



MIMESweeperTM for SMTP

5.3

Evaluation Guide

Revision 2

Revision 2, 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 Evaluation Guide	iii
Related documentation	iv

Introduction

Deploying MIMESweeper for SMTP

Initial deployment checklist	4
Configuring and using Clearswift Managed Downloads	4
Registering your license for Managed Downloads	5
First installation	6
Preparing an outline of your content security policy requirements	6
Obtain the Software installation kit	6
Obtain the configuration information that the installation requires	7
Installing MIMESweeper for SMTP	8
Installation process	9

The MIMESweeper user interface

MIMESweeper Policy Editor	11
MIMESweeper Manager	12
Personal Message Manager	13

Setting up a policy

Key components of a MIMESweeper for SMTP policy	15
Using the Initial Policy Wizard to define content security policy	17
Modifying your initial policy	19
Modifying your policy	19
Configuring SMTP mail routing and relay policy	20
Saving and applying your policy	22

Contents

Testing your policies

Managing your installation

Enabling message tracking	27
Configuring administrator access	29
Configuring auditing and producing reports	31
Managing spam and personal messages	33
Setting up PMM	34
Notification of withheld messages	34
Accessing a user's PMM messages	34
Policy Editor - How to disable / enable Personal Message Manager (PMM) features	35
Monitoring system health	37

Performing backups and other system tasks

Creating a backup	41
-------------------------	----

APPENDIX A Working with MIMESweeper for SMTP policies

Using the New Policy Wizard to create new policy items	39
Configuring a Managed Downloads password	42
Re-setting the password	42
Testing your Managed Downloads password	43
Creating a scenario that uses a managed reference	43
Other Managed Lists and Clearswift's Anti-spam service	45
Policy Editor – Review and modify content security policy	46

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 Evaluation Guide



This Evaluation Guide introduces the main features of MIMESweeper for SMTP and provides the information you need to plan, deploy and manage your MIMESweeper for SMTP deployment. The information in this Evaluation Guide supplements that contained in the Reference and the online help.



The Evaluation Guide is intended primarily to assist organizations in exploring the functionality of MIMESweeper for SMTP. However, it also contains information that is useful for organizations deploying MIMESweeper for SMTP for the first time.

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

- **Reference**

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

- **Getting Started Guide**

The Getting Started Guide provides information on deployment planning, preparing for an installation, and installing the MIMESweeper for SMTP software.

- **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>.

EVALUATION

Introduction

This document is designed to ensure that the fundamental components of MIMESweeper for SMTP are configured correctly in a new deployment. All features can then be evaluated effectively without the need to research and plan a full deployment.

This document consists of the following areas:

- Deploying MIMESweeper for SMTP.
- Setting up a Policy.
- Modifying your initial Policy.
- Testing your policies.
- Managing your installation.



The processes described in this document do not represent all of the configuration options available for MIMESweeper for SMTP.

See the *MIMESweeper for SMTP Reference*, and the Online Help systems for more information.

Introduction

Deploying MIMESweeper for SMTP

Typically, a MIMESweeper for SMTP deployment consists of:

- A Primary Configuration Server (PCS), that controls the installation.
- One or more Policy Servers that process messages.
- Database servers, as required, to host functionality such as auditing and message tracking.

The PCS is the central server in a MIMESweeper for SMTP deployment and hosts the configuration for the MIMESweeper system. The PCS replicates policy and configuration changes to the Policy Servers in the deployment. In addition to the Policy Servers, the PCS also controls the Web Server and the Audit Server.

The PCS also hosts the Operations database which holds a summary of all messages held and queued on Policy Servers. This enables fast searching and filtering of messages from the MIMESweeper Manager.



For smaller organizations, or for evaluation purposes, you can install and manage the entire MIMESweeper for SMTP product on a single machine. A single machine deployment is recommended for your initial installation, as it is the easiest way to install and evaluate MIMESweeper for SMTP's functionality and features.

Deploying MIMESweeper for SMTP consists of the following:

- Initial deployment.
- Configuring Clearswift managed downloads.
- First installation.

Initial deployment checklist

For any software deployment exercise, planning is the most critical phase. If errors are made in the plan, or if all business requirements are not accounted for, it can create long-term problems for administrators and users. A poorly implemented, short-term solution usually requires a complete re-deployment at a later date, when all issues are taken into account.

