



MIMESweeperTM for SMTP

5.3

Getting Started Guide

Revision 5.3

Revision 5.3, June 2008

Published by Clearswift Ltd.

© 1995—2008 Clearswift Ltd.

All rights reserved.

The materials contained herein are the sole property of Clearswift Ltd. No part of this publication may be reproduced or disseminated or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise stored in any retrievable system or otherwise used in any manner whatsoever, in part or in whole, without the express permission of 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.

The Clearswift Logo and Clearswift product names including MIMESweeper™, MAILsweeper™, e-Sweeper™, IMAGEmanager™, REMOTEmanager™, SECRETsweeper™, ENTERPRISEsuite™, ClearPoint™, ClearSecure™, ClearEdge™, ClearBase™, ClearSurf™, DeepSecure™, Bastion™ II, X.400 Filter™, FlashPoint™, ClearDetect™, ClearSupport™, ClearLearning™, SpamLogic™ are trademarks or registered trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England. 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.

Copyright © 1997-2008 Kaspersky Labs. 10 Geroyev Panfilovtsev St., 125365 - Moscow, Russian Federation. The Kaspersky Logo and Kaspersky product names are trademarks of Kaspersky Labs.

Licensed under US Patent No. 5,623,600

Protected by UK Patent 2,366,706



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

About the Getting Started Guide	iii
Related documentation	-iv

CHAPTER 1 Introduction

Overview	1-2
Policy types	1-2
Developing policies	1-7
Key components	1-7

CHAPTER 2 Deployment Planning

Overview	2-2
General deployment information	2-3
Deploying the MIMESweeper for SMTP host with a firewall	2-7
Deployment options	2-12
Sample deployment models	2-17

CHAPTER 3 Installation

Overview	3-3
Preparing the database environment	3-3
Installation options	3-9
Preparing to install MIMESweeper for SMTP	3-10
Installation Routes	3-12
Post installation tasks	3-28
Subsequent installations	3-29
Upgrading to a newer version	3-32
Licensing MIMESweeper for SMTP	3-37

CHAPTER 4 Getting Started with MIMESweeper Policies

Overview	4-2
Creating a policy with the Initial Policy Wizard	4-3

Contents

CHAPTER 5 Security

Overview	5-2
Securing the environment	5-2
Securing the MIMESweeper Manager application server	5-5
Securing database communications between machines	5-6
Securing routing and relay through an SMTP Mail Policy Server	5-8
Securing access to MIMESweeper for SMTP	5-10

CHAPTER 6 System Startup and Quicktour

Overview	6-2
Opening and closing the console	6-3
Touring the MIMESweeper Policy Editor user interface	6-4
MIMESweeper Manager	6-17
Personal Message Manager	6-19

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.

About the 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 *MIMESweeper for SMTP Reference* and the online 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.
<i>This type</i>	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.
<u>Underline</u>	A URL for a site on the World Wide Web.
	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 this guide 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

The MIMESweeper for SMTP product is supplied with various documents. The Getting Started Guide is intended to help you to start using MIMESweeper in a relatively short period of time. In addition to this guide the document suite contains:

- **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.

- **Reference**

The *MIMESweeper for SMTP 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.

- **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.

- **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>.

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	1-2
Policy types	1-2
Deployment policy	1-3
Routing and relay policy	1-3
Content security policy	1-4
Policy routing	1-5
Email processing	1-5
Auditing and reporting	1-6
Developing policies	1-7
Key components	1-7
MIMESweeper Policy Editor user interface	1-8
MIMESweeper Manager user interface	1-8
MIMESweeper services	1-8
MIMESweeper folders	1-10
Message areas	1-10
Scenarios	1-11
Classifications and actions	1-12
Personal Message Manager	1-12

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 guide 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**
A deployment policy defines the way you want to implement MIMESweeper for SMTP in your email network
- **Routing and relay policy**
A routing and relay policy defines the SMTP security rules you want MIMESweeper for SMTP to enforce.
- **Content security policy**
A content security policy defines the email processing rules you want MIMESweeper for SMTP to enforce.

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 whole organization or for 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
Installing MIMESweeper for SMTP	Chapter 3

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.

Introduction

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 of the <i>MIMESweeper for SMTP Reference</i>
Testing configured routes	Appendix I

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 of the <i>MIMESweeper for SMTP Reference</i>
Configuring reporting elements of content security policies with the Report Center	Chapter 11 of the <i>MIMESweeper for SMTP Reference</i>
Housekeeping tasks	Appendix E of the <i>MIMESweeper for SMTP Reference</i>
Testing content security policy elements	Appendix H of the <i>MIMESweeper for SMTP Reference</i>

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.

Introduction

- 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 message tracking reports.

You can configure the following types of reports:

- Top Senders
- Top Recipients
- Top Threats
- Top Format Types
- Top Classifications
- Policy Usage Reports

- 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 already has 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 services
- MIMESweeper folders
- 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

This is where you create and maintain your organization's email policies.

The user interface is based on a Microsoft Management Console (MMC) snap-in which 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, System Center, Report Center, and Security Center in a web browser window.

For further information about	See
The MIMESweeper Policy Editor user interface	Chapter 6
The MIMESweeper Manager user interface	Chapter 6
Configuring content security policies	Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>
Configuring routing and relay policies	Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>

MIMESweeper services

The MIMESweeper services process 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**
The Audit Consolidator service takes all the audit data generated by the system, consolidates it into a format suitable for the audit database, and passes it to the Audit Disposer Service.

- **Audit Disposer service**

This runs on the Audit Disposer server. The Audit Disposer Service commits consolidated audit data to the audit database. The audit database holds this consolidated version of the audit data, which is used to create reports.

- **Tracking service**

This runs on the Message Tracking server. The Tracking service is responsible for collating tracking data and writing it to the message tracking database.

Figure 1-1 illustrates how these MIMESweeper services process messages coming through the Internet and local domains.

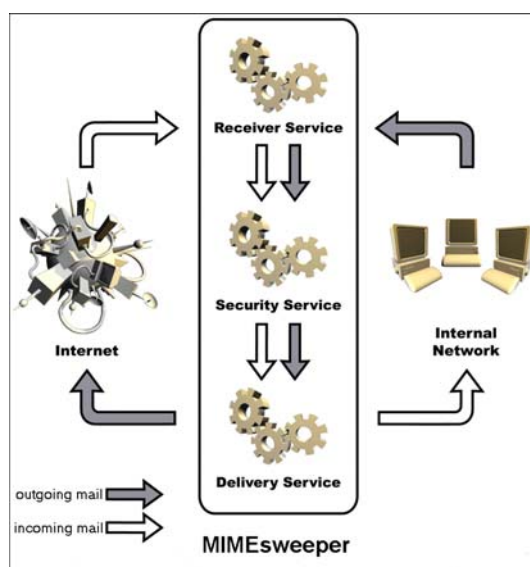


Figure 1-1: MIMESweeper services

For further information about	See
Starting and stopping the MIMESweeper services	Chapter 8 of the <i>MIMESweeper for SMTP Reference</i>
How the MIMESweeper services process messages	Appendix G of the <i>MIMESweeper for SMTP Reference</i>

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 F of the <i>MIMESweeper for SMTP Reference</i>
The location and contents of MIMESweeper folders	Appendix F of the <i>MIMESweeper for SMTP Reference</i>

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 called a message area. You specify a message area when you define a classification (for further information, see *Classifications and actions* on page 1-12).

Emails in message areas are held until they are either:

- 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.
- Automatically released for delivery during a defined release period.
- Automatically deleted after a defined period of.

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 9 of the <i>MIMESweeper for SMTP Reference</i>
How MIMESweeper uses message areas	Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>
The location of message area folder on the hard disk	Appendix F of the <i>MIMESweeper for SMTP Reference</i>

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 where 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
Configuring scenario folders	Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>
MIMESweeper scenario types	Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>
<i>MIMESweeper for SMTP References</i> for text analysis scenario types	Chapter 5 of the <i>MIMESweeper for SMTP Reference</i>

Classifications and actions

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
Configuring classifications and actions	Chapter 3 of the <i>MIMESweeper for SMTP Reference</i>
MIMESweeper classification and action types	Chapter 3 of the <i>MIMESweeper for SMTP Reference</i>
Tokens that can be used with actions	Appendix I of the <i>MIMESweeper for SMTP Reference</i>

Personal Message Manager

To help cope with the increasing amount of spam that 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 classed as spam. Users who have access to PMM receive a digest message from the MIMESweeper system notifying them of the messages that have been put into their PMM area. Users can delete or release these messages as required.

PMM also provides functionality for tracking messages. Users can view tracking records of messages either sent to them or messages that they have sent. For example, you can use this functionality to determine when a message that you sent was delivered.

For further information about	See
Configuring Personal Message Manager	Chapter 10 of the <i>MIMESweeper for SMTP Reference</i>
Using Personal Message Manager	Chapter 10 of the <i>MIMESweeper for SMTP Reference</i>

CHAPTER 2

Deployment Planning

This chapter describes considerations for planning a deployment of MIMESweeper for SMTP on your network.

Overview	2-2
General deployment information	2-3
Edge Server integration	2-3
Routing messages between your organization and the Internet	2-3
Routing messages through MIMESweeper for SMTP	2-5
Securing the MIMESweeper for SMTP servers	2-6
Deploying the MIMESweeper for SMTP host with a firewall	2-7
On the demilitarized zone network	2-8
Firewall port configurations	2-10
Additional configurations	2-11
Deployment options	2-12
General recommendations	2-13
Machines and connections	2-14
MIMESweeper for SMTP system description	2-15
Port configuration	2-16
Sample deployment models	2-17
Machine summary	2-17
Dual site machine summary	2-18
Key to illustrations	2-19
Single host deployment	2-20
Sample two host deployment	2-22
Sample multiple host deployment	2-24
Sample dual site deployment	2-26

Overview

When you are planning how to deploy MIMESweeper for SMTP, the deployment model you choose depends on your organization's network architecture, Internet connection method, and email management preferences.

MIMESweeper for SMTP is typically introduced into an existing network architecture that already has communications established between a host machine in the organization and the Internet. For details on how email messages are routed before you deploy MIMESweeper for SMTP, see *Routing messages between your organization and the Internet* on page 2-3.

Routes determine where the Delivery service directs incoming and outgoing mail. When you introduce MIMESweeper for SMTP into your network architecture, you must configure how MIMESweeper is to deliver mail between your organization's host machine and the Internet. Depending on your network architecture, you may need to configure other machines (such as a firewall) to route messages through MIMESweeper for SMTP.

This key concept is described in *Routing messages through MIMESweeper for SMTP* on page 2-5.

A key aspect of ensuring the safety of your network after introducing MIMESweeper for SMTP is discussed in *Securing the MIMESweeper for SMTP servers* on page 2-6.

The remaining sections in this chapter describe options for where in your network layout you can deploy MIMESweeper for SMTP components. The flexibility of MIMESweeper enables you to either deploy the complete MIMESweeper system onto a single machine, or distribute components to multiple machines, so that specific machines can perform distinct tasks, and to spread the processing load.

General deployment information

This section discusses some of the general aspects of MIMESweeper for SMTP deployment.

Edge Server integration

The MIMESweeper Edge Server acts as an email firewall for your MIMESweeper for SMTP installation. You can use an Edge Server to detect and block spam messages, messages with dangerous file type attachments, and messages that contain viruses.

An Edge Server or servers are typically installed in front of your MIMESweeper for SMTP installation. For information on deploying a MIMESweeper Edge Server, see the *MIMESweeper Edge Server Deployment Guide*.

Routing messages between your organization and the Internet

Each organization that sends and receives email messages through the Internet has one or more host machines designated to handle its email. Figure 2-1 illustrates a basic network architecture with an organization's email host machine and the Internet.

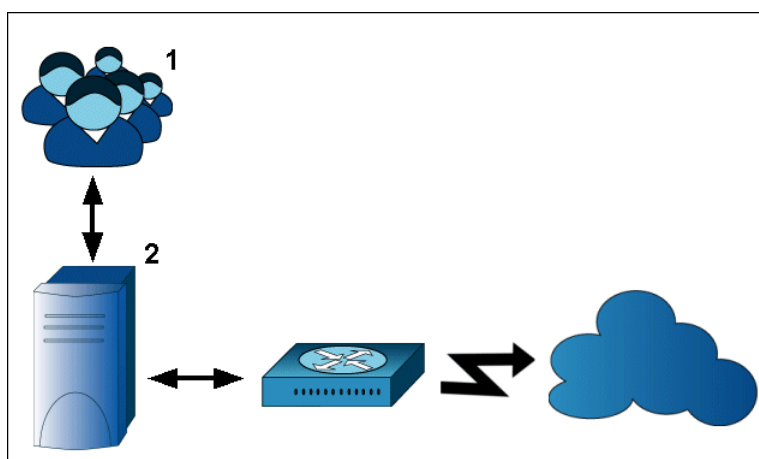


Figure 2-1: Basic email network architecture

Email messages from the user network (1) are routed between an organization's host machine (2) and the Internet using the *Domain Name System (DNS)*. The DNS is a distributed database system for mapping the *host name* of a computer on a TCP/IP network to its numeric *Internet Protocol (IP) address*:

Host name The *Fully Qualified Domain Name (FQDN)*, for example:
`sales.your-companyname-here.com`, for the host machine designated as an organization's email server. The host name comprises the host name of your computer and the domain name.

IP address A numerical address, such as 164.17.0.4, which uniquely identifies the host machine. The IP address is composed of four fields, but has three elements. The first element of the address identifies a class, the second element identifies the specific network, and the third element identifies the individual host machine on the network.

The address class determines which of the four fields make up which element of the address. For example, in a class B address, the first two fields identify the network address, and the last two fields identify the host address.

Host machines with the same network address can communicate with each other without a router. Host machines that have different network addresses must use a router to communicate with each other.

Each domain registered in the DNS administers its own name server. Each name server stores host name to IP address mapping tables and *MX records* identifying the relative priority of host machines in its registered domain. This numerical priority is called an *MX preference*, where lower MX preference values take precedence over higher ones.

Typically, MX preference values can be utilized to give priority to your primary mail server (for example: value = 0). A secondary mail server, used for backup support for your primary mail server, could be given a lower priority (for example: value = 10).

When a host machine receives an email message, it can query a DNS server to identify a specific host machine designated to receive messages for the domain specified in the email address. DNS queries can take the following forms:

- **Host name resolution**
Request a mapping from a host name to an IP address.
- **Reverse address lookup**
Request a mapping from an IP address to a host name.
- **MX lookup**
Request a list of host name to IP address mappings sorted in MX preference order (from the lowest to highest value) if there is more than one host machine for a specified domain name.

The information stored on one name server is available to other name servers in the DNS, so if your DNS server does not have the requested information, it forwards the query to other DNS servers on the system.

Routing messages through MIMESweeper for SMTP

When you introduce MIMESweeper for SMTP into your network architecture, you must configure how it delivers mail between your organization's host machine and the Internet.

To do this, you configure a number of routes to specify where the Delivery service is to direct email messages for your domain (*incoming mail*) received from the Internet and where it is to direct email messages for domains other than your own (*outgoing mail*). Depending on your network architecture, you may need to configure other machines (such as a firewall) to route messages through MIMESweeper for SMTP for inbound or an outbound SMTP Relay to send outbound. If you do not define a specific route, MIMESweeper for SMTP automatically uses the DNS to direct mail straight to the destination.



When MIMESweeper for SMTP receives a message for your local domain address, it queries the DNS for a host and may have its own domain name returned. To prevent this loop, either define a specific route or use a different DNS server.

After installing MIMESweeper for SMTP, you can provide the following mail routing address information in the Initial Policy Wizard. If you are upgrading you can choose to inherit your existing configuration.

- **Default domain name**

The domain name for your organization, for example, `your-companyname-here.com`. This is used to create routing information for your local domain.

- **Host machine for incoming mail**

The host name or the IP address of the host machine on your domain used for forwarding incoming mail. Depending on your network architecture, the host machine for incoming mail can be:

- An SMTP gateway
- A proxy-based firewall
- One of a chain of mail servers

- **Host machine for outgoing mail**

The host name or the IP address of the host machine on your domain used for forwarding outgoing mail. Depending on your network architecture, the host machine for outgoing mail can be:

- A proxy-based firewall
- An ISP server
- A dedicated mail server to direct mail (Smarthost)

If you enter these details in the Initial Policy Wizard, MIMESweeper for SMTP is automatically configured to forward incoming and outgoing mail to these machines on the specified default domain.

You must manually configure incoming and outgoing mail routes in MIMESweeper for SMTP if:

- You did not enter these details in the Initial Policy Wizard.
- You want to change the details you entered in the Initial Policy Wizard.
- Your organization has more than one domain.

For each domain, you can configure the following types of manual routes in MIMESweeper for SMTP:

- **Forced route**

This route is always used instead of referring to the DNS for delivering email messages received for the specified domain.

- **Additional route**

This route information is merged with the list of hosts returned by the DNS when there are multiple hosts for the specified domain. The Delivery service then delivers the email message to the host with the lowest MX preference value.

- **Default route**

This route is used if a query to the DNS server fails for any reason.

You can define one or more of each type of manual route. You configure manual routes in the **Routing** item under the **SMTP Relay** folder of the MIMESweeper Policy Editor. For information about configuring routes, see Chapter 6 of the *MIMESweeper for SMTP Reference*.

Securing the MIMESweeper for SMTP servers

After deploying a MIMESweeper for SMTP host on your network, you must secure the host machine to protect it from unauthorized access and to prevent it from providing access to the rest of your network.

Securing the MIMESweeper for SMTP host machine involves:

- Ensuring the physical security of the MIMESweeper for SMTP host machine. For example, locating it in a secured room.
- Disabling IP forwarding to prevent the MIMESweeper for SMTP host from acting as a router. For information, see your Windows documentation.
- Disabling the WINS client (TCP/IP) binding to the server service to prevent remote access to shared resources over TCP/IP. For information, see your Windows documentation.



If TCP/IP is the only network protocol used, disabling this binding may affect other network operations, such as logging in to Windows domains.

- Considering security settings for other elements of your environment, such as the Windows Registry, RPC access and disk access.

- Setting specific access rights on the Windows folders containing the MIMESweeper for SMTP configuration files and on the cache to prevent unauthorized access.

Deploying the MIMESweeper for SMTP host with a firewall

You must decide on which side of your firewall to deploy MIMESweeper for SMTP.



You are recommended **not** to install MIMESweeper for SMTP on the firewall machine itself. However you should install on the Demilitarized Zone (DMZ) network within the firewall.

After you introduce MIMESweeper for SMTP into your network, you then need to configure incoming and outgoing mail routing on the following:

- SMTP gateway
- MIMESweeper for SMTP host
- DNS server
- Firewall

The configuration depends upon the type of firewall in place:

- **Transparent proxy-based or packet-based firewall**

You must configure the firewall to allow MIMESweeper for SMTP to pass mail through it. You do not need to configure MIMESweeper for SMTP to pass mail through the firewall.

- **Proxy-based firewall**

You must configure MIMESweeper for SMTP and the firewall to pass mail to one another.

On the demilitarized zone network

You can deploy MIMESweeper for SMTP on a separate DMZ network within the firewall. Organizations typically deploy machines that are internal to the organization but accessed by others outside of the organization, such as web servers, on the DMZ. This deployment option for MIMESweeper for SMTP is shown in the illustration Figure 2-2.

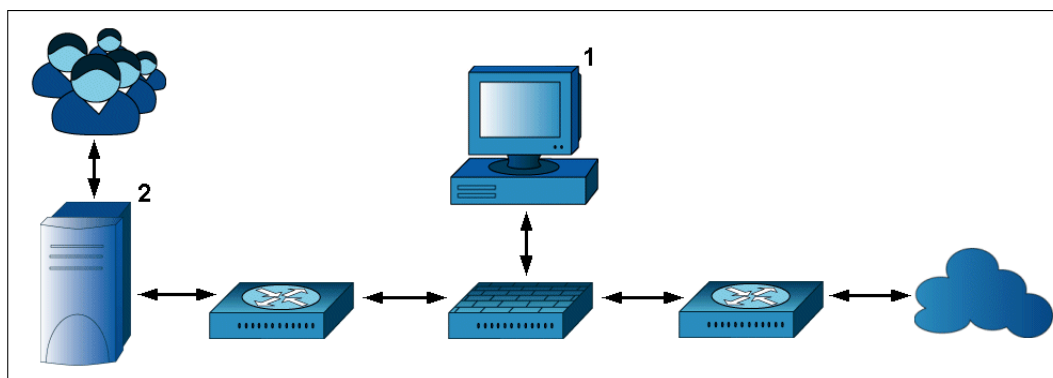


Figure 2-2: Single machine deployment - on the DMZ network

In this deployment model, the firewall must pass incoming mail received from the Internet (or router) to the MIMESweeper for SMTP host (1). The MIMESweeper for SMTP host then must pass the incoming mail back to the firewall to forward to the SMTP gateway machine (2). Conversely, the firewall must pass outgoing mail received from the SMTP gateway machine to the MIMESweeper for SMTP host. The MIMESweeper for SMTP host then must pass the outgoing mail back to the firewall to forward to the Internet (or router).

To deploy MIMESweeper for SMTP on the DMZ network:

1. Configure the SMTP gateway or the firewall to forward outgoing mail to the MIMESweeper for SMTP host:
 - For a **packet-based** or **transparent proxy-based** firewall configure the SMTP gateway to forward outgoing mail to the MIMESweeper for SMTP host.
For details on how to do this, refer to your network administrator or the documentation for your gateway.
 - For a **proxy-based** firewall, change routing on the firewall to send outgoing mail to the MIMESweeper for SMTP host.
For details about how to do this, refer to your firewall administrator or the documentation for your firewall.

