Queues

The Message Center provides support for monitoring and managing messages that have been parked for later delivery, quarantined for review, or are currently queued within the system.

This section below contains a summary of the number and size of messages currently held or queued on the Policy Servers. If you click on one of the buttons, you can drill down to view the messages in each area.

Held Messages	Count	Size	Queued Messages	Count	Size
Parked messages	0	0 bytes	Waiting for analysis (Analysis)	0	0 bytes
Quarantined messages	0	0 bytes	Ready for Dispatch (Checked)	0	0 bytes
Problem messages	0	0 bytes	Dispatch Retry (Delivery)	0	0 bytes

This section below contains a summary of the number and size of messages currently held or queued on the registered Edge Servers. Additional Edge servers can be registered in the Systems Center.

Edge Held Messages	Count	Size	Edge Queued Messages	Count	Size
Message Processing Failures	0	0 bytes	Waiting for analysis (Analysis)	0	0 bytes
Quarantined messages	16	263 KB	Ready for Dispatch (Checked)	0	0 bytes
Problem messages	0	0 bytes	Dispatch Retry (Delivery)	0	0 bytes

Figure 9-1: Message Center Home Page

The Message Center Home Page provides the following information and user choices:

- **You are logged on as**: Details of the user currently logged on to the MIMEsweeper Manager application. Click **Logoff** to log off the current user and return to the MIMEsweeper Manager logon page. The **Logoff** option is available from each area in MIMEsweeper Manager.
- **Refresh interval:** The frequency with which the displayed status details are updated. This can be chosen from: **Off** (the page is never updated), **30 seconds**, **1 minute**, **2 minutes**, or **5 minutes**.
- **Held Messages:** A summary of the number of email messages and their combined size that are currently held in the system, including counts for each of the following categories:
    - **Parked messages**

  - **Quarantined messages**
  - **Problem Messages**
- **Queued messages:** A summary of the number of email messages and their combined size that have been placed in message queues by the system:
  - **Messages waiting for analysis**
  - **Messages approved for delivery**
  - **Messages ready for despatch**
- **Edge Held Messages:** Appears only if MIMEsweeper Edge Servers are installed. A summary of the number of email messages and their combined size that are currently held on the Edge Server, including counts for each of the following categories:
  - **Message Processing Failures**
  - **Quarantined messages**
  - **Problem messages**
- **Edge Queued messages:** Appears only if MIMEsweeper Edge Servers are installed. A summary of the number of email messages and their combined size that have been placed in message queues on the Edge Server, including counts for each of the following categories:
  - **Messages waiting for analysis**
  - **Messages approved for delivery**
  - **Messages ready for despatch**
- **Message Tracking:** Allows you to configure and enable the message tracking database, and search for messages in the database. This enables you to view a message's history as it passes through the MIMEsweeper system. For more details on the message tracking database, see *Tracking Messages* on page 9-23.
- **Pre-Classified Image Database**: Allows the management of a database of images, pre-classified as being suitable, or unsuitable, for delivery by the MIMEsweeper system. For more information on the pre-classified image database, see *Manage pre-classified images* on page 9-32.
- **Personal Message Manager**: Allows the configuration of Personal Message Manager (PMM) to allow individual users to manage messages addressed to them, which have been processed and retained by the MIMEsweeper system. It also allows viewing of the list of Inactive Users. For more information on PMM, see *Personal Message Manager* on page 10-1.

For details about the content of the Message Center Home Page, see the MIMEsweeper Manager help.

Views onto Parking, Quarantine and Problem Message areas

The message areas in Parking Areas, Quarantine Areas and Problem Messages contain copies of processed email messages to be stored for backup or review according to your organization's email archiving policy.

You can view copies of messages that have been placed in message areas by clicking the **Parking Areas**, **Quarantine Areas** and **Problem Messages** buttons on the Message Center Home page.

In the case of Parking Areas and Quarantine Areas a window is displayed showing a list of views for the chosen area, in the case of Problem Messages you are taken directly to the Problem Messages view.

The screen showing the list of views for Parking Areas and Quarantine Areas provides the following details:

- **Name:** The name of the message area view. Click on the desired message area view to see a list of the messages it contains.
- **Description:** A brief description of the contents of the message area view.
- **Count:** The number of messages in the message area view.

In addition to the default message area views, you can create your own views to specify which messages are displayed together.

Add View

By creating additional views you can:

- Limit the size and scope of the list of messages displayed in a view by customizing its parameters to suit your requirements.
- Control access to the message management and subsystems by assigning permissions to the views created.

Additional views can be created for the Parking and Quarantine Areas and the Queues by clicking on the **Add View** button on the relevant area view page. The New View wizard then takes you through the following steps:

- **Step 1: Server**

  This provides the option of restricting the view to a single server.

  Choose from **All servers** or **This server**. If **This server** is selected you must then choose one of the available servers from the drop-down list which becomes available. Click **Next.**

- **Step 2: Area**

  This provides the option of restricting the view to one or more selected areas.

  Choose from **All areas**, or **These areas**. If **These areas** is selected you must then check the required areas in the list. All available areas can be selected, or deselected, by clicking the ☑ button. Click **Next**.

- **Step 3: Name**

  Enter a name for the new view in the **Name** field.

Clicking **Finish** will complete the wizard and add the new view to the list.

For more details about creating and managing message area views, and the content of the views, see the MIMEsweeper Manager help.

You can refresh a view by right-clicking and selecting **Refresh**.

Contents of message areas

In the Parking, Quarantine, Problem Messages and Queues areas you can view a list of messages contained in a specific message area view by clicking on the name of the desired view.

In the case of the Queues area a table is shown giving the size of the queues for the servers included in the view. Clicking on the message count for a queue will produce a list of messages currently held within that queue.

In the case of Parking, Quarantine or Problem Message areas the contents view shows a list of email messages in the message area view with their details described under the following headings:

- **From:** The email address of the message sender. To view the message in detail click on the address to open the Message Body page. See *View Message* on page 9-14.
- **To:** The email address of the recipient. Multiple recipients are separated by a semi-colon (;).
- **Sent:** The date and time the message was sent.
- **Subject:** The subject line of the message.
- **Size**: The size of the message in KB.
- **Attachment Count**: The number of attachments included with the message.
- **Created Time**: The time that the message entered the message area.
- **Machine Name**: The name of the Policy Server that processed the message.
- **Expires**: The date and time that the message is to be removed from the system.
- **Classifications**: The classifications that have been applied to the message.
- **Recipient Count**: The number of recipients the message was sent to.
- **Envelope ID**: The ID that has been assigned by the downstream relay.

- **Internal ID**: The ID that has been assigned by MIMEsweeper services.
- **Original ID**: The ID of the message before reprocessing or splitting by the MIMEsweeper system.
- **Message URi**: The ID assigned by the Quarantine area.
- **Area Name**: The message area where the message is held.
- **Client Id**: The message ID, if present, in the message header.

Click on the **Configure Columns** button to choose the columns that you want to see in the display.

Click the check box beside the message to select it for manual processing. Click the ☑ button to select or deselect all messages in the view.

The following buttons are available in each view:

- **Filter View**: Opens the Filter View page allowing you to specify the conditions to be met to restrict the messages shown in the view. For more details see *Filter View page* on page 9-34.
- **Batch Operation**: Allows a batch operation to be performed using **Release**, **Forward**, **Reprocess**, **Delete** or **Set Expiry Date** on all messages in the view.
- **Export Messages**: Displays the **Export Messages** window which allows the selection of the columns of information to be exported, and also allows the order that they are presented in to be changed. Clicking **Export** will open the Windows **File Download** dialog box, where clicking **Save** will display the **Save As** browser, allowing you to choose a name and location for the file. The file will be saved in the format of a Microsoft Excel Comma Separated Values (CSV) file with the extension `.csv`.

Do not change the file extension. It must remain as `.csv`

- **Configure Columns:** Allows the selection of the columns to be displayed in the view, and allows the order that they are displayed in to be changed.
- **Release:** (Not available on Problem Messages) Releases the message from the message area and queues it for delivery. A confirmation message is shown asking if you wish to release the message and if it is to be deleted from the view after release. A confirmation message is shown when the Release operation has been completed. Multiple messages can be selected for this operation.
- **Reprocess**: One or more messages can be selected to be reprocessed in one of the following ways:
  - Using the original policy that it has been processed by. This is useful in a situation where the original policy has been changed since the message entered the MIMEsweeper system.
  - Re-evaluating the policy before using it to reprocess the message. This allows the message to be processed as a new message.
  - Reprocess the message using a different policy chosen from the drop-down list. This provides a manual override to allow reprocessing to be achieved using an alternative policy.

  The option is given to delete the message after reprocessing.

- **Forward:** A button to display the Forward Message page in which you can choose to forward selected messages to either the originator, original recipients, or a specified recipient together with an optional message.
- **Non Deliver**: (Not available on Problem Messages) One or more messages can be selected to non-deliver, which simulates a delivery failure. A comment can be added to show the reason for non-delivery. The messages can be removed from the message area following the non-delivery action. A confirmation is shown when the message has been non-delivered.
- **Set Expiry**: (This is not available on Problem Messages) One or more messages may be selected and have their expiry period set, or be set to never expire.
- **Delete**: Manually deletes selected messages from the system. The system requests confirmation that the messages are to be deleted, clicking **OK** will complete the deletion. A confirmation message is shown, confirming that the delete operation has been completed. Should the view contain more messages than can be shown on one page, navigation is provided at the bottom of the page. The current page number is shown together with the total number of pages and messages in the view. A drop down list, accessed by clicking on the down arrow, allows any of the pages of message listings in the current view to be accessed. Navigational arrows are provided at each side of this, allowing the pages to be stepped through individually, or to go instantly to the first or last page of the view.

You can specify the type of email messages that will displayed in a specific message area view by clicking on the **Filter View** button. For details, see *Filter View page* on page 9-12.

You also can examine the properties and content of individual messages contained in the message area. For details, see *View Message* on page 9-14.

For more details about displaying messages in selected message area views, see the MIMEsweeper Manager help.

Filter View page

By filtering a view you can restrict the number of messages displayed by specifying certain parameters. This is useful when working with views which contain a large number of messages.

You can specify the type of email messages displayed in a specific message area view in the Filter View page which is accessed by clicking the **Filter View** button on a message area view page.

All remaining messages are held in the view and can be viewed by clearing the filter.

The fields available in the Filter View page are as follows:

- **Messages:** Filters based on email message header contents:
  - **From:** The email address of the message sender. Separate multiple addresses with a semi-colon (;).

  - **Sent to:** The email address of message recipients. Separate multiple addresses with a semi-colon (;).
  - **Subject contains:** Text to search for in the message subject line.
- **More Choices:** Additional filters based on email message properties:
  - **Sent:** The time period when the email message was sent, one of: **Any**, **Today**, **Yesterday**, **In the last 3 days**, **In the last 7 days**, **Last week**, **This month**, **Last month**, **Week beginning**, **Month beginning**, or **Quarter beginning**.

    If you specify **Week beginning**, **Month beginning**, or **Quarter beginning**, an additional field is displayed to enable you to specify the beginning date.
  - **Size:** An operator and size for the email message, one of: **Any**, **Equals**, **Between**, **Less than or equal to**, or **More than.**

    If you specify an option other than **Any**, additional fields are displayed to enable you to specify the size of the message and the unit of measure.
  - **Attachments:** The number of attachments, one of: **Any**, **None**, **One or more.**
  - **Expiry Time**: The time when the message expires, one of: **Any**, **Never**, or **Within the next.**

    If you specify **Within the next**, an additional table is displayed to enable you to specify the number of days before the message expires.
  - **Classifications**: The classification assigned to the message when it was analyzed.
- **Advanced:** Additional filters based on message processing:
  - **Processed:** The time period the email message was processed, one of: **Any**, **Today**, **Yesterday**, **In the last 3 days**, **In the last 7 days**, **Last week**, **This month**, **Last month**, **Week beginning**, **Month beginning**, or **Quarter beginning**.

    If you specify **Week beginning**, **Month beginning**, or **Quarter beginning**, an additional field is displayed to enable you to specify the beginning date.
  - **Message ID**: The unique string identifying the message. You can view the message ID in the message header. For details, see *View Message* on page 9-14.

The buttons available in the Filter View page are as follows:

- **Apply:** A button to apply the specified filters and re-display the Contents of the message area view with the messages that match the specified filter criteria. A status note indicating that a filter has been applied is displayed in the navigation bar at the top of the Contents of the message area view page.
- **Cancel:** A button to cancel any filters currently specified in the Filter View page and return to the previously displayed message area view.
- **Clear:** A button to remove any previously specified filters and re-display all of the original contents of the message area view.

View Message

You can examine the contents of email messages that are held in a message area in the View Message page for a selected email message. You select an individual message to examine by clicking the hyperlink in the **From** field of a message summary in the Contents page of a message area.

The View Message page is displayed, with the following tabs:

- **Summary Analysis -** See *Summary Analysis* on page 9-16.
- **Body -** See *Body* on page 9-16.
- **Images -** See *Images* on page 9-16.
- **Structure -** See *Structure* on page 9-16.
- **Text Analysis -** See *Text Analysis* on page 9-16.
- **Spam Analysis -** See *Spam Analysis* on page 9-17.
- **Raw Data -** See *Raw Data* on page 9-17.

Each tab displays the following buttons:

- **Release:** Releases the message being viewed from the message area and places it in a delivery queue. A confirmation message is shown asking if the user wishes to release the message and if it is to be deleted from the view after release. A confirmation message is shown when the Release operation has been completed. Multiple messages can be chosen for this operation.
- **Reprocess**: Reprocesses the message in one of the following ways:
  - Using the original policy that it has been processed by. This is useful in a situation where the original policy has been changed since the message entered the MIMEsweeper system.
  - Re-evaluating the policy before using it to reprocess the message. This allows the message to be processed as a new message.
  - Reprocess the message using a different policy chosen from the drop-down list. This provides a manual override to allow reprocessing to be done using an alternative policy.

  The option is given to delete the message after reprocessing.
- **Forward:** A button to display the Forward Message page in which you can choose to forward the message being viewed to either the originator, the original recipients or specified recipients together with an optional message. The option is given to delete the original message after the forwarding operation has been carried out. A confirmation message is displayed when the forward operation has been successfully completed.
- **Non-Deliver**: The message being viewed can be non-delivered, which simulates a delivery failure. A comment can be added to show the reason for non-delivery. The messages can be removed from the message area following the non-delivery action. A confirmation is shown when the message has been non-delivered.
- **Set Expiry**: Allows the expiry period to be set in days, or to be set to never expire.

- **Delete**: Deletes the message being viewed from the system. The system requests confirmation that the message is to be deleted, click **OK** to complete the deletion. A message is shown, confirming that the delete operation has been completed.
- **Export Message**: Saves the file being viewed to disk in zipped format for uses such as training the spam engine or forwarding to technical support. A **Save As** browser window is displayed allowing the save location to be selected. Clicking save in this window will complete the operation.

Do not change the file extension. It must remain as `.zip`.

Below this row of buttons the following fields are shown on each tab page:

- **From:** The email address of the message sender.
- **To:** The email address of message recipients. Multiple recipients are separated by a semi-colon (;).
- **Subject:** The message subject line.
- **Sent:** The date and time when the message was sent.
- **Message ID:** The unique alphanumeric string identifying the message.
- **Expires**: The date and time and time period remaining (in days and hours) when the message expires. Click on **Edit** to change the time specified. A dialog opens in which you can enter a new expiry time, or select **Never expire**.
- **Retained Attachments**: Lists the attachments which are included with this message following processing.

This field is not displayed unless you have configured a strip and retain scenario, such as the Attachment Manager scenario, and are actually viewing the modified message.

- **Stripped Attachments**: Lists the attachments which have been removed from the message while being processed.

This field is not displayed unless you have configured a strip and retain scenario, such as the Attachment Manager scenario, and are actually viewing the modified message.

Three navigation buttons are provided at the bottom of the page:

- **Previous Message:** ◂ Displays the previous message in the same format as you are currently viewing.
- **Next Message:** ▸ Displays the next message in the same format as you are currently viewing.
- **Close**: Closes the message and returns the user to the contents of the message area view page.

View Message Tabs

The tabs on the View Message page display details of the message as follows:

- **Summary Analysis**
  - **Processing Analysis**: Provides a description of the server, time and policy used to process this message. Defines the classification given to the message, and shows where the message was moved to, together with details of the reason the classification was used, and which parts of the message it matched.
  - **Why was the message classified as '**`XYZ`**'**: Describes why the message was classified as specified, and lists the parts of the message that matched the classification.
- **Body**

  The body of the message is displayed, and the following options are available:

  - **Body format**: The drop-down menu gives options of Plain Text, HTML and Rich Text on the drop-down menu, depending on the nature of the message. Plain text is the default method of display.
  - **Export body**: Allows the body of the message to be exported as a `.txt` file.
- **Images**

  Presents the following details for the message, presented as columns:

  - **Name**: The names of the individual images contained in the message.
  - **Type**: The file type of each the image.
  - **Classification**: The classification assigned to each image in the MIMEsweeper Pre-classified Image Database.

ℹ The classification of the image that is shown is the one that was active when the message was processed. This may not be the one which would be applied to that image now, due to updating of the classifications in the system since first processing.

One button is provided on the bar above the image list:

- **Select Image and Classify**: By selecting an image and clicking **Select Image and Classify** you are presented with the Image Classification wizard, which allows you to enter the image in the Pre-classified Image Database. All images in the list can be chosen by clicking the ☑ button at the top of the **Name** column. For more details see *Manage pre-classified images* on page 9-32.

- **Structure**

  The following details for the message are displayed:

  - **Detail:** Select **Full** or **Typical** from the drop-down list.
  - **Responses**: Shows the responses of the MIMEsweeper system while processing the message under the headings **Action**, **Scenario** and **Description.**
  - **Properties**: Represent data found and possibly classified by MIMEsweeper.
- **Text Analysis**

  Shows the breakdown of the parts of a message which has been processed by MIMEsweeper. The parts of the message which triggered classification responses are indicated by an icon.

- **Spam Analysis**

  Shows details of the search expressions which were found in the message.
- **Raw Data**

  Shows the data received from the downstream relay in its native form. In this form the message can be seen to contain information not visible in other types of message display. The form of the message contents are described in RFC2822.

For more details about examining the content of email messages in a message area view, see the MIMEsweeper Manager help.

Views onto message queues

You can view email messages that are queued for processing by MIMEsweeper for SMTP by clicking the **Queues** button on the Message Center Home page.

Queues contain messages that are awaiting either analysis or delivery by the system. The following default queues are available:

- All Queued Messages
- Analysis Queues
- Checked Queues
- Delivery Queues

The Queues view shows the following:

- **Name:** The name of the message queue view. Click on the name of the desired message queue view to see a summary of the size of the queues in that view (for details, see *Queue Summary* on page 9-18).
- **Description:** A brief description of the contents of the message queue view.
- **Count:** The number of messages currently held in the message queue view.

You can refresh the view by right-clicking and selecting **Refresh**.

For more details about the content of the Queues page, see the MIMEsweeper Manager help.

Queue Summary

You can view a summary of the size of the queues for servers included in a specific message queue view in the Queue Summary page. You can access this page by clicking on the name of the desired message queue view in the **Name** column on the Queues page. To see the size of all the queues click **All Queued Messages**.

The contents view for a queue shows the following details, depending on whether a specific queue was chosen, or the **All Queued Messages** option:

- **Server:** A list of servers which are included in this view.
- **Message Delivery:** This column shows the total number of messages along with their size in KB that are waiting in this queue. Click on the figure, which provides a hyperlink to view a summary of the messages currently held within that queue. For details about this summary, see *Contents of a message queue* on page 9-18.

You can customize the number of messages that are displayed on each page of a view by configuring the `ContentsPageSize` parameter in the `ApplicationsSettings` section of the `web.config` file, located on the MIMEsweeper Application server in the Internet Publications directory. By default:

`C:\Inetpub\wwwroot\MIMEsweeper for SMTP\MSWSMTP`.

Contents of a message queue

You can examine a list of email messages that are held in a specific message queue in the Contents page. You can access this page by clicking the message count for a queue on a given server in the Queue Summary page. For details, see *Queue Summary* on page 9-18.

The Contents page displays a list of all messages in the queue, including the following summary details for each message:

- **From:** The email address of the message sender.
- **To:** The email addresses of message recipients.
- **Subject:** The subject line of the email message.
- **Message ID**: The unique alphanumeric string identifying the message.
- **Created:** The date (in `dd/mm/yyyy` format) and time (in `hh:mm:ss` format) that the email message entered the queue.
- **Queued for:** The length of time the message has been in the message queue (for example, `7 minutes, 1 second`).
- **Size:** The size of the message.
- **Status**: Either Normal, indicated by ✓ or Stuck, indicated by ✗.

For more details about examining the content of email messages in a message queue view, see the MIMEsweeper Manager help.

Message Delivery Queue

The Delivery queues table for a specific server is accessed by selecting **Message Delivery Queues** from the **Queues** list, then clicking on the message count for the required server in the **Message Delivery** column. The Domains page opens and shows the following information:

- **Server**: The name of the server where the delivery queue is held.
- **Msg Count**: The number of messages in each delivery queue.
- **Total Size**: The total size of the messages on each server awaiting delivery.

Clicking on the figure in the Msg Count column opens the Domains page which shows the following information:

- **Domain**: The domain that the queued message is in.
- **Count**: The number of messages queued.
- **Size**: The size, in bytes, of the messages in the queue.
- **Status**: A description of the delivery status.
- **Retry Count**: The number of times that the system has retried to deliver the message.
- **Last Retry Attempt**: The time of the last delivery retry.
- **Last Host Tried**: The last downstream mail relay contacted to deliver the item.

The following buttons are available in the Domains page:

- **Retry Delivery**: Clicking this button causes the system to immediately retry the delivery of the message.
- **Non Deliver**: Clicking this button aborts the delivery. No further attempts will be made to deliver the message, and it is removed from the system.

Configuring Message Tracking

You use message tracking to monitor mail that has been processed by the MIMEsweeper system. You can use this database to perform searches and access a detailed history of messages processed by the MIMEsweeper system.

Whereas the auditing and reporting functionality provides a high level view of the traffic that the system processes, message tracking provides a low level view of messages that the system has processed. For example, you can use the auditing and reporting functions to determine traffic profiles and trends, and you can use tracking to find records of individual messages or groups of messages that the system has processed.

You access message tracking from the **Message Center** page.

In the **Message Tracking** area:

- Use the **Configure Tracking** button to set up or change the audit tracking database.You can configure the database details, and the server on which it resides. You use a Microsoft SQL database.
- Use the **Track Messages** button to access message tracking records. You can perform searches of the message tracking database, for example to locate the details of a particular message or group of messages.

Data from the database can also be used to generate tracking summary reports. For more information, see *Report Center* on page 11-1.

Access to this area is dependent on the permissions assigned to the individual user. For details, see Chapter 5 of the *Getting Started Guide.*

Setting up the database

Initially you use the **Configure Message Tracking** wizard to configure the message tracking database. The wizard steps you through the configuration process. After you complete each step, click **Next** to move to the next step:

- **Step 1**: **Enable Tracking**: Gives the choice of selecting **Create new database** or **Use existing database.**
- **Step 2: Database Connection**: Presents the following fields:
  - **Server type**: From the drop-down list, select **SQL Server.**
  - **Server name**: Allows the option of picking a server from the list, or specifying a server to be used.
    - – **Pick server**: Choose the server name from the drop-down list.
    - – **Specify server**: Type the name of the server to use for tracking in the field provided.
  - **Instance name**: An optional field. If more than one instance of SQL Server is installed, specify the instance to be used by entering its name in this field.
  - **Port number**: An optional field. If the database software uses a port number other than the default, specify it here. The default port number is **1433**.

  - **Administrator** and **Password**: Enter valid database administrator access details.
- **Step 3: Database details**: If creating a new database for tracking, enter the database name in the **Specify database** field and the location in the **Database location** field provided. The database will be created in the location that you specify on the SQL Server.

  If using an existing database, you can select **Pick database** and then choose the relevant database from the drop-down list.

- **Step 4: Data Retention Period**: Enter a time interval in days. This sets the number of days after which data is automatically discarded. A system housekeeping task runs daily to delete records that are older than the data retention period.
- **Step 5: Tracking Log Rollover Period**: Enter the log rollover time in minutes. This sets the interval for message tracking details buffered by Policy Servers to be written to the database. The lower this figure the more frequently the data is updated by the system. The maximum time that can be entered here is 60 minutes.

The time interval that you use depends on how much traffic your system processes. Long periods between roll overs may cause high loadings on the system while the log is being processed. Shorter time periods result in a better distribution of this load.

- **Step 6: Tracking Summary**: Displays a summary of the settings you have chosen. Check the details and use the **Back** button if you need to make any changes.

  Click **Next** to apply the configuration. The `Message tracking was configured successfully` message appears. Click **Finish** to return to the **Message Center Home Page**.

When you create a new tracking database, using SQL Server, the MIMEsweeper system creates a database account and password for its own use. The account name is:

```
ul_<databasename>
```

where `<databasename>` is the name you specified for the audit database.

Do not delete this account from within the database software, or change its password. If you do, MIMEsweeper is unable to record information in the database. In this event, you will need to either remove and reinstall the database, or create a new database and manually migrate the data from the old database.

Changing configurations

To change any settings, click the **Configure Tracking** button. After the initial configuration, this button accesses the Configure Tracking page. You use this page to change the settings for the current message tracking database.

To configure a new database, from the Configure Tracking page, click on the link for the **tracking wizard** to re-run the Configure Message Tracking Wizard.

- **Tracking Status**

  This area displays whether or not tracking is enabled. If tracking is enabled, the name of the database and the server are displayed. Click **Disable** to disable tracking**.** This presents a confirmation message that tracking has been disabled successfully. To re-enable tracking choose **Enable**.

  Click **Disconnect database** to remove the database from the system. This functionality is currently not available.

- **Tracking Options**

  Retention period in days. Enter the number of days to retain tracking data in the field provided. The default is 30 days.

  Log rollover interval in minutes. Enter the log rollover time in minutes. This sets the interval for message tracking details buffered by Policy Servers to be written to the database. The lower this figure the more frequently the data is updated by the system. The maximum time that can be entered here is 60 minutes.

  The time at which the tracking purge task will start per day. Use the combo box to configure when the purge process starts each day. You can use this to set that the purge process does not conflict with other scheduled system maintenance tasks.

  Click **Save** to set the changes you make.

- **Purge Tracking Database**

  This option deletes records older than the time that you specify. You would use this option to delete records regardless of the retention rollover period. Specify the **Retention period in days** in the field provided, and click **Purge** to delete all data older than the specified number of days. The default is 30 days.

Tracking Messages

In the Message Center Home page, click the **Track Messages** button to display the **Track Messages** page.

Access to this area is dependent on the permissions assigned to the individual user. For details, see Chapter 5 of the *Getting Started Guide*.

The Track Message page consists of a **Find** area in which you create a search, and a **Results** area where the records found by the search are displayed.

Defining search conditions

Search conditions control the tracking data that a search returns. You define a search condition by setting the condition's **message property**, **operator** and **value**:

- **Message property** defines the message property to search on, for example the message subject or the date received.
- **Operator** defines the how the search compares the message property with the value. For example for **subject**, the available operators include **starts with**, **ends with** and **contains**. For **Time received**, the available operators include **on or after**, and **before**.
- **Value** defines the value of the message property to use in the search, for example the subject name or date received.

You can configure multiple search conditions. For example, you can search for messages with a specific subject received after a specific date. You use the **+** and **–** buttons next to each condition to add and delete search conditions. The search finds messages that meet all the conditions that you specify. That is, the search conditions are combined using the **AND** logical operator.

Click on the ▲ and ▼ buttons on the **Find title** bar to hide or show respectively the search criteria.

Specifying message properties

The message properties that you can search on depend on the MIMEsweeper for SMTP license type. For a standard license user, the following message properties are available:

- **From**: The email address of the sender.
- **Sent To**: The email address of the recipient.
- **Subject**: Text to search for in the subject line.
- **Time Received**: The date and time that the message entered the MIMEsweeper system. Select the month and day from the calendar, and enter the time in 24 hour clock format.
- **Status**: The last known status of the message, for example **Delivered**, **Rejected**, and **Queued for Quarantining**. See *Message Status values* on page 9-31 for a list of possible statuses and their meanings.
- **User Action**: The action taken on the message by an administrator or a user, one of **Release**, **View**, **Delete**, **Forward**, **Reprocess**, **Non-deliver**, **Set Expiry**, **Export**, or **Delete Personal Message**.
- **Attachment Name**: The name of the attachment included in the message.
- **Message ID**: The unique string identifying the message before reprocessing or splitting by the MIMEsweeper system. You can view the message ID in the message header.
- **User**: The name of the user who performed an action on the message.
- **Submitted By (Host)**: The host server that submitted the message.
- **Submitted By (IP)**: The IP address of the host server that submitted the message.
- **Relayed To (Host)**: The host server to which the message was relayed.
- **Relayed To (IP)**: The IP address of the host server to which the message was relayed.
- **Message Area**: The name of the message area in which the message was placed.
- **Message size:** The size of the message, including any attachments, in Kb.
- **Event**: The event that has been applied to the message. See *Event names* on page 9-29 for details.