The following checklist contains the items to consider when planning a MIMESweeper for SMTP deployment.

- Plan the deployment:
 - Choose the deployment model.
 - Prepare server platforms:
 - Confirm server naming format.
 - Install any prerequisite software, for example anti-virus tools.
 - Verify consistent name resolution.
 - Harden and secure operating system (optional).
 - Install and use only the necessary Windows network services.
 - Establish server baseline (optional).
- Review firewall policy requirements

Configuring and using Clearswift Managed Downloads

Clearswift Managed Downloads are references that are updated regularly by Clearswift, and made available for MIMESweeper for SMTP installations to download. Managed References allow your policies to maintain defences against current threats. There are many managed downloads lists that you can use. For example:

- The SpamLogic Signatures managed download allows your MIMESweeper for SMTP installation to detect spam messages.
- The Scams: Phishnet managed expression list allows your MIMESweeper for SMTP installation to detect current phishing attack messages.
- The Spam: Known Attachments checksum list allows your MIMESweeper for SMTP installation to detect messages with known spam message attachments.



In order to use Clearswift Managed Services, you require either:

- A valid MIMESweeper for SMTP license, with a Support and Maintenance agreement in place.
 - A valid evaluation license. Managed downloads operate for the evaluation period.
-

Registering your license for Managed Downloads

All MIMESweeper for SMTP 5.3 customers receive a MIMESweeper for SMTP 5.3 license key. This license key is used for both product activation and activation of the managed services. The license key has the following format:

LICENSE KEY:	XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX
SERIAL NUMBER:	nnnn-nnnn-nnnn-nnnn

Figure 1: License Key

The registration process applies to both standard MIMESweeper for SMTP licenses, and evaluation licenses.



You can perform this process before you start the MIMESweeper for SMTP Installation Wizard, during the installation, or after installation. The MIMESweeper for SMTP Installation Wizard provides a link to access the Clearswift website during installation, so you can configure the downloads password during the installation process.

To register your license and create a managed downloads password, see the following website.:

<https://www.clearswift.com/download/produpdates/register.aspx>

To access this site, you will be asked to login using your Membership Center login. (You will already be registered if you are an existing customer, or have previously downloaded any of Clearswift's products for evaluation.)

If you are not already registered, you can create a member account by following the instructions. Once you have logged in with your membership account, you can register your license key and set a password, so that your MIMESweeper for SMTP server can authenticate to receive Managed Services.

See *Configuring a Managed Downloads password* on page 46 for details of configuring the license password after installation.

See the *MIMESweeper Manager Help* for information on how to check that managed downloads are operating correctly.

First installation

The process for performing your first MIMESweeper for SMTP installation is as follows:

- Prepare an outline of your content security policy requirements.
- Obtain the software installation kit.
- Obtain the configuration information that will be required during the installation:
 - MIMESweeper product license keys.
 - Company domain name.
 - Corporate mail servers.
 - Database server access details.
 - Corporate email disclaimer text (optional).
- Install MIMESweeper for SMTP in the following order:
 - Primary Configuration Server.
 - Additional servers (optional).

These processes are described in detail in the following sections.

Preparing an outline of your content security policy requirements

MIMESweeper for SMTP enforces the email and communication policies of your organization. You can configure a MIMESweeper policy that implements the rules of your organization.

It helps to have a general understanding, before you even begin the installation process, of the policies that you will implement. For example the message attachment file types to detect, and other message content such as words and phrases that you will be detecting. It is just as important that you have an idea of the actions that you will take with detected messages.

When you open the Policy Editor after installing MIMESweeper for SMTP, an automated policy wizard runs to help you to implement a number of typical security policies. The Initial Policy wizard provides information about the policies that it can configure.

After you run the Initial Policy Wizard, you can modify the initial policy, to ensure that it reflects the requirements of your organization. This policy wizard is discussed in more detail in *Using the Initial Policy Wizard to define content security policy* on page 15,

For further information and assistance with designing your corporate content security policies, refer to <http://www.clearswift.com/support/cs/default.aspx> or contact your local MIMESweeper partner.