2. For a **proxy-based** firewall, ensure that the MIMESweeper for SMTP host has a forced route configured to forward outgoing mail back to the firewall (see *Routing messages through MIMESweeper for SMTP* on page 2-5).
3. For a **packet-based** or **transparent proxy-based** firewall, ensure that the MIMESweeper for SMTP host has a forced route configured to forward all incoming mail for your domain or domains to the SMTP gateway (see *Routing messages through MIMESweeper for SMTP* on page 2-5).
4. For a **proxy-based** firewall, change routing on the firewall to send incoming mail for your domain or domains to the MIMESweeper for SMTP host.
For details on how to do this, refer to your firewall administrator or the documentation for your firewall.
5. For a **proxy-based** firewall, ensure that the MIMESweeper for SMTP host has a forced route configured to forward incoming mail to the firewall (see *Routing messages through MIMESweeper for SMTP* on page 2-5).
6. Secure the firewall so that:
 - Outgoing SMTP mail can come only from the MIMESweeper for SMTP host.
 - Incoming SMTP mail can go only to the MIMESweeper for SMTP host.For details on how to do this, refer to your firewall administrator or the documentation for your firewall.
7. For a **packet-based** or **transparent proxy-based** firewall, change the MX records on your DNS server from the address of your SMTP gateway to the address of the MIMESweeper for SMTP host.

Secure the MIMESweeper for SMTP host to protect it from unauthorized access and to prevent it from providing access to the rest of the network. For details on how to do this, see *Securing the MIMESweeper for SMTP servers* on page 2-6.

Firewall port configurations

For a single host deployment in the DMZ, the typical firewall configurations would be:

Table 2-1: Single host firewall configurations

Protocol	Usage	Default port	From	To
HTTP/S	Access managed service updates	80/443	MSW host	Internet
SMTP	SMTP message traffic	25	MSW host	Mail server
SMTP	SMTP message traffic	25	Mail server	MSW host
TCP/IP	No	No	No	No
DNS	Resolve names to IP addresses	53	MSW host	DNS server
LDAP	Address list lookups	389/3268/636	MSW host	LDAP server
ICMP	No	No	No	No
SNMP	Network management events	161	MSW host	SNMP manager

For a multi-host deployment with a Policy Server (PS) in the DMZ and the Primary Configuration Server (PCS) in the 'clean' network, the firewall configurations for the PS would be:

Table 2-2: Multi host deployment firewall configurations, Policy Server firewall ports

Protocol	Usage	Default port	From	To
HTTP/S	No	No	No	No
SMTP	SMTP message traffic	25	Policy Server	Mail server
SMTP	SMTP message traffic	25	Mail server	Policy Server
TCP/IP	Clearswift infrastructure service and operational data	23953	Policy Server	PCS
DNS	Resolve names to IP addresses	53	Policy Server	DNS server
LDAP	Address list lookups	389/3268/636	MIMESweeper host	LDAP server
ICMP	Ping	Not needed	Policy Server	PCS
SNMP	Network management events	161	Policy Server	SNMP manager
TCPIP	SpamLogic Signature Service	23956	Policy Server	PCS

For a multi-host deployment with a Policy Server (PS) in the DMZ and the Primary Configuration Server (PCS) in the 'clean' network, the firewall configurations for the PCS would be:

Table 2-3: Multi host deployment firewall configurations, PCS firewall ports

Protocol	Usage	Default port	From	To
HTTP/S	Access managed service updates and SpamLogic Signature Service	80/443	PCS	Internet
SMTP	No	No	No	No
TCP/IP	Clearswift infrastructure and operational data	23953	PCS	Policy Server
DNS	Resolve names to IP addresses	53	PCS	DNS server
LDAP	No	No	No	No
ICMP	Ping	Not needed	PCS	Policy Server
SNMP	No	No	No	No
TCP/IP	SpamLogic Signature	23956	PCS	Policy Server

Additional configurations

You need to open the following port to allow access through firewalls:

- Port 23956 on the Primary Server and all additional servers. This is required for receiving updates from the Primary Server, and for communicating with the SpamLogic Signatures detection engine.

If your PCS and Database server are separated by a firewall, you will need to open the port that your database server has been configured to listen on. This is port 1433 by default.

If you move a PCS from the DMZ into the Clean network, you must hold ports 23952 and 1433 open for the duration of the move operation. These ports do NOT need to be open at any other time and are normally closed.

Deployment options

The flexibility of the MIMESweeper system provides numerous deployment options.

For smaller organizations, or for evaluation purposes, the whole MIMESweeper for SMTP product can be installed and managed from a single machine. A single machine deployment is recommended for your initial installation. The Installation program is designed so that a single machine deployment is the most direct route through the Installation wizard.

Alternatively MIMESweeper for SMTP can be deployed across multiple machines, so that specific machines can perform certain tasks on different parts of the network. Several suggested deployment options are discussed later in the chapter, see *Sample deployment models* on page 2-17.

The initial installation of MIMESweeper for SMTP on a single machine creates a Primary Configuration Server (PCS). Subsequent installations of components on additional servers, create multiple machine deployments.



The PCS is the central server in a MIMESweeper for SMTP deployment and hosts the configuration for the MIMESweeper system. The PCS replicates changes to these files to other servers in the deployment, for example the Web Server, Audit/Message Tracking Server and Policy Servers. The PCS also hosts the Operations database which holds a summary of all held and queued messages, allowing fast searching and filtering of messages from the MIMESweeper Manager.

General recommendations



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.

- Install a Firewall in front of MIMESweeper for SMTP and the Internet.
 - Consider hosting the Primary Configuration Server (PCS), the web application, Audit Disposer service and the tracking server on a dedicated machine on the clean network, if you expect a high volume of PMM activity and reporting requirements.
 - Maintaining message tracking data is a resource-intensive operation. To get the best results from message tracking, consider using a dedicated database server running SQL Server software for message tracking. Due to the volume of data that message tracking generates, SQL Server 2005 Express is not suitable for live deployments.
 - PMM notifications are sent from the PCS and Web Server, not the Policy Servers. This fact has routing implications in a multiple machine deployment.
-

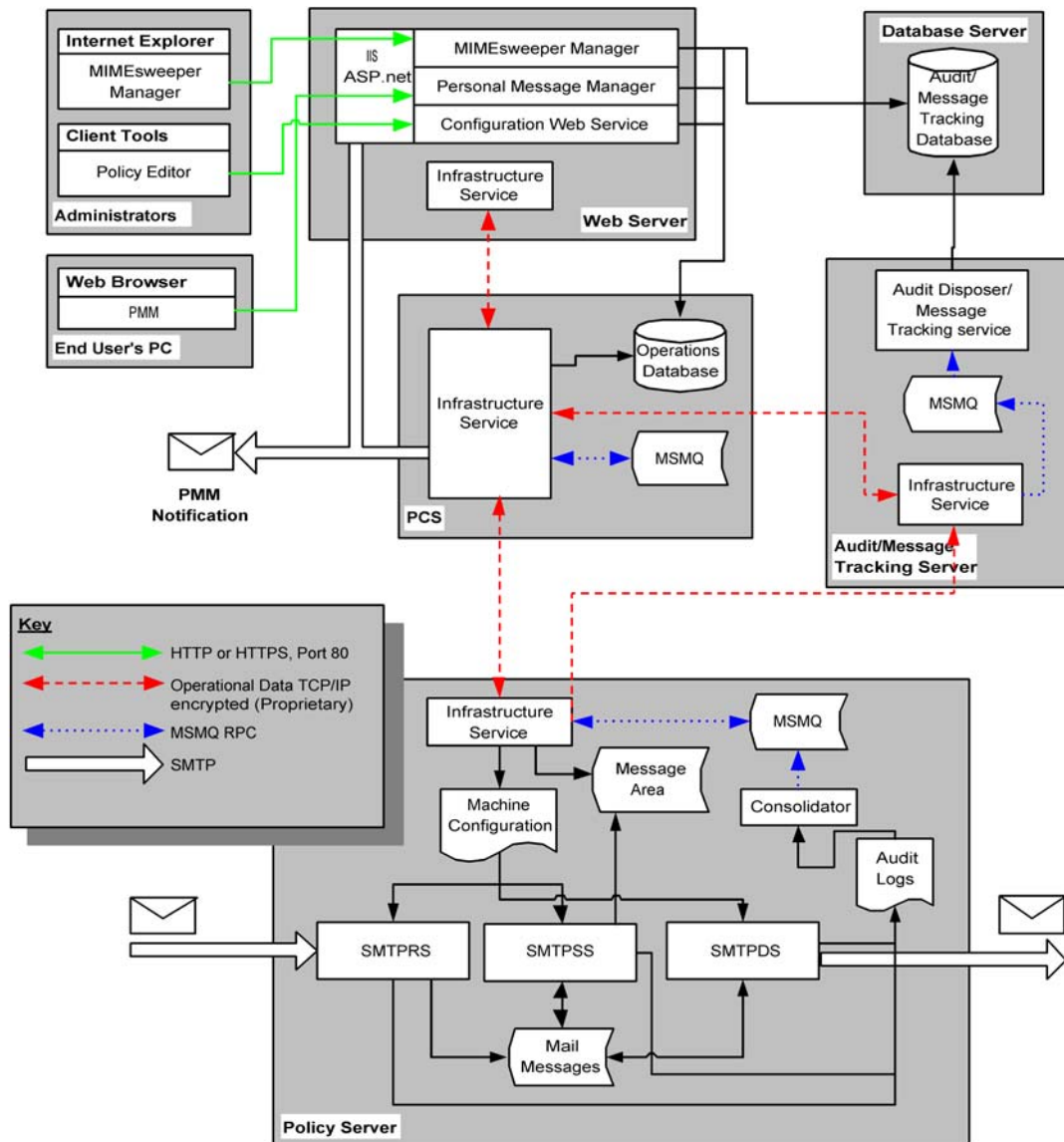


It is recommended that you install the MIMESweeper for SMTP system on a static IP Address. If you choose to change the IP Address you must restart every machine in the deployment

Do not change the name of any machine in the deployment. If you change the name of a machine, you will have to re-install the product.

Machines and connections

Figure 2-3 shows the MIMESweeper system and components distributed over a theoretical network. The major components are described in the following section.



MIMESweeper for SMTP system description

The major MIMESweeper for SMTP systems and components shown in Figure 2-3, are described below:

- **Administrators**

MIMESweeper Policy Editor - Hosts the MMC user interface which facilitates the Policy Editor.

MIMESweeper Manager - Provides the interface which provides access to areas of MIMESweeper for SMTP where you can configure, control and monitor your system.

- **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.

- **Personal Message Manager (PMM)** - Provides the interface which allows end users to manager their own spam messages.

- **Primary Configuration Server (PCS)**

The PCS is the central server in a MIMESweeper for SMTP deployment and:

- Hosts the configuration for the MIMESweeper system.
- Replicates changes to the configuration to the Web Server, Tracking Server, Audit Server and MIMESweeper for SMTP Policy Servers.
- Is accessed by clients to change any configuration settings and to add or remove machines from the deployment.
- Hosts the **Operations database**.
This database holds a summary of the contents of messages held and queued by the Policy Servers, allowing fast searching and filtering of messages from the user interface.

- **The Policy Server**

The Policy Server processes your emails. Deployed on the DMZ, these servers host the Security, Receiver and Delivery Services. These services validate connections for incoming emails, check the content against your configured security policies and deliver them to the next host machine on the route.

- **Audit Consolidator service** - This service runs on each Policy Server. It consolidates the audit data collected by the server and passes it to the Audit Disposer service. The Audit Disposer service consolidates the audit data received from each Policy Server and forwards it to the Audit Database server for writing to the audit database.

A large deployment can have up to eight Policy Servers enabled simultaneously to process mail.

Deployment Planning

- **Message Tracking Server**

Tracking service - This service runs on the machine designated as the Message Tracking Server. The service consolidates the message tracking data collected from each Policy Server and passes it to the Database Server for writing to the message tracking database.

- **Audit Server**

Audit Disposer service - Commits consolidated audit data to the Audit database.

- **Database Server**

Audit database - Holds a condensed version of all audit data generated by the system. This data is used to generate reports in the Report Center.

Message Tracking database - Holds all message tracking data generated by the system. This data is used to display message tracking details, and to generate reports in the Report Center.

Port configuration

If your Primary Configuration Server and Audit Server are deployed on the clean network, open internal firewall ports 23953 to allow access.

Allow port 80 access to the Web Server from all web client machines which are going to access Personal Message Manager and MIMESweeper Manager.

Operation	Port
Audit data	TCP/IP encrypted, Port 23953
Tracking data	TCP/IP encrypted, Port 23953
Tracking web services	23954
SMTP messages	Installation specific
Operational data	TCP/IP encrypted, Port 23953
Database connections	Vendor specific
User connections	HTTP or HTTPS Port 80
LDAP address lists	Generic LDAP Port 389

Sample deployment models









The deployment of MIMESweeper for SMTP depends on many factors such as the size of your organization and the type and volume of traffic you expect.

You may wish to deploy MIMESweeper for SMTP initially on a single host while you evaluate some of the default policies and features provided with the product, before deploying components over a wider network in a more efficient configuration.

Machine summary

Table 2-4 summarizes of the number of machines required for the deployments suggested, and lists the components installed on each machine. In these examples, the policy configuration and management tools (MIMESweeper Policy Editor and MIMESweeper Manager) are shown installed on Remote Desktop PCs.




Table 2-4: Single site machine summary

Single host	Two host	Multi-host
 Admin PC <ul style="list-style-type: none"> • Policy Editor • Management Browser 	 Admin PC <ul style="list-style-type: none"> • Policy Editor • Management Browser 	 Admin PC <ul style="list-style-type: none"> • Policy Editor • Management Browser
 PCS Web Server Policy Server Audit/Message Tracking Server Audit/Message Tracking database	 PCS Web Server Policy Server Audit/Message Tracking Server Audit/Message Tracking database	 PCS Web Server Audit/Message Tracking Server Audit/Message Tracking database
	 Policy Server Web Server	 Policy Servers (up to four)
<p>In this model all components are installed on a single host.</p> <p>See <i>Single host deployment</i> on page 2-20.</p>	<p>In this model mail processing is done on the DMZ.</p> <p>See <i>Sample two host deployment</i> on page 2-22.</p>	<p>In this model mail processing is done on the DMZ, by up to four Policy Servers.</p> <p>See <i>Sample multiple host deployment</i> on page 2-24.</p>

Dual site machine summary

Table 2-5 describes the configuration for a two-machine installation.

Table 2-5: Dual site machine summary

Site A	Site B
 Admin PC <ul style="list-style-type: none">• Policy Editor• Mngmnt Browser	 Policy Server
 PCS Web Server Policy Server Audit/Message Tracking Server Audit/Message Tracking database	





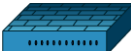




In this model mail processing is done on the DMZ by Policy Servers at two different sites.

For more information, see *Sample dual site deployment* on page 2-26.

Key to illustrations

Table 2-6 describes the symbols used to represent the various components of a MIMESweeper for SMTP deployment. The basic server symbol is overlaid with an icon which represents the components hosted by a particular server.

Table 2-6: Illustration key

Symbol	Icon	Definition	Symbol	Definition
		Primary Configuration Server		Administrator's desktop with client tools
		Policy Server		Firewall
		Audit/Message Tracking Database		End Users
		Audit/Message Tracking Server		
		Web Server		

Single host deployment

In this deployment model all MIMESweeper for SMTP features are installed on a single host on the firewall. All access to the MIMESweeper host, by both the end users and administrator, is through the firewall.

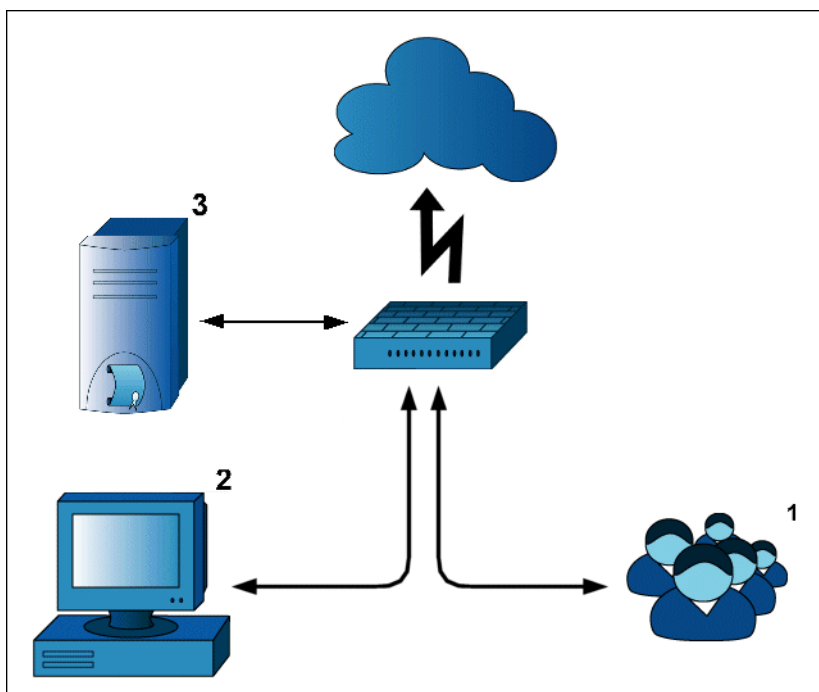


Figure 2-4: Single host deployment model

This deployment can function as an initial deployment to allow you to evaluate features and further plan your deployment, and can be a satisfactory solution for smaller organizations.

Item	Location	Description
1	Clean Network	Users who access the mail servers and their PMM message area.
2	Clean Network	Administrator - hosts the MMC user interface which facilitates the Policy Editor and the MIMESweeper Manager user interface.

Item	Location	Description
3	DMZ	MIMESweeper Host - All components installed on a single host: <ul style="list-style-type: none">• Primary Configuration Server• Web Server• Policy Server• Audit/Message Tracking database• Audit/Message Tracking Server

The major steps to implement this deployment are:

1. HTTP or HTTPS access to the MIMESweeper host (3).
2. Install all components on the MIMESweeper host (3).
During installation select the **Primary Server** deployment type, and the **Typical** setup type.
See *Installing a Primary Configuration Server* on page 3-18.
3. Install client tools on the desktop PC (2).
During installation select the **Client Tools Only** deployment type.
See *Installing Client Tools* on page 3-25.

Sample two host deployment

In this deployment model all processing is carried out in the DMZ, requiring only one port through the firewall to be open. Administrative tasks are kept inside the clean network.

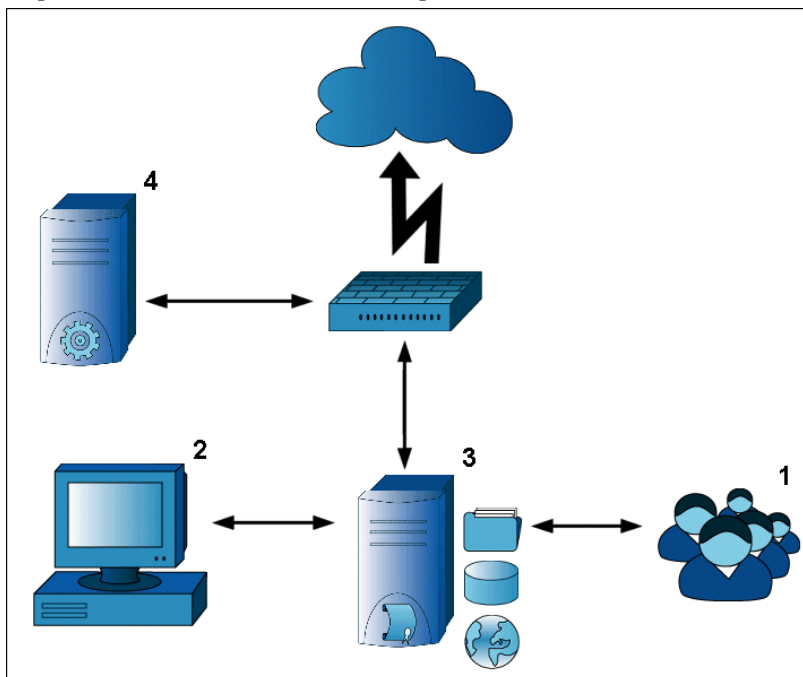


Figure 2-5: Two host deployment

All communications between administrators, end users and the PCS takes place on the clean network for added security.

Item	Location	Description
1	Clean Network	Users who access the mail servers and their PMM message area.
2	Clean Network	Administrator - hosts the MMC user interface which facilitates the Policy Editor and the MIMESweeper Manager user interface.
3	Clean Network	This machine is used for: <ul style="list-style-type: none"> • Primary Configuration Server • Audit/Message Tracking Server • Audit/Message Tracking database • Web Server

Item	Location	Description
4	DMZ	This machine is used for: <ul style="list-style-type: none"> • Policy Server

The major steps to implement this deployment are:

1. HTTP or HTTPS access on the clean network between the end users (1), the desktop PC (2) and the MIMESweeper host (3).
2. Open ports 23953 and 23954 between machine (3) and the Policy Server (4).
3. Create a PCS on machine (3) on the clean network first.

During installation select a **Primary Server** deployment type, and a **Custom** setup type.

On the **Custom Setup** page of the wizard de-select the features you do not want to install on this machine, in this example **Policy Server** and **Client Tools**.

See *Installing a Primary Configuration Server* on page 3-18.

4. Install the policy engine on machine (4).
During installation select the **Additional Server** deployment type and the **Typical** setup type. Note that the server will not be enabled initially.

See *Installing an additional server (typical)* on page 3-22.

5. Install client tools on the desktop PC (2).
During installation select the **Client Tools Only** deployment type.

See *Installing Client Tools* on page 3-25.

6. On the desktop PC initialize the policy.
You create your initial policy using the Initial Policy Wizard which starts when you open the MIMESweeper Policy Editor for the first time. In the wizard you select the server that you intend to route incoming and/or outgoing mail to.

7. Enable the Policy Server (4).
All installed Policy Servers will be visible in the MIMESweeper Policy Editor in the **Servers** folder of the **MIMESweeper for SMTP** container. Select a server, access the context menu and select **Enabled**.