For an Advanced or Enterprise license user, the following additional message properties are available:

- **Policy server**: The Policy Server that handled the message
- **Policy/Scenario**: The scenario folder that processed the message.
- **Classification**: The classifications that have been applied to the message.
- **Content Analysis Queue**: The content analysis queue to which the message was allocated.

Specifying search operators and values

The search operators and values that you can use vary depending on the type of message property. There are four possible value types:

- String values
- System parameter values
- Time values
- Numerical values

String values

For message properties that can be represented as a text string, for example a subject or an attachment name, you enter a text string value. Note that searches are **not** case sensitive. The following search operators are available with string values:

- **starts with**—finds messages with properties **starting** with the string you specify
- **ends with**—finds messages with properties **ending** with the string you specify
- **contains**—finds messages with properties **that contain** the string you specify
- **doesn't contain**—finds messages with properties **that do not contain** the string you specify
- **is (exactly)**—finds messages with properties that **match exactly** the string you specify
- **isn't**—finds messages with properties that do not equal the string you specify

The following message properties use string values:

- **From**
- **Sent to**
- **Subject**
- **Attachment Name**
- **Message ID**
- **User**
- **Submitted by (Host)**
- **Submitted by (IP)**
- **Relayed to (Host)**
- **Relayed to (IP)**

System parameter values

For message properties with a discrete number of system-configured parameters, for example a policy scenario or an action, you select the value from a pull-down list of available parameters.

The following search operators are available with system parameter values:

- **is**—finds messages with the system parameter that you select
- **isn't**—finds messages that do not have the system parameter that you select.

The following message properties use system parameter values:

- **Status**
- **Action**
- **Server**
- **Policy/Scenario**
- **Classification**
- **Message area**
- **Content Analysis Queue**
- **Event**

Time values

For time values, the following search operators are available:

- **On or after**—finds messages received on or after the time specified
- **Before**—finds messages received before the time specified
- The **Time received** message property is the only one that uses a time value

Numerical values

For numerical values, the following search operators are available:

- **At least**—finds messages with size values equal or larger than the number specified
- **Less than**—finds messages with size values less than the number specified

The **Message Size (KB)** property is the only message property that uses a numerical value.

Saving and re-using searches

You can use the **Save Search** button to save a search definition and use it at a later date. When you save a search, it becomes available from the **Saved Searches** pull down list. You can use the **Manage Searches** button to access a list of saved searches. From this list, you can rename or delete saved searches.

Running a search

Once you have defined the search conditions, click the **Find Now** button. Matching message tracking details are displayed in the area at the bottom of the page. Use the navigation area at the bottom of each page to access results of more than a page. The navigation area provides arrows to navigate through the pages, and displays a total showing how many messages and pages are in the list.

In the results area, next to each message tracking record, the following icons display the current status of each message:

- ✓ The message has been delivered to all recipients
- ✗ The message has been deleted

- ⚙ The message is currently being processed
- ⚠ User action is required, for example the message has been quarantined for one or more recipients

In addition to the status icons, by default, the following columns display information on each message:

- **From**: The message sender's email address.
- **Subject**: The message's subject line.
- **Time Received**: The date and time that the message entered the MIMEsweeper system.
- **Sent To**: The message recipients' addresses. Multiple recipients are separated by a semi-colon (;).
- **Last known status**: The status of the message at the last data rollover, for example whether it has been delivered or quarantined. For a complete list of available statuses, see *Message Status values* on page 9-31.
- Message ID: The identifier that MIMEsweeper has assigned to the message.

You can view the current status of the message for each recipient by clicking on ⊞ to the left of the status icon. The drop-down list shows the following details:

- **Sent To**: The email address or addresses of the message recipients.
- **Status**: The current status of the message as it is processed through the MIMEsweeper system. See *Message Status values* on page 9-31 for details.

Customizing the display

You can use the **Configure Columns** button to choose the columns to display, and the order in which they are displayed. The **Configure Columns** dialog box allows you to add and remove columns, and to set the order in which columns are displayed.

You can sort messages according to particular results columns. The columns available for sorting are:

- **From**
- **Subject**
- **Time Received**
- **Size**

The column on which messages are currently sorted is shown with either an upwards arrow (^) to indicate that the lowest number or oldest message is at the top of the list, or a downwards arrow (v) to indicate that the highest number or newest message is at the top of the list.

To change the sort order, click the column name at the top of the column on which you want to sort. The upwards arrow (^) is shown to indicate that results are sorted based on the column, in the default order of lowest to highest. Once the arrow appears, click the column name again to reverse the sort order.

For more details about the content of the Track Messages page, see the MIMEsweeper Manager help.

Viewing a message’s history

You can view a message’s history in detail by clicking the message’s **From** hyperlink in the results view. The Message History page appears.

The Message History page is available only if you are using the Advanced license.

The Message History page is divided into two panes:

- The left-hand pane displays the event history options that you can select.
- The right-hand pane displays detailed information on the currently selected event history option.

That is, in the left hand pane, you select an event history option to display detailed information in the right hand pane. The three available event history options are:

- **Received**
- **Analyzed**
- **Delivered**

Select the **Received** option to display information on the message as it was accepted by the system. The following information is displayed:

- The message **Size**, in bytes
- The **Client ID**, or the ID supplied by the client from which the message was sent, for example Microsoft® Outlook
- **Server**, or the Policy Server that processed the message
- **Upstream host name**, or the host from which the message arrived
- **Upstream host IP address**, or the host from which the message arrived
- **Message ID**, or the MIMEsweeper for SMTP message identifier
- The message **Sender**
- The message **Recipients**
- The message **Subject**
- The **Content Analysis Queue name** to which the message was allocated

Select the **Analyzed** option to display the following details:

- **Classification names**, or the classifications that have processed the message
- **Server**, or the Policy Server that processed the message
- **Policy name**, or the policy folder under which the message was processed
- **Processing duration** in milliseconds

Select the **Delivered** option to display the current status of the message, for example the delivery date and time details for each recipient.

You use the **View:** pull-down list to select the amount of delivery information that is displayed. The **Detailed** option displays additional routing split information for each message recipient, for example the queues to which the message has been assigned.

Exporting search results

You can export search results so that you can use them with other applications, for example Microsoft Excel®. From the **Track Messages** page, click the **Export Results:** button to displays the **Export Messages** window. You use this window to select the columns to be exported, and the order in which they are presented. When you have configured the columns, click **Export** to open the Windows **File Download** dialog box. The file is saved as a Microsoft Excel Comma Separated Values (CSV) file with the extension `.csv`. You can export up to 50,000 messages. That is, if the list contains more than 50,000 messages, the first 50,000 only are exported.

For more details on the contents of the Message History page, see the MIMEsweeper Manager help.

Event names

The following table lists the possible events that you can search on, and the meaning for each event.

Event	Meaning
Analyzed	The Security service has analyzed the message.
Approved for Delivery	The Security service has processed the message and approved delivery.
Approved for Relay	The message has been approved for relaying via the route defined in the security policy.
Copied to Archive Account	The system sent a copy of the message to the archiving mail account as a Bcc user.
Copied to Archive folder	A copy of the message was saved to disc, with an .idx file.
Copy Forwarded	A copy of the message was forwarded to an individual as specified in the content security policy.
Copy Saved	A copy of the message was saved to disc.
Deleted	The Security service has deleted the message.
Deleted from Message Area	The message has been deleted from a message area by a user or the system.
Deleted from PMM	The message has been deleted by a PMM user.
Delivered	The Delivery service successfully delivered the message.
Delivery Attempted	The Delivery service has attempted to deliver the message but there was a temporary failure - delivery of the message will be retried.

Event	Meaning
Delivery Status Notification generated	A Delivery Status Notification generated message has been generated.
Exported	The message has been exported from a message holding area.
Forwarded	The message has been forwarded to another set of recipients.
Held as Problem Message	The PCS has added the message to the system view of Problem Messages area.
Non Delivered	The message has been failed by the administrator.
Non-Delivery Report Sent	The system generated a non-delivery report as specified in the content security policy.
Notification Sent	The system generated an Inform message as specified in the content security policy.
Parked	The PCS has added the message to the system view of the Parked Messages area.
Quarantined	The PCS has added the message to the system view of the Quarantined Messages area.
Queued as a Problem Message	The Security service has added a message to the pending queue for the Problem Messages area.
Queued for Double Processing	The message is to be processed by two sets of scenarios.
Queued for Parking	The Security service has added a message to the pending queue for a Parking area.
Queued for Quarantine	The Security service has added a message to the pending queue for a Quarantine area.
Queued for Reprocessing	The message is to be re-processed by the security policy.
Queued for Routing	The Delivery service has accepted the message for each recipient.
Received	Receiver Server has accepted the message for delivery.
Rejected	The message was rejected by the mail server
Released	The Security service has released the message for delivery.
Released for Double Processing	A message was released but was queued for further analysis.
Reply Sent	The system generated an automated reply message as specified in the content security policy.
Set to Expire	The message has been set to expire in a message holding area.

Event	Meaning
Split for Analysis	The system has split the message in order to apply content security policy. Each fragmented message shares the same message ID as the original message.
Unable to deliver	The system could not deliver the message, for example it was rejected by the relay, or MIMEsweeper was unable to contact the host.
Viewed	The message has been viewed by a user.

Message Status values

The following table lists the possible message status values and the meaning for each one:

Status	Meaning
Approved for Delivery	The Security service has processed the message and approved delivery.
Deleted	The Security service has deleted the message.
Held as Problem	The PCS has added the message to the system view of Problem Messages area.
Parked	The PCS has added the message to the system view of the Parked Messages area.
Quarantined	The PCS has added the message to the system view of the Quarantined Messages area.
Queued as Problem	The Security service has added a message to the pending queue for the Problem Messages area.
Queued for Analysis	The message has been received, and has been placed in a queue awaiting analysis.
Queued for Paring	The Security service has added a message to the pending queue for a Parking area.
Queued for Quarantining	The Security service has added a message to the pending queue for a Quarantine area.
Queued for Routing	The Delivery service has accepted the message for each recipient.
Rejected	.The message was rejected by the mail system.

Manage pre-classified images

Pre-classified images are stored in the image database.

You can view the images that have been placed in the database by clicking the **Manage Pre-Classified Images** button on the Message Center Home Page.

The database view displays a list of all the images in the database, and displays a thumbnail of each image. Each page includes the following options:

- **Purge all images**: Click to delete all images in the database. A confirmation message is shown. You should use this option with caution.
- **Add**: Allows images to be imported from a disk using a wizard.
- **Filter View**: Restrict the images shown in the view by specifying **Filename**, **Description**, **Classification** and **Expiry Time**. All other images will still be in the database, and can be viewed by clearing the filter.
- **Select/Unselect all images**: ☑ Allows the selection of all images in the database to enable an action to be carried out on them all simultaneously.
- **Delete:** Deletes the selected image.
- **Classify:** Displays the Classify Image(s) page in which you can select the classification for the selected image.
- **Set Expiry:** Displays the Set Image Expiry page where you specify when the selected image is to be removed from the database.
- **Previous:** A hyperlink to display the previous page of images in the database.
- **Next:** A hyperlink to display the next page of images in the database.

For more details about the content of the Manage Pre-Classified Images page, see the MIMEsweeper Manager help.

Contents of an image

You can view the contents of an image that is held in the database in the View Image page. You can access this page by clicking the image in the Manage Pre-Classified Images page.

The View Image page displays the image selected including the following summary details:

- **Filename:** Name of the image.
- **Thumbnail**: A thumbnail of the image.
- **Classification:** The type of image classification, chosen from a drop-down list.
- **Expiry Time**: The time when the image expires, one of: **Never**, or **Delete after** x **days**.
- **Description:** A description of the image.
- **Save:** A button to save any changes made to the image and re-display the Manage Pre-Classified Images page, where a note indicating that the image details are successfully updated, is displayed.
- **Cancel:** A button to cancel any changes made to the image in the View Image page and return to the Manage Pre-Classified Images page.

Adding Images

You add images to the image database in the **Import Images From Disk** page. You can access this page by clicking **Add** in the Manage Pre-Classified Images page.

This starts the **Import Images From Disk Wizard**, in which you can add a new image to the database. For details about using the wizard and on adding and managing images, see the MIMEsweeper Manager help.

If you try to import images from a zip file, the file size is limited to 4 MB.

The limitation is due to the **MaxRequestLength** attribute which is a default set by Microsoft in the machine configuration file, and indicates the maximum file upload size supported by ASP.NET. The specified limit can be used to prevent denial of service attacks caused by users posting large files to the server. The size specified is in kilobytes. The default is 4069 KB (4 MB).

Filter View page

You can customize the display of images in the Image Filter View page by clicking the **Filter View** button on the Manage Pre-Classified Images page.

The Filter View page shows the filter conditions that can be applied:

- **Filename:** Filters based on email message header contents.
- **Description:** Additional filters based on email message properties.
- **Classification:** The type of image classification, one of: **Any**, or **Select classification.**

  If you specify **Select classification**, an additional drop-down list is displayed to enable you to select a suitable classification for this image.

- **Expiry Time**: The time when the message expires, one of: **Any**, **Never**, or **Within the next**.

  If you specify **Within the next**, an additional field is displayed to enable you to specify the number of days until the image expires.

- **Apply:** A button to apply the specified filters and display the Manage Pre-Classified Images > (Filter Applied) page with the images that match the specified filter criteria. The status note **(Filter Applied)** is displayed in the navigation bar at the top of the page to indicate that a filter is applied to the view shown.
- **Cancel:** A button to cancel any filters currently specified in the Image Filter View page and return to the previously displayed Manage Pre-Classified Images page.
- **Clear:** A button to remove any previously specified filters and re-display all of the original contents of the Manage Pre-Classified Images page.

CHAPTER 10

Personal Message Manager

This section briefly describes how the Administrator can configure the Personal Message Manager (PMM) component of MIMEsweeper for SMTP globally. It also describes how end users can configure and use PMM to manage their own withheld messages.

Overview

This chapter describes how to use the MIMEsweeper for SMTP PMM functionality.

PMM removes some of the administrative demand caused by spam messages by allowing end users to manage their own withheld messages. PMM does this by:

- Notifying end users that some messages sent to them have been identified as a potential threat, and withheld.
- Providing the end user with a link to access their withheld messages.
- Enabling the end user to either release withheld messages to their Inbox, or delete them.
- In an Integrated Windows Authentication, enabling delegated users to manage spam messages sent to an organization’s group or public folders, for example a general enquiries address.

The first time that a message is sent to a user’s PMM area, a PMM account is automatically created for the message address. A digest email is generated and sent to the address, containing a link to the user’s PMM area. Unless you use Integrated Windows Authentication, the notification message includes a password to access the account. See *Authentication Settings* on page 10-6 for more information.

Users may also create their own PMM account before any qualifying messages are processed by the system.

Users who do not access their PMM account within a predetermined period are classified as inactive users.

Multiple quarantine areas can be PMM-enabled. This allows you to select messages that users can review and delete. See *Enabling message areas for access by PMM* on page 10-8 for details. End users who access PMM see only one area containing their withheld messages, no matter how many message areas are PMM-enabled.

Message tracking

With the Advanced and the Enterprise MIMEsweeper for SMTP licenses, PMM also provides users with message tracking functionality, to track messages that either they have sent, or have been sent to them. For example, a user can:

- Determine if a message that they sent has been blocked, or when it left the system
- Determine if the system has blocked a message that they expected to receive

Configuring Personal Message Manager

You access the Configure Personal Message Manager page from the Message Center home page. The Personal Message Manager at the bottom right of the page has two buttons:

- You use the **Configure PMM** button to configure the PMM system settings
- You use the **View Inactive Users** button to manage PMM users and their spam messages

The page shows the following links and editable fields:

Managing messages in public folders

In a system that uses Windows Integrated PMM, you can configure your PMM system so that delegated users can manage messages in your organization's public folders. Public folders typically do not have a dedicated user account, and are used for mail such as general enquiries.

> This functionality is applicable only where you use Windows Integrated PMM. It is not an issue when using manual authentication, since users can access public folders using their PMM password.

To configure a delegated user:

- On your mail server use Exchange System Manager to grant the user delegate permissions on the public folder to be managed.
- The next time the user accesses his or her Personal Message Manager **Options** screen, **Additional Mailboxes** appears in the **Options** area. Delegated users can then configure the public folders to which they have delegate permissions.

  See the MIMEsweeper Manager online help for more information.

Configuring the system settings

When you click the Configure PMM button, you access the Configure Personal Message Manager page. This page has three tabs:

- Global Settings
- Per Domain Settings
- Authentication Settings

Global Settings

The Global Settings tab contains the following:

- **Mail Server**

  Notification emails will be sent using the server and originator details defined here:

  - **Server**: The name of the server you wish to use to send the notification emails.

- **Port**: The port number to be used. This is normally port 25.

PMM notification messages are sent by the web Server and by the Primary Configuration Server (PCS). Ensure that the mail server has been configured to accept mail from these machines, otherwise no PMM notification messages will be sent.

- **Digest Settings**

  Here you define the parameters of the digest email:

  - **Emails per digest**: The maximum number of emails that will be included in each digest message sent to the individual user.
  - **Start time**: The time, in the 24 hour clock format, that digest emails will begin to be sent out by the system.
  - **Maximum duration**: The period over which the system will spread the sending of digest messages following the start time defined above. Using this feature reduces the loading on the system.

- **Releasing Messages**

  By default, PMM users have the ability to release messages from their PMM area to their in-box. If this contravenes company policy, clear the **Allow users to release their messages** check box. In this event, the system administrator is responsible for managing quarantined PMM messages.

- **Tracking Messages**

  With Enterprise and Advanced licenses, by default, PMM users have the ability to track messages that they have sent, or that have been sent to them. De-select the **Allow users to track their messages** check box to disable this functionality.

- **Log Files**

  Enter a number of days in the **Retention period** field to define the period that the log files will be retained before they are deleted by the system.

Click **Save** to implement your changes.

Per Domain Settings

If you use multiple domains, the **Per Domain Settings** tab allows you to configure different settings for each domain. Use the **Domain:** pull-down list at the top right of the screen to select the domain to configure.

The Per Domain Settings tab contains the following:

- **Originator Email Address**

  The email address that will appear as the sender on the notification messages.

- **Default Language**

  The default language setting for new PMM accounts. When they access their accounts, PMM Users can override this setting if they choose.

The only difference between English (United States) and English (United Kingdom) is the way in which the data and time is displayed.

- **New Account Template**

  A system generated email message is sent to a user if they create a PMM account, or when they receive messages into their PMM area for the first time.

  - **Subject**: Text to create the subject line for the notification email. The default text, which is already entered, is **MIMEsweeper PMM New Account Notification**. This can be modified or added to as required.
  - **Annotation**: Enter text here to create the annotation for the notification email, including a simple outline of what users are expected to do with the messages which have been placed in their individual PMM area, and why they have been placed there by the system. This annotation is added as a footer to the notification message.

- **Password Reset Template**

  When a user requests a reset password when attempting to sign in to PMM, they will automatically be sent an email message.

  - **Subject**: Text to create the subject line for the password email. The default text, which is already entered, is **MIMEsweeper PMM Password Notification**. This can be modified or added to as required.
  - **Annotation**: Enter text here to create the wording of the annotation which will appear as a footer in the password notification message.

- **Digest Template**

  Every user who has had messages placed into their individual PMM area in the previous 24 hours will be sent a notification email.

  - **Subject**: Text to create the subject line for the digest email. The default text, which is already entered, is **MIMEsweeper PMM Update**. This can be modified or added to as required.
  - **Annotation**: Enter text here to create the wording of the annotation which will appear as a footer in the digest message.

- **Delegation Assignment Template**

  Users who are delegated the management of another user’s PMM messages are sent a notification message telling them that they have been delegated.

  - **Subject**: Text to create the subject line for the delegation assignment email. The default text, which is already entered, is **MIMEsweeper PMM Delegation Assignment Notification**. This can be modified or added to as required.

  - **Annotation**: Enter text here to create the wording of the annotation which will appear as a footer in the delegation assignment message.

- **Delegation Removal Template**

  Users who are currently delegated to manage another user's PMM messages are sent a removal notification message when the delegation is removed by the originating user.

  - **Subject**: Text to create the subject line for the delegation removal email. The default text, which is already entered, is **MIMEsweeper PMM Delegation Removal Notification**. This can be modified or added to as required
  - **Annotation**: Enter text here to create the wording of the annotation which will appear as a footer in the delegation removal message.

Authentication Settings

You use the Authentication Settings area to define how users are authenticated when they log in to their PMM accounts. Integrated Windows authentication uses the Windows Active Directory server to authenticate PMM users. This provides the following functionality:

- PMM users are not allocated a password when their account is created, and are not prompted for a password when they access their PMM accounts.
- User aliases for a mailbox are combined automatically for the user's PMM account. That is, by default, a user can access the PMM messages for all his or her aliases for a mailbox, without the need to use message management delegation.
- For users with multiple mailboxes, Integrated Windows authentication provides the ability to combine the mailboxes so that messages can be managed from a single PMM account.
- In systems using Windows Integrated PMM, you can delegate that designated users can manage your organization's public mailboxes, for which there is no login account. See *Managing messages in public folders* on page 10-3 for details. This is not required for systems using manual PMM authentication. In these systems, users can use their PMM passwords to access public folders.

To configure the authentication settings:

- Select the **Manual Authentication** radio button to set that users are authenticated manually. That is, when MIMEsweeper for SMTP creates a new account for a user, it allocates a password. Users must enter this password when they log on to their PMM account.
- Select the **Integrated Windows Authentication** radio button to set that users are authenticated via their Windows logon authentication.
- Primary directory is the active directory server that authenticates users:
  - **Server**: The Active Directory server name.
  - **Port**: The port that the Active Server directory uses
  - **User Name**: A valid logon name to the Active Server directory
  - **Password**: The password for the logon name

- Secondary directory

  You can configure a secondary Active Server directory that PMM will check if the user is not found in the primary server.

- Use fully qualified domain names in notification emails

  Select this option to set that the notification email link to users' PMM website uses a fully qualified domain name.

Each PMM notification message contains a links to users’ PMM sites. If you select the **Use fully qualified domain names in notification emails** check box, this link consists of a fully-qualified domain name.

The default setting for this option is **unchecked**. If you check this option to use fully qualified domain names in PMM links, by default, users are prompted for authentication when they select the link.

View Inactive PMM Users

Clicking the **View Inactive PMM Users** link on the Configure Personal Message Manager page opens the View Inactive Users page. This page lists all the users who have received emails potentially containing junk or spam, but have never used the PMM system to manage these messages.

You use this page to identify users who are not managing their personal messages, in order that you can notify them. To delete personal messages, for example for a user who has left the company, you access the **Personal Messages** quarantine area, where you can delete the messages.

- **Email address**: The email address of the inactive user.
- **Last login**: The date and time that the inactive user last logged into the system to view or manage their messages. This assumes that the user has actually logged in. If they have never logged into the system this field will be blank.
- **Last Action**: The last action performed by the inactive user.
- **Count**: The total number of messages for the inactive user which are currently in the PMM system awaiting release or deletion by the user.

Enabling message areas for access by PMM

Although PMM is typically used for spam messages, you can allow users to review messages quarantined by any classification. By default, all messages classified as `Detected Spam` are written to the Personal Messages quarantine area. You can configure any quarantine area as a PMM-enabled message area. For example you can configure a scenario that traps all messages with multimedia attachments and quarantines them in a PMM area. Personnel could then use PMM to review these messages and release or delete them.

In the Policy Editor, via a message area's property page, you can set quarantine areas to be PMM-enabled. Under the **Management** tab, you use the **Allow area to be managed by PMM** check box to set that messages from the quarantine areas are included in the PMM digest.

Only those messages that arrive in this quarantine area after it has been reconfigured are included in future digests. Any messages in the area written before you configured it will not be included. The digest lists all the messages that have been held within these message areas. It does not specify from which quarantine area the messages are from.

For more information on setting an area to be used for PMM, see Chapter 2. For more information on quarantine areas, see Chapter 9.

Handling users with multiple addresses

How you handle users with multiple addresses depends on whether or not your installation uses Integrated Windows authentication. If you use Integrated Windows authentication:

- Alias addresses for a mailbox are available from a single PMM account.
- Within PMM, users with multiple mailboxes can combine PMM message management for their mailboxes.

  See *Authentication Settings* on page 10-6 for details of how to configure Integrated Windows authentication.

Without Integrated Windows authentication, by default, PMM issues a daily digest for each address that has received one or more spam messages. Each address is treated as a different user, and a PMM account is created for each address. By default a user with multiple addresses will receive a digest for each address, and will need to log in to the PMM account for each address in order to manage the withheld messages for the address.

To make it easier for users with multiple addresses, you use the **Delegation** functionality within PMM to issue a single digest for multiple accounts. For users with multiple addresses:

1. Choose a primary address to receive their spam digest
2. Access PMM from a secondary account, and use the **Delegation** functionality to delegate the digest for their other address to the primary address. For more information, see *Delegation* on page 10-15.

Removing stale PMM accounts

An automated task scans PMM accounts every day for accounts that appear to be unused or 'stale'. Any PMM accounts which match the following conditions are removed.

The conditions are:

- The account has not been delegated to another account. An account is deemed to be still in use if it has been delegated to by another account.
- The account has not received an email for 3 months
- The account has not been logged into for 3 months

Following the removal of an unused PMM account the PMM log file is updated.

Using PMM

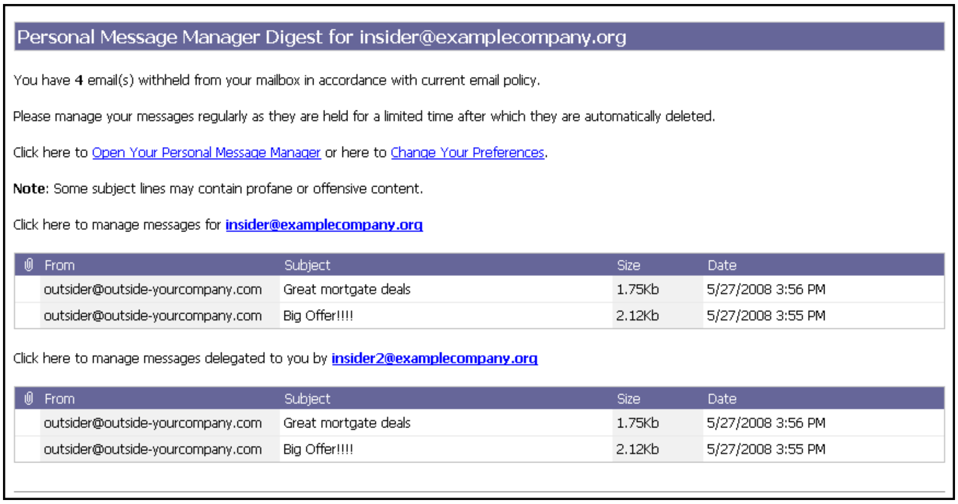
Once the end-user receives the first new account notification message, they can then start controlling their own PMM messages.

- If the system uses manual authentication, new users are allocated a password that they use to log in to their PMM accounts.
- If the system uses Integrated Windows Authentication, the link on PMM notification messages takes you straight to your PMM account without the need to enter a password. See *Authentication Settings* on page 10-6 for details.

Notification of withheld messages

The system sends a notification email or digest telling users that there are messages for them, or users who have delegated the management of their PMM messages to them, in the PMM message area. A notification message is sent each day to users who have new messages quarantined as spam.

The System Administrator sets the digest transmission time.



Personal Message Manager Digest for insider@examplecompany.org

You have **4** email(s) withheld from your mailbox in accordance with current email policy.

Please manage your messages regularly as they are held for a limited time after which they are automatically deleted.

Click here to Open Your Personal Message Manager or here to Change Your Preferences.

Note: Some subject lines may contain profane or offensive content.