Obtain the Software installation kit

The MIMESweeper for SMTP installation software is available either on a CD, or you can download it from the Clearswift website (<http://www.clearswift.com>). If you have specific media requirements for the software then please contact your usual MIMESweeper partner.

Obtain the configuration information that the installation requires

Before starting the installation, ensure that you have the following configuration information:

- **Any Operating system administration usernames and passwords**

The installation of MIMESweeper for SMTP will create and modify operating system and database components. For this reason you **MUST** ensure that you have the username and password for an account with the appropriate permissions.

- **Database server login details, if required**

The installation software includes a version of Microsoft SQL Server 2005 Express. You can install and configure the login details for this as part of the pre-requisite software configuration process. You then use these login details when configuring database access in the MIMESweeper for SMTP Installation Wizard.

If you intend to use existing database software, for example an SQL Server installation, the information that you require depends on the authentication method that the database installation uses:

- If your installation uses Windows authentication, you need to set up an Applications Server Account to use. See the *Getting Started Guide* for details.
- If your installation uses SQL Server authentication, you need the database server access details, and you configure these as you would for the default Microsoft SQL Server 2005 Express installation.

- **MIMESweeper product License keys**

Your MIMESweeper license key will have automatically been issued to you as part of the download process, or directly from your MIMESweeper partner. The MIMESweeper product will not operate without a valid license key.

- **Company Domain name and Corporate Mail servers**

Part of the initial installation and configuration process will identify to MIMESweeper your primary email domain and your corporate mail server which hosts the associated mailboxes. Only the primary domain and mail server are entered as part of the configuration wizard.

- **Corporate email disclaimer text (optional)**

If you select one of the example security policy templates, a legal disclaimer is automatically added to the end of any outbound emails. This generic template is designed to be sufficient for most organizations, but you should obtain confirmation from the appropriate area of your organization before implementing this feature.

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 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 and all other Policy Servers. The PCS also hosts the Operations database which holds a summary of all messages held and queued by the Policy Servers. This enables fast searching and filtering of messages from MIMESweeper Manager.

This section first describes the installation of prerequisite software and then describes the installation procedure for single machine deployments and multiple machine deployments.

- **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.

- Install a PCS (all components)

Install all MIMESweeper for SMTP components on a single machine.

- **Multiple machine deployment**

- Install the PCS.

- Install an Additional Server (Typical)

After installing the PCS, install components on an additional server to create a multiple machine deployment.

- Install an Additional Server (Custom)

Select a sub-set of components to install on an additional server.

- 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.

- **Upgrade your existing MAILsweeper for SMTP**

Describes the installation process when upgrading from earlier products.

Installation process

To install MIMESweeper for SMTP in any of the above configurations navigate to the `setup.exe` file contained in either the downloaded software installation kit, or on the CD. If your CD drive has autoplay enabled, the user interface launches automatically. During installation, you are prompted for the information you obtained in the previous section relevant to your selection type.

The MIMESweeper user interface

The MIMESweeper for SMTP user interface consists of three key components that you use to configure and manage the application:

MIMESweeper Policy Editor

The Policy Editor, as shown in Figure 2: is where you create and refine your MIMESweeper for SMTP policies. You use the Policy Editor to configure the policy items and the email addresses to which they apply, and so construct your email policy, as described in *Setting up a policy* on page 13.