Sample multiple host deployment

In this deployment model all processing is carried out in the DMZ. All communications between administrators, end users and the PCS takes place on the clean network for added security.

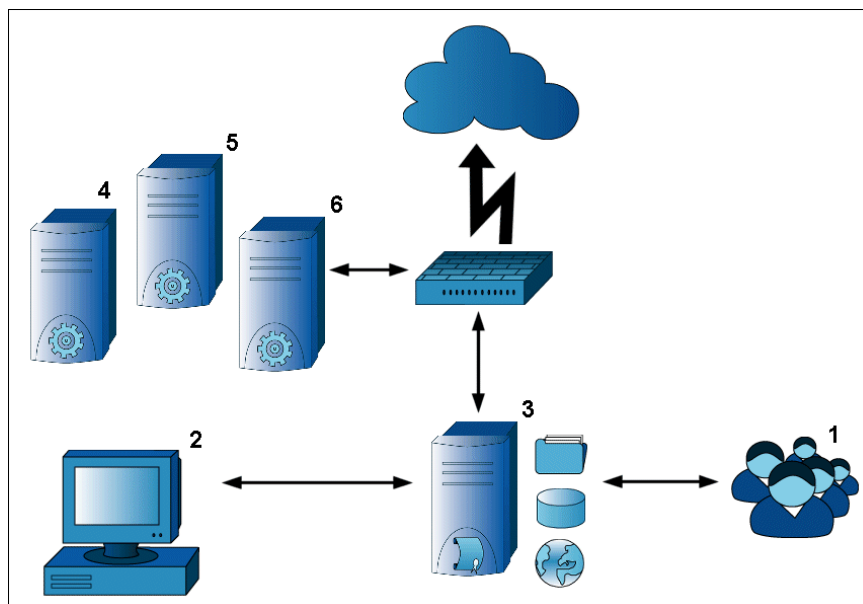


Figure 2-6: Multiple host deployment

In addition, multiple Policy Servers have been deployed to increase mail processing, requiring one port per server through the firewall to be open. A large deployment can have up to four policy engines enabled at any one time.

Item	Location	Description
1	Clean Network	Users who access the mail servers and their PMM message area.
2	Clean Network	Administrator - hosts the MMC user interface which facilitates the Policy Editor and the MIMESweeper Manager user interface.
3	Clean Network	This machine is used for: <ul style="list-style-type: none"> • Primary Configuration Server • Audit/Message Tracking Server • Audit/Message Tracking database • Web Server
4, 5, 6	DMZ	These machines are used for the Policy Servers.

The major steps to implement this deployment are:

1. HTTP or HTTPS access on the clean network between the end users (1), the desktop PC (2) and the MIMESweeper host (3).
2. Open ports 23953 and 23954 between machine (3) and the Policy Servers (4, 5 and 6).
3. Create a PCS on machine (3) on the clean network first.

During installation select the **Primary Server** deployment type, and the **Custom** setup type.

On the **Custom Setup** page of the wizard de-select the features you do not want to install on this machine, in this example, **Policy Server** and **Client Tools**.

See *Installing a Primary Configuration Server* on page 3-18.

4. Install the policy engine on machines (4, 5 and 6).
During installation select the **Additional Server** deployment type and the **Typical** setup type. Note that the server will not be enabled initially. Repeat the installation on all intended Policy Servers.

See *Installing an additional server (typical)* on page 3-22.

5. Install client tools on the desktop PC (2).
During installation select the **Client Tools Only** deployment type.

See *Installing Client Tools* on page 3-25.

6. On the desktop PC initialize the policy.
You create your initial policy using the Initial Policy Wizard which starts when you open the MIMESweeper Policy Editor for the first time. In the wizard you select the server that you intend to route incoming and/or outgoing mail to.

7. Enable the Policy Server (4).
All installed Policy Servers will be visible in the MIMESweeper Policy Editor in the **Servers** folder of the MIMESweeper for SMTP container. Select a server, access the context menu and select **Enabled**.

Sample dual site deployment

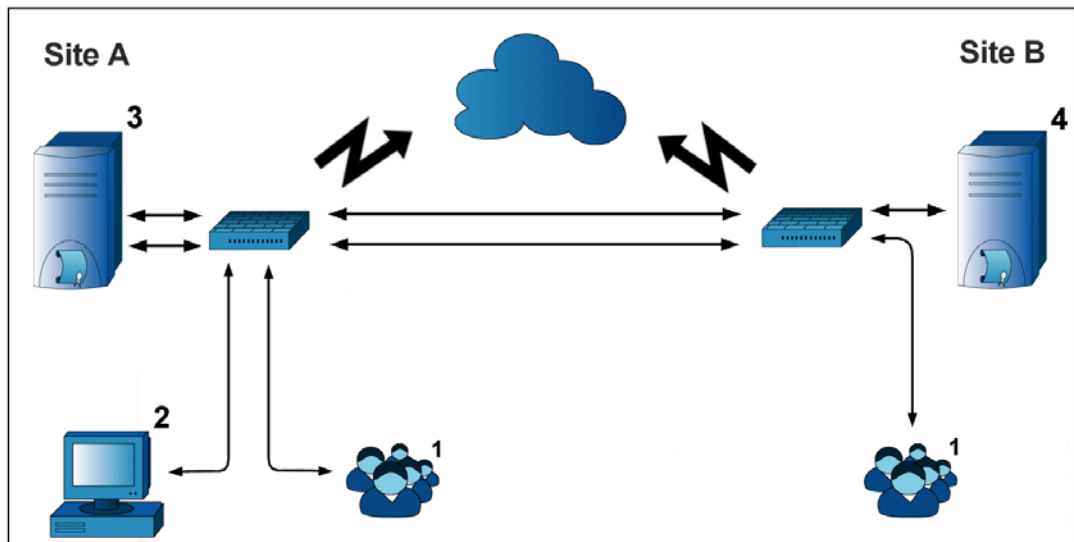


Figure 2-7: Dual-site deployment

In this deployment model, mail processing at both sites is done in the DMZ. The PCS is installed at one site only (Site A) and management and policy configuration for both sites is done by the Administrator from one site.

Item	Location	Description
1	Clean Network	Users who access the mail servers and their PMM message area.
2	Clean Network	Administrator - hosts the MMC user interface which facilitates the Policy Editor and the MIMesweeper Manager user interface.
3	DMZ	<ul style="list-style-type: none"> This machine is used for: Primary Configuration Server Policy Server Audit/Message Tracking Server Audit/Message Tracking database Web Server
4	DMZ	This machine is used for: <ul style="list-style-type: none"> Policy Server

The major steps to implement this deployment are:

1. Create a PCS on machine (3).
During installation select the **Primary Server** deployment type, and the **Typical** setup type.
See *Installing a Primary Configuration Server* on page 3-18.
2. Install the policy engine on machine (4).
During installation select the **Additional Server** deployment type and the **Typical** setup type. Note that the server will not be enabled initially. Repeat the installation on all intended Policy Servers.
3. Install client tools on the desktop PC (2).
During installation select the **Client Tools Only** deployment type.
See *Installing Client Tools* on page 3-25.
4. On the desktop PC initialize the policy.
You create your initial policy using the Initial Policy Wizard which starts when you open the MIMESweeper Policy Editor for the first time. In the wizard you select the server that you intend to route incoming and/or outgoing mail to.
5. Enable the Policy Server (4).
All installed Policy Servers will be visible in the MIMESweeper Policy Editor in the **Servers** folder of the **MIMESweeper for SMTP** container. Select a server, access the context menu and select **Enabled**.

Deployment Planning

CHAPTER 3

Installation

This chapter describes how to install MIMESweeper for SMTP. For details about where on your network to deploy MIMESweeper for SMTP, and for information about various deployment models, see Chapter 2.

Overview	3-3
Preparing the database environment	3-3
Database software options	3-3
Installing your database for MIMESweeper for SMTP	3-4
Installing Microsoft SQL Server 2005 Express	3-4
Database authentication options.	3-5
Granting System Administration right to a database login	3-5
Configuring Windows authentication.	3-5
Creating an Applications Service account for a trusted subsystem	3-6
Creating the Applications Service account for a delegated subsystem	3-6
Configuring SQL Server authentication	3-7
Securing your database server	3-7
Configuring database server communications.	3-8
Installation options	3-9
Preparing to install MIMESweeper for SMTP.	3-10
Installation prerequisites	3-10
Managed Downloads licensing prerequisites	3-10
Installing message queueing.	3-11
Pre-installation preparations.	3-11
Installation checklist	3-11
Installation Routes.	3-12
Installing Windows components	3-14
Installing Microsoft Message Queuing	3-14
Installing Internet Information Services (IIS)	3-14
Installing MIMESweeper for SMTP	3-15
Prerequisite Software Wizard	3-16
Installing a Primary Configuration Server	3-18
Installing an additional server (typical).	3-22
Installing an additional server (custom)	3-23
Installing Client Tools	3-25
Creating an Oracle audit database	3-26
Performing a purge on an Oracle audit database	3-27
Configuring the Audit database	3-27
Configuring the Message Tracking database	3-28

Installation

Post installation tasks	3-28
The Initial Policy Wizard.	3-29
Subsequent installations	3-29
Updating MIMESweeper for SMTP	3-29
Removing MIMESweeper for SMTP	3-31
Upgrading to a newer version	3-32
Before upgrading	3-32
After upgrading	3-33
Upgrading on a single server	3-33
During installation.	3-33
Upgrading on a multiple server deployment.	3-34
Maintaining message processing throughout an upgrade	3-34
Before upgrading in a multiple server environment	3-34
Upgrade sequence	3-35
Handling errors during installation	3-35
Performing the upgrade	3-36
Licensing MIMESweeper for SMTP	3-37
Additional functionality available in the Advanced and Enterprise licenses.	3-37

Overview

This chapter describes the process of installing MIMESweeper for SMTP including prerequisites.

In addition, it also describes how you can upgrade an existing MIMESweeper for SMTP installation, modify an existing installation and remove an existing installation.



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.

Preparing the database environment

A MIMESweeper for SMTP installation uses database software, for example, SQL server to record the message management, auditing, and tracking information generated by the system.

The database software hosts and maintains the following databases:

- The Operations database maintains records of system configuration, and records of all held and queued messages held on the Policy Server. MIMESweeper Manager uses this database to provide message searching and filtering.
- The Message Tracking database maintains records of the messages that the system has processed, and the system events that happened to each message.
- The Audit and Reporting database maintains records of system usage, for example, top senders and recipients, and policy usage.

This section describes how to install and configure the database software, and how to configure the database authentication options.

Database software options

The MIMESweeper for SMTP 5.3 installation software includes a version of Microsoft SQL Server 2005 Express. If there is no existing SQL software installed, Microsoft SQL Server 2005 Express can be installed as part of the prerequisite software installation process.

Microsoft SQL Server 2005 Express has a maximum database size of 4 GB. This can be sufficient for small to medium-sized organizations where message tracking functionality is not required.



To manage your Microsoft SQL Server 2005 Express installation, you should download and install the SQL Server Management Studio Express management tool. This is freely available from the Microsoft web site.

Installing your database for MIMESweeper for SMTP

Before installing the MIMESweeper for SMTP software on a system with no database server, you must:

1. Install the database software using the MIMESweeper for SMTP installation wizard. The Wizard prompts you to install the database software as part of the installation process. See *Installing Microsoft SQL Server 2005 Express* on page 3-4 for details.
Pause or halt the installation after the database software has been installed.
2. Depending on the database authentication method being used, set up the database authentication that the MIMESweeper for SMTP installation requires.
 - If you are using Windows authentication, set up the Applications Service Account. See *Configuring Windows authentication* on page 3-5 for details.
 - If you are using SQL Server authentication, see *Configuring SQL Server authentication* on page 3-7.
3. Continue and complete the MIMESweeper for SMTP installation process.

Installing Microsoft SQL Server 2005 Express

When you install MIMESweeper for SMTP on a system without database software, the installation process prompts you to install Microsoft SQL Server 2005 Express.

To install Microsoft SQL Server 2005 Express:


1. On the Install Required Third Party Software screen, select **Install** to display the End User License Agreement screen. Accept the licence and click **Next**.
2. On the Installing Prerequisites screen, click **Install** to install any required prerequisites. After the prerequisites have been installed, click **Next** to continue.
3. On the SQL Server Installation Wizard welcome screen, click **Next**.
4. On the System Configuration Check screen, verify that the **Success** message is displayed and click **Next**.
5. On the Registration screen, enter your name and company details.
6. On the Feature Selection screen, configure your install path if required, and click **Next** to accept the default software configuration.
7. On the Authentication Mode screen, select the authentication mode that your system uses, and click **Next**. See *Database authentication options* on page 3-5 for more information:
 - For Windows authentication, select **Windows Authentication Mode**.
 - For SQL Server authentication, select **Mixed Mode**, and enter a password for the sa administration account that the installation creates.

8. On the Ready to Install screen, click **Install** to begin the installation and install the software.
9. When the installation completes, at the Setup Progress screen, verify that the installation was error-free, and click **Next**, then **Finish** to complete the process.

Database authentication options

In order to manage the databases, MIMESweeper for SMTP must have access rights to the database servers, and the databases. Two types of authentication are available for securing access to the database server:

- **Windows Authentication:** At installation, the local Windows User account must have System Administrator rights on the database server: This account is used to create the operations database. See *Granting System Administration right to a database login* below for details.

 After installation, the System Administrator rights for the local Windows User account can be revoked.

- **SQL Server authentication:** At installation, you supply a database administrator username and password that has been granted System Administrator rights on the database server: This could be the `sa` account, or a specific login created manually in the database using the Management Studio.
 - When you install MIMESweeper for SMTP with an existing database, you configure the database connection and authentication details during MIMESweeper for SMTP installation.

Granting System Administration right to a database login

To grant System Administration right to a database login, follow the steps below:

1. Open SQL Server Management Studio Express.
2. In the left hand pane, select **Security, Logins**, and right-click the database login. From the list that is displayed, select **Properties**.
3. In the Properties page, select **Server Roles**, and in the right hand pane, select **sysadmin** if it is not already selected.
4. Click **OK** to save, then close SQL Server Management Studio Express.

Configuring Windows authentication

If you have configured your SQL Server database to use Windows Authentication, you must setup an Application Service Account before you install the MIMESweeper for SMTP software.

This account is used to grant the various MIMESweeper for SMTP applications the ability to access and update the various databases used by the system. The account is a Windows user account and should be created either locally or on the domain controller depending on your system topology, using the standard operating system Local Users and Groups Management Console.

Installation

The method used to set up Windows authentication depends on the architecture on which your system operates: trusted subsystem or delegated subsystem:

- Trusted subsystem: MIMESweeper for SMTP operates in a secure domain. All servers in the domain are trusted, and the domain login provides access to all required servers.
- Delegated subsystem: the MIMESweeper for SMTP servers do not operate in a trusted domain, and each server requires separate authentication.

Creating an Applications Service account for a trusted subsystem

In the Trusted Subsystem, the Application Service Account should be created by your Domain administrator to be accessible to all servers upon which you plan to install MIMESweeper for SMTP.



When creating the account, the password must be configured to never expire.

When the account has been created, it should then be added to the local Administrators group on each of the following servers:

- The Primary Configuration Server.
- The Web Applications Server or servers.

For all other servers in your MIMESweeper for SMTP deployment, the account should be added to the Users group.



Record these account details. You will need them when performing system maintenance operations such as backing up, restoring, and relocating the PCS.

Creating the Applications Service account for a delegated subsystem

In a Delegated Subsystem, to enable the distributed MIMESweeper for SMTP and database servers to communicate with each other, the Application Service Account must be created as a local Windows user account on each of the following servers:

- The Primary Configuration Server.
- The Web Applications Server or Servers.

The user account on each server must meet the following criteria:

- The name and password of the account must be identical on all servers.
- The password must never expire.

When the account has been created, it should then be added to the local Administrators group on each of the following servers:

- The Primary Configuration Server.
- The Web Applications Server or servers.

For all other servers in your MIMESweeper for SMTP deployment, the account should be added to the Users group.



Record these account details. You will need them when performing system maintenance operations such as backing up, restoring, and relocating the PCS.

Configuring SQL Server authentication

If you have configured your SQL Server database to allow SQL Server Authentication you can configure your MIMESweeper for SMTP software to communicate with your database server using the SQL Server Administrator login you created during the installation of the SQL Server database software.

This account is normally referred to as the sa login. It is important that you record the sa login password—you will be prompted to enter it during installation, and for post-installation database configuration tasks such as configuring tracking or auditing.

Securing your database server

To further secure the Database Server, once you have installed the MIMESweeper for SMTP Primary Configuration Server, you can revoke the System Administrator right from the Database login used to create the Operations Database if necessary. The login is based on the authentication type you have chosen:

- Windows Authentication: the login will be the local Windows user account.
- SQL Server Authentication: the login will be a SQL login account.



Before you do this, check that the login's access rights are not required by other applications.

To revoke the System Administration right from a database login, reverse the steps that you performed on *Granting System Administration right to a database login* on page 3-5:

Configuring database server communications

To allow the MIMESweeper for SMTP applications to communicate with the Database Server, you must enable communications over TCP/IP between the applications and the database server. This is not enabled by the default SQL Server Express installation and must be manually configured using the following steps:

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 Services and Connections** to display the **Surface Area Configuration** tool.
3. In the tree at the left of the panel, select **Server, Database Engine, Remote Connections**, and in the right panel, select **Using TCP/IP only**.
4. Click **OK**, then close the SQL Server Surface Area configuration tool.

Installation options

As previously discussed in Chapter 2, Deployment Planning, MIMESweeper for SMTP can be deployed in many ways.



Do not install the MIMESweeper system on a domain controller. The local ASPNET user account is not created when installing the .NET Framework on a domain controller, and this can cause issues to arise. For more information, see the Microsoft Knowledge Base Article 315158.

- **Single machine**

For your initial installation we recommend that you install the full MIMESweeper for SMTP product on a single host. When you become more familiar with the product, you can perform further installations to distribute components to create a multiple machine deployment. The MIMESweeper for SMTP product consists of:

- **Server**
 - Policy Server (Receiver, Security and Delivery service)
 - Audit Disposer service
 - Message Tracking service
 - Web Applications (MIMESweeper Manager, PMM, Initial Policy Wizard)
- **Client Tools**
 - MIMESweeper Policy Editor

The setup program creates an MMC console containing the MIMESweeper Policy Editor snap-in. When you start the MMC for the first time, the console automatically loads the snap-in (if you have installed the full product) and runs the Initial Policy Wizard.

- **Multiple machine**

After the initial single machine installation, the process can be repeated on one or more additional servers, to redeploy some MIMESweeper for SMTP components, so that specific machines can perform certain tasks.



It is recommended that you install the MIMESweeper system on a static IP Address. If you choose to change the IP Address you must restart every machine in the deployment.

Do not change the name of any machine in the deployment. Machine names are written to the various configuration files during installation and cannot be updated. If you change the name of a machine, you will have to re-install the product.

Preparing to install MIMESweeper for SMTP

The following sections describe the:

- Hardware and software you need to run MIMESweeper for SMTP.
- Preparations you need to make before you install MIMESweeper for SMTP.
- Information you need when you install MIMESweeper for SMTP.

Installation prerequisites

Before you can install and run MIMESweeper for SMTP, the machine on which you intend to deploy MIMESweeper for SMTP must already have certain hardware and software installed and configured. The Installation Wizard will check your system for these prerequisites and will run the Prerequisite Software Wizard if necessary. See *Prerequisite Software Wizard* on page 3-16.

The *Prerequisites* release document provides details of the prerequisite hardware and software that you need to run MIMESweeper for SMTP. The *Prerequisites* release document is available on the product CD-ROM.

Managed Downloads licensing prerequisites

As part of the installation's License Details configuration process, you can configure a Managed Downloads password. You can also configure this password after installation using the Policy Editor. See the Policy Editor help for more information. The License Details configuration page provides a link to the Clearswift website, where you can configure a Managed Downloads password to enter.



To configure a Managed Downloads password, you must have a valid Support and Maintenance agreement in place.

Configuring a Managed Downloads password enables your installation to receive automatic updates to the managed references used by some scenarios, for example, the SpamLogic spam-detection scenario.

The installation software includes a version of each managed reference. When you configure a Managed Downloads password, these managed references are updated by Clearswift on a regular basis. This ensures that you are protected against spam and other threats as they change and evolve.

Installing message queueing

A MIMESweeper for SMTP installation requires Microsoft Message Queueing software to be installed. The installation routine checks that this software is installed, and prompts you to install it if it is not. If Microsoft Message Queueing software is not installed on the installation machine, install it as follows:



On a Windows 2003 system, the Message Queueing Services are part of the Application Service group of components.

1. From the Windows Control Panel, open the Add/Remove Programs dialog box.
2. On the left side of the dialog box, select the **Add/Remove Windows Components** button to display the list of available Windows components.
3. From the list, select **Message Queueing Services** and ensure that it is checked.
4. Click **Next** to install Message queueing services.
5. When the process is completed, click **Finish**.

Pre-installation preparations

Before you install MIMESweeper for SMTP on any host machine, you must:

- Determine the configuration required for your network and prepare it for MIMESweeper for SMTP deployment.
- Ensure you are logged on to the host machine using an account that has administrator privileges.
- Ensure that you have sufficient free disk space on the PC on which you install this release of MIMESweeper for SMTP. For details, see *Prerequisites* release document.
- Make sure your anti-virus software is disabled.



The server applications cannot be installed on machines which are part of a domain containing non-ASCII characters, for example, ü, ñ etc. However, you can install client tools on such machines.

Installation checklist

During installation, you are prompted to enter information about your environment. Before you start the installation process, use the following checklist to ensure you have the information you need:

- A valid MIMESweeper for SMTP license.
- A valid IMAGEmanager license.
- The MIMESweeper for SMTP System Administrator account and password that you propose to use, or have previously set up if you are installing an additional server.