Click here to manage messages for **insider@examplecompany.org**

	From	Subject	Size	Date
	outsider@outside-yourcompany.com	Great mortgate deals	1.75Kb	5/27/2008 3:56 PM
	outsider@outside-yourcompany.com	Big Offer!!!!	2.12Kb	5/27/2008 3:55 PM

Click here to manage messages delegated to you by **insider2@examplecompany.org**

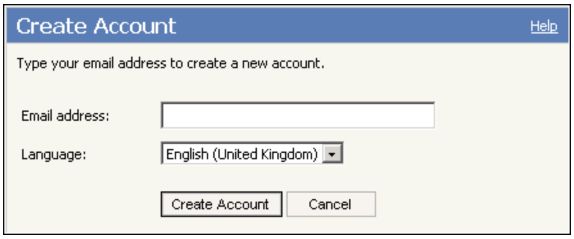
	From	Subject	Size	Date
	outsider@outside-yourcompany.com	Great mortgate deals	1.75Kb	5/27/2008 3:56 PM
	outsider@outside-yourcompany.com	Big Offer!!!!	2.12Kb	5/27/2008 3:55 PM

Figure 10-1: PMM Digest Message

The digest contains hyperlinks which take the user to pages where they can manage their own messages, the messages of users who have delegated their PMM management to them, or to an area where they can change their preferences.

Creating a PMM account manually

If a user does not yet have a PMM account they can create an account by going to the Sign In page and clicking on **Get One Now**. The Create Account dialog box is shown.



Create Account

Type your email address to create a new account.

Email address:

Language: English (United Kingdom)

Figure 10-2: PMM Create Account Dialog Box

To create a new PMM Account:

1. Enter your email address
2. From the drop-down list select the language that you want the PMM pages and notifications to be displayed in.

   English (United States) displays in English and uses standard US English date and time formats.

   English (United Kingdom) displays in English and uses standard UK English date and time formats.

   PMM pages are initially displayed in the language set by the Administrator in the **Configure Personal Message Manager** pages of the MIMEsweeper Manager, as described in *Per Domain Settings* on page 10-4.
3. Select **Create Account**.

   The system sends the user an email containing a PMM password.

Accessing PMM messages

You access your PMM messages by:

- Clicking the link in the digest email.

  or

- Entering the URL for the Sign In page: `http://<servername>/MSWPMM`

  Where `<servername>` is replaced with the name of the server running MIMEsweeper for SMTP.

  or

- If the MIMEsweeper application is installed on your machine, from the Windows **Start, Programs, MIMEsweeper for SMTP** menu, select **Personal Message Manager**.

You can access your PMM web page easily by adding it to your list of Favorites.

When you access PMM from a notification message:

- If your system uses Integrated Windows Authentication, the system logs you in to your PMM area
- If your system uses manual authentication, the sign-in page is displayed and you are prompted for the password. This password is specified in the new account notification message.

If you have forgotten your password, click **Forgot your password** and the system will send you an email reminder of it.

Checking **Keep me signed in on this computer unless I sign out** ensures that the user's connection to the system remains active and does not time-out until they click **Sign Out**.

When you log in, the PMM Home Page is displayed.

The PMM Home page provides links to the **My Messages**, **Delegated Messages, Track Messages,** and **Options** pages. These are accessible from either the MIMEsweeper menu bar, or from the hyperlinks in the text.

This page also displays a total count for messages currently held in the My Messages area. If you use Integrated Windows authentication and use multiple addresses, the PMM messages for each address are shown at the bottom of the screen. Click on a number link to access the messages for the address.

My Messages

The My Messages page provides a full list of the messages which have been held by the system and put into the user's PMM area. Columns in this list show whether each message has attachments, the sender, the subject, the date and time that they entered the MIMEsweeper system, and the size of the message in Kilobytes.

The page has the following four buttons to allow the user to manage the messages held there:

- **Delete All**

  Having reviewed the list, and decided that none of the messages are of any importance, the user clicks **Delete All** to remove all messages from the list. A confirmation dialog box is displayed. Click **Yes** to delete all messages.

- **Refresh**

  If it has been some time since the user opened the My Messages page they can click **Refresh** which adds any messages to the list which have recently been directed to their PMM area by the system.

- **Select Mailbox:**

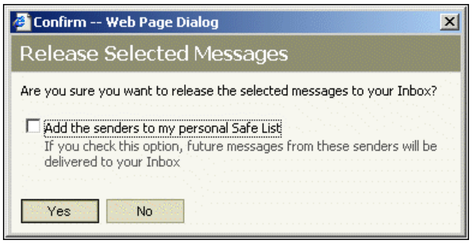
  If your system uses Integrated Windows authentication, you can use the Select Mailbox pull-down list to select the address to manage.

- **Delete**

  The user selects the messages in the list that they have decided have no importance by selecting the boxes next to each in the left hand column and then clicks **Delete** to remove them from the list.

- **Release**

  The user selects the messages in the list that they wish to release to their mailbox and then clicks **Release.** A confirmation dialog box is displayed.



Confirm -- Web Page Dialog

Release Selected Messages

Are you sure you want to release the selected messages to your Inbox?

□ Add the senders to my personal Safe List

If you check this option, future messages from these senders will be delivered to your Inbox

Figure 10-3: Release Messages Confirmation Dialog

A user can add the details of the senders of the messages to their personal Safe List. This ensures that any future emails from these senders will appear in their inbox and not be directed to PMM.

The ability to release messages from the user's PMM area is dependent upon the administrator settings for PMM which are determined by the policies implemented within your organization.

Should the list require more than one page to display all messages then navigation is provided by arrows at the bottom of each page, together with a total showing how many pages and messages are in the list.

Delegated Messages

The Delegated Messages page is where all messages sent to users who have delegated their PMM management to this user are displayed. Users with multiple addresses can use this to consolidate their notification messages. See *Handling users with multiple addresses* on page 10-9 for details. See *Managing messages in public folders* on page 10-3 for information on delegating users to manage messages in an organization’s public mail folders for systems using Windows Integrated PMM.

Track Messages

The Track Messages page allows users to search the Message Tracking database for details of messages that they have sent, or messages that have been sent to them. Message tracking for PMM users is available only with the Advanced and the Enterprise MIMEsweeper licences.

For example, with this functionality a user can determine if the system has blocked a message that they have sent, or if the system has blocked a message that they expected to receive.

Users can find message tracking details using one or more of the following search criteria:

- The sender or recipient address
- The message subject
- The message attachment name
- The time sent or received

For messages that the system finds, the following details are displayed:

- **Time Received**, or the date and time that the message entered the MIMEsweeper system
- **To**, or the recipient address
- **From:** or the sender address
- The message **Subject**
- The **Status** of the message, for example, delivered, quarantined, or parked.

Options

The Options page is where you can customize your PMM settings. It consists of four areas, as outlined below:

- **Delegation**

  Delegating messages allows you to delegate your PMM management to someone else, or to consolidate notification messages from multiple addresses that you may have. For more information, see *Delegation* on page 10-15.

- **Safe List**

  Allows you to maintain a list of email addresses that are considered trustworthy. For more information, see *Safe List* on page 10-16.

- **Change Password**

  Allows you to change the PMM password if your system requires a password. For information on changing the password, see *Change Password* on page 10-16.

- **Preferences**

  Select the language you would like to use when viewing PMM and email notifications. For information on selecting the language to use, see *Preferences* on page 10-17.

Delegation

Select **Delegation** from the Options area to display those options specific to delegating messages, including who you want to delegate messages to, and who has delegated messages to you. You use the functionality to delegate messages to a single address for the user, to avoid receiving a digest for each address. See *Handling users with multiple addresses* on page 10-9 for details.

- **Delegating My Messages**

  The MIMEsweeper system gives the user the choice of delegating the management of their messages to another user. The original user can directly manage their own messages if necessary while delegated.

ℹ The delegation of messages can also be used to allow a user with more than one email address to delegate them to a single address. This allows all their PMM messages to be managed from one place.

The options are:

- **Yes I want to delegate to email address**

  Enter the email address of the user who the management of this user's PMM messages is to be delegated to. All withheld messages appear in the original user's own PMM area as well as in the PMM area of the user that they have been delegated to. The user nominated can choose to reject this request.

- **No, I want to manage my own messages**

  This is the default. All messages addressed to the user, which are classified by MIMEsweeper as suspect, are directed to the user's own PMM area only.

Click **Save** to apply the choices.

ℹ A user who has messages delegated to them cannot delegate their messages to another user.

- **Users Who Have Delegated To Me**

  A list of system users who have delegated the management of their PMM area to this user is displayed here. Should this user wish to reject any or all of these users, they can select the check box beside their email address and then click **Reject**. The selected entry will be removed from the list and only their own PMM messages will appear in their PMM area.

Safe List

Select **Safe List** from the Options area to display details of the email addresses which are considered to be trustworthy, and email sent by them will be processed and released to the user's inbox.

The options are:

- **Type an email address**

  In this field the user can type any email address that they would like to add to the Safe List. Click **Add** to add the address to the list.

  Wildcards can be used in these addresses, as follows:

  - `*@<domain>` will add everyone in the named domain. For example, `*@a-differentcompany.com` will regard mail from anyone in a-differentcompany as safe.
  - `<mailbox>*@domain` will add mail from an address that has invariant and variant parts in the address.

    For example, `mailing-list*@a-differentcompany.com` will regard any mail from a-differentcompany whose mailbox begins with 'mailing-list' as safe .
  - `*<mailbox>@domain`, as above but with the wildcard before the invariant part.

  Addresses can also be added automatically when releasing acceptable messages from their PMM area to their Inbox. See *My Messages* on page 10-12 for further details.

- **Select addresses and Delete**

  Any address can be removed from the Safe List by selecting the box adjacent to it, then clicking **Delete**.

Change Password

Select **Change Password** from the menu in the Options area to display the Change Password area where the user can change the password that they are currently using to access the PMM application.

The options are:

- **Old password**

  Enter the current password being used to access the user's PMM application.

- **New password**

  Enter the new password to use.

- **Confirm new password**

  Re-enter the new password to confirm it.

Click **Save** to implement the changes on the system.

Preferences

Select **Preferences** from the Options area to display any other preferences you can change such as the language used to view PMM.

- **Language**

  From the drop-down list select the language that you want the PMM pages and notifications to be displayed in.

The only difference between English (United States) and English (United Kingdom) is the way in which they display the date and time.

PMM pages are initially displayed in the language set by the Administrator in the **Configure Personal Message Manager** pages of the MIMEsweeper Manager as described in Chapter 9. Configure a different language here or in the PMM Options pages.

Click **Save** to implement the changes on the system.

CHAPTER 11

Report Center

This chapter describes the MIMEsweeper Manager Report Center and the options available for viewing reports.

Overview

This chapter describes how to generate and view reports based on information collected for your MIMEsweeper for SMTP system in the Report Center in both the audit log and the message tracking database. The Report Center is accessed from the MIMEsweeper Manager Home Page.

The Report Center contains a list of available reports, categorized into a number of report groups. For details about the types of report available, see *Available reports* on page 11-7.

You must configure auditing and message tracking first to access these reports. For more information on configuring auditing, see *Configure Auditing* on page 11-5, and for message tracking, see Chapter 9.

Why use Report Center?

The Report Center provides reports that you can use to provide an overview of the current MIMEsweeper system, or to analyze individual threats and patterns in email messages processed by a Policy Server. You configure reports to monitor and display the way Policy Servers process email messages, and to track the receipt and delivery of individual email messages passing through the system.

For example, you can use reports to assess information such as:

- Users who send or receive the most email messages.
- Format trends in email messages.
- Usual time and volume of peak email traffic.

How to access the Report Center

You access the Report Center from MIMEsweeper Manager which accesses message data held on the MIMEsweeper Manager Operations database on the Primary Configuration Server (PCS).

If you are already logged on to MIMEsweeper Manager

To display the Report Center Home Page, select **Report Center** from the Getting Started Page or from the site navigation bar at the top of any MIMEsweeper Manager page.

If you are not logged on to MIMEsweeper Manager

When users log on to the MIMEsweeper Manager from a web browser, they must supply the name and password of an MIMEsweeper user account that has been assigned permissions to access the MIMEsweeper Manager application. The MIMEsweeper Manager application authenticates these log on credentials before providing access to the MIMEsweeper Manager application containing the Report Center. For details about user names and passwords, and for details about assigning access permissions to user accounts, see Chapter 12.

To logon and access the Report Center from the Start menu

1. Click **Start**.
2. Select **Programs**.
3. Select **MIMEsweeper for SMTP**.
4. Click **MIMEsweeper Manager.**

   The MIMEsweeper Manager Getting Started page is displayed.
5. Click on **Report Center** or select it from the Site Navigation Bar at the top of the page

   The MIMEsweeper Manager logon page is displayed.
6. Enter a valid MIMEsweeper user name and password and click **Logon.**

   If the logon is successful the Report Center Home Page is displayed.

To logon and access the Report Center from a web browser:

1. Enter the URL for the MIMEsweeper Manager application in the form:

   `http:/<ServerName>/mswsmtp/`

   `where <ServerName>` is replaced with the name of the server running MIMEsweeper.

`https:/"ServerName"/mswsmtp/` must be used if your system is secure.

   The MIMEsweeper Manager Getting Started page is displayed

2. Click on **Report Center** or select it from the Site Navigation Bar at the top of the page

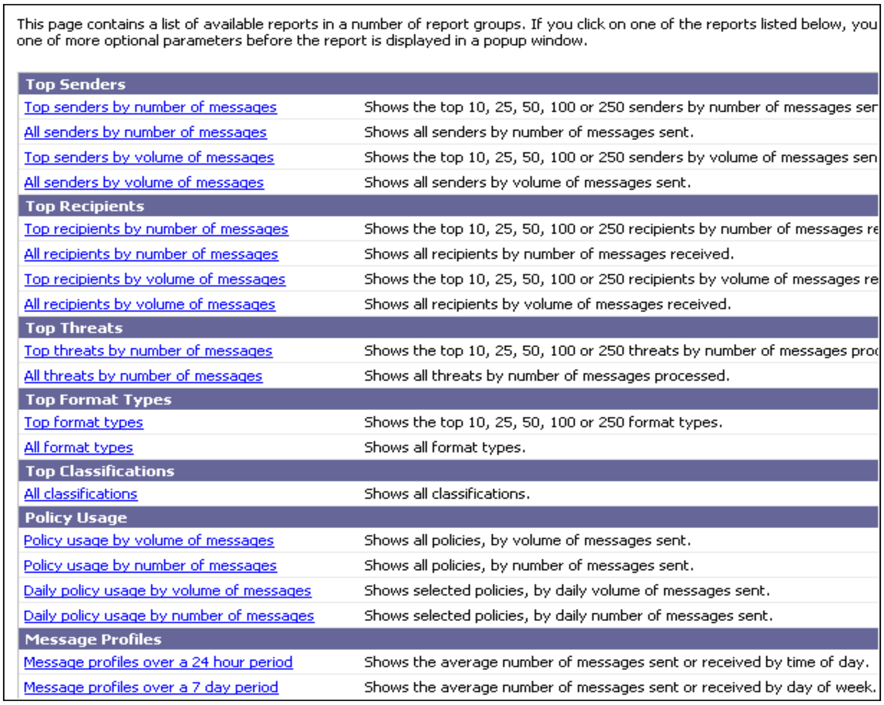
   The MIMEsweeper Manager logon page is displayed.
3. Enter a valid MIMEsweeper user name and password and click **Logon.**

   If the logon is successful the Report Center Home Page is displayed.

Once logged on, users can use only those areas of the Report Center that they have been assigned access permissions within the Report Center itself. For details, see Chapter 12.

Report Center Home Page

The Report Center Home Page displays the name of the user who is logged on, a list of available reports, and links to enable the configuration of auditing and purge options. Each of these is described in more detail in the following sections.



This page contains a list of available reports in a number of report groups. If you click on one of the reports listed below, you one of more optional parameters before the report is displayed in a popup window.

Top Senders	
Top senders by number of messages	Shows the top 10, 25, 50, 100 or 250 senders by number of messages ser
All senders by number of messages	Shows all senders by number of messages sent.
Top senders by volume of messages	Shows the top 10, 25, 50, 100 or 250 senders by volume of messages sen
All senders by volume of messages	Shows all senders by volume of messages sent.
Top Recipients	
Top recipients by number of messages	Shows the top 10, 25, 50, 100 or 250 recipients by number of messages re
All recipients by number of messages	Shows all recipients by number of messages received.
Top recipients by volume of messages	Shows the top 10, 25, 50, 100 or 250 recipients by volume of messages re
All recipients by volume of messages	Shows all recipients by volume of messages received.
Top Threats	
Top threats by number of messages	Shows the top 10, 25, 50, 100 or 250 threats by number of messages proc
All threats by number of messages	Shows all threats by number of messages processed.
Top Format Types	
Top format types	Shows the top 10, 25, 50, 100 or 250 format types.
All format types	Shows all format types.
Top Classifications	
All classifications	Shows all classifications.
Policy Usage	
Policy usage by volume of messages	Shows all policies, by volume of messages sent.
Policy usage by number of messages	Shows all policies, by number of messages sent.
Daily policy usage by volume of messages	Shows selected policies, by daily volume of messages sent.
Daily policy usage by number of messages	Shows selected policies, by daily number of messages sent.
Message Profiles	
Message profiles over a 24 hour period	Shows the average number of messages sent or received by time of day.
Message profiles over a 7 day period	Shows the average number of messages sent or received by day of week.

Figure 11-1: Report Center Home Page

You are logged on as

Displayed at the top right of each page in the Report Center this gives details of the user currently logged on. Click **Logoff** to log off the current user and return to the MIMEsweeper Manager Logon page.

This logoff option is available from each area in the Report Center.

Configure Auditing

Click **Configure Auditing** on the Report Center Home Page to open the Configure Auditing page. You use this page to configure a new audit database to change an existing audit database, and to enable or disable auditing.

Auditing

On this page you can change the current audit settings. To audit a different database:

- Choose **Disable**, or **Enable**. To disable auditing choose **Disable** and click **Save.** This will present a confirmation message that auditing has been disabled successfully.
- To enable auditing choose **Enable**, where the database and sever to be audited are shown, and then select **Classifications**, **Threats** or **Formats** as required by checking the boxes. Clicking **Save** will enable the auditing using the parameters you have chosen.
- Choose the time to roll over the audit data log. The lower the figure entered here, the more frequently the data base will be updated by the system. The default is 60, while the maximum time that can be entered here is one full day, which is 1440 minutes.

Auditing Wizard

Click on the link for the **Auditing Wizard** to display step 1 of the wizard:

Before you use the Auditing Wizard to change the configuration, stop the Audit Disposer service. For details on how to stop the Audit Disposer service, see *Managing services* on page 8-5.

- **Step 1**: **Enable Auditing**: Gives the choice of selecting **Create new database** or **Use existing database**. Click **Next** to move to the next step.
- **Step 2: Database Connection**: Presents the following fields:
  - **Server Type**: Choose the server type from the drop-down menu.
  - **Server name**: Allows the option of picking a server, or specifying one to be used.
    - **Pick server**: Choose the server name from the drop-down list.
    - **Specify server**: Type the name of the server you wish to audit in the field provided.
  - **Instance name**: An optional field. If more than one instance of SQL Server is installed, specify the instance to be used by entering its name in this field.
  - **Port number**: An optional field. If the database software uses a port number other than the default specify it here.
  - **Administrator**: Enter a valid administrator name for the database you have specified to be audited in the steps above.
  - **Password:** Enter the password for the Administrator name that you have just entered.

  Once you have completed this page click **Next** to move to the next step.

- **Step 3: Database Details**: Allows you to select **Specify database** and then type the name of the database to be audited into the field provided, or select **Pick database** and then choose the relevant database from the drop-down list.

  Click **Next** to move to the next step.

- **Step 4: Audit Settings**: Define the audit settings by checking the boxes for **Classifications**, **Threats** and **Formats**. One or more of these setting can be checked.

  Click **Next** to move to the next step.

- **Step 5: Audit Log Rollover**: Enter the time in minutes between roll overs of the auditing log. The lower this figure the more frequently the data will be updated by the system. The maximum time that can be entered here is one day - 1440 minutes.

Long periods between roll overs may cause high loadings on the system while the log is being processed due to the amount of data which has been gathered. Shorter time periods will result in a better distribution of this load.

- **Step 6: Time Zone**: Choose the time zone required from the drop-down list.
- **Step 7: Audit Summary**: A summary of the settings you have chosen as you have gone through the wizard is displayed.

  Clicking **Next** here will apply the configuration you have chosen, and, if this is successful will display a message to that effect.

  Click **Finish** to return to the **Report Center Home Page**.

When you create a new audit database, using either SQL Server or Oracle, the MIMEsweeper system creates a database account and password for its own use. The account name is:
`ul_<databasename>`
where `<databasename>` is the name you specified for the audit database.

Do not delete this account or change its password; otherwise MIMEsweeper is unable to record information in the database. If you do delete or amend an audit database account you will need to remove and reinstall the database, or create a new database and manually migrate the data from the old database.

Purge Options

Clicking on the Purge Options link on the Report Center Home Page will open a configuration page allowing parameters to be set for retaining and purging data in the database.

Data Retention Period

In order to prevent the database from growing too large a limit can be put on the period over which the data is retained by the system.

Enter the number of days to retain data in the field provided and click **Save** to apply it. The default is 30 days.

Purge Database

A manual purge of the database can also be carried out. To do this specify the period in days in the field provided. When **Purge** is clicked all data older than the specified number of days will be deleted from the database.

The default is 30 days.

Reports

MIMEsweeper Manager can produce reports based on information stored in either the auditing or message tracking database. These reports monitor and display information about the way the services process data and contain information such as the top senders by numbers of messages and top senders by volume.

> The auditing database will enable reports to be produced for individual users. Check local legislation to determine whether this is permissible in your country.

For each report you can view a short summary explaining the information it contains as well as more specific details about selected portions of the report. When you select a report to display, MIMEsweeper reads the data from the relevant database and generates a report. If the data set is returned empty, the report is not displayed and a message is displayed advising of this.

You can print reports or export report data to other file formats for use in other reporting tools.

For each report you must specify a date range over which the report should run. For certain reports you must also specify a user’s Email address. The wizard prompts you for this information. For details see *Producing a report* on page 11-12.

You can select portions of an individual report to view more specific information.

The data generated by a report can be exported into a choice of file formats. For details, see *Exporting the report data* on page 11-13.

Available reports

The Report Center Home Page displays a list of the report groups and a description of the reports each group contains.

Top Senders

A group of reports that identify the users that send high levels of email messages.

- **Top senders by number of messages**

  Shows the top 10, 25, 50, 100, or 250 senders by the number of messages sent over a defined period. The results are presented in the form of a graph, and also in a table with senders ranked by the number of messages sent, and as their percentage of the total.

- **All senders by number of messages**

  Shows all senders by the number of messages sent over a defined period. The results are presented in a table with senders ranked by the number of messages sent, and the percentage of the total. At the bottom of the table a figure is given for the total messages sent.

- **Top senders by volume of messages**

  Shows the top 10, 25, 50, 100, or 250 senders by the volume of messages sent over a defined period. The results are presented in the form of a graph in kilobytes, and also in a table with senders ranked by the volume in kilobytes, number of messages sent, and the percentage of the total. At the bottom of the table figures are given for the total volume of messages sent by the top senders, in kilobytes, along with the percentage of all messages sent which have been sent by them.

- **All senders by volume of messages**

  Shows all senders by the volume of messages sent over a defined period. The results are presented in a table with senders ranked by the volume in kilobytes, number of messages sent, and the percentage of the total. At the bottom of the table a figure is given for the total volume of messages sent in kilobytes.

Top Recipients

A group of reports that identify the users that receive high levels of email messages.

- **Top recipients by number of messages**

  Shows the top 10, 25, 50, 100, or 250 recipients by the number of messages received over a defined period. The results are presented in the form of a graph, and also in a table with recipients ranked by the number of messages received, and the percentage of the total. At the bottom of the table figures are given for the total number of messages received by the top recipients, along with the percentage of all messages received which have been received by them.

- **All recipients by number of messages**

  Shows all recipients by the number of messages received over a defined period. The results are presented in a table with recipients ranked by the number of messages received, and the percentage of the total. At the end of the table a figure is given for the total number of messages which have been received.

- **Top recipients by volume of messages**

  Shows the top 10, 25, 50, 100, or 250 recipients by the volume of messages received over a defined period. The results are presented in the form of a graph, in kilobytes, and also as a table with recipients ranked by the volume in kilobytes, number of messages received, and the percentage of the total. At the bottom of the table figures are given for the total volume of messages received by the top recipients, in kilobytes, along with the percentage of all messages received which have been received by them.

- **All recipients by volume of messages**

  Shows all recipients by the volume of messages received over a defined period. The results are presented in a table with recipients ranked by the volume in kilobytes, number of messages received, and the percentage of the total. At the end of the table a figure is given for the total volume of messages, in kilobytes, which have been received.

Top Threats

This group of reports identifies the threats or potential threats MIMEsweeper has logged in the Audit database. For these reports to return meaningful data, make sure that threat logging is enabled in the Audit database. To enable threat logging, use the **Configure Auditing** page, accessed from the Report Center Home Page.

- **Top threats by number of messages**

  Shows the top 10, 25, 50, 100 or 250 threats or potential threats identified and processed by Security service over a defined period. The threats to include in the reports are selected in the report Wizard.

- **All threats by number of messages**

  Shows all threats or potential threats identified and processed by Security service over a defined period. The threats to include in the reports are selected in the report Wizard.

Top Format Types

A group of reports that identify the number of attachments associated with messages processed during the specified period.

- **Top format types**

  Shows the top 10, 25, 50, 100 or 250 format types.

- **All format types**

  Shows all format types.

Top Classifications

A group of reports that identify the number of classifications processed during the specified period.

- **All classifications**

  Shows all classifications of messages handled by the system. The results are presented in a graph, and in a table with classifications ranked by the number of occurrences of an action, and as a percentage of the total. At the bottom of the table a figure is given for the total number of actions performed.

Policy Usage Reports

A group of reports that identify the scenarios that MIMEsweeper is using to process messages. That is, you can use these reports to determine the scenarios that messages are triggering.

- **Policy usage by volume of messages**

  For the specified time period, shows the number of messages processed under each scenario that has been used. The report shows the volume of data in Kb that each scenario processed,.

- **Policy usage by number of messages**

  For the specified time period, shows the number of messages processed under each scenario used. The report shows the number of messages that each scenario processed.

- **Daily policy usage by volume of messages**

  As with the Policy usage by volume of messages report, except that the data is listed per day.

- **Daily policy usage by number of messages**

  As with the Policy usage by number of messages report, except that the data is listed per day.

Message Profiles

A group of reports that identify the average number of messages passing through the Policy Server in a specified period of time.

- **Message profiles over a 24 hour period**

  Shows the average number of email messages processed in any 24-hour period. The results are presented in a graph with the average number of messages plotted against the hour of the day. A table is also shown containing the same data plus an hourly average figure. At the bottom of the table a figure is given for the hourly average.

- **Message profiles over a 7 day period**

  Shows the average number of email messages processed in any 7-day period. The results are presented as a graph showing the average number of messages plotted against the days of the week. A table is also shown containing the same data plus an daily average figure. At the bottom of the table a figure is given for the daily average.

- **Message profiles over a monthly period**

  Shows the average number of email messages processed in any monthly period. The results are presented as a graph showing the average number of messages plotted against the days of the month. A table is also shown containing the same data plus an average figure for each day of the month.

Traffic Analysis

A group of reports that identify the actual trend of email messages passing through the Policy Server

- **Traffic levels by hour**

  Shows the number of messages processed over a specified number of hours. The results are presented in a table showing the date, time, number of messages and the total volume in kilobytes. Figures are shown at the end of the report for the grand total and hourly averages for both the number of messages and the volume.

- **Traffic levels by day**

  Shows the number and volume of messages processed over a specified number of days. The results are presented in a graph with the number of messages plotted against days. A table is also shown containing the date, number of messages, and the volume of messages in kilobytes. Figures are shown at the end of the report for the grand total and daily averages for both the number of messages and the volume.

- **Message actions by day**

  Shows the actual number of actions performed on messages processed over a specified number of days. The results are presented in a table showing the date, action, and the number of messages. A figure is shown at the end of the report for the total number of messages.

- **Format categories**

  Shows the size and type of attachments, broken down by category, in messages processed over a specified number of days. The results are presented in a table showing the ranking, category, number of attachments, and the percentage of the total in each category. A figure for the grand total is given at the bottom of the table.

- **Format size**

  Shows the actual attachment size bandings in messages processed over a specified period of time. The results are presented in a bar chart, with the size bandings plotted against the number of attachments.

- **Unique email addresses**

  Shows the number of unique email addresses within the domain specified. The results are presented in a list, displaying the figure for the number of unique email addresses.

Transaction Reports

A report to identify the number of messages processed over a particular time period.

- **Transaction report**

  Shows the number of messages processed over a specified period of time. The report is presented as a table showing the Main Policy Array, the Transaction Start Date, Newest Message Date and the transaction count. At the bottom of the table a figure is given for the total transactions.

Message Tracking Reports

A group of reports that identify the volume of email messages sent from a specified sender to a specified recipient.