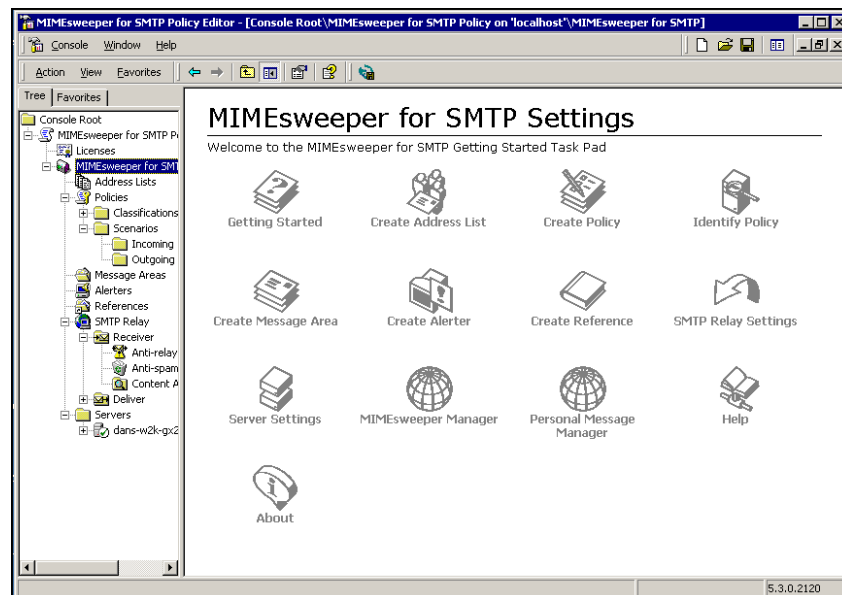


Figure 2: Policy Editor

MIMESweeper Manager

MIMESweeper Manager, as shown in Figure 3: is where you manage your installation, and the messages that your policies detect, as described in *Managing your installation* on page 23. MIMESweeper Manager consists of four management centers and a system health window. You access the MIMESweeper Manager from a Web browser.

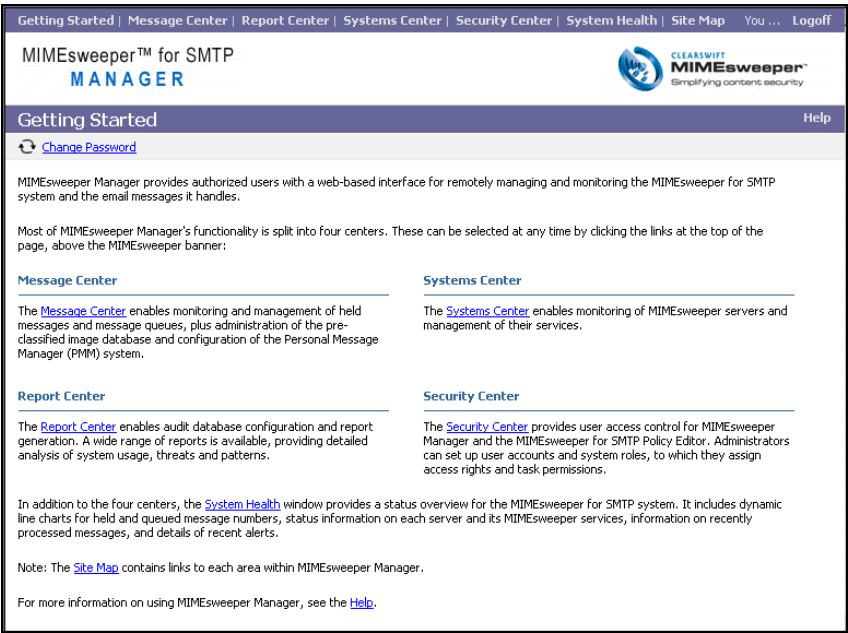


Figure 3: MIMESweeper Manager opening screen

Personal Message Manager

The Personal Message Manager (PMM) administration area, as shown in Figure 4: provides management and monitoring of PMM messages areas, as described in *Managing spam and personal messages* on page 32. PMM allows end users to manage their spam messages that have been quarantined. You access PMM Administration from MIMESweeper Manager.