- If using SQL server authentication, the SQL server System Administrator account and password if SQL server is already installed. See *Configuring SQL Server authentication* on page 3-7 for details.



Make sure that the SQL Server authentication mode is set to **SQL Server and Windows**, on any server that you intend to include in the deployment. This option is configured in the **Security** tab of the **SQL Server Properties (configure)** dialog box.

If you have Microsoft SQL Server 2005 Express installed and Windows authentication, you must apply this configuration change using the SQL Server Client Tools.

- If using Windows authentication, the Applications Service account details. See *Configuring Windows authentication* on page 3-5 for details.
- The Personal Message Manager (PMM) configuration, including the name of the Policy Server and the TCP/IP port used for SMTP connections to the host server.
- The email address of the sender of notification messages that you propose to use.

Installation Routes

Figure 3-1 shows the possible routes through the Installation wizard. Using the wizard you can create your initial PCS and then, choosing different options you create additional servers on which to install MIMESweeper for SMTP components. The possible routes are:

- **Route 1**

This is the default route through the installer and creates a full MIMESweeper for SMTP installation on a single machine.

- **Route 2**

This route installs a PCS and allows you to select other components to be installed on the same machine. After selecting a **Primary Server** deployment type, choose a **Custom** install setup type. At the **Custom Setup** screen you can select the component you want to install with the PCS.

- **Route 3**

This route installs a Policy Server on an additional machine. After selecting an **Additional Server** deployment type, choose a **Typical** install setup type.

- **Route 4**

This route allows you to install selected components on an additional server. After selecting an **Additional Server** deployment type, choose a **Custom** install setup type. At the **Custom Setup** screen you can select the component you want to install on the additional server.

- **Route 5**

This route installs the Client Tools only. Use this to install the Policy Editor on to a desktop PC.

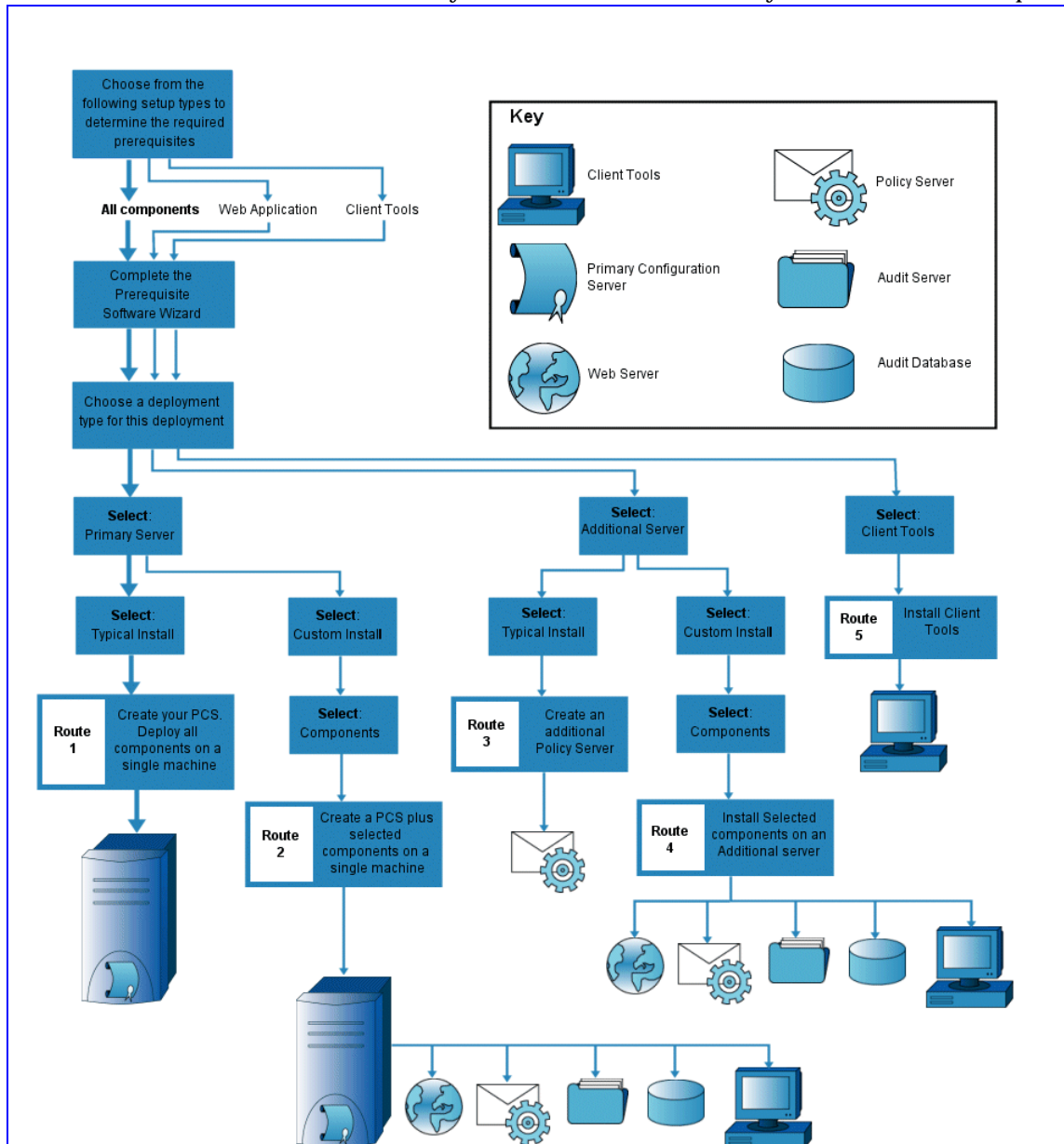


Figure 3-1: Installation Routes

Installing Windows components

The installation of the Message Queuing Service and the Internet Information Services are required to enable MIMESweeper for SMTP to process your messages.

Installing Microsoft Message Queuing

If you do not have Message Queuing Services installed:

1. From the start menu select **Control Panel** from the **Settings** menu.
2. Open **Add/Remove Programs** applet and click the **Add/Remove Windows Components** button from the side navigation bar.
3. From the list of Windows components select **Message Queuing Services**.
For Windows 2003 users the Message Queuing Services are part of the **Application Server** group of components.

Installing Internet Information Services (IIS)

Web applications require IIS installed with ASP.NET support. If you do not have IIS installed:

1. From the start menu select **Control Panel** from the **Settings** menu.
2. Open **Add/Remove Programs** applet and click the **Add/Remove Windows Components** button from the side navigation bar.
3. From the list of Windows components select **Internet Information Services (IIS)**.



If you are installing on a Windows 2003 platform, the Internet Information Services (IIS) are part of the **Application Server** group of components.

You must also select the **ASP.NET** component.

4. To view the IIS subcomponents, click **Details**.
5. Make sure that the correct sub-components are selected. To do this clear all check boxes and select **World Wide Web Server**. The other IIS components you need are selected automatically.
6. When the IIS installation has completed you are recommended to install the latest IIS patches, available from Microsoft's website.

Installing MIMESweeper for SMTP

When you install MIMESweeper for SMTP for the first time it is recommended that you perform a single machine deployment. Where all components are installed on the Primary Server, see *Installing a Primary Configuration Server* on page 3-18.



A Primary Server installation creates a Primary Configuration Server (PCS). The PCS is the central server in a MIMESweeper for SMTP deployment and hosts the configuration for the MIMESweeper system. The PCS replicates changes to these files to the Web Server, Audit Server, Message Tracking server and all Policy Servers. The PCS also hosts the Operations database which holds a summary of all messages held and queued by the Policy Servers, allowing fast searching and filtering of messages from the MIMESweeper Manager.

This section describes the installation procedure for single machine deployments and multiple machine deployments.



For full instructions regarding the installation of the Message Queuing Services and IIS, refer to the Windows documentation appropriate to your Operating System.

- **Single machine deployment**
 - Prerequisite Software Wizard
The installation wizard scans for prerequisite software. If any software is missing, you are guided through the pre-installation process. See *Prerequisite Software Wizard* on page 3-16.
 - Install a PCS (all components)
Install all MIMESweeper for SMTP components on a single machine. See *Installing a Primary Configuration Server* on page 3-18.
- **Multiple machine deployment**
 - Install an Additional Server (Typical)
After installing the PCS, install components on an additional server to create a multiple machine deployment, see *Installing an additional server (typical)* on page 3-22.
 - Install an Additional Server (Custom)
Select a sub-set of components to install on an additional server, see *Installing an additional server (custom)* on page 3-23.
 - Install client tools only
Install the client tools on a local PC to provide remote access to the policy configuration from the MIMESweeper Policy Editor, see *Installing Client Tools* on page 3-25.
 - Upgrade your existing MAILsweeper for SMTP
Describes the installation process when upgrading from earlier products, see *Upgrading to a newer version* on page 3-32.

To install MIMESweeper for SMTP in a single machine deployment:



You should exit all Windows programs, and you must disable anti-virus software before you run the Installation Wizard. The installation process checks that you have disabled your anti-virus software.

1. Insert the CD-ROM. The product CD front end should start automatically when you insert the CD-ROM. If it does not, choose **Run** from the **Start** menu. Navigate to the file `contents.exe` on the CD-ROM and then click **OK**.
2. From the CD-ROM, click `setup.exe`.
3. Follow the instructions on each wizard page, and click **Next** to move to the next page. During installation, you are prompted for certain information.

Prerequisite Software Wizard

If all prerequisite software is installed, the Prerequisite Software Wizard is bypassed. In that instance you will start at the **Welcome to the MIMESweeper for SMTP Install Wizard** page, see *Installing a Primary Configuration Server* on page 3-18.

Welcome to Prerequisite Software Wizard

MIMESweeper for SMTP has detected that you need to install prerequisite software.

The following pages will determine what type of installation you propose to carry out and what prerequisite software you require.

Click **Next**.

Determine Required Prerequisites

Select **Yes** or **No** as appropriate to the type of installation you require, and to expose further questions until the wizard can determine the prerequisites you require.

Select **Next** to progress to the next stage of the wizard.

The first option is for a full installation of all MIMESweeper for SMTP on this machine.

The second option installs the client tools only on this machine to remotely administer your configuration.

The third option indicates that you are planning to host web applications only on this machine.

Install Required Windows Components

This page is only displayed if updates to your Windows system are required. It lists the required Windows components that you need to install. Prerequisites vary depending upon the selection made in the previous page.

You do not need to quit the installation program to install Windows components.

Install the required Windows Components using the Windows Add/Remove Programs applet. For more information, see *Installing Windows components* on page 3-14.

To check what components need to be installed, click **Refresh**.

Install Required Windows Components

This page confirms that the required Windows components are installed.

Click **Next**.

Install Required Third Party Software

MIMESweeper for SMTP has detected that you need to install third party software.

For each item listed click **Install**.

For information about installing the default database, Microsoft SQL Server 2005 Express, see *Installing Microsoft SQL Server 2005 Express* on page 3-4.


Prerequisite Software Wizard Completed

If required, click **Reboot** to continue with the installation. The Install Wizard continues automatically when your computer restarts.

To continue, see *Installing a Primary Configuration Server* on page 3-18.

Installing a Primary Configuration Server

This procedure installs all MIMESweeper for SMTP components on a single machine.

Welcome to the Installation Wizard	<p>If all prerequisites are installed, the installation starts here.</p> <p>This wizard starts when you click <code>setup.exe</code> or following the Prerequisite Software Wizard reboot.</p> <p>Make sure your anti-virus software is disabled.</p> <p>Click Next to start the installation process.</p>
License Agreement	<p>Read the license agreement carefully. You must accept the terms of the agreement to continue with the installation.</p> <hr/> <div> Please ensure that your deployment option conforms with the requirements of the license agreement.</div> <hr/>
Deployment Type	<p>Select Primary Server for your initial installation.</p> <p>Server applications cannot be installed on machines which are part of a domain containing non-ASCII characters.</p>
Setup Type	<p>Select Typical to install all components onto a single machine.</p> <p>Having selected Primary Server on the Deployment Type page and Typical on this page, you will create a single machine deployment (all components).</p> <p>Selecting Custom enables you to select which components to install on the Primary Server, see <i>Installing an additional server (custom)</i> on page 3-23.</p>
System Administration	<p>Enter the PCS Administrator Account password. This is the name and password set up to administer MIMESweeper.</p> <p>Confirm the password. Ensure that you record the password and name for future usage. The administrator can subsequently setup other users with administrative rights, but only this account can be used to install MIMESweeper for SMTP.</p>

Licensing

Configuration information for your license:

Company Name - The name of your company .

License Key - A 30-digit alphanumeric key.

Serial Number - A 16-digit number.

Password - your Managed Downloads password. This allows your Managed References, for example the reference used by spam defences, to be updated automatically. If you do not have a password, click the **Register** button at the bottom of the screen to access the Clearswift website, and configure one. You must have a valid Support Maintenance contract in place before you can configure a password. See *Managed Downloads licensing prerequisites* on page 3-10 for more information.

Alternatively, leave the fields blank and create the license later. For more information about licences, see *Licensing MIMESweeper for SMTP* on page 3-37.

Database Server Login

The Operations database holds a summary of all message and archive areas.

In the Connection Details area, select the authentication type for the installation.

See *Preparing the database environment* on page 3-3, for information on the options for configuring and *Database authentication options* on page 3-5 for more information.

Advanced SQL Setup

Click **Advanced** to access the SQL port and instance name settings if your installation requires these to be set.

Use these options to specify a port and an instance of SQL server other than the defaults.



After installing MIMESweeper for SMTP, do not change the port number or instance of the Operations Database. This results in the MIMESweeper system being unable to communicate with the Operations database, leading to system failure.

Installation

Application Service Account	<p>If you use Windows authentication to authenticate database access, enter the Application Service Account details here. This screen does not appear if you have chosen to use SQL Server authentication. See <i>Configuring Windows authentication</i> on page 3-5 for more information.</p>
Personal Message Manager Configuration	<p>Personal Message Manager (PMM) allows end users to manage their own withheld messages by notifying them that some messages sent to them have been identified as a potential threat.</p> <p>From Mail Address - The sender address of notification messages.</p> <p>Mail Server - The server where email notifications are sent from, for example: exchange server.</p> <p>Port - The TCP/IP port used for SMTP connections to the host server.</p> <p>A PMM message area called Personal Messages is now created in the Message Area directory.</p>
Ready to Install the Program	<p>Check the I confirm all anti-virus software has been stopped checkbox. You are now ready to install MIMESweeper for SMTP to create the Primary Configuration Server.</p> <p>Click Install to start the process.</p>
Completing the process	<p>When the installation process is completed, the system checks that there is a valid Support and Maintenance contract in place for your license, and displays a License validation completed successfully message if the operation completes successfully.</p> <p>After the validation process, the installation prompts for a system reboot to complete the process.</p>



When you install the MIMESweeper for SMTP Primary Configuration Server, the installation creates a database login on your local Database server to allow the MIMESweeper for SMTP applications to communicate with the Operations database. The name of the login is dependent on the database authentication type selected during installation:

- If you selected Windows Authentication, the account is the Application Service Account.
- If you selected SQL Authentication, the account is called `ul_ClearswiftPmiApp`.

Do not delete this account or change its password. If you do, MIMESweeper is unable to record information in the database. If you do delete or amend this Operations Database account you will need to reinstall the MIMESweeper system.

If you are hosting MIMESweeper for SMTP on a single machine, your system setup is now complete.

If you are planning a multiple machine deployment and want to add an Additional Server, see *Installing an additional server (typical)* on page 3-22.

Installation

Installing an additional server (typical)

A Typical install with **Additional Server** selected installs the Policy Engine (Policy Server) on an additional server.

Welcome	Click Next to start the installation process.
License Agreement	Read the license agreement carefully. You must accept the terms of the agreement to continue with the installation.
Deployment Type	<p>Select Additional Server to install an additional server in the MIMESweeper for SMTP deployment.</p> <p>Server applications cannot be installed on machines which are part of a domain containing non-ASCII characters.</p>
Setup Type	<p>Selecting Typical installs the components necessary to create a mail Policy Server.</p> <p>Selecting Custom enables you to select which components to install on the additional server. See <i>Installing an additional server (custom)</i> on page 3-23.</p>
System Administration	Enter the name of the PCS in the Host Name field. You may need to enter the fully qualified domain name as well depending upon your network layout. Enter the Administrator account name and password installed on your PCS.

Ready to Install the Program

Click the **View Settings** button to review the settings for the installation. Use the **Back** button to change settings. Check the **I confirm that all anti-virus software has stopped** check box to confirm that you have disabled your anti-virus software.



After installing MIMESweeper for SMTP, do not change the port number or instance of the Operations Database, configured in the **Advance Settings**. This results in the MIMESweeper system being unable to communicate with the Operations Database, leading to system failure.

This is not an active installation of the Operations Database on the Additional Server. It is installed to allow the Additional Server to be promoted to become the PCS at a later time.

You are now ready to install Policy Server components. Click **Install** to start the process.

Installing an additional server (custom)

A **Custom** install with **Additional Server** selected enables you to deploy one or more MIMESweeper for SMTP components on an additional server.

Setup Type

Continued from *Installing an additional server (typical)* on page 3-22 (if you selected **Custom**).

Selecting **Custom** enables you to select which components to install on the additional server.

System Administration

Enter the name of the PCS in the **Host Name** field. You may need to enter the domain name as well depending upon your network layout.

Enter the Administrator account name and password installed on your PCS.

Operations Database

Enter the local SQL Server logon details to create the database on the Additional Server.

This is not an active installation of the Operations Database on the Additional Server. It is installed to allow the Additional Server to be promoted to become the PCS at a later time.

Installation

Custom Setup

Select which MIMESweeper for SMTP components to install on the Additional Server.

Click on a feature icon .

A pop-up menu enables you to install the feature on your hard drive, or install the feature plus its sub-features. The options are:

- **Policy Server**
Receiver, Security and Delivery Service and Consolidator Service.
- **Audit Disposer service**
Commits consolidated audit data to the Audit database
- **Web applications**
MIMESweeper Manager, PMM and Initial Policy Wizard.
- **Tracking server**
Manages message tracking data.
- **Client Tools**
Required for remotely administering the policy configuration.

Disk Space Requirements

This page highlights any drives that do not have sufficient disk space available for the selected features.

You can select a different destination drive by clicking the **Change** button on the Custom Setup page.

Click **OK** to return to the Custom Setup page.

Personal Message Manager Configuration	<p>Mail Address - The address shown as the sender in PMM notification messages.</p> <p>Mail Server - The server where email notifications are sent from, for example: exchange server.</p> <p>Port - The TCP/IP port used for SMTP connections to the host server.</p> <p>A PMM message area called Personal Messages is now created in the Message Area directory.</p>
Ready to Install the Program	<p>Click the View Settings button to review the settings for the installation. Use the Back button to change settings. Check the I confirm that all anti-virus software has stopped check box to confirm that you have disabled your anti-virus software.</p> <p>Click Install to start the process.</p>

Installing Client Tools

Installing the Client Tools only installs the tools required for remote administration of your policy configuration. For example, you may want to install Client Tools on your desktop PC, which is remote from the lab containing your PCS and Additional Servers.

Deployment Type	Select Client Tools Only.
Destination Folder	To select a destination folder for the MIMESweeper for SMTP files, other than the default destination folder, click Change .
System Administration	<p>Enter the name of the PCS in the Host Name field. You may need to enter the domain name as well depending upon your network layout.</p> <p>Enter the Administrator account name and password installed on your PCS.</p>
Ready to Install the Program	<p>Click the View Settings button to review the settings for the installation. Use the Back button to change settings. Check the I confirm that all anti-virus software has stopped check box to confirm that you have disabled your anti-virus software.</p> <p>Click Install to start the process.</p>

Creating an Oracle audit database



In order to use Oracle, you must create an Oracle audit database before configuring the audit database in the Report Center. For more information about configuring audit databases, see *Configuring the Audit database* on page 3-27.

If you are creating a new Oracle audit database the MIMESweeper Manager auditing wizard fails and displays the following messages:

```
Unable to connect to the specified database server  
System.Data.OracleClient requires Oracle client software version 8.1.7 or  
greater
```

This error occurs after the Oracle server is chosen from the available list, and you have entered the administrator details, then chosen **Next** to proceed. To stop this problem you must change the Oracle audit database configuration file, and set up the Oracle Security Properties.

To change the Oracle audit database configuration file:

1. Stop the MIMESweeper for SMTP Receiver, Security, and Delivery services.
2. Close the MIMESweeper for SMTP console.
3. In a text editor open the Oracle audit database configuration file `SQLNET.ora` (by default, `c:\oracle\ora92\Network\Admin\SQLNET.ora`), and add the following text:

```
SQLNET.AUTHENTICATION_SERVICES= (none)  
SQL.AUTHENTICATION= (none)
```
4. Save the file.

To set up the Security properties:

1. Access the Security Properties folder of the Oracle audit database.
2. Add the following accounts:

```
IUSR_<machine name>  
IWAM_<machine name>
```
3. Select the **Allow inheritable permissions from parent to propagate to this object** check box.
4. Restart IIS.
5. Restart the MIMESweeper for SMTP Receiver, Security and Delivery services.



If, after restarting the Receiver, Security and Delivery services, you are still experiencing problems, restart your machine.



To use the Oracle audit database you must install the Oracle client locally and configure a connection to a remote Oracle audit database.

During installation of an audit database using either SQL Server or Oracle, a matching user name and password is automatically generated. This generated password must not be changed by the Administrator. If the password is changed, the MIMESweeper system cannot record information in the audit database. If you change the password, the audit database must be removed and reinstalled, or a new database created and the data manually migrated from the old database.