- **Point to Point Summary**

  Shows the number of messages processed over a specified period of time. The report is presented as a table showing the sender address, recipient address, the number of messages between each and the volume of messages in Kilobytes. At the bottom of the table, a figure is given for the total count and size.

- **Point to Point By Date**

  Shows the number of messages processed over a specified period of time, grouped by date. The report is presented as a table showing the sender address, recipient address, count and size of messages for each day specified. At the bottom of the table, a figure is given for the total count and size.

- **Policy Usage Report**

  Lists details of messages processed by each policy.

For details about configuring, viewing, and working with reports in the **Report Center**, see the MIMEsweeper Manager help.

Producing a report

1. From the Report Center Home Page, click on the report you require.

   A report wizard for the selected report type opens.

2. Using the wizard specify the parameters for the report.

After producing the report, you can export the report data using a choice of file formats, For details, see *Exporting the report data* on page 11-13.

Specifying the report parameters

Before producing a report, you need to specify the report parameters in the relevant wizard. The parameters available depend upon the report chosen and may not appear for all reports.

- **Report size**

  Specify the maximum number of entries you wish to view.

- **Date range**

  Specify the time period to be covered in the report.

- **Message size**

  Specify a particular size (in Kilobytes) or a range of sizes of email messages to be covered in the report

- **Sender’s email address**

  Specify the email address of the sender to be included in the report.

- **Recipient's email address**

  Specify the email address of the recipient to be included in the report.
- **Threats**

  Specify the type of message threats to be included in the report.
- **Format size**

  Specify an attachment size for the report.
- **Format types**

  Specify the attachment types of categories which are to be included in the report.
- **Classifications**

  Specify the classifications to generate the report for. If no classifications are chosen the report will cover all classifications.
- **Message direction**

  Specify the direction of messages to be included in the report: in, out or within your system.
- **Sorting**

  Specify the way in which the results of the search will be sorted to be included in the report.

Exporting the report data

You can export report data into a number of file formats. This facility is useful, for example, to mail the report information or incorporate the information into a report.

To export the report data:

1. Choose the required format type from the **Export** list at the top of the report page.

   Formats available are:

   - Crystal Report
   - Microsoft Excel
   - HTML 3.2
   - HTML 4.0
   - PDF
   - Rich Text
   - Microsoft Word.
2. Click **Go**.
3. In the File Download window, click **Save**.

Report Center security

Access and permissions for the Report Center are controlled from the MIMEsweeper Security Center. For details on Report Center security, see Chapter 12.

CHAPTER 12

Security Center

The following sections provide details on the use of the MIMEsweeper Security Center, including how access permissions for user accounts are used to control access to folders in the Message Center.

Why use Security Center

The Security Center provides facilities to control user’s access, define roles assigned to users and control access to the various features of the MIMEsweeper Manager application using permissions.

How to access the Security Center

You access the Security Center from MIMEsweeper Manager which accesses data held on the MIMEsweeper Manager server.

If you are already logged on to MIMEsweeper Manager

To display the Security Center Home Page, select Security Center from the MIMEsweeper Manager Getting Started page or from the site navigation bar at the top of any MIMEsweeper Manager page.

If you are not logged on to MIMEsweeper Manager

When users log on to the MIMEsweeper Manager from a web browser, they must supply the name and password of a MIMEsweeper user account that has been assigned permissions to access MIMEsweeper Manager. MIMEsweeper authenticates these logon credentials before providing access to MIMEsweeper Manager, which contains the Security Center. For details on user names and passwords, and for details on assigning access permissions to user accounts, see *Available user accounts* on page 12-5.

To logon and access the Security Center from the Start menu:

1. Click **Start**.
2. Select **Programs**.
3. Select **MIMEsweeper for SMTP**.
4. Click **MIMEsweeper Manager**.

   The **MIMEsweeper Manager** Getting Started page is displayed.
5. Click on **Security Center** or select it from the site navigation bar at the top of the page

   The MIMEsweeper Manager Logon page is displayed.
6. Enter a valid MIMEsweeper user name and password and click **Logon.**

   If the logon is successful the Security Center Home Page is displayed.

To logon and access the Security Center from a web browser:

1. Enter the URL for the MIMEsweeper web browser application.
   (`http:/<ServerName>/MSWSMTP/` where `<ServerName>` is replaced with the name of the server running MIMEsweeper.)

   The MIMEsweeper Manager Getting Started page is displayed

2. Click on **Security Center** or select it from the Site Navigation Bar at the top of the page.

   The MIMEsweeper Manager Logon page is displayed.

3. Enter a valid MIMEsweeper user name and password and click **Logon.**

   If the logon is successful the Security Center Home Page is displayed.

Once logged on, users can use only those areas of the Security Center that they have been assigned access permissions for within the Security Center itself.

Security Center Home page

The Security Center Home Page has three areas:

- **Users**

  A user defines an individual within your organization to whom you can explicitly allow or deny access.

  The total number of current users is displayed in this area.

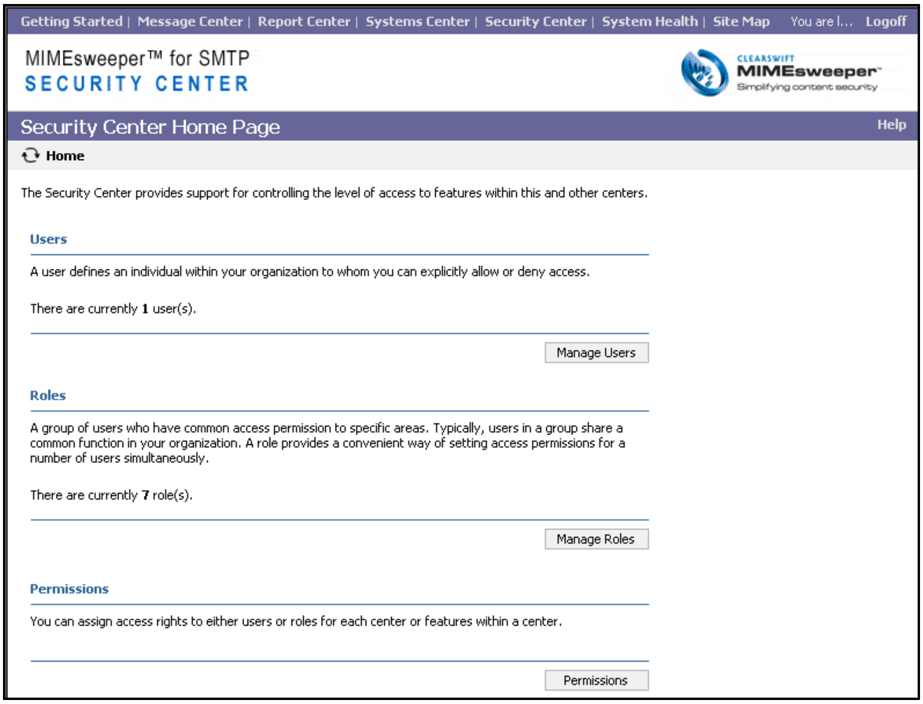
- **Roles**

  A role defines a group of users who have common access permission to specific areas. Typically, users in a group share a common function in your organization. A role provides a convenient way of setting access permissions for a number of users simultaneously.

  The total number of current roles is displayed in this area.

- **Permissions**

  Using permissions you can assign access rights to either users or roles for each center or feature within a center in MIMEsweeper Manager.


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map
You are l...
Logoff
MIMEsweeper™ for SMTP
SECURITY CENTER
CLEARSWIFT
MIMEsweeper™
Simplifying content security
Help
Manage Users
Manage Roles
Permissions

Security Center Home Page

Home

The Security Center provides support for controlling the level of access to features within this and other centers.

Users

A user defines an individual within your organization to whom you can explicitly allow or deny access.

There are currently **1** user(s).

Roles

A group of users who have common access permission to specific areas. Typically, users in a group share a common function in your organization. A role provides a convenient way of setting access permissions for a number of users simultaneously.

There are currently **7** role(s).

Permissions

You can assign access rights to either users or roles for each center or features within a center.

Figure 12-1: Security Center Home Page

Why use user accounts?

A user account defines an individual user or a role within your organization that can be explicitly allowed or denied access to specific folders in MIMEsweeper for SMTP. Assigning access permissions to user accounts enables you to control which individuals or groups are permitted to log on to MIMEsweeper for SMTP and to configure and manage specific aspects of your content security policy.

Using user accounts enables you to secure your system from unauthorized access and to delegate policy configuration and management responsibilities. For example, you could split the maintenance tasks over a number of users and roles, then assign these users and roles only the access permissions that they need to perform their administrative tasks.

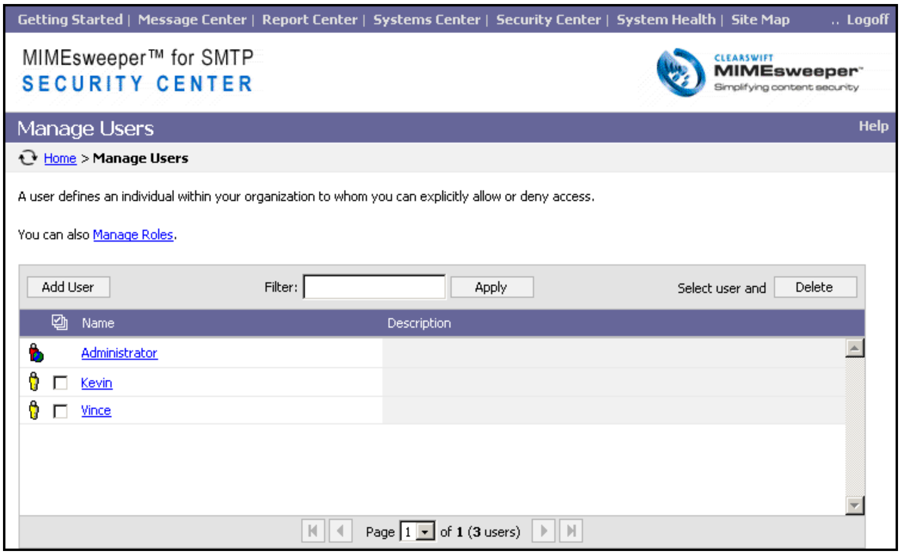
MIMEsweeper Manager provides a super-user account, called Administrator. In addition to the default Administrator user you can create and manage additional users in the **Manage Users** page, accessed by clicking **Manage Users** on the Security Center Home Page.

A user account is required to log on to MIMEsweeper Manager. Whenever users start MIMEsweeper Manager, they are prompted to enter a user name and password. The user name and password are used to authenticate the user's permissions.

Once logged on to MIMEsweeper Manager, the user name and password are used to identify which areas in the application the user has permission to view and manage. Each folder in the Message Center has its own associated set of access permissions. You can modify these permissions, and add permissions for any users you create, to customize the security for your environment.

Available user accounts

You can view a list of the users to which you can assign roles, change passwords and update details for in the **Manage Users** page, accessed by clicking **Manage Users** on the Security Center Home Page. The **Manage Users** page is shown in Figure 12-2.


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map .. Logoff
MIMEsweeper™ for SMTP
SECURITY CENTER
CLEARSWIFT MIMEsweeper Simplifying content security
Manage Users
Help
Home > Manage Users
Add User
Filter:
Apply
Select user and
Delete
Page 1 of 1 (3 users)

A user defines an individual within your organization to whom you can explicitly allow or deny access.

You can also Manage Roles.

Name	Description
Administrator	
□ Kevin	
□ Vince	

Figure 12-2: Manage Users

The Manage User list shows the name and a description of each user. To filter the list, click the initial letter of the required user names in the index list to the right of the **Add User** button.

Users

You can create additional user accounts to represent individuals within your organization responsible for specific policy or system management functions. Users can be assigned to roles—this allows them to inherit a set of defined access permissions from the role. See *Roles* on page 12-9.

> User accounts to which you can assign access permissions for folders in the Security Center are not the same as user objects to which you apply a unique set of policy rules in the policy tree.

Administrator

MIMEsweeper for SMTP provides a default super-user account, called Administrator. This account is required, initially, during Policy Server installation.

The Administrator super-user account always has full access permissions to all areas of MIMEsweeper for SMTP, regardless of the current security settings for a folder. You are recommended to severely restrict access to this Administrator account; you should not use it for day-to-day management of the system.

- **You cannot:**
  - Delete the Administrator account
  - Create another Administrator account
- **You can:**
  - Change the password for the Administrator account
  - Change the Administrator user details, including the account name.

To change the Administrator account password:

1. Open the MIMEsweeper Manager and log on as the Administrator.
2. Go to the **Getting Started** screen and select **Change Password.** Enter your old password and a new password.

To change the Administrator account details:

1. Open the MIMEsweeper Manager and log on as the Administrator.
2. Go the **Security Center** and select **Manage Users**.
3. Select the Administrator account from the list of accounts and edit the name and any other information in the **User Details** screen.

User properties

In addition to the default Administrator user, you can create as many new users as you require to meet your organization's requirements. Only a user who has permissions to Configure Security Center can create new user accounts. You create and manage users in the **Manage Users** page of the Security Center, accessed by clicking **Manage Users** on the Security Center Home Page, which will display a list of all users on the system.

Adding a user

Clicking on **Add User** will show the **Add User** screen where you can enter details for the user to be created.

- **User Details**

  Required fields:

  - **Name**: This is the account name. It is displayed in the left-hand column in the **Manage Users** page, and is used to log on to MIMEsweeper for SMTP. The user name is not case sensitive.

    User account names are restricted to alphanumeric characters (A-Z, a-z, 0-9) plus spaces, dashes and underscores, and must be less than 50 characters long.

  - **Password**: Enter the password that the new user is to use to access the system.

    User account passwords must use only alphanumeric characters: A-Z, a-z, 0-9.

  - **Confirm Password**: Re-enter the password to confirm it.

  Optional fields:

  - **Description**: Enter some text to describe the user.
  - **Email address:** The email address for this user.
  - **Phone Number:** The telephone number for this user.
  - **Locality:** The physical location of this user (for example, the Paris office).

  Select one or more of the following options to secure the user account:

  - **User must change password at next logon:** The user must change the administrator-assigned password to one of their own choosing the next time they log on to the system.
  - **User cannot change password:** The user cannot change the administrator-assigned password. This option is typically used for user accounts to be shared among several people, to prevent one user from locking out other users.
  - **Account is disabled:** The user account is disabled to prevent the user logging on to the system. The default Administrator user account cannot be disabled.

- **Roles**

  A list of the roles available on the system is shown, and you can optionally assign this user to one or more of these.

- The left-hand pane lists roles to which the user is currently assigned.
- The right-hand pane lists all available roles.
- To assign a user to a role, highlight the role in the right-hand pane, and click **Add**.
- To remove a user from a role, highlight the role in the left-hand pane and click **Remove**.
- For details, see *Role properties* on page 12-10. For details, see the MIMEsweeper Manager help.

If adding a large number of entries, in both Users and Roles, avoid using the same initial letter for every name. This will allow easier access when retrieving details, since the **Manage Users** and **Manage Roles** pages group the entries alphabetically.

You cannot create a new User or a Role if the name you have entered in either the **Add User** or **Add Role** page already exists as either a User or a Role on the system.

- **Domains**

  A list of the domains within the organization that the user can manage. You can assign domains to roles or to users. The user can administer messages to or from the configured domain or domains only, and reports that a user generates relate only to the configured domains.

If you do not configure any domains, the user is able to manage all domains configured in the Policy Editor’s SMTP Properties configuration.

Editing a user

Clicking on the name of a user in the list will show the **Edit User** screen where you can configure the following details for the chosen user:

- **User Details**
  - **Name**: This is the account name. It is displayed in the left-hand column in the **Manage Users** page, and is used to log on to MIMEsweeper for SMTP. The user name is not case sensitive.
  - **Description**: Enter some text to describe the user.
  - **Email address:** The email address for this user.
  - **Phone Number:** The telephone number for this user.
  - **Locality:** The physical location of this user in your organization (for example, the Paris office).

  Change Password: Clicking this button allows you to enter a new administrator assigned password for the user.

  Select one or more of the following options to secure the user account:

  - **User must change password at next logon:** The user must change the administrator-assigned password to one of their own choosing the next time they log on to the system.

  - **User cannot change password:** The user cannot change the administrator-assigned password. This option is typically used for user accounts to be shared among several people, to prevent one user from locking out other users.
  - **Account is disabled:** The user account is disabled to prevent the user logging on to the system. The default Administrator user account cannot be disabled.
- **Roles**

  A list of the roles available on the system is shown, and you can optionally assign this user to one or more of these.

  - The left-hand pane lists roles which the user is currently assigned to.
  - The right-hand pane lists all available roles.
  - To assign a user to a role, highlight the role in the right-hand pane, and click **Add**.
  - To remove a user from a role, highlight the role in the left-hand pane and click **Remove**.

For details, see *Role properties* on page 12-10. For details on creating and configuring user accounts, see the MIMEsweeper Manager help.

- **Domains**:

  Add or remove the domains that a user can manage. Leave the **Selected Domains** field empty if the role can manage all configured domains.

  The domains assigned at the user level are additional to domains assigned at the role level. That is, the user can administer domains assigned at the user level in addition to those defined at the role level. See *Domains* on page 12-11 for more information.

Roles

A role defines a group of users who share a common function in your organization, such as policy administrators or network managers, to whom you can explicitly allow or deny access to specific areas of MIMEsweeper for SMTP. A role provides a convenient way of setting access permissions for a number of users simultaneously. For example, you could create a role for maintaining review areas and then grant access to review areas to that role only. Any individual users who are members of that role would then have permission to access and manage review areas.

Users can be assigned more than one role, but a role cannot include another role. Roles cannot be used to log on to MIMEsweeper for SMTP.

Default roles

A number of default roles are provided as part of a MIMEsweeper for SMTP installation. Table 12-1 lists and describes the default roles.

Table 12-1: Default roles

Role	Permissions
Domain Mail Administrator	Access and manage messages sent to or received from a specific domain or domains within the organization.
MIMEsweeper Administrator	Access-all-areas. Allowed to perform all tasks associated with both the MIMEsweeper Manager and the Policy Editor.
Help Desk Operator	Able to view mail and manage queues. Also has basic access to other parts of the system.
Network Administrator	Allowed to configure the network elements of the system. Can manage queues, configure auditing and restart services.
Network Operator	Very basic access to the system. Allowed to access and manage the queue areas.
Security Manager	Full access to the Security Center. Able to define users and roles and assign access rights.
Policy Administrator	Full access to the Policy Editor. Able to view all areas within the Policy Editor, make amendments and save and apply changes.

These roles could be used in combination to define the required access to the system. For example a user could belong to both the Operator and the Message Administrator roles. They would then have full access to the Message Center and restricted access (view only) to the rest of the system.

You can modify these default roles and create new roles to meet your organization’s requirements. For details, see *Role properties* on page 12-10. Each of these default roles is automatically assigned access permissions to the relevant folders in the Message Center. The access the default roles have is outlined in Table 12-2.

Role properties

In addition to the default roles you can create as many new roles as you require to meet your organization’s requirements. Only a user who has permissions to Configure Security Center can create new roles.

You create and manage roles in the Manage Roles page of Security Center, accessed by clicking the **Manage Roles** button on the Security Center Home Page.

The Manage Roles page shows the name and a description of each role. To filter the list, click the initial letter of the required role in the index list to the right of the **Add** button.

Add a role

To add a new role, click **Add Role** in the **Manage Roles** page, which opens the **Add Role** page.

- **Name:** A name for the role. This name is displayed in the left-hand column in the Manage Roles window of Security Center.
- **Description:** A brief description about the role (for example, you may wish to describe which aspects of the system the role is to be allowed or denied to configure or manage). This text is displayed in the right-hand column in the Manage Roles window of Security Center.

  Click **Add**. You are returned to the **Manage Roles** page and the role is added to the list

Configure a role

You can edit the following details in the **Edit Role** page of Security Manager, by clicking on the name of the role in the **Manage Roles** page:

- **Name**: Replace or edit the existing name as required.
- **Description:** Replace or edit the existing description as required.
- **Domains**: Add or remove the domains that a role can manage. Leave the **Selected Domains** field empty if the role can manage all configured domains. See *Domains* on page 12-11 for more information.

  Click **Save**. You return to the **Manage Roles** page where the role is updated in the list.

For details on creating and configuring user accounts, see the MIMEsweeper Manager help.

Once you have created a role, you can assign individual users as members of the role. You can then assign access permissions for the role to enable its members to access specific messages areas in the Message Center.

Domains

You can restrict the messages that a user or a role can manage. The domains available for selection are those configured in the Policy Editor's **SMTP Relay, Properties**, **Domain** configuration. You can assign domains to roles or to users.

When you assign a domain or domains, the user can administer messages to or from the configured domain or domains only, and reports that a user generates relate only to the configured domains.

ℹ If you do not configure any domains, the user or role is able to manage all domains configured in the Policy Editor's SMTP Properties configuration.

Permissions

Clicking on **Permissions** in the Security Center Home Page will display the **Permissions** page. This is divided into two sections: the left-hand side displays a tree of all securable items in MIMEsweeper, while the right-hand side shows a list of roles and users for MIMEsweeper Manager applicable to any item highlighted in the tree on the left.

You use this page to control access to the various features of the MIMEsweeper Manager and MIMEsweeper Policy Editor.

Highlighting an item in the tree will display the following:

- **Type**: An icon indicating a user 👤 or a role 👥.
- **Name**: The name of the roles currently applied to the item.
- **Access Scope**: The level that the permissions are defined at.

Available access permissions

You can assign permissions to default or user-defined users and roles to allow or deny access to areas of MIMEsweeper for SMTP. For example, you could create a role for maintaining review areas and then grant access to review areas to that role only. The default Administrator super-user has full access to all policy and management capabilities.

Access permissions for default roles

MIMEsweeper for SMTP has the following default roles: MIMEsweeper Administrator, Help Desk Operator, Network Administrator, Network Operator, Security Manager and Policy Administrator.

Each of the default roles is automatically assigned access permissions to the relevant areas and features in MIMEsweeper for SMTP. Table 12-2 shows the default access permissions for these. The roles are listed on the top, with the areas which are allowed or disallowed access shown on the left hand side.

Table 12-2: Default Roles Access

	MIMEsweeper Administrator	Help Desk Operator	Network Administrator	Network Operator	Security Manager	Policy Administrator
Access MIMEsweeper Manager	Allow	Allow	Allow	Allow	Allow	Allow
Access Message Center	Allow	Allow	Allow	Allow	Allow	Allow
Configure PMM	Allow	-	Allow	-	-	Allow
Access Images	Allow	Allow	-	-	-	Allow

Table 12-2: Default Roles Access

	MIMEsweeper Administrator	Help Desk Operator	Network Administrator	Network Operator	Security Manager	Policy Administrator
Configure Images	Allow	-	-	-	-	Allow
Access Message History	Allow	Allow	-	-	-	-
Access View	Allow	Allow	-	-	-	-
Execute Batch Jobs	Allow	-	-	-	-	-
Modify View	Allow	-	-	-	-	-
Access Message	Allow	Allow	-	-	-	-
View Message Body	Allow	Allow	-	-	-	-
List Attachments	Allow	Allow	-	-	-	-
Open Attachments	Allow	Allow	-	-	-	-
Release Message	Allow	Allow	-	-	-	-
Forward Message	Allow	Allow	-	-	-	-
Export Message	Allow	-	-	-	-	-
Delete Message	Allow	-	-	-	-	-
Reprocess Message	Allow	-	-	-	-	-
Set Message Expiry	Allow	-	-	-	-	-
Non-deliver Message	Allow	-	-	-	-	-
Access Queue View	Allow	Allow	Allow	Allow	-	-
Modify Queue View	Allow	-	Allow	-	-	-
Manage Queues	Allow	Allow	Allow	Allow	-	-
Retry Delivery	Allow	Allow	Allow	Allow	-	-
Non-deliver	Allow	Allow	Allow	Allow	-	-
Track Messages	Allow	Allow	-	-	Allow	-

Table 12-2: Default Roles Access

	MIMEsweeper Administrator	Help Desk Operator	Network Administrator	Network Operator	Security Manager	Policy Administrator
Configure Tracking	Allow	-	Allow	-	-	-
Access Report Center	Allow	Allow	Allow	-	-	-
Configure Report Center	Allow	-	Allow	-	-	-
Access System Center	Allow	Allow	Allow	-	-	-
Control Services	Allow	-	Allow	-	-	-
Access Security Center	Allow	-	-	-	Allow	-
Configure Security Center	Allow	-	-	-	Allow	-
Access System Health	Allow	Allow	Allow			
Access Policy Editor	Allow	-	-	-	-	Allow
Configure Policy Editor	Allow	-	-	-	-	Allow

Access permissions inheritance

A lower-level folder located beneath a higher-level folder in **Securable items** automatically inherits the access permissions from its higher-level folder unless they are explicitly over-ridden. This means that you can specify security settings for all folders in **Securable items** by assigning access permissions for the top-level folder. However, if you explicitly assign access permissions to a sub folder, they override the permissions assigned for the top-level folder. The **Allow** or **Deny** check boxes are dimmed for permissions that are inherited from higher level folders.

MIMEsweeper for SMTP determines a user's access to a folder in **Securable items** as follows:

1. MIMEsweeper for SMTP checks the current folder for explicit access permissions assigned for the user.
2. MIMEsweeper for SMTP then checks the current folder for explicit **Allow** access permissions assigned for any of the roles of which the user is a member.
3. MIMEsweeper for SMTP then checks the current folder for explicit Denied access permissions assigned for any of the roles of which the user is a member.
4. If after checking the entire tree and finding that no explicit permissions have been assigned, access would be denied.

Understanding this evaluation order will help you to make effective use of the **Securable items** in assigning access permissions and provide you with greater control over the security of your system.

This hierarchical relationship for the selected role is shown on the **Change Permissions** page, and is also shown in the **Access Scope** column on the **Permissions** page.

By default, access is denied if a permission has not been explicitly set. Therefore **Deny** is only required when overriding an inherited **Allow**.

Assigning access rights

You assign access permissions to a user or role for any item shown in the tree in the **Permissions** page. You assign access permissions to any default or user-defined users or roles (other than the default Administrator role, which always has full rights to all areas).

If a user has conflicting access permissions arising from membership of different roles, the system resolves this by ensuring that **Deny** access takes priority over **Allow** access. Additionally, user access permissions override role access permissions.

Change Permissions

To change the permissions for a securable item select the item and click **Change Permissions** in the **Permissions** page. This will display the **Change Permissions** page.

A list of the roles / users available on the system is shown, and you can optionally assign or remove one or more of these from the item previously selected.

- The left-hand pane lists roles / users which are currently assigned.
- The right-hand pane lists all available roles.

To add a specific role or user to the **Selected Roles/Users** lists, highlight it in the **Available Roles/Users** list and click **Add.**

To remove a particular role or user from the **Selected Roles/Users** lists, highlight it and click **Remove.**

To set or modify permissions for a particular role or user, highlight it in the **Selected Roles/Users** list and use the check boxes below the list titled **Allow** and **Deny.** Select or clear these as appropriate.

Click **Save** when all of the required changes have been made.

You can only remove a role or user if it has been defined at the level you are viewing and is not inherited from a higher level.

For details on how to assign access rights to a user or role, see the MIMEsweeper Manager help.

Part III

Appendices

APPENDIX A

Auto-responders

This appendix provides examples of how you can configure a policy to have MIMEsweeper for SMTP provide automatic responses to email messages.

The information in this appendix supplements the information in Chapter 4 on configuring email policies using scenarios.

You do not need to create auto-responders unless they are specifically required. This information is provided for users who want to configure MIMEsweeper for SMTP to send automatic responses to email messages.

Overview

You can configure a policy to provide automatic responses to email messages. This type of policy is called an auto-responder.

Example auto-responders

The examples in this appendix show how you can use an auto-responder to automatically send a response email message to:

- **Acknowledge receipt of the original message**

  This type of auto-responder would be useful, for example, for an organization that has an email address for its Support group (for example, `support@inside-yourcompany.com`). The organization could create an auto-responder to automatically send:

  – A reply to a customer who had sent an enquiry to the Support group. This reply could assure the customer that their message had been received and would be followed up. It also could include additional information like contact numbers, web addresses, and technical information.

  – A message to one or more individual Support group engineers. This message could ask the engineer to follow up on the customer's enquiry within 24 hours. The message would not need to include the customer's original message as an attachment, as the engineer could view the message in the Support group email account.

- **Provide a contextual response to a question in the original message**

  This type of auto-responder would be useful, for example, for an organization that has a number of standard responses for common questions sent to an email address for its Customer Services group (for example, `info@inside-yourcompany.com`). The organization could create an auto-responder to automatically:

  – Analyze the contents of a message to identify phrases used in common questions and reply with the appropriate, standard text. For example, if an email contained a question, such as "What is your address?", the auto-responder could return to the sender the original message with an attachment containing the organization's address.