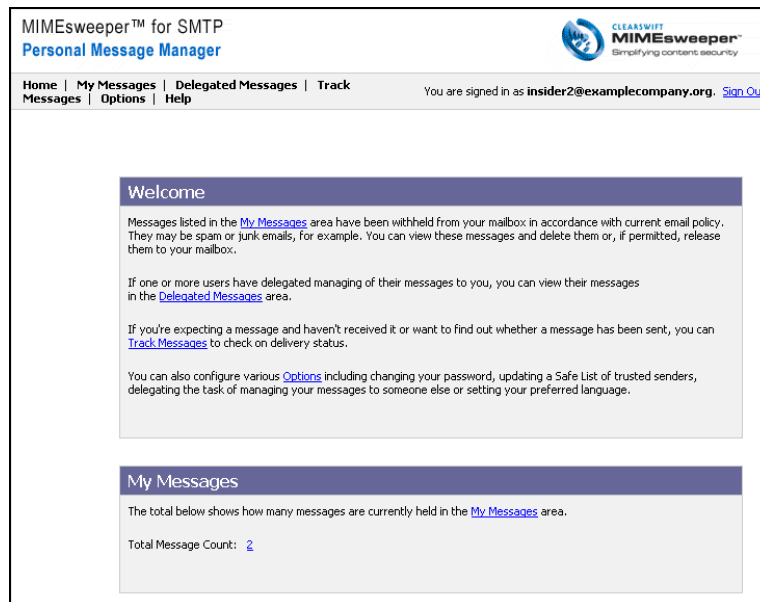


Figure 4: Personal Message Manager Home page

The MIMESweeper user interface

Setting up a policy

This section describes how to set up MIMESweeper for SMTP policies. It describes:

- The structure and key components of a policy.
- The Initial Policy wizard, that runs the first time that you open the Policy Editor.
- How to use the Create Policy wizard to quickly create policy items.

For more information on this process, refer to the *MIMESweeper for SMTP Reference*, and the *Policy Editor online help*.

Key components of a MIMESweeper for SMTP policy

You use the Policy Editor to configure a MIMESweeper for SMTP policy. A MIMESweeper for SMTP policy applies rules, or scenarios, to messages between sender and recipient address pairs that you define:

- Scenario folders define the sender and recipient addresses to which scenarios will apply. You can define address ranges using wildcards, using text-based address lists, or using LDAP address definitions.
- The scenarios detect the messages defined by your policies. For example, the **SpamLogic** scenario detects spam messages.
- Scenarios can use references, to detect messages. For example, the **Checksum Matcher** scenario can use the **Clearswift ThreatLab** managed checksum reference to detect messages that contain known threats.
- The scenario's **Classification**, and the Classification's **Actions** define what happens to detected messages. For example, the default **Dirty In** classification contains a **Quarantine Message** action that prevents detected messages from being delivered.
- Message areas hold detected messages that have been blocked. For example, the **Quarantine Message** action forwards messages to the **Dirty In** message area. Detected messages remain in the message area until they are either deleted, or released for delivery.

For example, if you select the **Block Executables** item in the Initial Policy Wizard, the Wizard:

- Creates a scenario named **Data Type Manager**.
- Creates a classification named **Executables**.
- Creates a Quarantine message area named **Executable Messages**.

By default, this scenario blocks all messages containing executable attachments, and quarantines them in the **Executable Messages** area. These messages are not delivered unless a System Administrator releases them.

Setting up a policy

You can refine your policies by creating scenario folder hierarchies. By default, lower-level folders inherit scenarios from higher folders—you can disable scenarios from higher folders, or create scenarios in lower-level folders to refine your policies.

For example, in the policy below,:

- By default, the Images scenario in the Incoming folder detects and blocks messages with image files larger than 50 KB.
- In the sales/Widget sales folder, this scenario has been disabled. Personnel in the Widget sales department can receive messages with images larger than 50 KB.