Performing a purge on an Oracle audit database

To perform a purge on an Oracle audit database:

1. In SQL * Plus, log on as SYS.
2. Add your company's password and Host String.
3. Enter the command line:

```
execute$oracle_home/rdbms/admin/userlock.sql
```

4. Click Enter.

An Oracle audit database example is shown below:

1. Enter the command line:

```
connect sys/<password>@<database name> as sysdba
```

2. Click Enter.

3. Enter the command line:

```
@ c:\oracle\ora92\rdbms\admin\userlock.sql
```

4. Click Enter.

A confirmation message is displayed on the screen.



You must perform this procedure on each Oracle audit database server that you wish to connect to.

Configuring the Audit database

To be able to use the MIMESweeper for SMTP Report Center you must configure an Audit database. An Auditing wizard is provided in the Report Center to allow you to do this.

From the MIMESweeper Manager Getting Started page select **Report Center**, then click **Configure Auditing**.

For details on creating a new database or changing your database settings, see the MIMESweeper Manager online help.

Configuring the Message Tracking database

To be able to use the MIMESweeper for SMTP message tracking functionality, you must configure a Message Tracking database. Similar to auditing, a Message Tracking wizard is provided in the Message Center to allow you to do this.

From the MIMESweeper Manager Getting Started page select **Message Center**, then click **Configure Tracking**.

For details on creating a new database or changing your database settings, see the MIMESweeper Manager online help.



Maintaining message tracking data is a resource-intensive operation. To get the best results from message tracking, ensure that you have sufficient database resources available, or consider using a dedicated database server for message tracking.

Post installation tasks

Before you can start to process incoming and outgoing emails there are some configuration tasks that you need to carry out. These are:

- **Company configuration information**

The name of your company and the default domain name for your company. The default domain is used to construct default routes and the default addresses.


- **Network layout**

The options for having MIMESweeper for SMTP forward incoming or outgoing mail to a particular host, which is identified by the IP address or host name for the gateway, proxy, or proxy firewall machine.


If you have not inherited your previous policy configuration, these configuration tasks must be carried out in the Initial Policy Wizard.

The Initial Policy Wizard


The Initial Policy Wizard runs the first time you attempt to start the MIMESweeper Policy Editor.

-
-  Do not run the Initial Policy Wizard until after you have installed at least one Policy Server. If you attempt to run the Initial Policy wizard before you install a Policy Server, the anti-virus software will not be configured correctly. This could apply in situations where you only install a PCS without a Policy Server, and then attempt to run the Initial Policy Wizard before you install the Policy Server.
-

The wizard takes you through the initial steps of setting up authentication, domains, routing and anti-virus details, and then presents a list of individual items that can be selected to use as part of the policy.

-
-  The Initial Policy Wizard will not run if you have upgraded and inherited your previous policy and company information, and routing is already configured.
-

After completing the wizard you can open the MIMESweeper Policy Editor where you can refine your policy as you become more familiar with the product's features.

-
-  Policy Servers installed after the Initial Policy Wizard has run, are not enabled. Use the MIMESweeper Policy Editor to enable or disable servers individually, by right-clicking the server icon and selecting **Enabled** or **Disabled** as required.
-

Subsequent installations

After installing MIMESweeper for SMTP, you can:

- Update an installed version
- Remove an installed version
- Upgrade to a newer version

Details on these operations are provided in the following sections.

Updating MIMESweeper for SMTP

You can update MIMESweeper for SMTP to modify or repair the current installation:

- You may want to modify MIMESweeper for SMTP to add a system feature that you did not select when you first installed the system. For example you may wish to install your web applications on a recently installed Web Server, or to remove a system feature that you no longer wish to use.


-
-  Do not install the Web Applications on a domain controller. The local ASPNET user account is not created when installing the .NET Framework on a domain controller, and this can cause issues to arise. Microsoft has issued Microsoft Knowledge Base Article 315158 relating to this.
-

- You may want to repair MIMESweeper for SMTP to fix installation errors such as missing or corrupt files, shortcuts, and registry entries.

You need the product CD-ROM or the network location containing the MIMESweeper for SMTP setup program, `setup.exe`.

To modify or repair MIMESweeper for SMTP system features:

1. In Control Panel, double-click **Add/Remove Programs**.
2. Select **MIMESweeper for SMTP** and click **Change**. You are prompted for information as follows:

Welcome to InstallShield Wizard	On the Welcome page, click Next .
Program Maintenance	<p>On the Program Maintenance page, select Modify and click Next.</p> <p>If you select Repair at this point, Ready to Repair the Program is displayed and the setup program repairs the current MIMESweeper for SMTP installation.</p>
MIMESweeper for SMTP Server Logon	<p>Enter the PCS Administrator Account Details.</p> <p>If you are installing on an Additional Server enter the name of the PCS in the Host Name field. You may need to enter the domain name as well depending upon your network layout.</p>
Custom Setup	<p>Select which MIMESweeper for SMTP components to change.</p> <p>Click on a feature icon .</p> <p>A pop-up menu gives you the option to install the feature, or to install the feature and its sub-features.</p> <p>Click Next.</p>
Ready to Modify the Program	Click Install . The MIMESweeper for SMTP setup program installs the selected features on the local hard drive.

Removing MIMESweeper for SMTP

You can remove MIMESweeper for SMTP from your machine. You may want to do this if, for example, you have installed a MIMESweeper system for testing, or you want to move the system to a different machine.

To remove MIMESweeper for SMTP:

1. From the Control Panel, access the **Add/Remove Programs Properties**.
2. Select **MIMESweeper for SMTP** and click **Change**. You are prompted for information as follows:

Welcome to InstallShield Wizard On the Welcome page, click **Next**.

MIMESweeper for SMTP Server Logon

Enter the PCS Administrator Account Details.

Enter the name of the PCS in the **Host Name** field. You may need to enter the domain name as well depending on your network.

Enter the Administrator account name and password installed on your PCS.

Operations Database

This page is only displayed if you are uninstalling the PCS.

Add the SQL Server logon Details.

Select the check box if you wish to remove the Operations Database. If you do this your policy and deployment configuration will be lost.

Clear the check box to leave the database intact.

Remove the Program

Click **Remove** to uninstall MIMESweeper for SMTP.



You cannot uninstall the PCS until you have uninstalled MIMESweeper for SMTP components from all other servers in the deployment.

If for any reason you have difficulties uninstalling MIMESweeper for SMTP using **Add/Remove programs** in the **Control Panel**, you can use the following command from within a command prompt:

```
msiexec /x "MIMESweeper for SMTP.msi"
```

Please note that this method must only be used when you cannot uninstall MIMESweeper for SMTP using the remove procedure described above.

Upgrading to a newer version

You can use the MIMESweeper for SMTP 5.3 installation software to upgrade from MIMESweeper for SMTP 5.2 Service Pack 2 or higher versions.



- When you complete an upgrade process, in MIMESweeper Manager, for each server that you upgrade, check the **MIMESweeper log** for invalid expression messages. These are of the form:
`<expression> is not a valid expression`
 where `<expression>` is an expression defined in a Policy Editor reference. These messages indicate that expressions that you have defined in user-defined expression list references are not compatible with MIMESweeper for SMTP 5.3. See the Policy Editor Help for information on upgrading expressions for MIMESweeper for SMTP 5.3.
 - For more information on the upgrade process, see the *ReadMe for MIMESweeper for SMTP 5.3*.
-

If you run a separate test environment, we recommend that you upgrade this first before upgrading your live system.



- Before you upgrade, check the Clearswift Support web site for any additional advice on upgrading your current installation.
-

Before upgrading

Before you begin an upgrade process, perform the following to prepare your system for the upgrade. These processes apply to both single and multiple server environments. For processes that you must perform in a multiple server environment, see *Before upgrading in a multiple server environment* on page 3-34:

- **Clear the MIMESweeper for SMTP system of messages that are being processed:**
 - Stop the Receiver service.
 - Allow received messages to be processed.
 - Stop the Security and Delivery services.
- **Close all instances of the Policy Editor**
 You must close all instances of the MIMESweeper Policy Editor that may be open. If you do not, any changes to your content security policy may not be saved and applied.
- **Disable anti-virus tools**
 You must disable all anti-virus tools before you upgrade.

- **Perform a System Backup of the MIMESweeper system**

You are recommended to perform a system backup before an upgrade:

- On single machine deployments, perform a Level 4 backup.
- On multiple machine deployments, perform a Level 4 backup on Policy Servers, and a Level 3 backup on the PCS and other servers.

To perform the System Backup task:

- a. From the Windows **Start** menu, run the MIMESweeper **System Maintenance Utility** and log on.
- b. On the **Choose Maintenance Task** page of the System Maintenance Utility wizard, select **System Backup**.
- c. Follow the instructions in the wizard to backup your system data.

For information about backup levels and the System Backup and System Restore tasks, see the *Housekeeping* appendix of MIMESweeper for SMTP *Reference*.

- **Inform PMM users**

You should inform all Personal Message Manager (PMM) users that PMM is not available during the upgrade.

After upgrading

After the upgrade process completes, you need to perform the following tasks:

- If you are currently using the IMAGEmanager scenario, you must manually add a new IMAGEmanager license in the Policy Editor after the upgrade.



If you do not add the new IMAGEmanager license for MIMESweeper for SMTP 5.3, the MIMESweeper Security Service will not start.

- On each Policy Server, when installation is complete, ensure that the Audit Consolidator Service and the Infrastructure Service are re-enabled and running.

Upgrading on a single server

This section provides notes on upgrading a single server deployment.

During installation

You may need to enter authentication details on an additional wizard page:

- **Enter audit database administrator name and password**

If auditing was configured for your previous installation, the **Upgrade Audit Database** page appears after the **License Agreement** page of the installation process. The **Upgrade Audit Database** page displays read-only fields showing the existing audit database **Server Name** and **Database Name**. You must complete the audit database **Administrator** and **Password** fields.

Upgrading on a multiple server deployment

This section provides notes on upgrading a deployment of MIMESweeper for SMTP 5.2 that includes two or more servers.

Maintaining message processing throughout an upgrade



If you need to maintain message processing throughout the upgrade, you must disable and stop the Audit Consolidator Service and the Infrastructure Service on each Policy Server, as described below.

After either the Web Applications Server or the Primary Configuration Server (PCS) is upgraded, it replicates a new policy to each Policy Server. This replication causes the Policy Server services to stop and restart. On restarting, the Policy Server services recognize a version mismatch and terminate immediately, halting all mail processing on the Policy Server.

After the Policy Servers have been upgraded, the version mismatch no longer occurs, policy is replicated and mail processing restarts, but in the intervening period no email is processed.

Stopping the Infrastructure Service and the Audit Consolidator Service on each Policy Server prevents policy replication from the PCS or the Web Applications Server when each is upgraded. The Policy Server services do not restart and there is no interruption in mail processing.

Before upgrading in a multiple server environment

In addition to the actions at the beginning of this section, you are recommended to:

- **Disable and stop the Audit Consolidator service**

On each Policy Server, disable and stop the MIMESweeper for SMTP Audit Consolidator service, which consolidates the data that is passed to the Audit Disposer service for processing and forwarding to the Audit Server. Disabling this service ensures that the audit data is maintained on the Policy Server during the upgrade process.

To disable and stop the Audit Consolidator service:

1. From the **Start Menu**, select **Settings**, then select **Control Panel**.
2. Double-click **Administrative Tools**, then double-click **Services**.
3. Double-click **MIMESweeper for SMTP Audit Consolidator** to open the properties dialog, then select the **General** tab.
4. Select **Disabled** in the **Startup type** drop-down list and click **Stop**.
5. Click **OK**.

- **Disable and stop the MIMESweeper for SMTP Infrastructure Service**

On each Policy Server, disable and stop the MIMESweeper for SMTP Infrastructure Service to prevent the PCS from replicating the new policy version to the Policy Servers when it is upgraded. The Policy Server will continue handling messages.



You must shut down the MIMESweeper Policy Editors before you disable and stop the Infrastructure Service.

To disable and stop the Infrastructure Service, repeat steps 1 to 5 above, but in step 3 double-click MIMESweeper for SMTP Infrastructure.

The Receiver, Security, and Delivery Services will still be running on the Policy Servers. Each service will continue to process mail according to its current policy.

Upgrade sequence

When you are upgrading a deployment of two or more servers, the server hosting the Web Applications Server must be upgraded first. This server may be your PCS or a dedicated Web Applications Server.

You can upgrade the remaining machines in your deployment in any order.

Handling errors during installation

If the installation process encounters an error, it stops and displays an error message describing the problem. When you click **OK** on the error message, the installation rolls back automatically to your original version of MIMESweeper for SMTP. When rollback is complete, you are prompted to restart the machine.

- If automatic rollback occurs during an upgrade of the server hosting the Web Applications (the first server that you upgrade in a multiple server deployment), then you are returned to a working deployment of your original version of MIMESweeper for SMTP.
- If automatic rollback occurs during an upgrade of a second or subsequent server (following successful upgrade of the server hosting the Web Applications and, possibly, one or more other servers), note the problem and contact your normal support provider.

Performing the upgrade

The following sections describes the upgrade process screens that are displayed. You can install Additional Servers after the initial installation process. When upgrading, the Installation Wizard detects the server type: PCS or Policy Server, and the Deployment Type page is not displayed.

Welcome	Click Next to start the installation process.
Server Logon	<p>Enter the password for the PCS Administrator Account. This is the name and password set up to administer MIMESweeper for SMTP.</p> <p>Confirm the password.</p> <p>Ensure that you make a record of the password and name for future usage. The administrator can subsequently setup other users with administrative rights, but only this account can be used to install MIMESweeper for SMTP.</p>
License Details	<p>Configuration information for your license:</p> <p>Company Name - The name of your company.</p> <p>License Key - A 30-digit alphanumeric key.</p> <p>Serial Number - A 16-digit number.</p>
Operations Database	<p>The Operations database contains a summary of all message and archive areas, allowing fast searching and filtering of messages from the user interface.</p> <p>Enter the SQL Server logon details to upgrade the database on the specified server.</p>
Ready to Install the Program	<p>You are now ready to install MIMESweeper for SMTP.</p> <p>Click Install to start the process.</p>

Licensing MIMESweeper for SMTP

Before you can start the MIMESweeper for SMTP services, you must add a valid license on the machine on which you installed a full MIMESweeper for SMTP product, if you did not enter your license details during installation.

Once you have installed a license, you can start the Delivery, Receiver, and Security services. Licenses are added in the MIMESweeper Policy Editor, for details on adding and removing licenses, see the MIMESweeper Policy Editor online help.



Keep a copy of the license key in case you need to reinstall MIMESweeper for SMTP.

Licenses are cumulative. For example, if you have a license for 100 users and request an upgrade for another 100 users, enter the details of the new license. Your system is then licensed for the sum of the two licenses, that is, 200 users.

There are three levels of license that you can purchase with MIMESweeper for SMTP:

- The **Standard** license allows you to install one Primary Configuration Server and two policy servers, and provides the basic product functionality.
- The **Advanced** license allows you to install one Primary Configuration Server and four policy servers, and provides additional functionality.
- The **Enterprise** license allows you to install two Primary Configuration Servers up to eight policy servers, and provides the additional functionality available in the Advanced license.

Additional functionality available in the Advanced and Enterprise licenses

The additional functionality provided by the Advanced and Enterprise licenses is as follows:

- **System maintenance tool:** Advanced and Enterprise licenses provide the ability to:
 - Promote an existing server in the MIMESweeper deployment to become the Primary Configuration server for the installation, in emergency maintenance mode.
 - Move the Operations database to another SQL server other than the PCS.
 - Move the web applications, that is MIMESweeper Manager and PMM web sites, to another web server
- **Message tracking:** Advanced and Enterprise licenses provide additional options when configuring searches for message tracking details. There are certain additional message properties that you can include in your tracking database search configurations. These are Policy server, Classification, Scenario folder, and Content Analysis Queues.
- **PMM:** Advanced and Enterprise licenses provide PMM users with the ability to track messages that they have sent, or messages that have been sent to them.

CHAPTER 4

Getting Started with MIMESweeper Policies

This chapter describes how the Initial Policy Wizard helps you to create your first policy

Overview	4-2
Creating a policy with the Initial Policy Wizard	4-3
Initial Policy Wizard policy elements	4-7
Anti-spam Detection	4-7
Anti-Virus	4-7
Block Confidential Expressions	4-8
Block Executables	4-8
Block GLBA Expressions	4-8
Block HIPAA Expressions	4-9
Block Large Images	4-9
Block Large Incoming Messages	4-9
Block Microsoft Class 1 File Extensions	4-10
Block Multimedia	4-10
Block PCI Expressions	4-10
Block PII Expressions	4-11
Block SEC Expressions	4-11
Block SOX Expressions	4-11
Block Virus Hoaxes	4-12
Disclaimer	4-12
Edge Dangerous File Classifier	4-12
Edge Spam Classifier	4-13
Edge Virus Classifier	4-13
PowerPoint and Word Attachment Compression	4-13
Profanity	4-14
Script	4-14

Overview

This chapter provides information about the steps required after installing MIMESweeper for SMTP and describes how the Initial Policy Wizard helps you to create your first policy. The wizard takes you through the initial steps of selecting the type of policy template you require and selecting individual elements that are to be used as part of the policy. You then set up authentication, domains, routing and anti-virus details.



The Initial Policy Wizard runs the first time you open the MIMESweeper Policy Editor.

However, if you are upgrading from MAILsweeper for SMTP, you can choose to inherit your existing policy configuration at installation. If you do this, the Initial Policy Wizard is bypassed.

When the Initial Policy Wizard is complete the MIMESweeper Policy Editor opens. The MIMESweeper Policy Editor then contains scenarios, classifications and message areas that the Initial Policy Wizard has created, based upon the selections you made. It also contains the company information, domain and routing addresses that you specified.

The Initial Policy Wizard only runs the first time you open the MIMESweeper Policy Editor. When it is completed, it cannot be run again. However, all configuration options provided by the Initial Policy Wizard are also available in the MIMESweeper Policy Editor.

You can subsequently refine the policy created with the wizard as you become more familiar with the MIMESweeper Policy Editor's features.

The Initial Policy Wizard offers three Policy Templates:

- **Basic Policy**
Provides a simple policy that includes an anti-virus scenario and a Disclaimer for outgoing messages. This policy is good for using as a base on which to build your own more comprehensive policy.
- **Demonstration Policy**
Provides a policy that includes most scenario types that you are likely to need. This policy is used for demonstrating the capabilities of MIMESweeper for SMTP, and should not be used in a production environment. Be aware that you will not be able to use the Initial Policy Wizard again to create a working policy.
- **Typical Policy**
Provides a policy that blocks the common types of content security threats and fulfills the requirements of most businesses in a production environment.

The first section of this chapter describes in detail the individual pages of the Initial Policy Wizard, and what you need to do at each stage. The second section describes the policy elements available and looks at what the Initial Policy Wizard will create.

Creating a policy with the Initial Policy Wizard

The Initial Policy Wizard will only run the first time you open the MIMESweeper Policy Editor. To start the wizard:

1. Make sure you are logged on as a user with write access to the Windows registry, for example, as a local Administrator.
2. Click **Start**, point to **Programs**, click **MIMESweeper for SMTP**, then click **MIMESweeper Policy Editor**.
3. The Initial Policy Wizard starts, and prompts you to select whether or not a MIMESweeper Edge server or servers will be used with your installation. Select an option and click **Next**.

If your installation uses an Edge Server, the default policies that the wizard configures use the Edge classifier scenario to detect spam, dangerous file types, and viruses rather than the MIMESweeper for SMTP spam and virus detection scenarios.



If you use an Edge Server, refer to the MIMESweeper Edge Server Deployment Guide for information on how to configure and use your Edge Server with your MIMESweeper for SMTP installation.

4. On the Policy Template pages, follow the instructions on each wizard page, and click **Next** to move to the next page.

Welcome to the Initial Policy Wizard Click **Next** to continue.

Policy Template

Select the policy template (**Basic**, **Demonstration** or **Typical**) to use to create your template. The selection made here determines the policy elements available for selection on the following page.

A brief description of the policy's main features is displayed beneath the template title.

For details on the available elements, see *Initial Policy Wizard policy elements* on page 4-7.

Policy Customization

Select the elements that you want to include in your policy, for example, anti-spam detection, image blocking, large message blocking. To exclude the element from your policy, clear the check box.

Click the down arrow for a brief description of the element.

The elements you select here create the email policy applied to incoming and outgoing emails at the SMTP gateway.

Each element selected creates a scenario in the MIMESweeper Policy Editor. For each scenario created, associated classifications and Messages Areas are created.

See *Initial Policy Wizard policy elements* on page 4-7 for details of each policy element available with the Initial Policy Wizard.

Domain Configuration

The company name and default domain.

- **Company Name**

The name of your company taken from your domain name.

- **Domain Name**

The default domain for your company, for example, `your-companyname.com`, taken from the Fully Qualified Domain Name (FQDN).

The default domain is used to construct default routes and addresses.

After installation, you can change your default domain name in the **Domain** tab of the **SMTP Relay Properties** pages.

The default addresses are:

- **Server:** `mimesweeper@<domain>`
- **Administrator:** `postmaster@<domain>`

You can change the default addresses later in the **Addresses** tab of the **MIMESweeper for SMTP Properties** pages.

Mail Routing Configuration

Select mail servers to which MIMESweeper for SMTP directs incoming and outgoing mail. Enter the host name in the **Inbound Mail Server** and **Outbound Mail Server** fields.

The incoming and outgoing mail information is used to configure initial routing and SMTP relay properties.

By default the Initial Policy Wizard configures MIMESweeper for SMTP to bind to the standard SMTP port 25. The administrator must ensure that this does not conflict with any other existing SMTP stack already installed on the system.

You usually forward incoming mail to your SMTP gateway. MIMESweeper for SMTP considers mail to be incoming if the destination domain matches your local domain.

If you choose not to forward outgoing mail to a particular host, MIMESweeper for SMTP uses the DNS to forward outgoing mail.

If you choose not to select a server now, the mail routing configuration can be added later, or changed in the **Routing** folder of the **SMTP Relay** in the MIMESweeper Policy Editor.