These example auto-responders are described in the following sections.

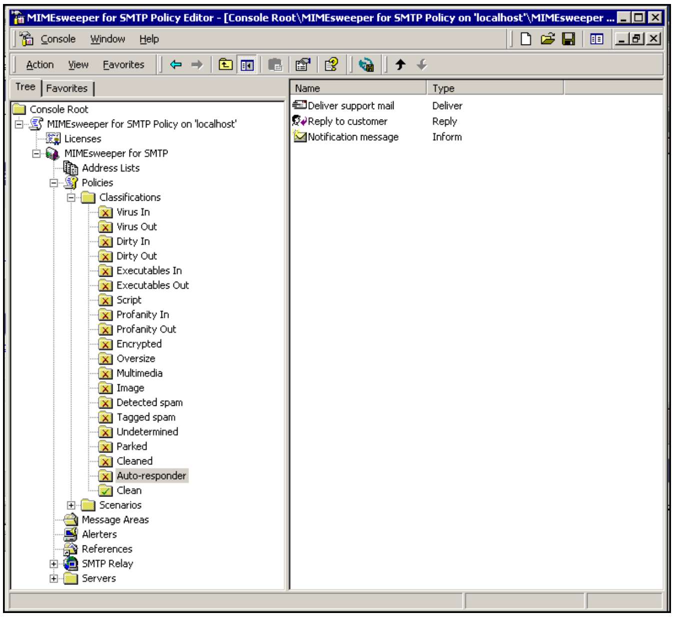
Auto-responder acknowledging message receipt

To create an auto-responder acknowledging receipt of a message:

1. Create an exclusive classification. You will use this classification to specify how MIMEsweeper for SMTP should process messages that match the scenario you associate with this classification. For information about classifications, see Chapter 3.

2. Create a new Deliver action for the classification. This action delivers incoming mail to the Support address (`support@inside-yourcompany.com`). For information about actions, see Chapter 3.
3. Create a new Reply action for the classification. This action sends a reply message to any email message sent to the Support group address. You specify the text of the reply message in this action. You can use tokens, for example, using `%SUBJECT%` will include the subject line of the original message. For information about actions, see Chapter 3. For information about tokens, see Appendix I.
4. Create a new Inform action for the classification. This action sends a new message to the individuals specified in the **To** field. MIMEsweeper for SMTP address lists are not supported in the recipient field for Inform actions. You must specify each recipient individually. You also specify the text of the message to be sent to individual support engineers in this action. You can use tokens such as `%SUBJECT%` to include the subject line of the original message, %DATE% to include the date the original message was sent, and `%SENDER%` to include the email address of the sender of the original message. For further information about tokens, see Appendix I.

   Figure A-1 shows a classification named **Auto-responder** with Deliver, Reply, and an Inform actions defined.



Name	Type
Deliver support mail	Deliver
Reply to customer	Reply
Notification message	Inform

Figure A-1: Auto-responder classification and actions

5. Under the **Incoming** scenario folder, create a new scenario subfolder. Include in the route for this folder the address specifications to which your classification should be applied. The address specification for the **Auto-responder** scenario folder in this example is shown in the following table.

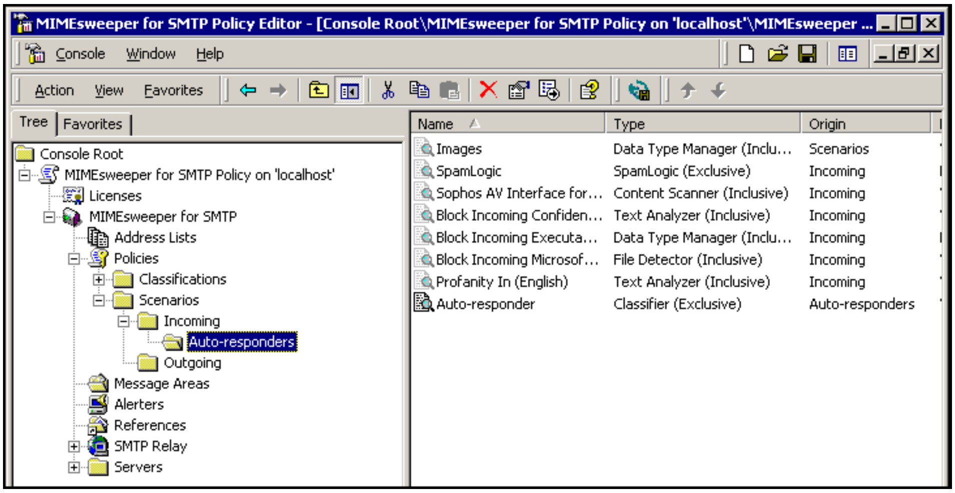
Route	Address list	Address specification
Sender	Everyone	*@*
Recipient	Support	support@inside-yourcompany.com

Remember that due to inheritance, this subfolder will inherit the scenarios defined in the **Incoming** scenario folder unless set their Enabled state to **No** in this **Auto-responders** subfolder or in the **Incoming** folder. For information about scenario folders and scenario folder inheritance, see Chapter 2.

6. In the new scenario subfolder, create a new Classifier scenario. A Classifier scenario provides a means of classifying email messages that match a particular sender/recipient route, so you can dispose of it according to the actions you specify in the associated classification.

Set the scenario's enabled and overridable states to **Yes**, and associate the scenario with your new Auto-responder classification. For information about the Classifier scenario, see Chapter 4. If you have created an exclusive scenario using the properties page rather than a wizard, see the ReadMe release document on the MIMEsweeper for SMTP CD-ROM.

Figure A-2 shows a scenario folder named **Auto-responders** containing a Classifier scenario named **Auto-responder**.



MIMEsweeper for SMTP Policy Editor - [Console Root\MIMEsweeper for SMTP Policy on 'localhost'\MIMEsweeper ...

- Console Root
  - MIMEsweeper for SMTP Policy on 'localhost'
    - Licenses
    - MIMEsweeper for SMTP
      - Address Lists
      - Policies
        - Classifications
        - Scenarios
          - Incoming
            - Auto-responders
          - Outgoing
      - Message Areas
      - Alerters
      - References
      - SMTP Relay
      - Servers

Name	Type	Origin
Images	Data Type Manager (Inclu...	Scenarios
SpamLogic	SpamLogic (Exclusive)	Incoming
Sophos AV Interface for...	Content Scanner (Inclusive)	Incoming
Block Incoming Confiden...	Text Analyzer (Inclusive)	Incoming
Block Incoming Executa...	Data Type Manager (Inclu...	Incoming
Block Incoming Microsof...	File Detector (Inclusive)	Incoming
Profanity In (English)	Text Analyzer (Inclusive)	Incoming
Auto-responder	Classifier (Exclusive)	Auto-responders

Figure A-2: Auto-responders scenario subfolder and scenario

If you subsequently create a scenario subfolder for the **Auto-responder** scenario subfolder, remember that this new subfolder will inherit the **Auto-responder** scenario. That means that customers and Support engineers specified in this new subfolder will be sent replies and inform messages intended for addressees specified in the **Auto-responder** scenario subfolder.

If this is not appropriate, ensure that the Classifier scenario in the **Auto-responders** subfolder is not enabled in the new subfolder.

Auto-responder containing a contextual response

To create an auto-responder containing a contextual response to a message:

1. Create an exclusive classification. You will use this classification to specify how MIMEsweeper for SMTP should process messages that match the scenario you associate with this classification. For information about classifications, see Chapter 3.
2. Create a new Deliver action for the classification. This action delivers incoming mail to the Customer Services address (`info@inside-yourcompany.com`). For information about actions, see Chapter 3.
3. Create a new Inform action for the classification. This action sends a new response message to the sender, attaching the response to their questions.

   In the **To** field, specify the `%SENDER%` token. In the **From** field, specify the appropriate address, in our example, this is `info@inside-yourcompany.com`. You can use other tokens such as `%SUBJECT%` to include the subject line of the original message. In the **Body** text field, type in some text, for example:

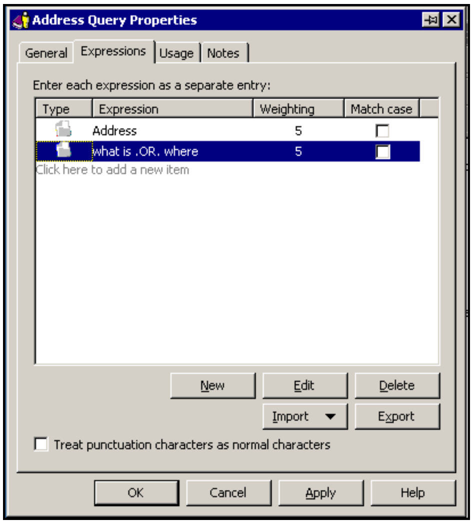
   ```
   "The intended recipient has received your message. Meanwhile, an automated
   response is attached to the message."
   ```

   Then select the option to forward attachments as modified by MIMEsweeper for SMTP.

   For further information about the Inform action, see Chapter 3. For information about tokens, see Appendix I.

4. In the **References** folder create an Expression List specifying the text to scan the message for.

   Figure A-3 shows an example Address Query Expression List, which is configured to look for phrases like “What is your address?” or “Where is your office?”.



Enter each expression as a separate entry:

Type	Expression	Weighting	Match case
	Address	5	□
	what is .OR. where	5	□

Click here to add a new item

□ Treat punctuation characters as normal characters

Figure A-3: Address Query Expression list

   Create as many Expression Lists as you need to identify the words or phrases in questions you intend to provide automatic replies for. For further information about Expression Lists used in References, see Chapter 2.

5. Under the **Incoming** scenario folder, create a new scenario subfolder. Include in the route for this folder the address specifications to which your classification should be applied. The address specification for the **Auto-responder** scenario folder in this example is shown in the following table.

Route	Address list	Address specification
Sender	Everyone	*@*
Recipient	Customer Services	info@inside-yourcompany.com

   Remember that due to inheritance, this subfolder will inherit the scenarios defined in the **Incoming** scenario folder unless you set their enabled state to No in this **Auto-responders** subfolder or in the **Incoming** folder. For information about scenario folders and scenario folder inheritance, see Chapter 2.

6. In the new scenario subfolder, create a separate Commercial Disclaimer scenario for each type of request for information for which you want to provide a standard response. A Commercial Disclaimer scenario scans the content of an email message and adds text to those containing specified words or phrases.

   For each Commercial Disclaimer scenario you create, set the enabled and overridable states to **Yes**. Specify the appropriate Expression list, search and proximity thresholds, and areas to scan. In the **Disclaimer** tab, type the text to be included in the automated response.

   For further information about the Commercial Disclaimer scenario, see Chapter 4.

7. In the scenario subfolder, create a new Classifier scenario. A Classifier scenario provides a means of classifying email messages that match a particular sender / recipient route, so you can dispose of it according to the actions you specify in the associated classification.

   Set the scenario’s enabled and overridable states to **Yes**, and associate it with your new Auto-responder classification. For information about the Classifier scenario, see Chapter 4. (If you have created an exclusive scenario using the properties page rather than a wizard, see the ReadMe release document on the MIMEsweeper for SMTP CD-ROM.)

   ℹ If you subsequently create a scenario subfolder for the **Auto-responder** scenario subfolder, remember that this new subfolder will inherit the **Auto-responder** scenario. This means that automatic replies will be sent for messages containing words and phrases in the specified Expression Lists.

   If this is not appropriate, ensure that the Classifier scenario in the **Auto-responders** subfolder is not active or enabled in the new subfolder.

APPENDIX B

Data Types

This appendix lists the data types and subtypes that MIMEsweeper for SMTP can detect when processing email messages based on data type recognition scenarios.

Overview

You can configure the data types and subtypes that MIMEsweeper for SMTP detects in email messages during processing. You can configure data type detection in the following data type recognition scenarios:

- Attachment Manager
- Commercial Disclaimer
- Content Scanner
- Data Type Manager
- Executable
- Reclassifier
- Text Analyzer
- Virus Manager

For details of these scenarios, see Chapter 4.

Specifying data types in scenarios

You can configure the data types and subtypes that you want MIMEsweeper for SMTP to detect, and optionally remove, when you are creating a new data type recognition scenario. You can change the configuration in the **Data Types** tab in the properties page for an existing scenario.

You can specify the following data types, their subtypes, and protection types:

- Binary
- Container
- Document
- Executable
- Image
- Multimedia
- PKCS

Selected data types and protection types are checked. If some, but not all, subtypes of a data type or protection type are selected, the check box for the format is dimmed.

You can specify options to control the way selected data types are processed:

- **Include all data types**

  The scenario processes messages containing all data types and subtypes. All data types and subtypes in the list, as well as any unrecognized data types, are processed.

- **Include selected data types**

  The scenario processes messages containing only the data types and subtypes selected in the list. No other data types or subtypes are processed.

- **Exclude selected data types**

  The scenario processes messages containing all data types and subtypes except those selected in the list. All other data types (that is, those that are not selected in the list as well as any unrecognized data types that do not appear in the list) are processed.

For information on specifying data types in a data type recognition scenario, see the MIMEsweeper Policy Editor help.

List of data types

Table B-1 shows the recognized data types and subtypes that you can select in scenarios that support the detection (and optional removal) of specified data types.

Table B-1: Data types and subtypes

Recognized data types and subtypes
Binary
Any binary format file
Container
ALSI protected documents
Apple Single
BZIP
Compressed archive file (ZIP)
LH ARC compresses archive (LZH)
Macintosh representation of a binary file using only printable characters (BINHEX)
Microsoft Cabinet compressed file (CAB)
Microsoft Compress
Microsoft Outlook Document (MSG)
Microsoft Transport Neutral Encoding Format (TNEF), used by Microsoft email clients when sending rich text messages
NEC infoCage protected format
PGP encrypted file (PGP)
PKware ZIP compressed archive
Pointsec encrypted files
Possible InstallShield

Table B-1: Data types and subtypes

Recognized data types and subtypes
Privacy Enhanced Mail (PEM)
RAR compressed archive (RAR)
Red Hat Package Manager (RPM)
Robert Jung ARJ compressed archive (ARJ)
Simple Mail Transfer Protocol message (SMTP)
Tape Archive (TAR)
UNIX compressed file (CMP)
UNIX Gzip compressed file (GZP)
UUEncoded file (UUE)
Windows Installer file (MSI)
Document
Adobe Portable Document Format file (PDF)
Apple Double Resource Fork
Compound Document Architecture file (CDA)
Electronic Facsimile (DCX)
Embedded OLE Object
Embedded OLE Package
HTML ActiveX Object
HTML encoded within RTF (HTML)
HTML with script (HTML
Hypertext Markup Language file (HTML)
Ichitaro document (JTD)
Lotus 1-2-3 file (123)
Microsoft Excel Spreadsheet (XLS)
Microsoft Office Embedded Objects
Microsoft Office editdata.mso
Microsoft Outlook file attachment
Microsoft PowerPoint Presentation (PPT)
Microsoft Project file (MPP)
Microsoft Visio document (VSD)
Microsoft Word Document (DOC)

Table B-1: Data types and subtypes

Recognized data types and subtypes
Open Office Calc Document (ODS)
Open Office Chart
Open Office Graphic Document (ODG)
Open Office Impress Document (ODP)
Open Office Master Document (ODM)
Open Office Math Document (ODF)
Open Office Writer Document (ODT)
Open Package Convention
Pattern Matched
Pretty Good Privacy Message (PGP) Message
Privacy Enhanced Mail (PEM)
Rich Text Format file (RTF)
Text file (TXT)
XML Document (XML)
Executable
DOS executable file (EXE)
Executable and Linkable Format (ELF)
Java executable file (JAVA)
Microsoft Office Embedded Objects
Win31 executable file (EXE)
Win32 executable file (EXE)
Win32 Library executable file (DLL)
Win32 Unknown executable file
Image
Autodesk Animator file (FLI)
Autodesk AutoCAD Drawing Exchange Format file (DXF)
Autodesk AutoCAD Drawing file (DWG)
Dr Halo Picture File (PIC)
Graphic Interchange Format file (GIF)
Icon (ICO)
Initial Graphics Exchange Specification (IGES)

Table B-1: Data types and subtypes

Recognized data types and subtypes
JPEG image file (JPEG)
Paint Shop Pro image file (PSP)
Portable Bitmap (PBM)
Portable Network Graphic file (PNG)
Portable Pixel Map (PPM
StarView Metafile (SVM)
Tagged Image File Format file (TIFF)
Windows Bitmap (BMP)
Windows Cursor (CUR)
Windows Meta File file (WMF)
Word Perfect Graphic (WPG)
ZSoft picture file (PCX)
Mulitimedia
3GP Multimedia
Advanced System Format (ASF)
Audio Interchange File file (AIF)
Advanced Systems Format (ASF)
Creative Voice file (VOC)
Flash video (FLV)
Free Lossless Audio Code (FLAC)
Google video (GVI)
Macromedia Flash (SWF)
Microsoft Audio/Video Interleaved format file (AVI)
Microsoft Wave file (WAV)
MIDI file (MIDI
Monkey’s Audio (APE)
MP3 sound file (MP3)
MP4 Audio
MPEG Movie file (MPEG)
Ogg Vorbis Compressed Audio File
PlayStation Portable Multimedia

Table B-1: Data types and subtypes

Recognized data types and subtypes
Quick Time Movie file (QTM)
RealMedia Audio file (RA)
RealMedia Movie file (RM)
Sun Sound File (AU)
PKCS
Opaque Signed Message
Signature of Clear Signed Message
Scripts
Javascript
Javascript Encoded
Unknown Script
VBScript
VBScript Encoded

APPENDIX C

File Formats

This appendix describes the format of configuration files that you can import into or export from MIMEsweeper for SMTP. You can import or export these configuration files between different versions of MIMEsweeper for SMTP.

Overview

The import/export configuration files are generated by the Policy Editor and should not be modified by the administrator. The following types of configuration files can be imported or exported from MIMEsweeper for SMTP:

- Address safe list files
- Alias files
- Banned address list files (import only)
- Banned host files (import only)
- File signature files
- Manual address list files (import only)
- Routing files
- Reference files

Do not edit any MIMEsweeper configuration files directly. Use the Policy Editor in the MIMEsweeper for SMTP Console to configure your email policies.

These import/export configuration files are described in the following sections. The sections are listed in alphabetical order.

Address safe list files

A safe list file is either an ASCII text file or a Unicode format file that contains one or more address entries specified in the standard email address format.

An address list file contains entries in the following format:

```
user@location
```

Each address must be on a separate line ending with a Carriage Return / Line Feed (CR / LF).

Figure C-1 shows entries in an example address list file.

```
amy@inside-yourcompany.com
debbie@inside-yourcompany.com
philip@inside-yourcompany.com
```

Figure C-1: Address safe list file example

Alias files

An alias file is a Unicode format file that contains one or more entries that map an existing email address (or group of addresses) to another. If you try to load an alias file in ASCII format, an error is generated.

An alias file contains entries in the following format:

```
[Alias]
alias_name=”source address”,”target address”
```

Each alias name must be on a separate line ending with a Carriage Return / Line Feed (CR / LF).

Figure C-2 shows an example alias file that directs all messages for `andy@inside-yourcompany.com` to `jean@inside-yourcompany.com`.

```
[Alias]

AndyToJoe=”andy@inside-yourcompany.com”,”jean@inside-yourcompany.com”
```

Figure C-2: Alias file example

You can import or export an alias file from the **Aliases** folder under the **SMTP Relay** folder in the Policy Editor. For details on aliases, see Chapter 6 and the MIMEsweeper Policy Editor help.

You can experience browser display problems when using Unicode. These result from the level of Unicode support required between browsers, and the absence of fonts installed on the machine.

Banned address list files (import only)

A banned address list file is either an ASCII text file or a Unicode format file that contains one or more address entries specified in the standard email address format.

A banned address list file contains entries in the following format:

```
user@location
```

Each address must be on a separate line ending with a Carriage Return / Line Feed (CR / LF).

Banned host files (import only)

A banned host list file is either an ASCII text file or a Unicode format file that contains one or more host entries specified in the standard email address format.

A banned host list file contains entries in the following format:

```
domainname
```

Each host must be on a separate line ending with a Carriage Return / Line Feed (CR / LF).

File signature files

A file signature file is a Unicode format file that contains details of the offset and byte pattern for one or more file types. If you try to load an alias file in ASCII format, an error is generated.

A file signature file contains entries in the following format:

```
[File Signature]
Description=file type
Pattern=”offset”,”byte pattern”
```

Each pattern must be on a separate line ending with a Carriage Return / Line Feed (CR / LF).

Figure C-3 shows an example file signature file that contains the byte pattern for Windows help files.

```
[HLPfiles]

Description=Windows Help (hlp) files
Pattern=”0”,”63,95,3,0”
```

Figure C-3: File signature file example

You can import a file signature file from either your PC or the MIMEsweeper website when you are creating a new Pattern Matcher scenario. You can export a file signature file from the **File Signature** tab in the properties page for a Pattern Matcher scenario. For details on the Pattern Matcher scenario, see Chapter 4 and the MIMEsweeper Policy Editor help.

Manual address list files

A manual address list file is either an ASCII text file or a Unicode format file that contains one or more address entries specified in the standard email address format.

An address list file contains entries in the following format:

```
user@location
```

Each address must be on a separate line ending with a Carriage Return/Line Feed (CR/LF).

Figure C-4 shows entries in an example address list file.

```
amy@inside-yourcompany.com
debbie@inside-yourcompany.com
philip@inside-yourcompany.com
```

Figure C-4: Address list file example

You can import address entries when you create a new address or when you change the properties of an existing address list in the **Address Lists** folder under the Policy Editor. You cannot export an address list. For details on manual and LDAP address lists, see Chapter 2 and the MIMEsweeper Policy Editor help.

Imported address list files are not limited by size, but they may generate large configuration files. If file size is an issue, consider using LDAP address lists.

Routing files

A routing file is a Unicode format file that specifies the delivery paths the Delivery services uses to direct incoming and outgoing messages. If you try to load a routing file in ASCII format, an error is generated.

A routing file contains entries in the following format:

```
[Routing]
route=”domain mask”,”route type”,”host”,”target socket”,”preference”
```

where:

- `route` is the display name of the route as it appears in the details pane when the **Routing** folder under the **SMTP Relay** folder is selected.
- `domain mask` is the domain to which the route applies.
- `route type` is:
  - 0 for Additional route
  - 1 for Forced route
  - 2 for Default route
- `host` is the host name or IP address of the host machine for the domain.

- `target socket` is the TCP/IP port to be used.
- `preference` is the MX preference value, and would only be used for **Additional** routes

Each route must be on a separate line ending with a Carriage Return/Line Feed (CR/LF).

Figure C-5 shows an example entry for a forced route for the domain address `inside-yourcompany.com`. All incoming mail is sent to the machine called `gateway`.

```
[Routing]
Conga=”inside-yourcompany.com”,”1”,”gateway”,”25”,”0”
```

Figure C-5: Routing file example

You can import or export a routing file in the **Routing** folder under the **SMTP Relay** folder in the Policy Editor. For details on routing, see Chapter 6 and the help.

You can experience browser display problems when using Unicode. These result from the level of Unicode support required between browsers, and the absence of fonts installed on the machine.

Reference files

A reference is a file that contains common text, as in expression and script lists, or checksums to be used during analysis.

The following types of reference files are used in MIMEsweeper for SMTP:

- Expression lists
- Checksum lists
- Script lists

You can import or export expression list files in the **References** folder under the Policy Editor. For details on expression lists, see Chapter 5 and the MIMEsweeper Policy Editor help.

Expression lists

An expression list file is a XML format file that contains a list of keywords and phrases, referred to as expressions. If you try to load an expression list file in ASCII format, an error is generated.

There are two types of expression list used in MIMEsweeper:

- Managed expression lists - maintained on the MIMEsweeper server, and updated regularly as expressions are added.
- User-defined expression lists - created and maintained by the user.

Checksum lists

The checksum of a file provides an almost unique identifier of that file. Each checksum included in the list consists of a unique 32 digit hexadecimal value.

There are two types of checksum list used in MIMEsweeper:

- Managed checksum lists - maintained on the MIMEsweeper server, and updated regularly as checksums are added.
- User-defined checksum lists - created and maintained by the user.

Script lists

The script lists contain scripts, together with the relative vale of each entry, used during script analysis.

There are two types of script list used in MIMEsweeper:

- Managed script lists - maintained on the MIMEsweeper server, and updated regularly as scripts are added.
- User-defined script - created and maintained by the user. Any expressions created must contain US-ASCII characters only.

APPENDIX D

IMAGEmanager

This appendix describes how you can use MIMEsweeper for SMTP’s built-in IMAGEmanager tool to help protect your organization from the distribution of unacceptable images.

Introduction

MIMEsweeper for SMTP 5.3 includes the built-in IMAGEmanager tool for analyzing image files to identify potentially unacceptable images and prevent their distribution.

You use the IMAGEmanager scenario to configure IMAGEmanager according to your organization's security policy. The IMAGEmanager scenario is inclusive, allowing you to create more than one IMAGEmanager scenario in the same folder, if required. For example, you can create specific scenarios for different file types.

The policy classification you use for unsuitable images that IMAGEmanager detects can include actions to delete the images and notifications to inform a specified recipient of detected messages.

How IMAGEmanager works

IMAGEmanager not only processes images directly attached to emails. MIMEsweeper for SMTP recursively disassembles attached documents to extract embedded images to pass to IMAGEmanager for processing. For example, if an email has an attached Microsoft Office document containing images, IMAGEmanager can scan the embedded images.

IMAGEmanager does not process Class 4 TIF files. These files are generally black-and-white images, for example fax pages.

IMAGEmanager analyzes each image as follows:

1. It checks the image to determine whether it meets the process criteria (image type, size) specified in the active IMAGEmanager scenario.
2. It checks the hash ("fingerprint") of the image against those in the pre-classified image database. This is a database of known acceptable and unacceptable image hashes that you build up for your organization. Each entry is pre-classified as acceptable or unacceptable.
3. If the image fingerprint is present in the pre-classified image database, IMAGEmanager accepts the associated pre-classification for that image. Step 4 is not required, saving time and processing power.
4. If the image is not pre-classified, IMAGEmanager scans the image to extract information about the presence of flesh tones and many other features. IMAGEmanager compares the extracted information with its built-in image feature database. This contains values for the features of thousands of categorized images. IMAGEmanager compares the features of the image being processed with the feature database, and finds the closest matches, or nearest neighbors, and their image classifications. If the Face Detection option is enabled, the comparison takes into account the extra information provided by this option. IMAGEmanager then uses the configured confidence level to determine whether to categorize the image as acceptable or unacceptable.

5. For messages containing one or more images it has identified as unacceptable, IMAGEmanager matches the policy classification to the message. If this is the highest priority classification, the classification's actions are performed, typically resulting in the message being quarantined.

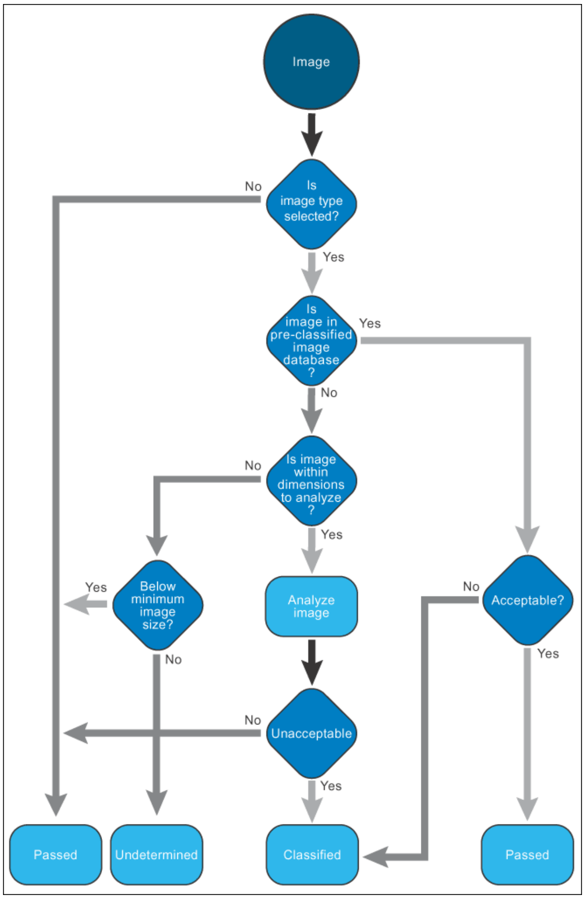


Figure D-1: How IMAGEmanager analyzes an image

The Pre-Classified Image Database

Use the pre-classified image database to identify known acceptable and unacceptable images for your organization.