Anti-virus Configuration	<p>This page is only displayed if you selected Anti-virus in the Policy Configuration page.</p> <p>In addition to the MIMESweeper for SMTP product, an anti-virus tool supplied by a third-party vendor is required to enforce your anti-virus policy.</p> <p>If you have selected the anti-virus option, you must have an anti-virus tool installed. Therefore you must select your anti-virus tool from those listed here, before continuing.</p> <p>The third-party anti-virus tools that can be integrated with MIMESweeper for SMTP are:</p> <ul style="list-style-type: none">• Installed Content Scanners Any supported COM-based content-scanning software currently installed on your computer that can be used with the Content Scanner scenario.• Legacy MIMESweeper for SMTP scenarios The DLL-based anti-virus tools that can be used with the appropriate scenario for the third-party anti-virus tool. For more information about third-party anti-virus tools, see the readme for anti-virus tools, available from the CD-ROM. <p>You can change the anti-virus tool in the scenario property pages.</p>
Disclaimer Message	<p>This page is only displayed if you selected Disclaimer in the Policy Configuration page.</p> <p>Edit the text directly in the annotation window if required.</p> <p>The Disclaimer is used by the Legal Disclaimer scenario to append a statement limiting your organization's legal liability for the contents of the message.</p>
Finish	<p>Complete the Initial Policy Wizard by selecting which of your Policy Servers to save your policy to. Click Finish. The completed policy is replicated and applied to the Policy Servers selected.</p> <p>The MIMESweeper Policy Editor opens. You will need a username and password to log in. For details about Advanced log in options, see Chapter 6.</p>

Initial Policy Wizard policy elements

The Initial Policy wizard creates a scenario for each policy element selected. For each Initial Policy Wizard element that you can select, this section provides the following information:

- A description of the functionality that the element provides, including details of whether it is included in installations that use Edge Servers.
- The MIMESweeper for SMTP scenario type that the element uses. See the *MIMESweeper for SMTP Reference*, or the *Policy Editor Online Help* for more information on these scenarios.
- The Initial Policy Wizard types, that is **Basic**, **Demo**, and **Typical** where the element is available.
- The message direction to which the element is applied, that is inbound messages, outbound messages, or messages in both directions. When the element is applied to messages in both directions, a scenario is created in both the **Incoming** and the **Outgoing** folders.
- How the element processes detected messages, for example, quarantining or delivering detected messages.

Anti-spam Detection

Description	Detects and blocks spam messages. Users can manage their messages using the Personal Message Manager (PMM). This element is not included for installations that use Edge Servers.
Scenario type used	SpamLogic.
Initial Policy Wizard types	All types.
Mail direction	Incoming only.
Classification and action	Quarantines detected messages in the Personal Messages message area.

Anti-Virus

Description	Detects and blocks messages identified by virus scanning software as containing viruses.
Scenario type used	Content scanner with your installed anti-virus tool. Anti-virus software is not supplied with the MIMESweeper for SMTP software.
Initial Policy Wizard types	All types.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Virus Messages message area.

Block Confidential Expressions

Description	Detects and blocks messages that contain terms defined in the Confidential Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo and Typical only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block Executables

Description	Detects and blocks messages that contain executable attachments, for example .exe files, java files, and DLL files. This element is not included for installations that use Edge Servers.
Scenario type used	Data Type Manager.
Initial Policy Wizard types	Demo and Typical only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Executable Messages message area.

Block GLBA Expressions

Description	Detects and blocks messages that contain terms defined in the Gramm-Leach-Bliley Act (GLBA) Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block HIPAA Expressions

Description	Detects and blocks messages that contain terms defined in the Health Insurance Portability and Accountability Act (HIPAA) Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block Large Images

Description	Detects and blocks messages that contain images larger than 50 Kb.
Scenario type used	Data Type Manager.
Initial Policy Wizard types	Demo and Typical only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Image Messages message area.

Block Large Incoming Messages

Description	Detects and blocks messages larger than 10 MB.
Scenario type used	Size Manager.
Initial Policy Wizard types	Demo and Typical only.
Mail direction	Incoming only.
Classification and action	Quarantine detected messages in Oversize Messages message area.

Block Microsoft Class 1 File Extensions

Description	Detects and blocks messages with Microsoft class 1 file attachments, for example file extensions such as .bat, .com, .exe, .hs, etc. This element is not included for installations that use Edge Servers.
Scenario type used	File Detector.
Initial Policy Wizard types	All types.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Executable Messages message area.

Block Multimedia

Description	Detects and blocks messages that contain multimedia file attachments, for example, audio or video files.
Scenario type used	Data Type Manager.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantine detected messages in the Multimedia Messages message area.

Block PCI Expressions

Description	Detects and blocks messages that contain terms defined in the Payment Card Industry (PCI) Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block PII Expressions

Description	Detects and blocks messages that contain terms defined in the Personally Identifiable Information (PII) Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block SEC Expressions

Description	Detects and blocks messages that contain terms defined in the US Securities and Exchange Commission (SEC) Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block SOX Expressions

Description	Detects and blocks messages that contain terms defined in the Sarbanes-Oxley (SOX) Expressions reference.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo only.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Dirty In or Dirty Out message area depending on the message direction (inbound or outbound).

Block Virus Hoaxes

Description	Detects and blocks messages that contain terms defined in the Hoax Virus Expression List .
Scenario type used	Text Analyzer.
Initial Policy Wizard types	Demo and Typical only.
Mail direction	Incoming only.
Classification and action	Quarantine detected messages in the Virus Messages message area.

Disclaimer

Description	Adds the default disclaimer to all outgoing messages.
Scenario type used	Legal Disclaimer.
Initial Policy Wizard types	All types.
Mail direction	Outgoing only.
Classification and action	Adds disclaimer text to the message body before delivery.

Edge Dangerous File Classifier

Description	Detects messages that have been pre-classified by an Edge server as containing dangerous file attachments.
Scenario type used	Edge Message Classifier.
Initial Policy Wizard types	All types where an Edge Server is configured.
Mail direction	Incoming only.
Classification and action	Quarantines detected messages in the Executable Messages message area.

Edge Spam Classifier

Description	Detects messages that have been pre-classified by an Edge server as spam messages.
Scenario type used	Edge Message Classifier.
Initial Policy Wizard types	All types where an Edge Server is configured.
Mail direction	Incoming only.
Classification and action	Quarantines detected messages in the Personal Messages message area.

Edge Virus Classifier

Description	Detects messages that have been pre-classified by an Edge server as containing a virus.
Scenario type used	Edge Message Classifier.
Initial Policy Wizard types	All types where an Edge Server is configured.
Mail direction	Incoming only.
Classification and action	Quarantine detected messages in the Virus Messages message area.

PowerPoint and Word Attachment Compression

Description	Detects outgoing messages that contain PowerPoint or Word Attachment over 5 MB in size, and compresses the attachments before delivery.
Scenario type used	Attachment Manager.
Initial Policy Wizard types	Demo only.
Mail direction	Outgoing only.
Classification and action	Compress attachment and forward to the Cleaned message area for delivery elements that cannot be compressed are quarantined to the Oversize Messages area.

Profanity

Description	Detects messages that contain profane terms defined in the Profanity List reference. The reference list used depends on the language. There is a Profanity List reference for each language that MIMESweeper for SMTP supports.
Scenario type used	Text Analyzer.
Initial Policy Wizard types	All types.
Mail direction	Both directions.
Classification and action	Quarantines detected messages in the Profane Messages message area.

Script

Description	Detects messages that contain dangerous scripts.
Scenario type used	Script Manager using the Virus Worm Script Commands reference.
Initial Policy Wizard types	Typical only.
Mail direction	Incoming only.
Classification and action	Quarantine detected messages in the Script Messages message area.

CHAPTER 5

Security

This chapter describes how to secure your network using MIMESweeper for SMTP.

Overview	5-2
Securing the environment	5-2
Securing the Primary Configuration Server	5-2
Securing Windows machines	5-3
Use a Windows NTFS file system	5-3
Do not install unnecessary default Windows software	5-3
Do not install unnecessary Windows network services	5-3
Review default Windows services	5-4
Restrict Windows user access	5-5
Securing the MIMESweeper Manager application server	5-5
Securing database communications between machines	5-6
Securing routing and relay through an SMTP Mail Policy Server	5-8
Secure the firewall to restrict email reception to a Policy Server	5-9
Secure routing through a Policy Server	5-9
Specify domains for which a Policy Server accepts inbound mail	5-9
Define domains for inbound and outbound email routing	5-9
Secure a Policy Server against relay attacks	5-10
Securing access to MIMESweeper for SMTP	5-10

Overview

This chapter describes how to secure the machines in your MIMESweeper for SMTP deployment to protect them and the rest of your network from unauthorized access from both those outside and from users of your own system.

After you have installed and configured the Primary Configuration Server (PCS) and reconfigured existing SMTP mail servers to route mail correctly through MIMESweeper Policy Servers, ensure that the surrounding environment is secured and configured correctly. For details on installing the Policy Servers and routing mail, see Chapter 3.

Securing your MIMESweeper for SMTP deployment involves:

- **Securing the environment**
Configuring operating system features on the PCS and other machines in your internal network.
- **Securing the Web Server**
Creating a secure communication channel between the MIMESweeper Manager application and the web server on which it is installed.
- **Securing communications between machines**
Protecting the transmission of sensitive data between MIMESweeper for SMTP machines and other machines in your internal network.
- **Securing routing and relay through a Policy Server**
Preventing the Policy Servers being used as an open relay.
- **MIMESweeper for SMTP security**
Restricting user logon to the PCS and access to MIMESweeper features.

Securing the environment

You must secure the PCS and other machines in the surrounding network to protect them from network abuse by unauthorized users in your organization.

Securing the Primary Configuration Server

Securing the PCS machine involves:

- Allowing only authorized access to the system by limiting the logon accounts to the Windows machine.
- Disabling IP forwarding to prevent the Policy Server from acting as a router. For details see your Microsoft Windows documentation.
- Ensuring that any non-essential network services are disabled or uninstalled.
- Considering security settings for other elements of your environment, such as the Windows Registry, RPC access, and disk access.

Securing Windows machines

Securing a Windows machine involves considerations both when installing and configuring the operating system. No machine to be secured should be taken from a previous deployment as a clean install is highly recommended.

The following sections provide guidelines on how to secure aspects of a Windows machine used in your MIMESweeper for SMTP deployment:

- *Use a Windows NTFS file system* on page 5-3
- *Do not install unnecessary default Windows software* on page 5-3
- *Do not install unnecessary Windows network services* on page 5-3
- *Review default Windows services* on page 5-4
- *Restrict Windows user access* on page 5-5

Use these guidelines in conjunction with your organization's IT Security policy to determine the actual settings you configure and services you enable.

Use a Windows NTFS file system

MIMESweeper for SMTP requires NTFS to operate securely in Windows. When you install Windows, ensure that you select NTFS when prompted for the file system to use when formatting your installation partition.

Do not install unnecessary default Windows software

To be as secure as possible, minimize the operating system software in use. When you install Windows, select as little of the optional software as possible, preferably not selecting any that is not a prerequisite for MIMESweeper for SMTP. You can install new components later if required, but removing components is not always simple or clean.

For details of the software required for a MIMESweeper for SMTP deployment, see the *Prerequisites* release document.

Do not install unnecessary Windows network services

If your Windows server is to be used exclusively as a Policy Server, minimize the networking components in use. When you install Windows, select only TCP/IP in the networking section.

Avoid installing unnecessary services. MIMESweeper for SMTP requires the following services, but ensure that they are disabled:

- File and Printer Sharing
- Microsoft Client or Server

Networking components apart from these two are not necessary, unless your network layout demands them for proper operations. Operating with unnecessary components will open more ports on your server.

Security

When configuring network settings after installation, on the WINS tab of the **Advanced TCP/IP Settings** dialog box accessed from Windows Control Panel:

- Clear the **Enable LMHOSTS** lookup option.
- Select the **Disable NetBIOS over TCP/IP** option.

For details on these options, see your Microsoft Windows documentation.

Review default Windows services

After installing Windows, continue to secure your machine by disabling unnecessary default services.

Do not disable the following services, which generally are necessary for basic operations:

- DNS Client
- DHCP Client (only if required by your network layout; otherwise, not recommended)
- Event Log
- Logical Disk Manager
- Message Queue
- Network Connections Manager
- Plug and Play
- Protected Storage
- Remote Procedure Call (RPC)
- RunAs Service

For details of the services required for a MIMESweeper for SMTP deployment, see the *Prerequisites* release document.

Other services may be necessary, depending on how you operate hosts on your network, and what other requirements you may have for the server in question. Your organization's IT security policies may list the software and services which are permissible on network boundary systems.

You can disable any other services that are not required for basic operations or by your IT policy in the Services dialog box accessed from Windows Control Panel. For details on doing this, see your Microsoft Windows documentation.

Restrict Windows user access

After installing Windows, configure the security levels for the local computer to reflect your organization's internal policies for the following areas:

- **User rights assignments**

Specify which users or groups have logon privileges on the computer. If your Windows server is to be used exclusively as a Policy Server, remember that standard users will never need to access the system. Any Active Directory configurations in use in your network need not be configured for the Policy Server, as it should function as a standalone system. Preventing local access for unprivileged users prevents a number of potential problems in refining user settings.

- **Auditing**

Specify which security events are recorded in the Security log, which can be viewed in the Windows Event Viewer. If your organization does not have an explicit auditing policy, at a minimum, you are recommended to audit logon events and account management.

You configure Audit Policy, User Rights Assignment, and Security Options policies in the Local Security Policy tool accessed from Windows Control Panel. For details on using this tool, see your Microsoft Windows documentation.

Securing the MIMESweeper Manager application server

The MIMESweeper Manager application server is the server that contains the following IIS hosted applications: Report Center, Message Center, Security Center and Systems Center. It is accessed from a web browser, and is a logical server which can be installed on a dedicated Web Server or on the same Windows server as another MIMESweeper server to suit your organization's requirements. This section uses the term Web Server to refer to whichever physical machine the MIMESweeper Application is installed on.

The MIMESweeper Manager application can use the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to establish an encrypted communication channel between a client and a server.

To protect sensitive data when a browser makes an HTTP request to the Web Server, you must secure the Web Server. This requires SSL to be set up on the Web Server and the client to use the HTTPS protocol to access SSL-configured files or directories. The Web Server must listen on TCP port 443 and have a server authentication certificate installed on it.

You can obtain a server certificate in either of the following ways:

- Request to have one issued by a Certificate Authority (CA).

A CA is an organization that issues independently authenticated digital certificates for use by individual or organizations, for example, Verisign. Certificates issued by a recognized CA are, by default, explicitly trusted.

- Generate your own based on a root certificate.

Certificate generation software, such as Microsoft Certificate Services, can create internal certificates. Certificates that originate from the same root recognize and, by default, trust each other.

Once the MIMESweeper Manager application authenticates the Web Server's certificate, the communications channel becomes encrypted until the browser session is closed.

To set up SSL on the Web Server using Microsoft Internet Information Services (IIS):

1. Generate and submit a certificate request (if you do not already have a valid server certificate). If the request is successful, the CA will send a validated certificate.
2. Install the certificate on the Web Server using Microsoft IIS.
3. Configure Web Server files and directories to require SSL for access:
 - MSWSMTP
 - MSWPMM
 - MSWconfigwebservice

Clients must then use the HTTPS protocol to access any of these files or directories.



You can choose to ignore SSL security on the Images and MiniIcons folders. Doing this will reduce the loading on the system.

For details on performing these steps, see your Web Server administrator or the IIS documentation.



If the certificate you specified was not created by a third-party CA authority or a root certificate, then the certificate is not explicitly trusted. In this case, the first time a user attempts to log on to MIMESweeper Manager, it displays a confirmation message asking the user to accept the certificate as trusted.

Securing database communications between machines

By default, data is transmitted between the following MIMESweeper for SMTP machines in an encrypted format to provide secure communications:

- PCS and Policy Server
- Policy Server and Audit/Message Tracking Server
- PCS and Web Server

See Chapter 2 for an overview of the way that machines are deployed in a network.

You must secure communications between MIMESweeper for SMTP machines and other machines on your internal network to prevent the unauthorized interception of any data transmitted between these machines:

- **Audit/Message Tracking Server and Database server**

The PCS contacts the Audit/Message Tracking Server to transfer information stored in its audit logs. The Audit/Message Tracking Server in turn writes this data to the database server containing the audit/Message Tracking database used to generate management reports and to provide message tracking functionality. For details on message tracking, auditing and reporting, see the Reference.

- **Web Server and Audit Server**

The Web Server accesses the audit/Message Tracking database on the database server to generate management reports based on information stored there. For details on message tracking, auditing and reporting, see the Reference.

- **Web Server and PCS**

When the Web Server is on a different machine to the PCS it will contact the PCS to access the Operations Database.

To secure communications between these machines in your MIMESweeper for SMTP deployment, you are recommended to set up a Microsoft Internet Protocol Security (IPSec) policy. IPSec encrypts all data sent between two specified computers to guarantee confidentiality. It requires both computers to have static IP addresses. IPSec is usually set up between an application server, for example, the PCS or the MIMESweeper Manager server, and a database server. That is, the database server or the PCS.



You are recommended not to enable communications between any other machines in your MIMESweeper for SMTP deployment. Additionally, do not enable any file browsing access on machines in the deployment.

To set up an IPSec security policy between a data server and an application server in your MIMESweeper for SMTP deployment:

1. Create an IP filter on the data server.
A filter consists of source and destination IP addresses, an IP protocol (such as TCP), and source and destination ports.
2. Create filter actions on the data server.
A filter action specifies the actions to take when a filter is invoked. For example, to enforce the use of encryption between the MIMESweeper Manager server and the database server.
3. Create filter rules on the data server.
A rule associates a filter with a filter action.

4. Export the IPSec policy from the data server to the application server.
5. Assign policies on both the data server and the application server.
6. Verify that it works using Network Monitor to confirm that data sent between the data server and the application server is encrypted.

For details on performing these steps, see your server administrator or the Microsoft Windows server documentation.

Securing routing and relay through an SMTP Mail Policy Server

You must secure communications between individual Policy Servers in your MIMESweeper for SMTP deployment and the outside world to prevent unauthorized email hosts or domains from routing or relaying SMTP email messages through your mail system.

Relay is an inherent feature of all SMTP-based servers. It can be used legitimately to pass mail between separate internal email systems. However, leaving the relay feature open by not specifying the hosts the SMTP server is permitted to forward mail to or receive mail from makes the system vulnerable to unauthorized use. An open relay can process mail that is neither for, nor from, users in your organization. This enables unauthorized senders to route large volumes of mail through your server or to conceal the actual source of the messages, thus exposing your organization to the following threats:

- Mail system crashes
An unauthorized user is effectively stealing network capacity, disk space, and processing power. A relay attack can render the mail system unusable, causing a denial of service attack, which can be costly and time-consuming to recover from.
- Damage to reputation
A relay attack can send large numbers of unsolicited email messages with the negligent organization's name on them. This can undermine an organization's reputation.
- Blacklisting
Some organizations publish blacklists of the domains and mail hosts responsible for sending large numbers of unsolicited mail. By falling victim, an organization can find itself blacklisted.

The following sections provide guidelines on how to secure communications between servers in your MIMESweeper for SMTP deployment and the outside world:

- *Secure the firewall to restrict email reception to a Policy Server* on page 5-9.
- *Secure routing through a Policy Server* on page 5-9
- *Secure a Policy Server against relay attacks* on page 5-10

Secure the firewall to restrict email reception to a Policy Server

When securing your firewall, you must take into account MIMESweeper for SMTP's place in your email network. For details on options for deploying Policy Servers, see Chapter 2. Typically, a Policy Server is deployed on a separate DeMilitarized zone (DMZ) network outside the firewall. In this deployment model, it is important to secure the firewall so that the port configured for email reception restricts access to Policy Servers only. By default, port 25 is reserved for SMTP email traffic, but you can configure a different port if required.

It is especially important to block ports if you have left RPC enabled on your Policy Server. Additionally, you are recommended to block inbound ICMP traffic other than types 3 (destination unreachable) and 4 (fragmentation needed).

You may need to configure additional settings for the firewall depending on the machine on which the Policy Server is installed, whether it is being used to deliver outbound mail, and what type of firewall is installed. You need to open ports 23953 and 23954 to the clean network to access the PCS and Audit/Message Tracking Servers.

Secure routing through a Policy Server

You must secure routing through a Policy Server to ensure that it accepts SMTP email traffic only from known sources. To do this, you specify the domains for which it accepts inbound email messages and configure how the PCS routes email to the external and internal message handling system.

Specify domains for which a Policy Server accepts inbound mail

When you create a policy configuration, you specify the domain name for which the PCS will accept inbound email. Any subdomains of the specified domain are included. This configuration restricts the domains for which the PCS accepts inbound email, which prevents it from being used to relay mail for other domains outside your organization.

If your organization has more than one domain, you can add these to an existing policy configuration to allow the PCS to accept mail for this domain and its subdomains as well.

For details on how to specify which domains a Policy Server is allowed to accept email for, see the MIMESweeper Policy Editor online help.

Define domains for inbound and outbound email routing

You configure the domains that a Policy Server uses to route email messages to the outside world and to your organization's internal message servers. To configure this domain routing go to the `Servers/<servername>/Routing` folder in MIMESweeper Policy Editor.

For details on how to configure domain routing, see the MIMESweeper Policy Editor online help.

Secure a Policy Server against relay attacks

You must secure a Policy Server against relay attacks to ensure that it relays SMTP email traffic only for listed domains. To do this, you specify the hosts and domains for which the Policy Server will accept or reject mail:

- Reject email messages from unidentified domains.
- Reject email messages from hosts listed in a web-based spam database.
- Reject or accept email messages from specified mail hosts.

Securing access to MIMESweeper for SMTP

You must secure user access to the PCS and specific system and policy management folders in the Message Center. You specify this type of system security by creating user accounts to which you can assign access permissions using the Security Center.

There are two types of user accounts:

- **Users**

A username and password for an individual user, which can be assigned access permissions to log on to the MIMESweeper Manager and the Policy Editor and to view and manage specific folders in the Message Center.

- **Roles**

A group of users, which can be assigned common access permissions to view and manage specific folders in the Message Center.

When users start the MIMESweeper Policy Editor, they are prompted to enter a user name and password in addition to the address of the PCS to connect to. The user name and password are compared against defined users to authenticate the user's permissions to access the specified Policy Server. This authenticated log on ensures that the correct access rights are enforced for each user.

Once logged on, the user name and password are compared to defined users and roles to identify which sections of MIMESweeper Manager and which folders in the Message Center the user can view and manage. Each folder in the Message Center has its own associated set of access permissions. The permissions assigned to the currently logged on user are determined by a number of factors, including what roles that user is a member of and what permissions are inherited from the folder's parent in the hierarchy.

MIMESweeper for SMTP automatically creates a super-user account, called Administrator, which always has full access permissions to all areas of MIMESweeper for SMTP. For details on the Administrator super-user account and on creating user and roles user accounts of your own, see the Reference.

CHAPTER 6

System Startup and Quicktour

This chapter introduces the interfaces for the MIMESweeper for SMTP components and describes the MIMESweeper Policy Editor in the Microsoft Management Console.

Overview	6-2
MIMESweeper Policy Editor	6-2
MIMESweeper Manager	6-2
Personal Message Manager	6-2
Opening and closing the console	6-3
Touring the MIMESweeper Policy Editor user interface	6-4
User interface components	6-5
Accessing MIMESweeper for SMTP commands	6-6
MIMESweeper Policy Editor snap-in	6-7
Save and Apply commands	6-8
MIMESweeper Policy Editor items	6-8
Accessing properties	6-14
Task Pad	6-14
MIMESweeper for SMTP wizards	6-15
MIMESweeper Manager	6-17
How to access MIMESweeper Manager	6-17
Personal Message Manager	6-19
Setting up PMM	6-19
Notification of withheld messages	6-19
Accessing a user's PMM messages	6-20

Overview

The MIMESweeper for SMTP user interface is provided by three components:

- The MIMESweeper Policy Editor is a Microsoft Management Console (MMC) snap-in and is used for setting policy and system configuration.
- The MIMESweeper Manager is a web browser application used for message management, system monitoring, reporting and security.
- The Personal Message Manager is a web browser application allowing the user to manage messages that have been classified as spam or potentially spam and forwarded to their Inbox. Users can also use the Personal Message Manager to track messages either sent by or sent to them, to determine a message's status.

MIMESweeper Policy Editor

The MIMESweeper for SMTP installation program creates a default MIMESweeper for SMTP Console which contains the MIMESweeper Policy Editor.

This chapter explains how to start the MIMESweeper Policy Editor and describes the folder and policy items that you use to construct your email policy. To start the MIMESweeper Policy Editor, see *Opening and closing the console* on page 6-3.

MIMESweeper Manager

You access the MIMESweeper Manager from a web browser. The Getting Started page provides access to the four management centers and a system health window. The centers are the **Message Center**, **System Center**, **Report Center**, **Security Center**. Use these to configure, control and monitor your system. An overview of the user interface is provided in *MIMESweeper Manager* on page 6-17.

Personal Message Manager

The Personal Message Manager (PMM) administration area provides management and monitoring of PMM messages areas. PMM allows end users to manage their own messages which have been quarantined, by providing them with a link from a notification email. PMM configuration is described in *Personal Message Manager* on page 6-19.

MIMESweeper for SMTP also provides an Initial Policy Wizard which runs the first time you open the MIMESweeper Policy Editor. This is provided to help new or infrequent users to create an initial email policy. For more information, see Chapter 4.

Opening and closing the console

Once you have installed MIMESweeper for SMTP, you can start the MMC with the MIMESweeper for SMTP Console loaded.



The Initial Policy Wizard runs the first time you attempt to start the MIMESweeper Policy Editor, unless you have upgraded and chosen to inherit your existing policy. For more information about the Initial Policy Wizard see, Chapter 4.

To open the default MIMESweeper for SMTP console:

- From the **Start** menu point to **Programs**, select **MIMESweeper for SMTP**, and then select **MIMESweeper Policy Editor**. The **Login** dialog is displayed.
- Enter the host name of your MIMESweeper Web Server in the **Server** field, if it is not already displayed.
- Enter your username and password and select **OK**.

The MIMESweeper for SMTP Console is displayed.



If you are using a proxy server, selecting **Advanced** adds further fields to the **Login** dialog where you enter detail of the proxy server.

Selecting **Advanced** also adds the **Port** field and the **Use HTTPS** check box to the upper part of dialog. This allows you to:

- Change the default port used if required.
 - Select **Use HTTPS** and enter the appropriate port (if you have secured your Web Server using SSL).
-

To close the MIMESweeper for SMTP console:

- From the **Console** menu, select **Exit**.
- If you have any unsaved changes to your configuration, you will be prompted to save them to the Primary Configuration Server (PCS).

The MIMESweeper for SMTP Console closes.

If you create your own console, by default the MMC saves it as a `.msc` file and creates a shortcut for the file in the **Administrative Tools** folder in the **Programs** menu in the Windows **Start** menu. Use this shortcut to open the console you have created. If you try to use the shortcut for the MIMESweeper for SMTP Console, the MIMESweeper installation program starts. For details on creating MMC consoles and on creating desktop shortcuts to open the MMC with the console loaded, see the MMC online help.

Touring the MIMESweeper Policy Editor user interface

MIMESweeper for SMTP uses the Microsoft Management Console (MMC) as the user interface.

The MIMESweeper Policy Editor snap-in provides the interface to manage licenses and to configure the way MIMESweeper for SMTP implements email policies. MIMESweeper provides two primary functions in an SMTP email network:

- SMTP mail routing and relay
- Content security

MIMESweeper for SMTP routes, relays, analyzes, and processes email messages passing through your domain according to the email policies you configure.

Figure 6-1 shows the MIMESweeper for SMTP user interface.

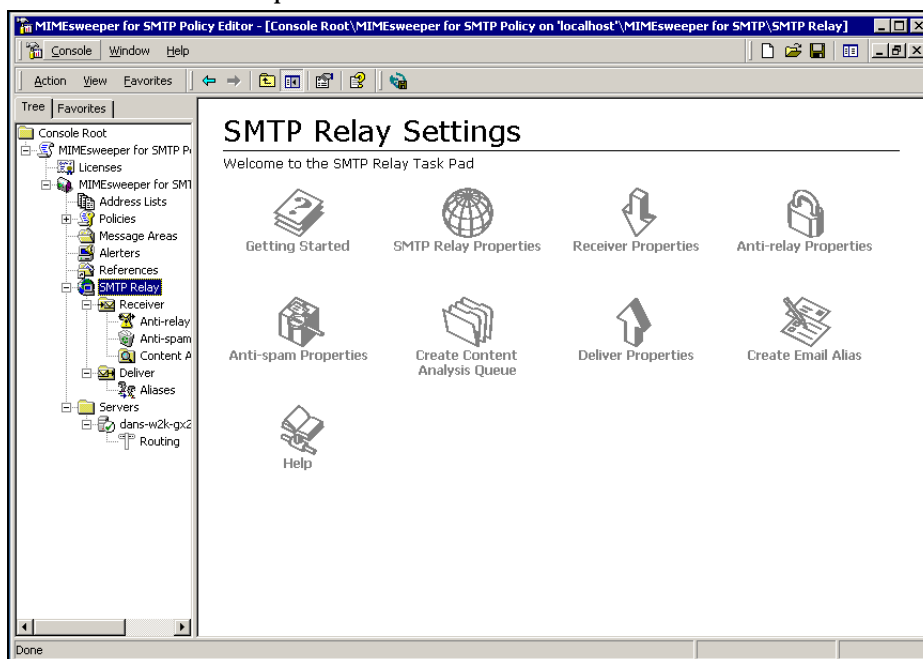


Figure 6-1: MIMESweeper for SMTP user interface

By default the MIMESweeper Policy Editor snap-in opens with the MIMESweeper for SMTP Settings displayed in the Details pane. This settings page is referred to as the Getting Started Task Pad, or the Task Pad. For more information, see *Task Pad* on page 6-14.

User interface components

Figure 6-2 identifies the components of the MIMESweeper Policy Editor user interface.

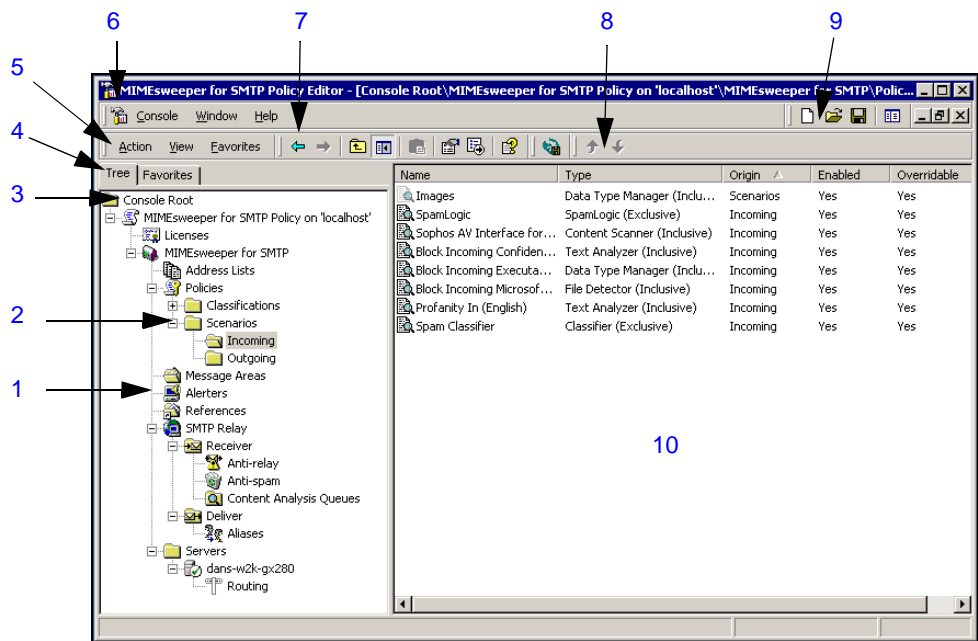


Figure 6-2: Components of the MIMESweeper Policy Editor user interface

The list below describes these user interface components.

No.	Component	Description
1	Leaf item	An item on the console tree that does not contain other console tree items. These are referred to simply as items in this guide.
2	Container	An item on the console tree containing other items. The types are: <ul style="list-style-type: none">Folder<ul style="list-style-type: none">Groups related items on a console tree.Viewable item<ul style="list-style-type: none">Displays a list, text, or graphics in the Details pane rather than additional items.
3	Console root	The container holding the MIMESweeper Policy Editor console tree.

No.	Component	Description
4	Console tree	The left-hand side of the user interface, which displays the items available in the MIMESweeper Policy Editor console.
5	MMC standard menus bar	A set of menus providing commands that act on the selected item in the console tree or on the contents of the console window, configure the appearance of the MMC window, and create and organize a list of favorites.
6	MMC main menu bar	A set of menus providing commands to control the appearance and behavior of the MMC entire console or the main window of the console and to access the MMC online help.
7	MIMESweeper Policy Editor toolbar	Buttons providing commands relevant to items in the MIMESweeper Policy Editor snap-in.
8	MIMESweeper Policy Editor scenario and classification promote/demote buttons	Buttons providing functionality to promote or demote scenarios and classifications.
9	MMC main toolbars	Buttons providing controls to create, open, and save an MMC console, to navigate through and show or hide the console tree, and to provide access to the MIMESweeper Policy Editor online help.
10	Details pane	The right-hand side of the user interface, which contains items related to the items in the console tree. The contents of the Details pane change to reflect the item selected in the console tree.

The next section describes how to access MIMESweeper commands from the MMC standard menus bar and the MIMESweeper Policy Editor toolbar.

Accessing MIMESweeper for SMTP commands

You access MIMESweeper for SMTP commands to control the behavior of items in the MIMESweeper Policy Editor snap-in from the following areas of the user interface:

- Action menu on MMC Standard menus bar
- MIMESweeper Policy Editor toolbar
- Context menu

For details on using the commands, see the MIMESweeper Policy Editor online help.

The following sections describe the containers and items displayed under the MIMESweeper Policy Editor snap-in container on the MIMESweeper Policy Editor console tree.

MIMESweeper Policy Editor snap-in



The MIMESweeper Policy Editor snap-in appears in the default MIMESweeper for SMTP Console as shown in Figure 6-3.

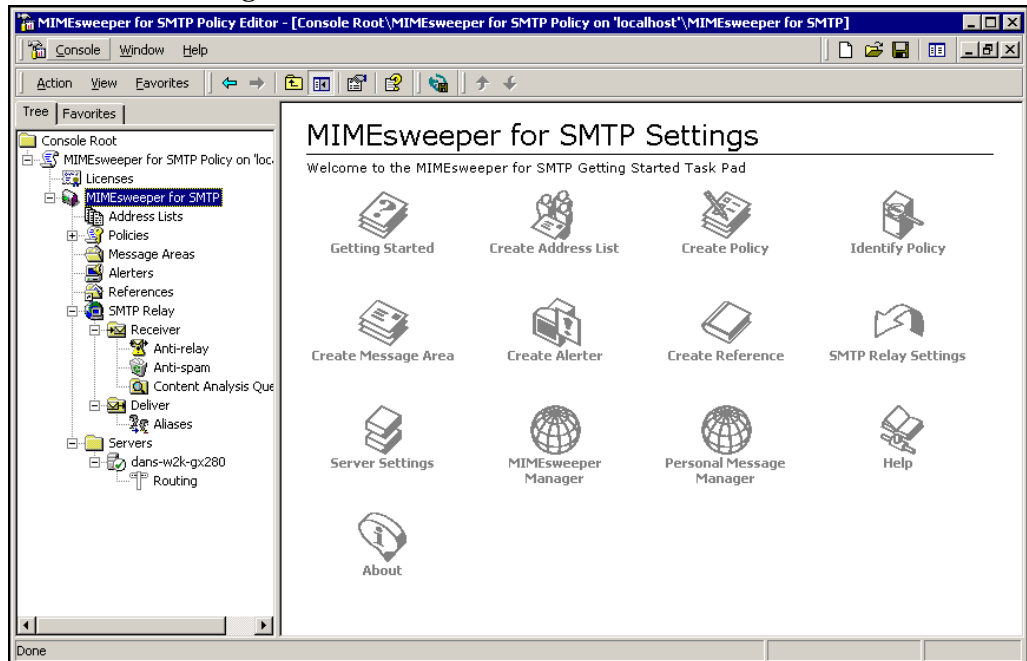


Figure 6-3: MIMESweeper Policy Editor snap-in

Save and Apply commands



The **Save the MIMESweeper Policy** button on the MIMESweeper for SMTP toolbar is enabled when an item is selected. When you are creating or editing policies in the MIMESweeper Policy Editor, you are effectively working on a draft version of the policy. The policy remains a draft version until it is applied to the Policy Servers.

Select **Save** to save your policy. The options given are:



- **Yes**
Saves the draft policy on the PCS and then applies the policy to the Policy Servers. This now becomes your active policy at the SMTP gateway.
- **No**
Saves the draft policy on the PCS. Use this command as you build up your policy.












If you do not save before closing down the MIMESweeper Policy Editor the changes to the draft policy will be lost.




MIMESweeper Policy Editor items





The following list describes the items under the MIMESweeper Policy Editor snap-in container in the console tree. Each entry notes what is displayed in the Details pane when you select an item in the console tree, and indicates where the item is documented in this guide. Items are listed in the order they appear on the user interface. To find further information on each item, select **Help** from the **Action** menu or the context menu.


Item	Used to
MIMESweeper Policy Editor snap-in 	Configure policies in MIMESweeper Policy Editor. The folders in this snap-in are displayed in the details pane.
Licenses 	Create, view, or delete MIMESweeper for SMTP product licenses. When added, licenses are displayed in the Details pane. For information about: adding licenses and configuring licenses, see Chapter 2 of the <i>MIMESweeper for SMTP Reference</i> .

Item	Used to
 <p>MIMESweeper for SMTP</p>	<p>Configure the way MIMESweeper for SMTP processes email messages and tracks this processing. This folder is referred to as the <i>MIMESweeper Policy Editor</i>. The Task Pad is displayed in the Details pane when it is selected. The Policy Editor subfolders are displayed beneath this folder in the console tree, and the Properties page can be opened from the menus.</p> <p>For information about:</p> <ul style="list-style-type: none"> • Configuring and tracking message processing in a deployment, see Chapter 9 of the <i>MIMESweeper for SMTP Reference</i>. • The Task Pad, see <i>Task Pad</i> on page 6-14.
 <p>Address lists</p>	<p>Configure address lists, which provide a single label for referring to a group of related email addresses. Any manual or LDAP address lists that have been created are displayed in the Details pane.</p> <p>For information about configuring address lists, see Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>.</p>
 <p>Policies</p>	<p>Configure email policies and how MIMESweeper implements them. Auditor items and the Policies subfolders are displayed in the Details pane, and the Properties page can be opened from the menus.</p> <p>For information about:</p> <ul style="list-style-type: none"> • Designing policies, see Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>. • Configuring auditing and email policies, see Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>.
 <p>Classifications</p>	<p>Configure classifications containing actions that define how MIMESweeper deals with messages and whom it notifies when an email message matches the scenario associated with the classification. The default classifications, and any user-configured ones, are displayed in the Details pane.</p> <p>For information about configuring classifications, see Chapter 3 of the <i>MIMESweeper for SMTP Reference</i>.</p>

Item	Used to
Scenarios 	<p>Configure scenario folders and create scenarios to implement email policies. Scenario folders specify the routes used to determine the policy to be applied to an email message. Scenarios check data in messages for specified characteristics and may also modify the data. Lower-level scenario folders or scenarios are displayed in the Details pane.</p> <p>For more information about configuring scenario folders and positioning scenarios in them, see Chapter 4 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Message Areas 	<p>Configure storage areas used to hold email messages flagged by email policies. The default message areas, and any user-configured ones, are displayed in the Details pane.</p> <p>For information about configuring message areas, see Chapter 9 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Alerters 	<p>Configure Alerters to generate notification messages to send to specified users or computers, and the email addresses it sends them to. All configured alerters are displayed in the Details pane.</p> <p>For information about configuring alerters, see Chapter 2 of the <i>MIMESweeper for SMTP Reference</i>.</p>
References 	<p>Configure common text and checksum lists to be used by scenarios that perform text analysis and content analysis. Any default or user-defined expression lists or checksum lists are displayed in the Details pane.</p> <p>For information about:</p> <ul style="list-style-type: none">• Configuring references, see Chapter 5 of the <i>MIMESweeper for SMTP Reference</i>.• Text analysis and checksum matcher and script manager scenarios, see Chapter 4 of the <i>MIMESweeper for SMTP Reference</i>.
SMTP Relay 	<p>Configure the routing and relay of email messages through the MIMESweeper Policy Editor and configure the security of SMTP relays. The domain item and SMTP Relay subfolders are displayed in the Details pane. The Properties page can be opened from the menus.</p> <p>For information about configuring mail routing and relay, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>

Item	Used to
Receiver 	<p>Configure the Receiver service parameters and relay security. These settings determine the prerequisites that connecting hosts must comply with for a successful connection to take place.</p> <p>Security measures include:</p> <ul style="list-style-type: none"> • Reverse address lookups in the DNS when a host attempts to connect to the MIMESweeper for SMTP gateway. • Server-to-server, domain-based SMTP authentication at the beginning of a connection. • User-configured lists of known safe hosts and addresses, from which mail can be accepted. <p>For information about Receiver service security, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Anti-relay 	<p>Configure relay security options to prevent other mail hosts from forwarding mail through MIMESweeper for SMTP.</p> <p>Create a list of relay target addresses to relay mail to. This is so that external SMTP servers can route messages through your network to other organizations or subsidiaries.</p> <p>Create a list of relay hosts allowed to relay email messages through MIMESweeper for SMTP, to domains other than your own. This is to protect your local domain from being used as a third-party mail relay.</p> <p>The anti-relay folder does not contain items for selection in the Details pane.</p> <p>For information about Anti-relay settings, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Anti-spam 	<p>Identify mail database lookup sites to block messages from known sources of spam. You can check if the mail host of an incoming email has been recorded in a web-based database of known spam source hosts. Define how MIMESweeper for SMTP processes messages from these hosts.</p> <p>This is different from the SpamLogic analysis, which looks for known spam sites within a message's contents.</p> <p>The Anti-spam folder does not contain items for selection in the Details pane.</p> <p>For information about Anti-spam settings, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>

Item	Used to
Content Analysis Queues 	<p>Configure Content Analysis Queues (CAQs) for the Receiver service to deposit mail into. Set up address lists to determine which queue a specific sender's mail is sent to and set a relative priority for each queue.</p> <p>This feature is typically used to enable priority mail from specified senders, to be accelerated through the Security service.</p> <p>For information on creating CAQs, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Deliver 	<p>Configure the parameters that determine how the Delivery service attempts to deliver email messages to the next host machine on the route to their intended recipients.</p> <p>The Delivery service authenticates itself to unspecified hosts, before a successful connection is made.</p> <p>If an email message is not successfully delivered to a valid host, the Delivery service attempts to resend the message. The number of attempts is determined by the user-configured Retry Schedule.</p> <p>For information on the Delivery service, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Aliases 	<p>Configure alias lists that map one email address, or group of addresses to another, in order to change an email's recipient address. Configured alias lists are displayed in the Details pane.</p> <p>For information about configuring aliases, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>
Servers 	<p>Configure properties for the mail processing servers (Policy Servers) on your system. You configure the delivery paths the Delivery service uses (the routes) for each server configured.</p> <p>Specify logging Receiver and Delivery services events.</p> <p>View and edit the paths of the various systems folders and base folder used by the Receiver and Delivery services.</p> <p>For information on server configuration, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.</p>

Item	Used to
Routing 	<p>Configure the delivery paths MIMESweeper for SMTP uses to direct incoming and outgoing email messages. Any configured SMTP relay routes are displayed in the Details pane.</p> <p>For information about:</p> <ul style="list-style-type: none">• Planning network routes, see Chapter 2.• Configuring SMTP relay routes, see Chapter 6 of the <i>MIMESweeper for SMTP Reference</i>.