For example, if an email contains an image as a file attachment that you know to be unacceptable, you can add this image to the preclassification database, and classify it as an unacceptable image. The pre-classified images are used to correct, refine and extend IMAGEmanager's automatic image analysis algorithms.

Adding known images to the pre-classified image database improves throughput, as the time it takes to compare hashes of images to hashes in the database is hundreds of times faster than full image analysis.

MIMEsweeper needs only a hash of the image in the pre-classified image database. The hash is like a fingerprint: it is unique to the image. The original image is not stored, since the hash contains enough information to identify the image, however you can optionally store a thumbnail to aid management.

Images that you should add to the pre-classified image database include:

- Images that IMAGEmanager incorrectly identifies as unacceptable.
- Images that cannot be correctly classified by the image analysis algorithm, such as confidential company images.
- Common images seen at the gateway, such as logos and banners that are known to be acceptable and do not need to be processed by IMAGEmanager each time they are seen.

The pre-classified image database is managed from MIMEsweeper Manager's Message Center. For information on managing the database, see the MIMEsweeper Manager help.

Detection rates

The identification of unacceptable images through image processing is not an exact science, and the categorization of an image is inevitably subject to a degree of uncertainty. In order to maximize the probability of detecting unacceptable images, IMAGEmanager is likely to categorize as unacceptable a certain proportion of harmless images. The categorization of an acceptable image as unacceptable is known as a false positive categorization.

You can control the level of false positive categorizations by configuring the confidence level with which the IMAGEmanager categorizes images as unacceptable. At the lowest confidence levels, the IMAGEmanager can detect most unacceptable images correctly, but also can return a relatively large number of false positives. Setting a higher confidence level reduces the number of false positive categorizations, but also decreases the detection rate of unacceptable images. There needs to be a balance found between too many false positives and the risks associated with letting unacceptable images through.

You can quantify this balance by looking at the expected unacceptable image rate. Some environments have more unacceptable images than others. Perhaps there is an established unacceptable image problem due to poor policy enforcement in the past. The degree of unacceptable images can only be determined by monitoring email.

It is important that administrators adjust the confidence level, as the percentages of unacceptable images in email will vary greatly from situation to situation.

The Face Detection option identifies portraits of human faces. Use of this option reduces the number of portrait images falsely categorized as pornographic.

Supported image types

Table D-1:shows the types of image file that IMAGEmanager supports.

Table D-1: Supported image types

Format	Description
BMP	Windows or OS/2 bitmap
GIF	Graphic Interchange Format
JPEG	Joint Photographics Experts Group
PNG	Portable Network Graphics bitmap
TIFF	Tag Image File Format bitmap

.

Embedding an image in a Microsoft Office document can convert the format of the image. If an IMAGEmanager scenario is to detect embedded images in a Microsoft Office document, make sure that you select all image types.

Establishing an image management policy

Your organization's security policy should determine how to handle unacceptable information, and should identify any legal implications of your actions. Establish the legal requirements and implications before you configure IMAGEmanager, and make sure that you educate members of your organization about your policy.

The legal requirements are country-specific. For example, in some countries, you need written consent from an individual before you can examine email sent to the individual.

Your organization’s security policy for objects that IMAGEmanager detects should define:

- What to do with potentially unacceptable images.
- How long potentially unacceptable material can remain on your organization’s network.
- Who is responsible for checking potentially unacceptable images.
- What to do if images identified as potentially unacceptable are acceptable.

Remember, the retention of unacceptable material on computer storage media may constitute a criminal offense in some countries.

Your policy may differ for inbound and outbound email, for example:

- **Inbound email**

  Deliver email but keep a copy of email containing images.

- **Outbound email**

  Quarantine all email containing pornography and confidential images, and send a message to an administrator informing them of the quarantined files.

A policy can also be refined to focus on particular groups of employees such as known policy rule breakers or a harassed employee receiving unwanted mail.

Creating a white list

It is possible to use the pre-classified image database as a white list. This can enforce a policy in which only 'approved' images pass. To do this, set the image maximum dimensions to just above the image minimum dimensions. IMAGEmanager classifies images above the maximum dimensions as undetermined and the messages are quarantined accordingly. However, images defined in the pre-classified image database as acceptable pass as clean even if they exceed the maximum dimensions.

Dealing with detected files

If messages are quarantined as part of your content policy, it is important to inspect the contents of the quarantine area used by IMAGEmanager scenarios on a regular and frequent basis in order to:

- Release for delivery any emails wrongly categorized as unacceptable.
- Delete unacceptable material.
- Add images to the pre-classified image database to improve detection performance.

⚠ The retention of unacceptable material on computer storage media may constitute a criminal offense in some countries.

Configuring IMAGEmanager

To configure IMAGEmanager you typically need to set up the following items:

- A quarantine area for unacceptable images.
- An classification to apply to unacceptable images.
- An action to quarantine unacceptable images.
- An inform message to warn the administrator, if required.
- An IMAGEmanager scenario, to define the types of image to process, and to set other options such as confidence levels and image dimensions

For details of creating quarantine areas, classifications, alerts and actions, refer to the MIMEsweeper Policy Editor help.

Creating an IMAGEmanager scenario

To create an IMAGEmanager scenario:

1. From the MIMEsweeper Policy Editor, select the scenarios folder in which you wish to create the IMAGEmanager scenario. On the **Action** menu, point to **New**, and select the **Scenario wizard...**
2. On the **Scenario Type** page, select **Unsuitable images** (IMAGEmanager scenario) and click **Next**.
3. On the Initial Scenario State page, select the initial state you require for the scenario, **Enabled** and / or **Overridable**, and then click **Next**.
4. On the **Image Types** page, select the types of image that the scenario is to detect; bmp, gif, jpeg, png, or tiff. By default, IMAGEmanager selects all the image types. Click **Next**.
5. On the **Classification** page, associate a classification to associate with unacceptable images. The classification determines the action to take and optionally who to notify if the scenario detects a message that contains at least one image that is unacceptable. Click **Next**.
6. On the **Scenario Name** page, enter a name for the scenario and add notes if necessary.
7. Click **Next**, then **Finish**.
8. Save the policy and apply the configuration to the Policy Servers so that the changes take effect.

Configuring additional options

To edit an existing IMAGEmanager scenario to set additional options, double-click the scenario, and in the **Properties** dialog box click the **Options** tab. From here you can set:

- Types of image to scan (you have already set using the Scenario Wizard, above).
- Minimum and maximum image sizes to scan (see below for details)
- Advanced Settings (see below for details):
  - Face Detection.
  - Confidence level (reducing the number of false positives).
  - Maximum image analysis time.

NOTE: If you make changes to the scenario, remember to save and re-apply the policy after you have finished.

Minimum and Maximum Image Dimensions

IMAGEmanager does not scan images that are smaller than the minimum or larger than the maximum dimensions specified in the Image Dimensions area. Enter the **Minimum Height** and **Width** and **Maximum Height** and **Width** in pixels.

The default dimensions are shown in the following table:

Table D-2: Default dimensions

Dimension	Default (pixels)
Minimum Width	100
Minimum Height	100
Maximum Width	3000
Maximum Height	2000

IMAGEmanager treats images below the minimum dimensions as acceptable. Images below the default minimum threshold of 100 pixels wide or 100 pixels in height are unlikely to contain pornographic or other inappropriate types of media. These images are more likely to be company logos, buttons or separators from HTML documents.

IMAGEmanager classifies messages containing images above the maximum dimensions as Undetermined, as the images may contain threats and have not been scanned. The reason for using a maximum is to limit processing: very large images take a long time to process.

If you want the scenario to analyze all images, uncheck the boxes.

The image dimensions apply to all selected image types.

Advanced Settings

We recommend that you do not change the **Advanced settings** without first determining the level of unacceptable images you are receiving.

Face Detection

Specify whether the scenario is to use the Face Detection option. Selecting the Face Detection option reduces the number of false positives, but increases processing time. By default, the option is not selected.

Confidence

The **Confidence** level specifies the level of confidence IMAGEmanager requires to categorize an image as unacceptable.

Move the slider towards the desired setting, as follows:

- **High**

  A High confidence level means that a high proportion of the nearest matches in IMAGEmanager’s image feature database must be unacceptable for IMAGEmanager to categorize the image as unacceptable. A high confidence level reduces the number of false positives, but can allow more unacceptable images to be classed as acceptable.

- **70%**

  More than 70% of the nearest neighbors in its image feature database must be unacceptable before an image is categorized as unacceptable.

- **Low**

  A Low confidence level means that the IMAGEmanager categorizes the image as unacceptable if a low proportion of the nearest neighbors in its image feature database are unacceptable. A low confidence level detects a higher proportion of unacceptable images, but can produce a high proportion of false positives. For example, a confidence level of **Low** without the Face Detection option activated means that an IMAGEmanager scenario detects most images that contain skin as unacceptable.

Maximum image analysis time

You can set a limit on the time the IMAGEmanager spends analyzing an image. The maximum is 999 seconds and the default is 120 seconds. If the image is not analyzed before the maximum time, the message is classified as Undetermined.

Testing the Policy

When you have configured an image management policy, you can test it to see how effective it is at detecting unacceptable and acceptable images. Keep in mind that image analysis will always tend to generate some false positives and allow some unacceptable images through. By testing your policy you can begin to refine confidence levels

To test the policy, compose a message with a JPEG file, for example, that contains an unacceptable image. Send another message that contains a similar image embedded in a Word document.

To see whether IMAGEmanager has detected and quarantined your test messages, open MIMEsweeper Manager and go to the **System Health** page. The Recent Messages table provides a log of recent messages that have been processed by MIMEsweeper for SMTP. Check the Classifications column. If the message does not trigger a policy, its Classifications entry will be “Clean”. If the message triggers an IMAGEmanager policy, its Classifications entry should be the classification defined for messages that trigger the policy.

Managing Detected Images

Examining held messages

If your IMAGEmanager implementation places quarantines messages containing unacceptable images, you can determine why IMAGEmanager classified the image. For example, if an IMAGEmanager scenario quarantines an email that has several attachments, you can view the message details to determine which of the attachments are unacceptable.

You should regularly examine messages IMAGEmanager scenario has quarantined, to check for false positives -- acceptable images that IMAGEmanager has classified as unacceptable.

To view a held message, select the **Message Center** in MIMEsweeper Manager. Select a View that includes the held message area you are using. The View lists all the messages in the quarantine area. Click the link to the message in the left column to view the details of the message. The **Summary Analysis** tab identifies the matching policy classifications. The **Images** tab identifies the images that IMAGEmanager scanned.

If your IMAGEmanager implementation places quarantines messages containing unacceptable images, you can determine why IMAGEmanager classified the image. For example, if an IMAGEmanager scenario quarantines an email that has several attachments, you can view the message details to determine which of the attachments are unacceptable.

For more information on using MIMEsweeper Manager’s message analysis options, see the MIMEsweeper Manager help.

Handling false positives

If you identify a message containing an acceptable image that IMAGEmanager has categorized as unacceptable:

1. Add the image to the pre-classified image database to prevent the false-positive recurring.
2. Reprocess the quarantined message from the quarantine area, to ensure that it receives the correct classification.

New images, or changes to images, may not become effective in the pre-classified image database immediately. By default the cache is updated every thirty minutes. You can force new images into the cache by saving and applying the policy from the MIMEsweeper Policy Editor.

It is possible when you reprocess a message to reprocess it through a different policy. This may be useful if you wish to remove images that are unacceptable but still deliver the body of the message. You could achieve this by including an Attachment Manager scenario in the scenario folder used for reprocessing.

The reprocessing policy can be linked to a different classification that has no alerts: if messages have already followed a classification that informs an administrator and the sender or recipient, then triggering informs or alerts a second time is unnecessary.

Troubleshooting

The following sections provide information on the action you can take to improve the operation of IMAGEmanager in certain situations.

Improving performance

To improve the throughput of IMAGEmanager, you can:

- Clear the **Enable Face Detection** option if your organization does not use portrait images as part of its daily business, as this can improve processing speed.
- Reduce the maximum size of images or increase the minimum size of images to scan.

  If your organization receives a large volume of small images that are unlikely to be unacceptable, you can specify that the IMAGEmanager scans only images above a certain size. Similarly, if your organization receives a large volume of images that exceed certain dimensions, you may want to decrease the maximum size of image that the IMAGEmanager processes.
- Check that the Policy Server(s) on which IMAGEmanager is running have enough memory. For more information, see Chapter 2 of the *Getting Started Guide.*
- Add more pre-classified images to the database to improve image throughput.

Improving detection rates

At the lowest confidence levels, IMAGEmanager can detect most unacceptable images correctly, but also can return a relatively large number of false positives. You need to find a balance between too many false positives and the risks associated with letting pornography through.

You can use the IMAGEmanager scenario's **Advanced Settings** dialog box to change the following settings for an IMAGEmanager scenario. The **Advanced Settings** dialog box is available from the **Options** tab within the scenario properties.

The more images from email you add to the pre-classified image database, the faster and more accurate IMAGEmanager will become.

Adjusting the confidence level

If the balance of incorrectly classified images is too far toward false positives or undetected unacceptable images, adjust the confidence level accordingly:

- If the proportion of unacceptable images that IMAGEmanager is detecting is too low, move the confidence level slider towards **Low**.
- If IMAGEmanager is returning too many false positives, move the confidence level slider towards **High**.

Using face detection

If IMAGEmanager is returning too many false positives, try using the Face Detection option (if it is not already selected). This option helps to reduce the number of facial portraits that IMAGEmanager categorizes as unacceptable.

APPENDIX E

Housekeeping

This appendix describes the housekeeping tasks you are recommended to perform to maintain your MIMEsweeper system. This chapter also includes some optional reconfiguring deployment tasks with guidelines about how you should manage a server failure.

Overview

To keep your MIMEsweeper for SMTP system running efficiently and to ensure that you optimize all computer resources, you must perform routine housekeeping tasks. To perform these tasks in MIMEsweeper for SMTP, the following tools and components are available:

- **MIMEsweeper for SMTP Manager**

  You can use the MIMEsweeper for SMTP Manager to assist in the housekeeping of the various folders used by the MIMEsweeper for SMTP system, when dealing with problems during the processing of email, for example, handling problem messages.

  For more details, see *Housekeeping for MIMEsweeper folders* on page E-3.

- **Automated Housekeeping tasks via the Infrastructure Service**

  You can use the MIMEsweeper for SMTP system to automatically perform certain housekeeping tasks, including:

  - Purging of expired data from the system database.
  - Creating emergency backup files
  - Cleaning unused or expired files from the system directories.

  For more details, see *Automated Housekeeping tasks* on page E-4.

- **System Maintenance Utility**

  You can use the System Maintenance Utility wizard to:

  - Reconfigure server roles within your existing MIMEsweeper deployment.
  - Create and restore MIMEsweeper system backups.
  - Configure your deployment for resilience and other miscellaneous tasks.

  For more details, see *System Maintenance Utility* on page E-5.

Housekeeping for MIMEsweeper folders

The MIMEsweeper Manager is used to manage messages processed by MIMEsweeper for SMTP and to perform certain housekeeping tasks. It is recommended that you carry out these housekeeping tasks to:

- Review problem messages that could not be processed by MIMEsweeper for SMTP.
- Prevent stored messages from consuming all disk space.

Reviewing the Recovery folder

If MIMEsweeper for SMTP cannot process a message, it places the message in the **Problem messages area**. The message is not delivered from the `Recovery` folder, instead the following items are generated:

- An entry in the Windows Application Log (for details, see Chapter 2).
- An alert using a configured alerter—Administrative Alerter, SNMP Alerter, or SMTP Alerter (for details, see Chapter 4).

You can monitor the number of messages in the `Recovery` folder by viewing the `Problem messages` area in the MIMEsweeper Manager.

If you want to resubmit messages held in the `Recovery` folder for delivery, you must select the message in the MIMEsweeper Manager, in the **Message Centre**, under the **Problem Messages** view, then select the **Reprocess** option. If the message is still not processed by MIMEsweeper for SMTP, you should contact your normal support provider and request that they analyze the messages.

For more information about the use of the `Recovery` folder, see Appendix G. For details on the location of the `Recovery` folder, see Appendix F.

Archiving messages in Save folder

You can configure MIMEsweeper for SMTP to save copies of email messages to a specified **Save** folder. MIMEsweeper for SMTP does not automatically delete copies of messages in the **Save** folder.

To reduce the risk of insufficient disk space, you are recommended to set up your own process to archive message copies from the **Save** folder. For information on the **Save** folder, see Chapter 2.

Automated Housekeeping tasks

In addition to the housekeeping tasks that you manually perform, the system performs a number of automated housekeeping tasks on the Primary Configuration Server (PCS).

The tasks are as follows:

- The **Operations database backup** task backs up the database information relating to configuration and policy information. This task is scheduled to run each night at approximately 1:15 a.m.

  The Operations database backup is automatically distributed to each machine in the MIMEsweeper deployment. This ensures that if the server hosting the Operations Database fails, it can be restored into the MIMEsweeper deployment.
- The **Deletion of old email addresses** task deletes redundant email addresses from the email address table. These email addresses are usually accumulated as a result of addresses contained in spam messages. This task is scheduled to run each night at 12:30 a.m.
- The **Deletion of activity log files** task deletes log files that have passed their retention time. The task is scheduled to run each night at 11:00 p.m.
- The **Deletion of expired messages** task deletes messages that have expired, that is, passed their retention date and time. This task is scheduled to run hourly.

With the exception of the **Deletion of expired messages** task, each task is scheduled to run at a fixed time when processing loads are low.

⚠ If other unrelated tasks are scheduled to run on the server at the same time, the processor may overload and cause problems with the scheduled tasks.

System Maintenance Utility

System maintenance tasks are facilitated by the System Maintenance Utility, which is accessed from the **Start** menu. These tasks can only be performed by a system administrator, and to perform most tasks you must enter the MIMEsweeper for SMTP installation's administrator username and password.

The way that the System Maintenance Utility tasks operates depends on the authentication method that your installation uses for database access. The two methods available are:

- Windows authentication: the installation authenticates database access using the current login ID in conjunction with an Applications Service Account. The Applications Service Account is configured during installation, and MIMEsweeper for SMTP. For some system maintenance tasks, you need to supply the Applications Service Account details.
- SQL Server authentication authenticates database access using the database SQL Server login details. For some system maintenance tasks, you need to supply the SQL Server account details.

For a full discussion of each authentication option and how they are applied, in the *Getting Started Guide* in *Chapter 3: Installation*, see the section on preparing the database environment.

Reconfiguring your MIMEsweeper for SMTP deployment

After the initial installation of your MIMEsweeper system, you can redeploy some components to fine-tune your installation. For example, using the System Maintenance Utility, you can:

- Move the Primary Configuration Server (PCS) role to another more powerful server
- Move the Operations database from your PCS to a SQL Server elsewhere, to reduce the load on your PCS or to centralize all your SQL databases.
- Change the authentication method used for selected databases. For example, you can configure the Operations Database, or the Audit and Tracking databases to change from SQL Server authentication to Windows authentication.

The list of maintenance tasks presented by the System Maintenance Utility, and the way that these tasks operate varies depending on your license type, the current server type (Primary Configuration Server, or Policy Server, or Additional Server) from which the Utility is started. An additional server is a server that has been installed with no particular role, but with the intention of assigning it a role at a later time.

The following table lists all tasks, and shows the license type and the server type on which they are available.

Table E-1: License types

Task name	License	Server role
Make this machine the Primary Configuration Server and Operations Database host	Standard only	Additional server only
Move the Operations Database to another SQL Server	Advanced and Enterprise	PCS only
Make this machine the Primary Configuration Server	Advanced and Enterprise	Additional server only
Change Operations Database to use Windows Authentication Authentication	All	PCS only
Configure Web and Audit Servers to use Windows Authentication Authentication	All	PCS only
Move the Web Applications	All	PCS only
Remove redundant Additional Server	All	PCS only

Standard and emergency tasks (Advanced and Enterprise only)

When you start the System Maintenance Utility on an additional server with an Advanced or Enterprise license you have the choice of standard or emergency tasks. Emergency tasks are a subset of tasks designed to recover from a server failure. Currently the only emergency task is **Make this machine the Primary Configuration Server**. This emergency task is to promote an additional server to the PCS role in the event of PCS failure, for example, hardware failure.

PCS redundancy (Advanced and Enterprise only)

The **Make this machine the Primary Configuration Server** task can be used to promote an additional server to the Primary Configuration Server role in the event of a PCS failure, for example, hardware failure. This task is available only in situations where the Operations database is not located on the PCS. To make this task available, use the **Move the Operations Database to another SQL server** task to move your Operations database as soon as possible.

To minimize PCS down-time in the event of failure, it is recommended that you:

- Install a dedicated additional server as a stand-by so that it is available and ready to be promoted in the event of system failure.
- Move the Operations database away from the PCS.

For example, if you have a dedicated additional server installed, consider moving the Operations Database to your additional server.

The other System Maintenance Utility options are:

- **Make this machine the Primary Configuration Server and Operations Database Host**

  This task is available on an additional server only with a standard license. This task transfers the role of the Primary Configuration Server (PCS) to the machine where you are running the System Maintenance Utility, and it transfers system data from the current PCS.

  The PCS holds the core operation data and manages all the other servers in your installation. The PCS replicates the changes to the Operations database, the Web Server, the Audit Server, and all other Policy Servers.

  When you create an additional server in your deployment, a non-active installation of the Operations database is installed. This is to allow the additional server to be promoted to the PCS at a later time if required.

  An example of the use of this task is that you have all the MIMEsweeper for SMTP components installed on a single machine which is located in the DMZ, and you want to move the Primary Configuration Server (PCS) and Web Server to a new server machine which is located inside your clean network, but retain the Policy Server in the DMZ processing mail.

  > ⚠ If you intend to promote an additional server which has SQL Server 2005 Express installed to the PCS role, be aware that there is a 4 GB limit on the database size. Check the size of your operations database to ensure that this size is sufficient.

  To move the PCS and Web Server from a single machine installation:

  - Install a new Web Server in the clean network area. This is an additional server with MIMEsweeper Manager and PMM enabled that needs to connect to your single machine deployment in the DMZ.
  - Run the System Maintenance Utility on the new Web Server and select the **Make this machine the Primary Server and Operations Database host** to move the Primary Configuration Server (PCS) from the single machine deployment in the DMZ to the clean network.

  When you are moving the PCS, all message processing is stopped and access to MIMEsweeper Policy Editor or MIMEsweeper Manager is blocked.

- **Move the Operations Database to another SQL server**

  This task is available on the Primary Configuration Server (PCS) only, with an Advanced or Enterprise license.

  This task moves the Operations Database from its current location to an alternative SQL server. See *Moving the Operations Database* on page E-9 for configuration details for this task.

- **Make this machine the Primary Configuration Server**

  This task is available on an additional server with an Advanced or Enterprise license.

  This task performs part of the role to **Make this machine the Primary Configuration Server and Operations Database Host** specified under *Make this machine the Primary Configuration Server and Operations Database Host* on page E-7. The difference between the two tasks is that the Operations Database host is not changed.

- **Move the Web Applications to another Web Server**

  This task is available on the Primary Configuration Server (PCS).

  This task moves the Web Applications to another Web Server.

- **Change Operations Database to use Windows Authentication**

  This task is available on the Primary Configuration Server (PCS). The task allows you to change the authentication method used by the Operations Database from SQL Server authentication to Windows authentication. For details on Windows authentication, in the *Getting Started Guide*, see *Chapter 3: Installation*, and refer to the section on preparing the database environment.

- **Configure Web and Audit Servers to use Windows Authentication**

  This task is available on the Primary Configuration Server (PCS). Similar to the previous task, this task allows you to change the authentication method used by the web and audit server databases from SQL Server authentication to Windows authentication. For details on Windows authentication, in the *Getting Started Guide*, see *Chapter 3: Installation*, and refer to the section on preparing the database environment.

- **Remove Redundant Additional Server**

  This task is available on the Primary Configuration Server (PCS).

  This task removes a redundant additional server from your MIMEsweeper for SMTP deployment. This task only appears if you have additional servers in your deployment.

Moving the Operations Database

The System Maintenance utility includes a function to move the Operations Database to another SQL Server. When you perform this operation, you need to configure the SQL Server software on the target machine to enable the use of the `xp_cmdshell` stored procedure. This procedure is disabled in the default SQL Server installation.

To return SQL Server to its default status, you can disable the use of the `xp_cmdshell` stored procedure once you have moved the Operations Database.

To enable the use of the `xp_cmdshell` stored procedure on the target server:

1. From the Windows **Start**, **Programs** menu, select **Microsoft SQL Server 2005**, **Configuration tools**, **SQL Server Surface Area configuration.**
2. In the Configure Surface Area for <hostname> area, select **Surface Area Configuration for Features** to display the Surface Area Configuration tool.
3. From the list, select **xp_cmdshell** to enable it.
4. Click **OK**, then close the SQL Server Surface Area configuration tool.

Backup and Restore

Use the wizard to choose a backup and restore maintenance task. The subsequent wizard pages displayed depend upon the task you choose. The tasks available are:

- System Backup
- System Restore

System Backup

Perform this maintenance task to back up some or all of your MIMEsweeper system data to a specified location. It is recommended that you perform a system backup at content security policy level (1) before each change to your policy configuration.

It is recommended that all message processing and updates to MIMEsweeper are stopped during system backup. This action is managed automatically when you select Level 3 or Level 4 standard backups.

Choose the level of backup you wish to perform:

- **Content Security Policy only - Level 1**

  This includes the MIMEsweeper Policy Editor elements you configure to implement your content security policy, scenarios, classifications, domains and routing information.

- **Above + System Configuration + PMM settings - Level 2**

  This includes your content security policy, the configuration of your deployed MIMEsweeper for SMTP components, and the configuration of your Personal Message Manager (PMM) system.

PMM settings include settings such as the mail server to use, the daily period to send out digest messages, and the templates for digest messages and password reminders.

The system performs a daily backup on the PCS at this level.

A Level 2 backup includes all the data of a Level 1 backup but you cannot perform a Level 1 restore from a Level 2 backup.

- **All above + Operational Database + SpamLogic Database + Diagnostic Logs - Level 3**

  This includes all of the above plus the operations database, SpamLogic database, and summary of the contents of messages held and queued by the Policy Servers.

- **All above + Mail Messages - Level 4**

  All of the above plus all messages queued or held in your messages areas.

The following notes apply to back up:

- The processing of mail is temporarily stopped during a Level 3 and Level 4 backup.
- The Operations database and PMM settings are only backed up or restored when performed on the PCS. When these operations are performed on a Client Tools host, the System Maintenance wizard only backs up or restores the content security policy.

The SpamLogic database is only backed up or restored when performed on the Policy Server.

System Restore

Perform this maintenance task to restore your system from previous backed up files. You can choose which parts of your system data you want to restore. The options for restoring your system data are the same as for the system backup maintenance task.

A system can only be restored to a machine with the same fully qualified name and installation directory as the machine originally backed up and performing the same role in the deployment, otherwise the restore options will not be available.

You can perform a System Restore to revert to a previous known configuration or to rebuild a server which has failed.

Message processing and access to MIMEsweeper are suspended during this operation.

Backup and Restore restrictions

The following restrictions apply when you back up and restore your system using the System Maintenance wizard. If any problems are detected you will be alerted:

- If the policy file has been edited since a system backup and that system backup is subsequently used for a Level 1 restore, you are warned that the policy has been changed and may corrupt your system. You are given the option whether to continue or not, but before proceeding you must consider the effects of restoring this policy.

- When you perform a restore, there is the potential to lose Message Center data collected between the time that the backup was performed and the time that the restore is performed. For details about how to recover this information, see *Recovering data lost after a restore* on page E-12.
- The MIMEsweeper server that you are restoring must match the fully qualified hostname of the MIMEsweeper machine where the backup was created.
- You must ensure that the MIMEsweeper server is configured to match the MIMEsweeper machine where the backup was created. For example, the folder structure must be identical and MIMEsweeper for SMTP must be installed in the same folder matching both in folder name and location.
- The additional MIMEsweeper server must be installed with identical MIMEsweeper for SMTP features to match the MIMEsweeper machine used when the backup was created.
- You must ensure that the MIMEsweeper server is the same server type, for example, Primary Configuration Server (PCS) or additional server to match the created backup.

Backup and Restore examples

The backup and restore examples are specified below:

- To replace an additional server with a faster machine.
  a. Carry out a Level 4 backup on the additional server and the PCS.
  b. Uninstall the old additional server.
  c. Give the new additional server the same name as the old additional server.
  d. Install the product on the additional server, into the same folder as the old additional server.
  e. Restore the level 4 backup in the same directory as the old server.
- Restore the policy from an earlier backup.