Accessing properties

You can access the properties of a container, folder or item in either the console tree or the Details pane. Be aware that the properties available for a container, folder or item in the console tree, may differ from the properties available for a corresponding item in the Details pane as shown below:

Console tree properties



Content Analysis Queues folder

- General
- Notes

Details pane properties



Content Analysis Queues item

- General
- Details
- Sender Addresses
- Notes

Task Pad

The MIMesweeper for SMTP Settings page is displayed in the Details pane when you select the MIMesweeper for SMTP folder under the MIMesweeper Policy Editor snap-in. This settings page is referred to as the Getting Started Task Pad, or the Task Pad as shown in Figure 6-4.

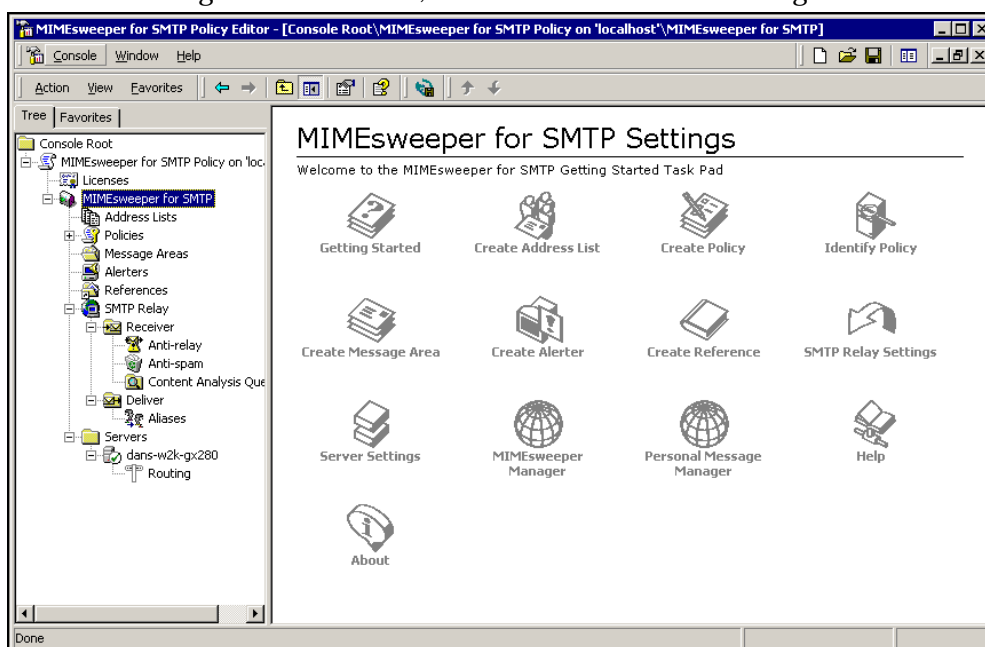


Figure 6-4: Getting Started Task Pad

The Task Pad is designed to help new or infrequent users to quickly get started using the MIMESweeper Policy Editor. The Task Pad provides a quick and easy way to access key MIMESweeper for SMTP wizards, the online help system, and system information. For details on wizards, see *MIMESweeper for SMTP wizards* on page 6-15.

Full details on the links available from the Task Pad are provided in the MIMESweeper Policy Editor online help.

MIMESweeper for SMTP wizards

You can create new folders or items under the MIMESweeper Policy Editor snap-in the console tree. MIMESweeper for SMTP wizards enable you to create entire policies, individual components, or specific items required to implement aspects of your organization's email policies. You can access wizards from the Task Pad or from the **Action** or a context menu from an item in the MIMESweeper Policy Editor.

The following types of wizards are available to help you to configure policies, depending on your level of experience; novice, intermediate or advanced.

- **Policy wizard**

The policy wizard guides a novice user through the whole process of building and configuring a policy. The policy wizard consists of three separate steps:

- Step 1: Creating the scenario
- Step 2: Assigning the scenario to the scenario folders
- Step 3: Defining the actions

Throughout this documentation, the parts of the policy wizard are described as components and items. A component is a group of related items, for example, scenarios. An item is one part of the group, for example, the Legal Disclaimer scenario. The policy wizard guides you through each of the components required to build a policy, enabling you to select and create specific item types for each component.

If you are new to MIMESweeper Policy Editor or use it infrequently, use the policy wizard several times to build up a complete policy.



The policy wizard is not the same as the Initial Policy Wizard which starts automatically the first time you open the MIMESweeper Policy Editor. The Initial Policy Wizard guides you through the initial steps of setting up authentication, domains, routing and anti-virus details, and then automatically creates classifications, scenarios and actions, according to the selected policy template; Demonstration, Basic or Typical.

- **Component wizards**

The component wizards guide novice and intermediate users through the process of creating individual components that can be used to build a policy. Each component wizard identifies the available item types, enabling you to select and create a specific item type.

If you know that you need to add a particular component to an existing policy, but you are not sure of the specific type of item you should create, use the component wizard to view the available choices and create the required item.

- **Item wizards**

The item wizards guide advanced users through the process of creating a specific item type that can be used as part of a policy.

If you know which specific item type you want to add to an existing policy, you can use an item wizard to quickly create the required item.



You can turn off item wizards in the **Welcome** page of an item wizard. You can then create all new policy items by configuring a blank properties page for the item. This option is not available for the policy wizard or component wizards.

If you want to revert to using the wizards to create new items, you can turn the wizards back on in the **Preferences** tab of the Properties page for the MIMESweeper Policy Editor snap-in.

The wizards enable you to create other item types that you may need to associate with the item you are creating. That means that you do not need to create any prerequisite item types before using a wizard.

When you finish creating an item in a wizard, the new item is displayed in the console tree or in the Details pane when you select the related folder or item in the console tree. The properties page for a new item contains tabs corresponding to each of the completed wizard pages. You can change the properties of an item by editing options in the tabs of its properties page.



Before new policies or changes to policies can be implemented, they must first be applied by saving. The **Save** button is located on the MIMESweeper Policy Editor Toolbar.

For details on using the **Save** button, see *Save and Apply commands* on page 6-8.

Always ensure you have adequate disk space before saving configuration edits. If disk space is less than minimum, edits may not save, and you may not get a warning that it has not saved. For details of disk space requirements, see the *Prerequisites* release document, or the MIMESweeper Policy Editor online help.

MIMESweeper Manager

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.

You can also use the Message Center to configure a message tracking database. You use this database to maintain records of messages that the system has processed. You can then search this database to obtain details of messages that have passed through the system, for example messages processed by a particular scenario, or messages addressed to a particular recipient.

- **Systems Center**

The Systems Center provides support for monitoring MIMESweeper servers and managing their associated services. It also monitors system performance.

- **Report Center**

The Report Center allows you to generate and view reports based on audit information collected from your MIMESweeper system.

- **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 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.

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, System, Report and Security Centers. For details on user names and passwords, and assigning access permissions to user accounts, see Chapter 7 of the *MIMESweeper for SMTP Reference*.

System Startup and Quicktour

To access MIMESweeper Manager from a web browser:

1. Enter the URL for MIMESweeper Manager.

The MIMESweeper Manager Getting Started page is displayed.

2. Select a center (Message, System, etc.) from either the MIMESweeper menu bar, or from within one of the areas on the Getting Started page. The Getting Started page is shown in Figure 6-5:

The MIMESweeper Manager Logon page is displayed.

3. Enter the username and password for a MIMESweeper user account that has permissions to access MIMESweeper Manager.
4. Click **Logon**. If the logon is successful the Home page for the center you selected is displayed.

Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map | You ... | Logoff

MIMESweeper™ for SMTP MESSAGE CENTER

Message Center Home Page Help

[Home](#) Refresh interval: 1 minute

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.

You can also view a message summary for all Edge Servers in your system by registering those servers. Edge servers can be registered in the [Systems Center](#).

This section below contains a summary of the number and size of messages currently in the system. 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

[Parking Areas](#) [Quarantine Areas](#) [Problem Messages](#) [Queues](#)

You can also monitor message activity, manage images in the pre-classified images database as well as managing and configuring various aspects of the Personal Message Manager.

Message Tracking

You can track messages to check on delivery status by searching the message tracking database using various criteria.

[Configure Tracking](#) [Track Messages](#)

Pre-Classified Image Database

The Pre-Classified Image Database contains images that have been identified and classified in order to improve the rate of detection of unsuitable images.

[Manage Pre-Classified Images](#)

Personal Message Manager

Personal Message Manager allows end users to manage emails withheld from their mailbox in accordance with current email policy.

[Configure PMM](#) [View Inactive Users](#)

Figure 6-5: MIMESweeper Manager Getting Started Page

Personal Message Manager

Personal Message Manager (PMM) allows end users to manage their own withheld messages by:

- Notifying them that some messages sent to them may contain a potential threat and are withheld.
- Providing them with a link to access their withheld messages.
- Enabling them to either release the withheld messages into their Inbox, or delete them.

Messages in the PMM enabled area have been withheld because the policy in place on the system has resulted in a classification that has directed them there. The recipient should then check them to determine whether they are legitimate mail or not.

Users can also use the PMM to track messages sent by or sent to them. For example, you can check if a message that you sent or has been sent to you has been blocked by the system.

Setting up PMM

A PMM account is automatically created by the system for a user as soon as the first message is directed to a PMM enabled message area.

Notification of withheld messages

A notification email, the digest, is sent out by the system telling the user that there are messages for them in the PMM message area. The digest contains a hyperlink to their PMM home page, where they manage their withheld messages.

Accessing a user's PMM messages

To access their PMM messages a users can click the link in the digest email that they have received
The PMM Home page provides links to the My Messages, Delegated Messages and Preferences pages.

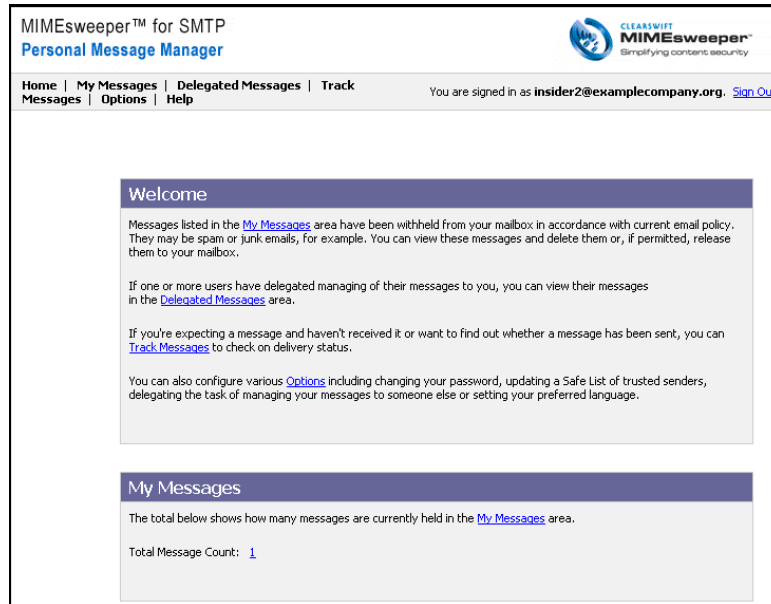


Figure 6-6: PMM home page

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 email 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 email 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 email 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.

Glossary

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

A

- accessing
 - command 6-6
 - MIMESweeper manager..... 6-17
- additional route 2-6
- additional server
 - install..... 3-22
- address
 - IP 2-4
- address list..... 1-5
 - in user interface..... 6-9
- administrator
 - super-user account 5-10
 - user account..... 5-10
- advanced user..... 6-15
- alerters
 - in user interface..... 6-10
- aliases
 - in user interface..... 6-12
- audit consolidator service..... 2-15
- audit database
 - configuring..... 3-27, 3-28
 - creating an Oracle database..... 3-26
 - purging an Oracle database..... 3-27
- audit disposer service ... 1-8, 1-9, 2-13, 2-15
- audit server 2-16
- auditing
 - policy 1-6
 - restrict Windows user access 5-5
- auditing and reporting
 - content security policy 1-4, 1-6

C

- classifications..... 1-5, 1-6
 - in user interface..... 6-9
- closing
 - MMC..... 6-3
- command
 - accessing..... 6-6
- component wizard 6-16

- configuring
 - DNS server 2-7
 - firewall..... 2-7
 - SMTP gateway 2-7
- console
 - creating 3-9, 6-3, 6-6
 - creating items 6-15
 - root..... 6-5
 - tree 6-6
- container 6-5
- content analysis 1-6
- content security policy
 - auditing and reporting 1-4, 1-6
 - email processing..... 1-4, 1-5
 - policy routing..... 1-5
- context menu 6-6
- creating
 - console..... 6-3, 6-6
 - console items..... 6-15
 - license..... 3-19, 6-8
 - policy 6-15
 - scenario 6-10

D

- database server..... 2-16
- default
 - domain name 2-5
 - route..... 2-6
- deploying MIMESweeper
 - on DMZ..... 2-8
- deployment
 - deployment options..... 2-12
 - general deployment information..... 2-3
 - general recommendations 2-13
 - machines and connections 2-14
 - port configuration 2-16
 - sample deployment models 2-17
 - system description..... 2-15
- deployment policy..... 1-7
- details pane..... 6-6
- developing
 - policy 1-7
- disabling wizard 6-16
- DMZ
 - deploying MIMESweeper..... 2-8

Index

DNS..... 2-3
 query 2-4
DNS server
 configuring 2-7
domain name
 default 2-5
Domain Name System 2-3
domains
 accept inbound mail from 5-9
 email routing 5-9

E

email processing
 classifications 1-6
 content analysis 1-6
 content security policy 1-4, 1-5
 policy identification. 1-5

F

file
 .msc 6-3
firewall
 configuring 2-7
 port configurations 2-10
 proxy-based 2-7
 securing..... 5-9
 transparent proxy-based. 2-7
folder
 MIMESweeper for SMTP 6-9
 MMC 6-5
folders
 scenarios 1-11
forced route 2-6

G

GUI 6-2

H

help -iv
host machine
 incoming mail 2-5
 outgoing mail..... 2-5
 securing..... 2-6
host name 2-3
 resolution 2-4

I

inbound email
 domains for routing 5-9
 domains to accept..... 5-9
incoming mail 2-5
 host machine 2-5
initial policy wizard..... 3-29
 basic policy 4-2
 creating a policy 4-3
 demonstration policy..... 4-2
 policy items 4-7
 typical policy 4-2
installation..... 3-1
 install an additional server 3-22
 installation checklist..... 3-11
 installing a PCS..... 3-18
 multiple machine 3-9
 post installation tasks..... 3-28
 pre-installation preparations 3-11
 single machine..... 3-9
 upgrading to MIMESweeper..... 3-32
insufficient space 3-11
intermediate user 6-15
Internet
 routing message 2-3
Internet Protocol address 2-4
IP address 2-4
IPSec security policy 5-7
 setting up 5-7
item wizard 6-16

L

leaf item 6-5
license
 agreement 3-18, 3-22
 creating..... 3-19, 6-8
 message tracking 3-37
licenses
 in user interface..... 6-8
log on
 MIMESweeper manager 6-17
logging on
 to PCS..... 5-10

M

main menu bar	6-6
main toolbar	6-6
management reporting	1-5
manual route	
additional	2-6
default	2-6
forced	2-6
menu	
action	6-6
context	6-6
MMC	6-6
message	
routing	2-3
message areas	1-10
user interface	6-10
message routing	
through MIMESweeper	2-5
message tracking	
database recommendations	2-13
deployment	2-12
license	3-37
message tracking database	2-16
configuring	3-28
message tracking service	1-9, 3-24
Microsoft IIS	5-6
Microsoft Management Console	3-9, 6-2
closing	6-3
console root	6-5, 6-6
console tree	6-6
container	6-5
folder	6-5
leaf item	6-5
main menu bar	6-6
main toolbar	6-6
opening	6-3
standard menus bar	6-6
viewable item	6-5
MIMESweeper	-iv
services	1-8
MIMESweeper for SMTP	
in user interface	6-9
toolbar	6-6

MIMESweeper manager	-iv
accessing	6-17
accessing from web	6-18
how to access	6-17
overview	6-17
MIMESweeper policy editor	-iv
MIMESweeper server	
securing	5-5
MMC	3-9, 6-2
closing	6-3
console root	6-5, 6-6
console tree	6-6
container	6-5
folder	6-5
leaf item	6-5
main menu bar	6-6
main toolbar	6-6
opening	6-3
standard menus bar	6-6
viewable item	6-5
.msc file	6-3
MX	
look-up	2-4
preference	2-4
record	2-4

N

network architecture	
basic	2-3
network services	
minimise	5-3
notification of withheld messages	6-19
novice user	6-15
NTFS file system	5-3

O

online help	-iv
opening	
MMC	6-3
operations database	3-19, 3-23
account name	3-21
password	3-21
Oracle database	
creating	3-26
performing purge	3-27

Index

outbound email
 domains for routing 5-9
outgoing mail..... 2-5
 host machine 2-5

P

packet-based firewall 2-7
PCS
 administrator account 3-18, 3-22, 3-23, 3-25
 installing 3-18
 logging on..... 5-10
 password..... 3-18, 3-22, 3-23, 3-25
 securing..... 5-2
 uninstall 3-31
personal message manager -iv, 6-19
 configuration 3-20, 3-25
 message area..... 3-20, 3-25
 setting up 6-19
policy
 creating 6-15
 deployment..... 1-7
 developing 1-7
 routing..... 1-4
 routing and relay..... 1-8
 types 1-2
 user interface 6-9
 wizard 6-15
policy editor
 user interface 1-8
policy identification 1-5
policy routing
 content security policy 1-5
policy server..... 2-15
policy wizard..... 6-15
ports, firewall configuration 2-10
primary configuration server 2-15
 install..... 3-18
 system administration 3-18
properties 6-16
proxy-based firewall..... 2-7

R

readme -iv
references
 in user interface 6-10

relay attacks
 securing against 5-10
release documents -iv
removing MIMESweeper for SMTP 3-31
reporting
 management 1-5
 policy 1-6
restrict user access
 auditing 5-5
 user rights assignments..... 5-5
reverse address look-up 2-4
roles 5-10
routing
 in user interface..... 6-13
 policy 1-4, 1-5
routing and relay
 securing 5-8
routing and relay policy 1-8
routing message 2-5
 to Internet..... 2-3

S

sample deployment models 2-17
 machine summary 2-17
 multiple host deployment..... 2-24
 single host deployment 2-20
 two host deployment 2-22
scenario 1-5
 creating..... 6-10
scenario folder 1-5
scenarios
 definition 1-11
 folders..... 1-11
scenarios folder..... 6-10
 in user interface..... 6-10
Secure Sockets Layer (SSL) 5-5
securing
 against relay attacks..... 5-10
 communications between machines . 5-6
 environment 5-2
 firewall..... 5-9
 MIMESweeper host 2-6
 MIMESweeper server..... 5-5
 PCS 5-2
 routing and relay 5-8
 Windows machines 5-3

- server authentication certificates
 - obtaining 5-5
- service
 - tracking..... 1-9
- SMTP gateway
 - configuring..... 2-7
- SMTP relay
 - user interface 6-10
- SQL server
 - advanced settings 3-19
- SSL
 - Secure Sockets Layer 5-5
 - set up on web server..... 5-6
- standard menus bar 6-6
- super-user account
 - administrator 5-10
- system startup and quick tour
 - MIMESweeper manager overview.. 6-17
 - personal message manager 6-19

T

- task pad 6-14
 - component wizard 6-16
 - item wizard 6-16
 - policy wizard..... 6-15
 - wizard..... 6-15
- TCP/IP..... 2-3
- tech note..... -iv
- TLS
 - Transport Layer Security..... 5-5
- toolbar
 - MIMESweeper for SMTP 6-6
 - MMC..... 6-6
- tracking
 - database recommendations..... 2-13
 - deployment 2-12
 - license 3-37
- tracking database 2-16
 - configuring..... 3-28

- tracking server
 - tracking service description 2-16
- tracking service 1-9, 3-24
 - description..... 2-16
- transparent proxy-based firewall 2-7
- Transport Layer Security (TLS) 5-5

U

- updating
 - MIMESweeper for SMTP 3-29
- upgrading to MIMESweeper 3-32
- user
 - advanced 6-15
 - intermediate 6-15
 - novice..... 6-15
- user accounts
 - administrator 5-10
 - roles 5-10
 - users..... 5-10
- user interface 6-2
 - address list 6-9
 - alerters 6-10
 - aliases..... 6-12
 - classifications 6-9
 - components..... 6-5
 - licenses..... 6-8
 - message areas..... 6-10
 - MIMESweeper for SMTP folder..... 6-9
 - policies..... 6-9
 - policy editor 1-8
 - references..... 6-10
 - routing..... 6-13
 - scenarios folder..... 6-10
 - SMTP relay 6-10
- user rights
 - restrict assignments..... 5-5

V

- viewable item 6-5

Index

W

web server	2-15
Windows machines	
minimise network services.....	5-3
minimise Windows software.....	5-3
NTFS file system	5-3
restrict user access.....	5-5
review Windows services.....	5-4
securing.....	5-3
Services dialog box	5-4
Windows services	
review.....	5-4
Windows software.....	5-3
withheld messages	
notification of	6-19
wizard	
component.....	6-16
disabling.....	6-16
in task pad	6-15
item.....	6-16
policy	6-15