  Perform a Level 1 restore on any machine in the deployment from the earlier backup. This will update the PCS and replicate to all servers.
- Backup and restore a multiple server deployment where the message area and message queue contents are required.
  a. Make Level 4 backups of all additional servers and the PCS.
  b. Restore the PCS to Level 4.
  c. Restore additional servers to Level 4.
- Backup and restore a multiple server deployment where the message area and message queue contents are not required.
  a. Repeat the above procedure using a Level 3 restore instead of Level 4.

Recovering data lost after a restore

When you perform a restore, there is the potential to lose Message Center data collected between the time that the backup was performed and the time that the restore is performed. To recover this information you must perform the following steps:

1. Select **System Restore** to start the restore procedure. From the warning message you must determine the creation date of the backup you are restoring.
2. From the restoring server, navigate to the message area directory containing the information to be restored. For example, for the Multimedia message area, you would typically access the following directory:

   `C:\Program Files\Clearswift\MIMEsweeper for SMTP\Mail\MessageAreas\Multimedia`
3. Under the message area directory, locate the **`Cache`** folder for the first day after the backup. The cache folder is structured on a date basis. For example, the cache folder for the first 1,000 Personal messages processed on October 19, 2005 is:

   ```
   C:\Program Files\Clearswift\MIMEsweeper for SMTP
   \Mail\MessageAreas\Personal\cache\2005\10\19\0000
   ```
4. Move all .qa files from the folder to the root message area folder. This move forces MIMEsweeper for SMTP to reprocess the messages. For example, for the cache folder shown in Step 3, you must move the .qa files to the following directory:

   `C:\Program Files\Clearswift\MIMEsweeper for SMTP\Mail\MessageAreas\Personal`
5. Repeat the process for all the folders under all days between the backup and the restore. The messages are reprocessed and the details are accessible from the Message Center.

Recovering lost data example

This example explains how you recover any lost Message Center data after a restore.

- The installation is a stand alone installation using the default paths.
- The restore date is 20th July 2005 and the backup was created on 18th July 2005.
- You want to restore the Message Center information for all messages quarantined in the **Viruses** message area.

To do this, you would use the following procedure:

1. Access the root message area folder for the `Viruses` message area:

   `C:\Program Files\Clearswift\MIMEsweeper for SMTP\Mail\MessageAreas\Viruses`
2. Below this directory, access the folder: `cache\2005\07\18`. This sub-folder contains all the messages processed on the 18th July.
3. Below this directory, access all sub-folders starting with `0000`, and move all `.qa` files up the tree to the `MessageAreas\Viruses folder`. The message files are reprocessed and the Message Center information is restored.

4. Repeat the process for the `19` and `20` sub-folders, to reprocess all messages sent on the 19th and 20th of July.
5. Check the Message Center to confirm that the message information is now visible.

Miscellaneous tasks

This section describes the remaining tasks available in the System Maintenance Utility. The wizard pages displayed depend upon the task you choose. The miscellaneous task options are:

- Queue Watcher
- Anti-spam filter training wizard
- Reset policy access

Queue Watcher

Queue Watcher monitors the Content Analysis Queues on your Policy Servers to detect error conditions that prevent the normal flow of mail. You can configure Queue Watcher:

- To alert the administrator and other recipients by email when error conditions occur.
- Optionally, to take corrective action.

The Queue Watcher is an automated task run as part of the Infrastructure service on each Policy server. By default, it is disabled.

Configuring Queue Watcher

To configure Queue Watcher:

1. From the **Start** menu, select **MIMEsweeper for SMTP** then **System Maintenance Utility**.
2. In the **Choose Maintenance Task** wizard page select **Miscellaneous** then **Queue Watcher**. Follow the instructions on each wizard page, and click **Next** to move to the next wizard page.

In the **Define the Queue Watcher schedule** wizard page you can enable and disable the time of day that the Queue Watcher is active. The possible states that can be configured for Queue Watcher are as specified in Table E-2.

Table E-2: Queue Watcher possible states

Green	Notify the MIMEsweeper administrator of any error conditions and take corrective action.
Orange	Notify the MIMEsweeper administrator of any error conditions but do not take corrective action.
Red	Do not notify the MIMEsweeper administrator of any error conditions and do not take corrective action.

The Queue Watcher schedule is divided into half-hour time slots, and you can define different schedules for weekdays and weekends. So, for example, you can choose notification only mode during normal working hours when an administrator is available to correct the condition manually, and corrective action mode during non-working hours. You can click or move the pointer over a range of time slots to change the condition.

In the **Define the error detection conditions** wizard page you can redefine the conditions that constitute an error situation. It is recommended that you do not changes these settings unless advised by your normal support provider. The options to specify are:

- **Take no action if messages are locked for processing**

  Specify to prevent an error condition being raised when a message is in the process of being scanned by the Security service. This condition is recognized by the presence of a .lck file in any of the Content Analysis Queue folders. By default, this option is enabled.

- **Minimum messages in the Content Analysis Queues before action is taken**

  Specify the threshold value when Queue Watcher starts checking for error conditions. The default threshold value is 50 messages.

  When the number of messages in the Content Analysis Queues exceeds the threshold value, it is the first sign that an error condition may have occurred. Although no action is taken, it triggers Queue Watcher to start inspecting the MIMEsweeper system more closely.

- **Minimum time (in minutes) the system stops processing before action is taken**

  If the specified threshold value in the Content Analysis Queues is reached, with no messages being processed in this period, it is assessed that an error condition has occurred. By default, the period is 10 minutes.

In the **Define how to respond to an error** wizard page you can specify the actions you want the MIMEsweeper system to perform if an error condition occurs. The options to specify are:

- **Move messages that did not complete processing to the Problem Message area**

  To move messages that did not complete processing to the **Problem Messages** area. You view problem messages in the MIMEsweeper Manager. By default, this option is disabled. The remaining options are to:

  - Restart the Receiver service
  - Restart the Security service
  - Restart the Delivery service

  By default, only the Security service is restarted.

In the **Define how to notify in response to an error** wizard page you specify whether an email notification is sent to the MIMEsweeper administrator. The options to specify are:

- **Send an email notification**

  To configure whether an email is generated each time an error condition is identified. This option is always enabled, if you define **Notification only** periods in the Queue Watcher schedule.

- **Server**

  The host name or IP Address of the SMTP server to connect to for sending the email notification.

- **Port**

  The port number of the SMTP server. By default, port 25 is specified.

- **Sender**

  The email sender address specified in the email notification.

- **Recipient(s)**

  The email recipient address specified in the email notification. You can specify multiple recipients by separating each email address with a semi-colon (;).

- **Subject**

  The subject line details to be specified in the email notification.

- **Body**

  The text to be added into the body of the email message. You can use tokens to add the MIMEsweeper system information. A list of available tokens are shown in Table E-3.

Table E-3: Tokens used by Queue Watcher

Restarted Services	The MIMEsweeper services that have been restarted by Queue Watcher as part of the corrective action.
Killed Services	The MIMEsweeper services that could not be stopped successfully, so had to be aborted by Queue Watcher before restarting.
Failed Services	A list of the MIMEsweeper services that Queue Watcher has tried to restart, but which have failed.
Problem Messages	A list of message IDs that Queue Watcher has moved into the **Problem Messages** area as part of the corrective action.

Table E-3: Tokens used by Queue Watcher

Stuck messages	A list of message IDs that Queue Watcher attempted to move into the **Problem Messages** area as part of the corrective action, but was unsuccessful. This problem may occur when a message with the same ID already exists in the **Problem Message** area, or if the message file is locked. To prevent the message being reprocessed by the Security service, a `.stk` file is created in the Content Analysis Queue folder.

In the **Confirm the selected task configuration settings** wizard page a list is produced of the configured Queue Watcher options.

Reset Policy Access

This wizard gathers the system information necessary to unlock access to the MIMEsweeper for SMTP policy. Resetting the policy access is useful in certain circumstances, such as:

- Access to the policy by a second administrator is required so that an urgent policy change can be made. In this case unsaved changes by the first administrator are lost.

Server failure

The following sections outline the actions you can take if a server is unavailable due to hardware failure.

Note that the System Maintenance Utility tasks (**Make this machine the Primary Configuration Server** and **Move the Web Applications to another Web server**) used in the procedures described in these sections are available only if your MIMEsweeper for SMTP license is an Advanced or Enterprise edition license.

Primary Configuration Server failure

If your original PCS fails, you need to convert one of the additional servers in your configuration to the PCS. The additional server that takes on the role of the PCS can be a Policy Server, a Web Applications Server, an Audit Server, or a Tracking Server.

To convert an additional server to a PCS when your existing PCS has failed:

1. On the additional server, run the System Maintenance wizard.
2. On the **Maintenance Type** page, select **Emergency Maintenance** and click **Next**.
3. On the **Authentication** page, enter your login details and click **Next**.
4. On the **Choose maintenance task** page, select **Make this machine the Primary Configuration Server** and click **Next**.
5. Follow the instructions in the wizard to transfer the PCS role to the additional server.

When you have completed the wizard, all tasks previously performed by the original PCS will be performed by the new PCS.

If you solve the problem with your original PCS without having to re-install MIMEsweeper for SMTP, then when the original PCS restarts it will acknowledge it is no longer the PCS.

If you have to reinstall MIMEsweeper for SMTP, you should install the software, with the same features previously selected, as an additional server.

Finally, if you want to restore the original PCS to be the active PCS again, you should do the following:

1. On the original PCS, run the System Maintenance wizard.
2. On the **Maintenance Type** page, select **Standard Maintenance** and click **Next**.
3. On the **Authentication** page, enter your login details and click **Next**.
4. On the **Choose maintenance task** page, select **Make this machine the Primary Configuration Server** and click **Next**.
5. Follow the instructions in the wizard to transfer the PCS role back to the original PCS.

Audit Server failure

If the Audit Server fails, you can specify another server to perform this role by doing the following:

1. Install the Audit Disposer feature on the selected server, if it is not already installed.
2. Open the MIMEsweeper Policy Editor.
3. Under **MIMEsweeper for SMTP**, right-click **Servers** and select **Properties**.
4. On the **Servers Properties** page, click the **Servers** tab.
5. Under **Select a server to act as the audit disposer**, select a server from the drop-down menu, and click **OK**.

This action assigns the task of updating the Audit database to the selected server.

If you solve the problem with the original server, you can restore your original configuration by following the steps above and specifying the original server.

Web Server failure

In the event of the Web Server failing, you can still access the features provided by the Web Applications by using the URL to any server in your deployment that has the Web Applications installed.

For example, if you need to update your policy but the original Web Server has failed, simply enter the qualified name of the server providing redundancy for the Web Applications in the **Server** field.

However, if you are using Personal Message Manager, you need to update your MIMEsweeper for SMTP deployment with the new Web Server details to ensure that any PMM notifications sent out to your users are routed to the new Web Server.

To update this information, follow the steps below:

1. On the PCS, run the System Maintenance wizard.
2. On the **Maintenance Type** page, select **Standard Maintenance** and click **Next**.
3. On the **Authentication** page, enter your login details. In the **Web server** field, specify the new Web Server. Click **Next**.
4. On the **Choose maintenance task** page, select **Move the Web Applications to another Web server** and click **Next**.

Follow the instructions in the wizard, specifying the qualified name of the new Web Server.

When you have completed the wizard, all PMM notifications will direct the user to the new Web Server.

If you solve the problem with the original Web Server, you can restore your original configuration by following the steps above and specifying the original Web Server.

Policy Server failure

To make your system resilient to Policy Server failure, you should install at least two Policy Servers in your deployment. If one Policy Server fails, the other will still continue to process mail traffic. The processing speed will be halved, so it is desirable to install as many Policy Servers as your license allows.

In the event of a single Policy Server failing, you will initially need to move the server providing redundancy into the DMZ if your system is configured in this manner. To enable the server in the Policy Editor, right-click the server name under **Servers** in the MIMEsweeper Policy Editor, and select **Enable**. This action allows the server to begin processing SMTP traffic.

System Backup/Restore configuration switches

The following sections describe additional configuration settings that can be used primarily in the Backup and Restore functionality. Each switch is used to work around very specific problems that some users might experience.

These switches are most commonly used by the various System Maintenance tasks which incorporate the backup and restore functionality, and additionally in automated tasks performed via the Infrastructure service.

Configuring Backup/Restore file thresholds

Switch name	`backupThreshold`
Application servers	All servers.
Configuration file	`SystemMaintenance.exe.config`
Configuration section	`appSettings`
Usage	Level 3 or 4 Backups.
Problem	When performing this type of backup, if the task encounters a very large file in situations where memory is low, the task can cause an out of memory error attempting to zip up the large file.
Purpose	This switch allows the user to specify a maximum file size threshold so that all files over this threshold are zipped up individually on disk rather than in memory.
Default	50MB

Switch name	`restoreThreshold`
Application servers	All servers.
Configuration file	`SystemMaintenance.exe.config`
Configuration section	`appSettings`

Usage	Level 3 or 4 Restore.
Problem	As with backupThreshold, this prevents out of memory errors occurring during a restore of large files.
Purpose	This switch allows the user to specify a maximum file size threshold so that all files over this threshold are unzipped on disk rather than in memory.
Default	40MB

Switch name	`backupStopServices`
Application servers	PCS or additional server.
Configuration file	`SystemMaintenance.exe.config`
Configuration section	`appSettings`
Usage	Level 3 or 4 Backups.
Problem	The backup process will now temporarily suspend any services. You may want to prevent the services from being suspended so that the flow of mail is not stopped.
Purpose	This switch allows you to prevent the services being suspended during the backup.
Default	By default, the services will be suspended during a level 3 or 4 backup. Set this switch to ‘`false`’ to prevent the service suspension.

Configuring Database Backup/Restore

Switch name	`backupDatabaseThreshold`
Application servers	PCS only.
Configuration file	`SystemMaintenance.exe.config`
Configuration section	`appSettings`
Usage	PCS Level 2, 3 or 4 Backups.
Problem	When performing this type of backup, in situations where the operations database backup is very large, the backup can fail with an out of memory error.
Purpose	The switch allows you to configure a maximum database backup file size threshold. All database backup files beneath this threshold will be zipped up in memory. All database backup files over this threshold will be zipped up on disk.
Default	256MB

Switch name	`restoreDatabaseThreshold`
Application servers	PCS only.
Configuration file	`SystemMaintenance.exe.config`
Configuration section	`appSettings`
Usage	PCS Level 2, 3 or 4 Backups.
Problem	As with backupDatabaseThreshold, this prevents out of memory errors occurring during a restore of large databases.
Purpose	The switch allows you to configure a maximum database backup file size threshold. All database backup files beneath this threshold will be restored from memory. All database backup files over this threshold will be restored from temporary disk file.
Default	128MB

Switch name	`backupDatabaseFolder`
Application servers	PCS only.

Configuration file	`SystemMaintenance.exe.config`
	`Pmi.is.exe.standard.config`
	`Pmi.is.exe.maintenance.config`

Configuration section	`appSettings`
Usage	• Level 2, 3 or 4 Backups • Primary Server and Operations Database Move (Standard license) • Operations Database Only Move (Advanced/Enterprise License) • Overnight Emergency Backups
Problem	All database backups are by default created in the folder `<installdir>\Data\Operations\Backup`. In the situation of low disk space, or large database backup, it can be impossible to perform a Backup/Restore/PCS move or Operations database move.
Purpose	This switch allows you to set a different location for all database backup files to be created in. This allows you to work around the problem of low disk space on the default installation partition.
Default	`<installdir>\Data\Operations\Backup`
Notes	In addition to the configuration file switch, you will also need to reconfigure the PMI_Operations and PMI_Operations_Backup devices on the Operations database host server. For each device, you must set the physical file path to the same location specified in the switch value. If your Operations database is remote from your PCS, you must ensure the UNC path currently defined for each backup device resolves to the same location on the PCS as specified in the switch value.

Switch name	`databaseBackupTimeout`
Application servers	PCS only.
Configuration file	`SystemMaintenance.exe.config`
Configuration section	`appSettings`
Usage	• Level 2, 3 or 4 Backups • Primary Server and Operations Database Move (Standard license) • Operations Database Only Move (Advanced/Enterprise license)
Problem	You may be unable to backup large databases because the default SQL connection timeout was exceeded.
Purpose	This switch allows you to set the timeout period for the backup/restore of a database over an SQL connection.
Default	1800 seconds (30 minutes).

Configuring Overnight Emergency Backup replication

Switch name	`replicateBackup`
Application servers	PCS only.
Configuration file	`Pmi.is.exe.standard.config`
Configuration section	`emergencyBackupMonitor`
Usage	Overnight Emergency Backup.
Problem	Large overnight backups can slow the MIMEsweeper system by replicating large backup files to all machines in the deployment.
Purpose	This switch allows you to stop the backup from being replicated around the deployment, and leaves it in the `<installdir>\Data\Operations\Backup` (or directory configured using the backupDatabaseFolder switch) instead.
Default	True (replicate the backup).

Relocating Operations database and transaction log files

When you use the System Maintenance task **System Backup**, the task may fail if there is insufficient space to perform the backup on the drive or drives hosting the Operations database data and transaction log files.

In the event of such a failure, the wizard will return a suitable error. Any error messages are written to the file `SystemMaintenance.exe.log`.

To avoid this problem and improve performance, it is good practice for SQL Server Administrators to set the default folders for the data and transaction log files on different partitions when you first install your SQL or SQL Server 2005 Express server. However, if you encounter the problem and need to relocate the data file or the transaction log file, or both, you can do so as shown in the following example.

Example

This example shows how to move the Operations database and transaction log from `C:\SQLData` to `D:\SQLData`.

1. Stop the MIMEsweeper services.
2. Open SQL Query Analyzer.
3. Execute the command:

   ```
   exec sp_detach_db N'PMI_Operations'
   ```
4. In Windows Explorer, move the files `PMI_Operations.mdf` and `PMI_Operations_Log.ldf` from `C:\SQLData` to `D:\SQLData`.
5. Execute the command:

   ```
   sp_attach_db
   @dbName=N'PMI_Operations',@filename1=N'd:\SQLData\PMI_Operations.mdf',
   @filename2=N'd:\SQLData\PMI_Operations_Log.ldf'
   ```
6. View the database properties in SQL Enterprise Manager. The file locations should point to the new locations.

Housekeeping for auditing and reporting

You are recommended to perform these housekeeping tasks to improve system performance and reduce disk storage areas.

Compacting auditing databases

If you are using a database for auditing, use the appropriate compact tools on a regular basis to remove the wasted space incurred following record deletions and to improve performance. For example, SQL server provides its own database compact functions.

APPENDIX F

MIMEsweeper for SMTP Folders

This appendix describes the folders created by MIMEsweeper for SMTP that are of interest to users.

Overview

The main MIMEsweeper for SMTP folders and files are held under the folder `<Install Drive>:\Program Files\Clearswift\MIMEsweeper for SMTP`.

MIMEsweeper for SMTP creates some subfolders during installation and other folders at run time, for example, when you configure specific areas or when MIMEsweeper processes messages.

The following sections provide details of folders that may be of interest to a system administrator and describe their contents. The list is not exhaustive, as many of the folders on the system are non-configurable, and for this reason are not described here.

Performance considerations

In order to ensure maximum performance from your system, especially if it is a busy one, it is recommended that the mail processing folders are configured on a separate physical disk to the one containing the operating system. Further performance improvements can be achieved by placing separate mail handling folders on different drives.

To help optimize the system performance it is recommended that you use the performance monitoring tools provided by:

- The Microsoft System Monitor to observe:
  - Disk queue lengths
  - CPU usage
  - Memory usage
- The **System Health** area in MIMEsweeper Manager to observe system performance.

MIMEsweeper for SMTP folder

The MIMEsweeper for SMTP folder (`<Install Drive>:\Program Files\Clearswift\MIMEsweeper for SMTP`) contains the following subfolders which contain areas which are of interest to the system administrator. Folders which should not be accessed are not listed here:

- Data
- Documentation
- Mail

These folders are described in the following sections.

Data

Contains folders for configuration and state information used by the system at run time.

\Configuration

⚠ This folder does not contain the master copy of these files and should not be changed in any way.

\Database

\Audit Contains the scripts used to create the Audit Database.

\Hive Contains the scripts used to create the message tracking database.

\Operations Contains the scripts used to create the Operations database. These are useful for reference by the database administrators.

\Logs

\Audit Contains the log files used by the system to generate consolidated data for the audit / reporting systems.

\Operational Receiver Service / Delivery service operational logs, if enabled.

\PMM Logs of PMM user activity.

\RecentMessages Contains the `.rml` files, and shows each message processed through the Security service.

\Tracking Contains the log files used by the system to generate data for the message tracking reports.

\Operations

\Backup Contains an automated backup of the core PCS configuration and can be used to restore the PCS from another machine in the event of a failure. The file is `PMI_Operations_Backup.dat`.

\Queues

\Tracking Contains subdirectories for Active and Failed.

Documentation

Contains the Read Me files and documentation for MIMEsweeper for SMTP as follows:

As PDF files:

- Reference guide
- Getting Started guide

As HTM files:

- ReadMe for MIMEsweeper for SMTP 5.3.
- Prerequisites for MIMEsweeper for SMTP 5.3.
- Anti-virus tools for MIMEsweeper for SMTP 5.3.
- New features in this release
- Features introduced in previous releases

Mail

Contains, by default, all messages which are in the system.

\ArchiveAction	Held on the Policy Server and, by default, contains all the archived messages. This folder can be reconfigured in the MIMEsweeper Policy Editor.
\SaveAction	Held on the Policy Server and, by default, contains all the saved messages. This folder can be reconfigured in the MIMEsweeper Policy Editor.
\MessageAreas	Held on the Policy Server and, by default, contains all quarantined and parked messages
\Queues	Contains the messages that are moving through the system. This folder can be reconfigured in the MIMEsweeper Policy Editor.

APPENDIX G

Message Processing

This appendix provides detailed descriptions of how MIMEsweeper for SMTP processes email messages based on your configured email policies.

The information in this appendix supplements the overview provided in Chapter 1on how key components of MIMEsweeper for SMTP are involved in message processing.

You do not need to understand message processing at this level of detail to use the system. This information is provided for the interest of advanced users.

Overview

The following MIMEsweeper components are involved in processing email messages based on your defined policy:

- MIMEsweeper services
- MIMEsweeper folders
- Message areas

MIMEsweeper keeps track of email messages it is processing by assigning each message a unique ID. These are described in the first section in this overview (*Message IDs*).

The remaining sections in this chapter describe more fully the MIMEsweeper components involved in processing messages.

Message IDs

MIMEsweeper assigns a unique ID to each email message it processes. The message ID is a 21-character (or longer) alphanumeric string, for example, `Tc2a85a15a84ad30452d3`. MIMEsweeper changes the prefix letter of message IDs at different stages of message processing, as shown in Table G-1.

Table G-1: Message ID prefixes

Prefix	Message processing stage
N	sending notification messages configured in actions
R	reprocessing messages
S	splitting messages
T	processing message routinely

You can view Message IDs by opening a message view in the Message Center of MIMEsweeper Manager. See Chapter 9 for further details.

The following MIMEsweeper for SMTP services are responsible for processing email messages:

- Receiver service
- Security service
- Delivery service

Receiver service

The Receiver service validates connections for incoming mail based on your routing policy. It then receives all incoming and outgoing email messages, and passes them to the Security service for processing. For details of the folders used during message processing, see Appendix F.

The Receiver service processes email messages by:

1. Creating for each received messages a `.rco` file with the routing information, and placing the `.rco` files in the `\Mail\Queues\Normal` folder.
2. For each received message:
   - Creating an `.msg` file, which stores the message.
   - Converting the `.rco` file to an `.rcp` file, which stores the routing information.

   The base names of all these file names match the message ID, for example, `Tc2a85a15a84ad30452d3` (for details, see *Message IDs* on page G-2).

Security service

The Security service checks the content of email messages held in the `\Mail\Queues\Normal` folder against configured policies. It takes messages from the folder on a first in, first out (FIFO) basis.

The Security service processes email messages by:

1. Generating a 0-byte `.lck` file to signify that the file is locked for processing.
2. Examining the routing information to identify the sender and recipients of the email.
3. Matching the email to the configured policies.

   If an email with multiple recipients matches multiple routes, the Security service makes a copy for each applicable route and places them in the `\Mail\Queues\Normal` folder. The prefix of the file name is changed to `S` to indicate a split message (for details, see *Message IDs* on page G-2).
4. Decomposing the email into its basic components. This process, known as recursive disassembly, enables MIMEsweeper for SMTP to search for threats or perform content analysis on each component of the email.
5. Applying any actions defined for the matched scenarios to the email.

   If the MIMEsweeper needs to send an Inform action for a message, the Security service creates a new ID and changes the prefix of the file name to `N` (for details, see *Message IDs* on page G-2).
6. Rebuilding the email with any resulting modifications or enhancements to the content.
7. Moving email messages to the appropriate folder under the MIMEsweeper for SMTPinstallation directory:
   - The `Mail\Queues\Checked` folder if it deems the message safe for delivery and the message matches a policy with a delivery action.
   - A message area folder if the message matches a policy with a quarantine or park action (for details, see *Message areas* on page G-5).
   - A Save folder if the message matches a policy with a Copy to Archive Folder action (for details, see Chapter 4).
   - The `Mail\Queues\Recovery` folder if it is unable to process the message.

8. Deleting the .lck file to signify that the file is no longer locked for processing.

Delivery service

The Delivery service attempts to deliver email messages held in the Mail\Queues\Checked folder to the next SMTP host machine on the route to their intended recipients.

The Delivery service process email messages by:

1. Creating a <domain_name> subfolder under the Mail\Queues\Domains folder for the domain to which the message is to be delivered and placing the .rcp file for the message in this subfolder.

   If a message is to be delivered to multiple recipients in different domains, the Delivery service places a copy of the .rcp file for the message in the subfolder for each domain.
2. Placing the corresponding .msg file for each message in the Mail\Queues\Holding folder.
3. Sending the message to the next SMTP host machine as specified in the **Routing** folder under the **SMTP Relay** area of the MIMEsweeper Policy Editor (for details, see Chapter 6).
4. Attempting to contact the next SMTP host machine, and:
   - Creating a domain.mri file in the <domain_name> subfolder and placing the message in a queue in the \Mail\Queues\Holding folder for later delivery according to the specified retry schedule if it is not able to contact the next host (for details on configuring the retry schedule, see Chapter 6). The domain.mri status file records the last call to the domain, the last reason for failure, and the total number of attempts to deliver the message.
   - Deleting the .rcp file and updating the count in the .lck file when it has contacted the next host and delivered the message.
5. Deleting the <domain_name> subfolder when all of the .rcp files in it have been deleted.
6. Placing messages it is unable to deliver in the Mail\Queues\Dead folder and issuing an alert using a configured alerter—Administrative Alerter, SNMP Alerter, or SMTP Alerter (for details, see Chapter 2). The event is also generated in the Microsoft Windows Application Log (for details, see Chapter 8).
7. Deleting the .msg and .lck files when it has delivered the message to all recipients.

MIMEsweeper folders

During message processing, MIMEsweeper for SMTP places email in the following subfolders under the Mail\Queues folder:

- **Checked**

  All email messages whose content has been checked and considered safe for the Delivery service to attempt to deliver to the recipient addresses.
- **Dead**

  Copies of messages that the Delivery service cannot deliver to a network gateway.

- **Domains**

  Subfolders hold routing information of message awaiting delivery by the Delivery service and status files for messages that cannot be delivered immediately.

- **Holding**

  Message bodies awaiting delivery by the Delivery service.

- **Recovery**

  Any messages that the Security service has failed to process.

- **Content Analysis**

  All incoming and outgoing email messages that have been accepted by the Receiver service but whose content has not yet been checked by the Security service.

- **Working**

  Used for unpacking messages when configured to do so.

See Chapter 2 and the MIMEsweeper Policy Editor help for details about folders, policy properties and their configuration.

Message areas

If MIMEsweeper flags an email message for delayed delivery in accordance with your email policy, it does not deliver the message immediately. Instead, MIMEsweeper stores or holds the message in a message area, where the individuals responsible for your organization’s email policy can review or change the message. All emails in a message area are held in a secure format, so that they can safely be reviewed and distributed, but not launched.

MIMEsweeper for SMTP uses two types of message area:

- **Parking**

  Parking areas are used for temporarily holding email messages whose delivery is to be delayed for release during specified periods. Parking areas are normally used for holding large email messages, or those with a large number of attachments, so that they can be released for delivery during off-peak times.

  Each parking area has an associated release schedule, which defines when email messages are released for delivery.

- **Quarantine**

  Quarantine areas are used for storing email messages that require operator intervention. Quarantine areas are normally used for storing email messages with undesirable characteristics (such as infection with a virus). Individuals with access permissions for the message area can then decide whether or not to allow the message to be delivered.

  Quarantine areas do not have associated release schedules, but they can be configured to delete email messages automatically after a specified period of time.

Individuals who have access rights for a message area can examine the properties of email in the message area and specify what action to take. You define access rights for message areas in MIMEsweeper Manager

For information on configuring access rights, see Chapter 12.

APPENDIX H

Testing

This appendix describes how to test the MIMEsweeper for SMTP policies and routes prior to using the system live.

Overview

After installing and configuring MIMEsweeper for SMTP, you should test the system offline before using it live on the organization’s network.

This chapter provides guidance on testing the following areas of your configured system:

- Policy routing
- Email processing

Testing policy routing

Ensure that configured routes for specific policies are correct for the intended sender / recipient pair.

- Check which sender and recipient addresses will be matched by checking the route details for each defined scenario folder in the **Route** tab of its properties page.
- Check which scenario folder will be applied to a specified sender / recipient pair by using the **Identify policy** dialog box. For details, see the MIMEsweeper Policy Editor help.

> If you have specified a large LDAP address list, there may be a delay before the **Identify Policy** dialog box is displayed. The cursor changes to a Busy pointer while MIMEsweeper for SMTP dynamically creates the LDAP address list and checks the route. For details on LDAP address lists, see Chapter 2.

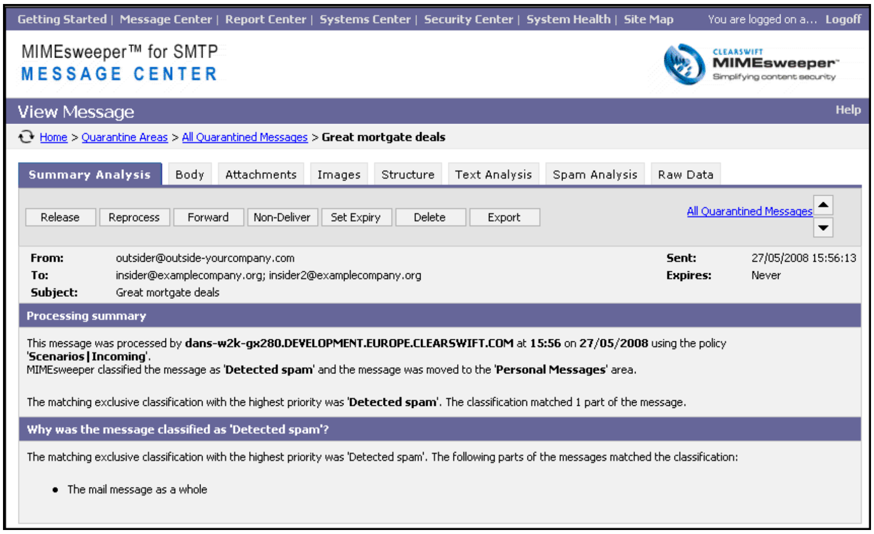
Testing email processing

You test email processing by placing all messages in quarantine areas on your system and by using special MIMEsweeper test accounts as described in the following sections.

Quarantine messages

To identify errors in email processing, quarantine all messages when you start testing your system. This enables you to view and analyze messages before manually processing them.

For example, you can use the **Reprocess** option for message in quarantine areas to monitor, test, and check the message route. For more information about processing options, see Chapter 9.


Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map
You are logged on a... Logoff
MIMEsweeper™ for SMTP
MESSAGE CENTER
CLEARSWIFT MIMEsweeper™ Simplifying content security
View Message
Help
Home > Quarantine Areas > All Quarantined Messages > Great mortgate deals
Summary Analysis
Body
Attachments
Images
Structure
Text Analysis
Spam Analysis
Raw Data
Release
Reprocess
Forward
Non-Deliver
Set Expiry
Delete
Export
All Quarantined Messages

From: outsider@outside-yourcompany.com

To: insider@examplecompany.org; insider2@examplecompany.org

Subject: Great mortgate deals

Sent: 27/05/2008 15:56:13

Expires: Never

Processing summary

This message was processed by **dans-w2k-gx280.DEVELOPMENT.EUROPE.CLEARSWIFT.COM** at **15:56** on **27/05/2008** using the policy '**Scenarios|Incoming**'.
MIMEsweeper classified the message as '**Detected spam**' and the message was moved to the '**Personal Messages**' area.

The matching exclusive classification with the highest priority was '**Detected spam**'. The classification matched 1 part of the message.

Why was the message classified as 'Detected spam'?

The matching exclusive classification with the highest priority was 'Detected spam'. The following parts of the messages matched the classification:

- The mail message as a whole

Figure H-1: Viewing a quarantined message

To view the properties of a quarantined message:

1. In MIMEsweeper Manager, open the Message Center. For details about the Message Center see Chapter 9.
2. Click on the **Quarantine Areas** button.
3. Select one of the message views by clicking on its name in the **Name** column. The contents of the view are shown.
4. Select a message by clicking on it in the **From** column. The View Message page for the chosen message is displayed. See Figure H-1 on page H-3.

For more information on viewing messages, see the MIMEsweeper Manager help.

Echo accounts

MIMEsweeper provides a number of email accounts that you can use for testing policies for the MIMEsweeper for SMTP system. These are known as echo accounts. You can send a message from your organization to any of the echo accounts. An automatic message reply is sent from the MIMEsweeper server.

Each Echo account can send back a text message. This test can simulate an incoming message containing a data type that needs to be blocked by your organization. The Echo accounts are shown in Table H-1.

Table H-1: Echo account references

Send an email to this account	To receive
`echo@clearswift.com`	A plain text message detailing the other echo accounts available.
`doc.echo@clearswift.com`	A UUE encoded Microsoft Word document.
`exe.echo@clearswift.com`	A UUE encoded small exe file.
`image.echo@clearswift.com`	A UUE encoded image file.
`virus.echo@clearswift.com`	A UUE encoded EICAR virus false positive.
`encrypt.echo@clearswift.com`	A UUE encoded password protected zip file.
`vbs.echo@clearswift.com`	Trigger text for VBS script checking.
`threat.echo@clearswift.com`	The trigger text only of the Sircam virus.
`spam.echo@clearswift.com`	A test spam message.

To use the echo accounts to test your system:

- Send a message to an echo account. For example, echo account `echo@clearswift.com` returns an email that:
  - Tests that messages can be sent to a remote system and that an automated response is generated.
  - Offers a list of threats to test against.

  All message attachments are sent from the MIMEsweeper server using the UUE format.

APPENDIX I

Tokens

This appendix lists the tokens you can use when configuring your MIMEsweeper for SMTP system.

Overview

A token is a variable whose value MIMEsweeper for SMTP substitutes during message processing. For example, the token %SENDER% can be used to match the sender of an email. During processing, the token is replaced with the actual address of the email sender.

You can use MIMEsweeper for SMTP tokens in the following areas:

- **Alert and Log actions**

  You can use tokens in the text of a broadcast message generated by an Alert action or of an event log entry generated by a Log action.

- **Executable scenarios**

  You can use tokens in an Executable scenario.

- **Non-delivery report**

  You can use tokens for Sender and Subject in a Non-delivery report.

- **Forward, Inform and Reply actions**

  You can use tokens in the subject and body of a notification message generated by a Forward, Inform, or Reply action.

- **Scenarios that support annotations**

  You can use tokens in the text of annotations added by Attachment Manager, Commercial Disclaimer, Content Scanner, File Detector, HTML Manager, Legal Disclaimer, Spoof Notifier, and Virus Manager scenarios as well as by MIMEsweeper scenarios for third-party anti-virus tools.

- **SMTP Alerter**

  You can use a token in an SMTP Alerter.

List of tokens

Table I-1 lists all available MAILsweeper tokens. For details of the display names and where these tokens can be used in MIMEsweeper for SMTP items, see the MIMEsweeper Policy Editor help.

Table I-1: List of tokens

Token	Description
%ADMIN%	The email address of the MAILsweeper administrator. This token is replaced by the address specified for the MAILsweeper administrator in the **Addresses** tab of **MAILsweeper for SMTP** properties page.
%AREANAME%	The name of the message area containing the message.
%DATE%	The date the original email message was sent.
%DETECTED%	A list of features detected by the scenario. If a detected threat has been removed from the email message, the name of the threat is not substituted for the token.
%FILENAME%	The file name of the email message component that matches the data type specified for the Executable scenario.
%LOGNAME%	The file name of the log file generated by the third-party executable program.
%LOGTEXT%	The text MAILsweeper is to extract from the log file generated by the third-party executable program.
%MESSAGE%	The text of the email alert message sent by the SMTP Alerter. If the alert is generated by the Alert action, this token is replaced with the text specified in the Message tab of the Alert Properties page. If the alert is generated by a system event, this token is replaced with the system message text.
%MODIFIED%	Details of the changes MAILsweeper content managers or format managers mae to the email message during message processing.
%POLICY%	The name of the scenario folder applied to the email message.
%RCPTS%	The email addresses of the recipients of the email.
%RECOGNISED%	A list of the format managers that have recognized items in the data stream.
%REMOVEDNAMES%	A list of attachments that were removed from the email message.
%RESPONSES%	The system-level responses that MAILsweeper content managers or format managers made during message processing.
%SENDER%	The email address of the sender of the email message.
%SERVER%	The email address of the MAILsweeper security service. This token is replaced by the address specified for the MAILsweeper service in the **Addresses** tab of the **MAILsweeper for SMTP** properties page.

Table I-1: List of tokens

Token	Description
%SUBJECT%	The subject of the email message.
%UNIQUEID%	The unique message ID MAILsweeper assigned to an email message.

APPENDIX J

Valid Names

This appendix lists the characters you can use to create valid names for items you create in MIMEsweeper for SMTP.

Overview

When you create a new item such as a scenario, alerter, or classification in the MIMEsweeper Policy Editor, you give it a meaningful names to help you identify the item in the details pane. You can also change the name of an existing item.

An item name can contain up to 60 characters. The first character of the name must be alphanumeric. The remaining characters can be alphanumeric, double-byte, or single-byte Japanese characters.

For details on naming or renaming items in the MIMEsweeper Policy Editor, see the help.

Permitted characters

Table J-1 lists the special characters that you can use in MIMEsweeper item names.

Table J-1: Permitted characters

Character	Name
&	ampersand
<	angle bracket (left)
>	angle bracket (right)
‘	apostrophe
*	asterisk
@	at sign
{	brace (left)
}	brace (right)
^	caret
:	colon
$	dollar
€	euro
#	hash
-	hyphen
¬	not
(	parenthesis (left)
)	parenthesis (right)
%	percent
.	period
+	plus
£	pound

Table J-1: Permitted characters

Character	Name
?	question mark
	space
[	square bracket (left)
]	square bracket (right)
~	tilde

Prohibited characters

Table J-2 lists the special characters that you cannot use in MIMEsweeper item names

Table J-2: Prohibited characters

Character	Name
\	backslash
,	comma
=	equal sign
!	exclamation mark
/	forward slash
“	quotation mark
;	semicolon
_	underscore
|	vertical bar

Part IV

Glossary

Glossary

Acceptable A category of an image in the preclassification database. The term also applies to images that have not been categorized as unacceptable.

Access Control List (ACL) A list that specifies the access to an object granted to particular users and groups. Different levels of access can be granted to different users or groups.

Action A policy element that determines what to do with an email that has been classified. See also *Classification*.

Address list A collection of email addresses used to associate messages with scenarios.

Alert A notification message issued to a predefined list of users and computers. Used in MIMEsweeper to notify administrators of the detection of specific data types within an email.

Alerter A mechanism that issues system alerts. MIMEsweeper can be configured to use an Administrative Alerter, and SMTP Alerter, or an SNMP Alerter.

Alias In DNS, a name that can be mapped to a host name, using the CNAME record in DNS See also *DNS*.
(2.) In MIMEsweeper, a mechanism for re-writing the recipient address(es) of a message.

Anti-virus (AV) tool A program to detect computer viruses. Some AV tools can also remove viruses.

Application event log A Windows log file that records events signalled by applications. Applications may write messages to this log on start-up or shutdown to report information, failures, and warnings. This log is viewed using the Event Viewer program.

Audit Consolidator Service The service that runs on each Policy Server to consolidate audit data and pass it to the Audit Disposer Service.

Audit database Holds the audit data collected by the system as it processes messages. This data is used to generate reports in the Report Center.

Audit Disposer service The service that collects audit data from each policy server and commits it to the Audit database.

Audit Server The PC that holds the audit database.

Categorize The process of applying a category of acceptable or unacceptable to an image in the preclassification database.

Category A term that describes if an image is acceptable or unacceptable in IMAGEmanager's preclassification database.

Classification A policy element that defines what to do with items that have been trapped by scenarios. Classifications contain actions that specify what to do with detected messages. See also *Action* and *Scenario*.

Clean One of the default MIMEsweeper classifications, used for delivering email messages to their intended recipients. See also *Classification*.

Clean network The section of the network that is inside the firewall.

Cleaned One of the default MIMEsweeper classifications, normally used for objects from which a threat, such as a virus, has been removed. By default, objects classified as Cleaned are delivered to their intended recipients. See also *Classification*.

Confidence level A setting that influences the proportion of features that must match values in the database if MIMEsweeper IMAGEmanager is to categorize an image as unacceptable.

Container A file, for example a zip file that can contain one or more files. These files may be in encoded form (compressed or encrypted), plain text or binary.

Content security policy Defines the email processing rules to enforce. It includes criteria for policy routing, email processing, and auditing and reporting. See also *Deployment policy* and *Routing and relay policy*.

Decryption The process of using a private key to decode data, for example a message, encrypted using the corresponding public key.

Delivery service The MIMEsweeper for SMTP service that delivers e-mail messages from the MIMEsweeper host to the next host. It uses DNS or MIMEsweeper routing information to determine where to send each email message after processing. See also *DNS*, *Receiver service* and *Security service.*

Deployment policy Defines the way MIMEsweeper for SMTP is implemented in an email network. It includes criteria for network architecture, internet connection method, responsibilities for policy configuration and system management, message throughput, and resilience. See also *Content security policy* and *Routing and relay policy*.

Digital signature Data added to an email to authenticate the sender and the message data. That is, a digital signature verifies a sender's identity, and that the message has not been tampered with since being signed.

Dirty in One of the default classifications, normally used to quarantine incoming email messages that are identified as potential security threats. See also *Classification*.

Dirty network The section of the network between the firewall and the router. This section is not protected by the firewall.

Dirty out One of the default classifications, normally used to quarantine outgoing email messages that are identified as potential security threats. See also *Classification*.

DMZ DeMilitarized Zone. A computer host or small network located between a clean network and a network either side of a firewall, between which there is no direct route. The DMZ is used to prevent outside users gaining access to the server. See also *Clean network* and *Dirty network*.

DNS Domain Name System. A system that converts host names to IP addresses, using a distributed database. This is the mechanism used by the Internet and most TCP/IP networks to resolve host names to IP addresses and vice versa. DNS provides a number of resolutions. The most important are the records used by SMTP to allow the transfer of mail. See also *MX record*.

Domain name The officially registered name by which an organization is referred to on the Internet.

DSN Data Source Name. A name used by *ODBC* to connect to an ODBC-enabled database.
2. Delivery Status Notification. A notification issued by an email gateway to advise that it has failed to deliver an e-mail message.

Email policy Policy regarding the use of email by members of an organization.

Encryption The process of converting data in such a way that makes it unreadable by anyone without the key to decrypt it. See also *Decryption*.

ESMTP Extended Simple Mail Transport Protocol. Extensions include Delivery Status Notifications and size constraints. See also *SMTP*.

Event log See *Application event log*.

Expression A keyword or phrase MIMEsweeper searches for in an e-mail message during a text analysis search.

Face Detection An option of the MIMEsweeper IMAGEmanager license that improves the correct identification of images that contain facial portraits.

Fail-safe system A computer system designed to continue operating without loss of or damage to programs and data when part of the system breaks down or seriously malfunctions.

Failover The process of taking processes from a failed node and reassigning the process to an operational node on the cluster.

False positive A term that describes an acceptable image that IMAGEmanager has categorized as unacceptable.

(2.) A legitimate message that SpamLogic has incorrectly classified as spam.

Fingerprint Unique feature of a file, by which it can be identified. It can be based on the file's content or, if this is not possible, by an attribute such as the file extension. Fingerprints are used to determine whether files should be blocked or allowed.

Firewall An IP gateway that blocks unauthorized access to and from your network.

Gateway An SMTP mail system that is prepared to take and process mail for other systems or domains.

Host name A DNS name that maps to a host's IP address. This is the unique name by which a computer is known on a network. See also *DNS*.

HTML HyperText Markup Language. The mechanism used to define the content and appearance of information displayed by a web browser.

IMAGEmanager A MIMEsweeper component that enables MIMEsweeper for SMTP to analyze images attached to email messages or embedded in email attachments for inappropriate content such as nudity or pornography.

IMAGEmanager scenario A type of scenario for configuring MIMEsweeper IMAGEmanager.

Incoming mail Email messages destined for the domain of the receiving *SMTP gateway*.

Inform messages Messages generated by MIMEsweeper from configurable subject and body text items, and sent to users defined by the policy.

Inheritance The means by which scenarios are effective not only in their own folders but also in folders at lower levels in the hierarchy. See also *Scenario*.

Initial Policy Wizard Activated immediately after installation. Configures an initial content security policy that is used when the system is first started.

IP address Internet Protocol address. A 32-bit number used to identify each machine on the network.

ISP Internet Service Provider. A company that provides end clients with access to the Internet and related services.

JPEG (also JPG) Abbreviation for Joint Photographic (Experts) Group format, pronounced "jay-peg". JPEG is the standard Internet format for photo realistic images. The JPEG format compresses image data to a color depth of 16 777216 colors (24 bits per pixel).

KNN An algorithm that returns an image classification based on the similarity of the features of that image to a preclassified database of image features. The value of K is the number of nearest feature-matches that are analyzed from the database.

LDAP Lightweight Directory Access Protocol. A protocol for accessing online directory services.

Loopback address A special IP address (`127.0.0.1`) that is designated for the software loopback interface of a machine. The loopback interface has no hardware associated with it, and it is not physically connected to a network.

MAPS Mail Abuse Prevention System. An organization whose goal is to prevent the abuse of Internet email.

Message area An area on disk used for holding parked or quarantined email messages. See also *Parking area* and *Quarantine area.*

Message Center The area within MIMEsweeper Manager where you monitor and manage email messages that have been blocked, retained for review or queued for processing. You also use the Message Center to access message tracking.

Message ID A unique identifier assigned to each message, used for tracking the progress of an email.

Message splitting The process by which the MIMEsweeper Security service splits a multi-recipient email message into copies. This enables the appropriate policy to be applied to a message depending on the recipient. See also *Security service.*

Message tracking The functionality that provides transaction-level reporting for messages that have been processed by MIMEsweeper for SMTP. Using message tracking, you can determine the complete lifecycle of a message, for example to determine whether messages have been delivered or blocked by the system. See Message tracking database

Message tracking database Contains information about the status of messages as they pass through the MIMEsweeper system. This data can be queried using the Track Message page. It is also used to generate point-to-point summary reports.

Message Tracking server The server that collects message tracking data from other components in the deployment and writes the data to the message tracking database.

MIME Multipurpose Internet Mail Extensions. Internet email encapsulation convention. Ref. RFC 2045/46/47/1521. A specification that allows non-text content, for example executable files and multimedia document formats to be transmitted via SMTP.

MIMEsweeper The family of products for the implementation of web, email, and intranet content security and policy management.

MIMEsweeper host In a stand-alone deployment, the computer on which the full MIMEsweeper for SMTP product is installed. This includes the Policy editor, MIMEsweeper Manager, and the message processing and delivery services.

MIMEsweeper Manager Web-based tool that provides access to Report Center, Security Center, Message Center and Systems Center where you can configure, control and monitor your system.

MMC Microsoft Management Console. A Microsoft Windows application that hosts administrative tools. Used to host the policy editor, where you create MIMEsweeper for SMTP security policies.

MX preference A number in the MX record indicating the relative priority of multiple host machines in a registered domain. Lower MX preference numbers take precedence over higher MX preference numbers.

MX record Mail eXchange record. A DNS resource record that identifies hosts that can handle SMTP mail for a particular domain. See also *DNS*.

Name resolution The process of mapping host names to IP addresses. See also *DNS* and *IP address*.

NetBIOS name A 16-character name used to identify a computer that is running the Network Basic Input Output System (NetBIOS) on a network.

Notification A type of MIMEsweeper action that issues information about email messages that have been classified. See also *Classification*.

ODBC Open Database Connectivity. A programming interface that enables applications to access data in a database management system that uses Structured Query Language (SQL) as a data access standard.

Open relay An SMTP host which allows unauthorized users to send mail, so anyone can route messages through the host. This could result in the host being used to transmit large volumes of spam messages. This can lead to a listing in web-based databases of spam hosts, such as the Realtime Black List maintained by the Mail Abuse Protection System. See also *RBL* and *MAPS*.

Operations database A database, managed by the PCS, that is used to store policy and configuration options for MIMEsweeper for SMTP.

Origin folder The scenario folder in which a particular scenario was created.

Outgoing mail Email destined for a domain other than that of the sending *SMTP gateway*.

Packet-based firewall A firewall that analyzes packets of data as they pass across its network interfaces.

Parking area A message area that has an associated release schedule that determines when email messages can automatically be released for delivery. Typically used to schedule the sending of large messages in off-peak times. See also *Message area*.

PCS See Primary Configuration Server.

PMM Personal Message Manager. Allows email system users to manage their own spam messages. Reduces the MIMEsweeper administration effort required. Each user receives a digest message from the MIMEsweeper system summarizing messages that have been put into their PMM area. If your license allows it, PMM users can also track messages that they send, or are sent to them.

PGP Pretty Good Privacy. A security package for signing and encrypting data.

Policy What MIMEsweeper uses to enforce content security. Policies are defined for particular routes, using scenarios and classifications. See also *Scenario* and *Classification*.

Policy Editor The MIMEsweeper for SMTP application used for configuring policies.

Policy Server Key component of a MIMEsweeper system. A server that processes emails and applies the content security policy. Normally deployed in the DMZ, a server hosts the Security, Receiver and Delivery services. You can have up to 8 Policy Servers connected to your PCS if your license allows.

Preclassification database A database of images that have been defined as either acceptable or unacceptable. Used to improve and speed up the image analysis process.

Primary Configuration Server Also known as PCS. Manages and co-ordinates the policy servers, distributes new and changed policies, holds the ‘master’ deployment configuration.

Private key The certificate used to authenticate, via signing, a message that you send, or decrypt a message sent to you encrypted using your public key.

Profanity list A list of expressions, phrases, and words that are considered unacceptable by the email policy. Messages containing these words are blocked.

Proximity In text analysis, a measure of how near two expressions joined by the .NEAR. expression operator must be for the message to be detected.

Proxy-based firewall A firewall that provides a series of application proxies to which hosts on either side of the firewall connect. The connecting hosts are responsible for transferring the data.

Quarantine area A configurable directory for holding messages that contravene the security policy. See also *Message area*.

RAID Redundant Array of Independent Disks. A category of disk drives that use a combination of two or more drives to provide fault tolerance and performance.

RBL Realtime Black List. The Mail Abuse Protection System (*MAPS*) real-time blacklist is an up-to-date list of relays and sites that are known to have been responsible for the widespread distribution of unsolicited email.

Receiver service The MIMEsweeper service that receives all incoming and outgoing email messages and passes them to the Security service for processing. The Security service then passes the message to the Delivery service for onward delivery. See also *Delivery service* and *Security service*.

Recursive disassembly The process by which MIMEsweeper breaks down compressed or embedded data to its component parts. If a component represents an archive, an encoding, or a compression, MIMEsweeper processes the component further until each component is recognized as a raw data type; for example, bitmap, binary file, text file, or executable file. This enables MIMEsweeper to process the basic components of an object, thus ensuring, for example, that threats hidden within layers of data are identified and dealt with according to policy.

Regular expression A facility for specifying text analysis rules.

Report Center Generates and views reports based on information collected in the MIMEsweeper Manager both from an audit database and from a message tracking database.

Resilience The ability of the MIMEsweeper system to continue operating without loss of or damage to programs and data when other systems it depends on (such as the network or a database) break down or seriously malfunction.

RFC 821 The original specification for the format of SMTP messages. It lists the basic constructs for headers and message presentation. Extensions to SMTP are specified in RFC1651-1653.

Round-robin A sequential, cyclical allocation of resources to more than one process or device.

Route The sender and recipients combination in an email, which MIMEsweeper uses to determine which policy to apply.

Routing and relay policy Defines the SMTP security rules MIMEsweeper is to enforce. It includes criteria for hosts MIMEsweeper is allowed to accept email from, hosts allowed to relay email through MIMEsweeper, number of recipients permitted, and size of email messages permitted.

S/MIME Secure Multi-purpose Internet Mail Extensions. A secure version of *MIME*. S/MIME is the industry standard for *Encryption* of email messages between the same and different types of email systems. S/MIME can use a range of different signature and encryption algorithms. Also see *PGP*.

Scenario A MIMEsweeper policy element that identifies a particular policy function, such as the detection of specified text within an object or potential threats within data.

Security Center The MIMEsweeper Manager interface that you use to secure the machines in your deployment to protect them and the rest of your network from unauthorized access.

Security service The MIMEsweeper for SMTP service that analyzes email messages and applies the appropriate configured policies. See also *Delivery service* and *Receiver service*.

Separator A character used in text analysis as word separators.

SMTP Simple Mail Transfer Protocol. Transmission protocol to *RFC 821* for receiving and sending email. SMTP belongs to the *TCP/IP* family of protocols. SMTP messages consist of a head containing at least a sender and recipient ID, and the actual message. The message is forwarded from the sender by an email program—the User Agent (UA)—to the network's own mail server—the Message Transfer Agent (MTA)—which, in turn, forwards the message to other MTAs along the transmission path according to the "Store and Forward" principle, until the message reaches its recipient. SMTP works with 7-bit ASCII, which means that accented and extended characters cannot be represented and unauthorized access cannot be prevented. ESMTP, in contrast, uses 8 bits for message transmission.

SMTP gateway A computer that connects networks using different communications protocols so that information can be passed from one to the other. An SMTP gateway both transfers information and converts it to a form compatible with the SMTP protocol used by the receiving network.

SMTPDS MIMEsweeper for SMTP *Delivery service*.

SMTPRS MIMEsweeper for SMTP *Receiver service*.

SMTPSS MIMEsweeper for SMTP *Security service*.

Snap-in The basic component of an MMC console. MIMEsweeper uses one snap-in—the Policy Editor snap-in.

SNMP Simple Network Management Protocol. A protocol for communication with devices connected to a TCP/IP network. The SNMP service allows a server to report its current status to a SNMP management system on a TCP/IP network.

Spam A term given to unsolicited or junk mail that is often sent simultaneously to many recipients (for example mailing lists to advertise goods or services). Some spam originators may also use remote servers to redistribute their messages, a technique known as mail relating.

Spoofing A method whereby the source address of a message is altered in such a way that the message appears to come from some source other than the actual sender.

Stand alone deployment The deployment where the full MIMEsweeper for SMTP system is deployed on a single MIMEsweeper host and, optionally, MIMEsweeper Manager is deployed on one or more remote workstations.

System Health Functionality of the MIMEsweeper Manager that gathers data from various parts of MIMEsweeper for SMTP system to provide an overview of the health of the system.

System Center Manages the MIMEsweeper Policy Servers and the deployment settings.

TCP/IP Transmission Control Protocol/Internet Protocol. A set of communications protocols.

Text analysis A method of searching an object, for example a message or its attachments, for specified words and phrases, as a means of determining if the object contravenes the security policy.

Throughput A measure of the message processing rate through the MIMEsweeper system.

Token A means of specifying a variable whose value is derived during the processing of an object, for example text to be included in an inform message.

Tracking service Responsible for collating tracking data from the Policy Server and writing it to the message tracking database, and for querying tracking data.

Transparent proxy-based firewall A firewall that appears to clients as a packet firewall and that intercepts packets, but behaves like a proxy-based firewall.

UNC Universal Naming Convention. A method of specifying resources on remote machines that enables the files on one computer to have the same path name when accessed by any of the other computers on the network. A UNC name takes the form \\machine\share\path.

Unacceptable A category that indicates that an IMAGEmanager scenario detects the image. Unless the image is in the preclassification database, the IMAGEmanager has to analyze the image in order to categorize it.

UUE Unix to Unix Encoding format. Enables binary data to be converted to a text-based system for transfer over the Internet.

UUEncode Unix to Unix Encoding. Popular encoding technique.

Virus A virus is program code that can be transmitted from one file or object to another. Viruses are defined by their ability to reproduce themselves. Viruses can infect other programs by copying themselves into another file or the boot sector of a disk drive.

Web server Hosts the web applications providing system management centers and management of messages. The users on the email network are provided with access to their spam message areas.

Index