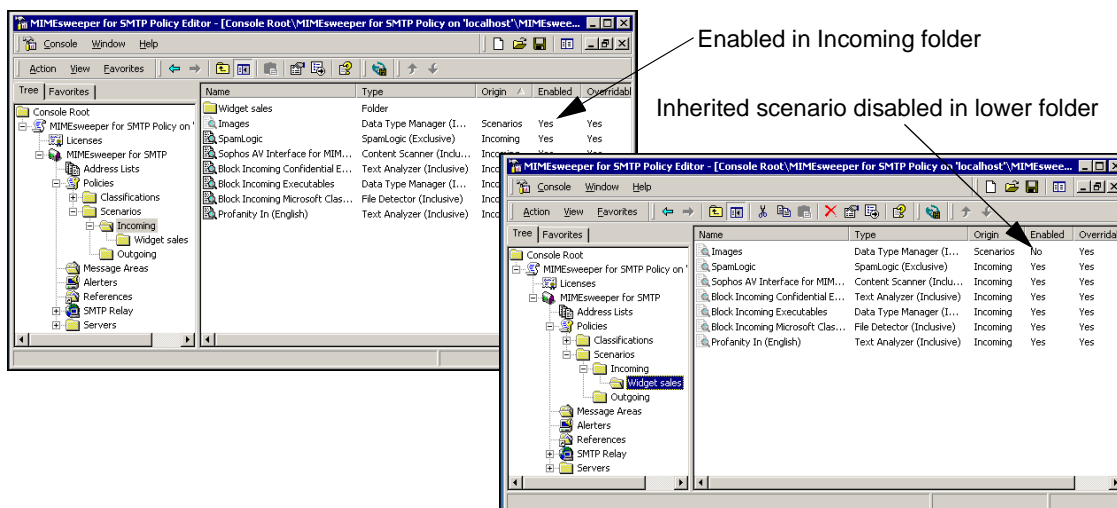


Figure 5: Scenario folders and scenarios

Using the Initial Policy Wizard to define content security policy

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



The Initial Policy Wizard runs once only. After that, you must use the Policy Editor to create and modify your policies.

The Initial Policy 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 asks you if your installation uses a MIMESweeper Edge Server. An Edge Server can be configured to act as an email firewall for your installation, to prevent spam messages and messages with threats such as viruses from entering your system. See the *MIMESweeper for SMTP Reference* for more information. If you use an Edge Server, the Initial Policy Wizard includes some additional scenarios that you can choose.

The Initial Policy Wizard offers you the choice of three policy types. Within each policy type, you can select or de-select items as required. The three policy types are:

- The **Basic** option configures basic protection such as blocking spam and messages with viruses. It also adds a disclaimer to outgoing messages.
- The **Demonstration** option is designed to demonstrate product functionality.
- The **Typical** option contains the scenarios that a typical organization would use.

To run the wizard after you have installed the software:

1. Ensure that you are logged on as a user with write access to the Windows registry, for example, as a local Administrator.
2. Either double-click the MIMESweeper Policy Editor icon on the desktop, or click **Start**, point to **Programs**, click **MIMESweeper for SMTP**, then click **MIMESweeper Policy Editor**.

The Initial Policy Wizard is displayed when the Policy Editor is opened for the first time. Follow the instructions on each wizard page, and click **Next** to move to the next page.

3. When prompted, select the policy template (**Basic**, **Demonstration** or **Typical**) to be used when creating your template, and click **Next**.

Depending on your selection, the Initial Policy Wizard lists the default policies in the template, and provides a brief description of each.

Setting up a policy

4. On the Policy Customization page, select or de-select items as required. The items that you select become a part of your policy. Click **Next**.

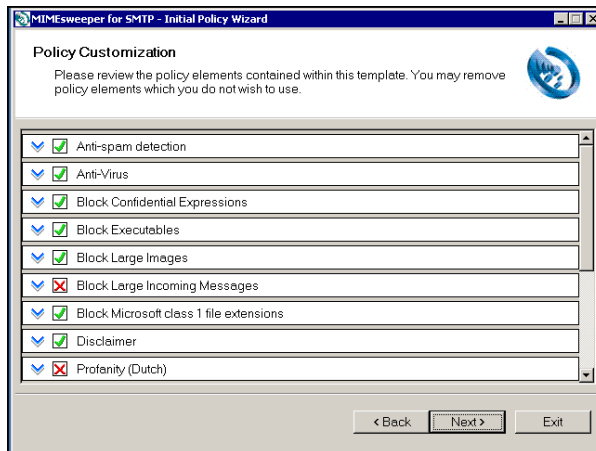


Figure 6: New Policy customization screen

5. On the Domain Configuration screen, enter your company name and the domain name, and click **Next**.
6. On the Mail Routing Configuration screen, enter the mail server names and ports for incoming and outgoing mail. The Initial Policy Wizard sets up the routes on which it forwards incoming and outgoing messages that it has processed. Click **Next**.
7. On the Anti-Virus Configuration Screen, select the anti-virus software that you use. The Initial Policy Wizard creates a scenario that uses the software that you select.
8. If you selected the **Disclaimer** item on the Policy Customization screen, on the Disclaimer Message screen, edit the text to add the disclaimer that will be added to all outgoing messages. Click **Next**, then click **Finish**. The Initial Policy Wizard creates your initial policy, and closes.

When the Wizard is finished the MIMESweeper Policy Editor opens allowing you to refine your policy as you become more familiar with the product's features. See the *MIMESweeper for SMTP Getting Started Guide* for details of the policies created by the Initial Policy Wizard.

Modifying your initial policy

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.

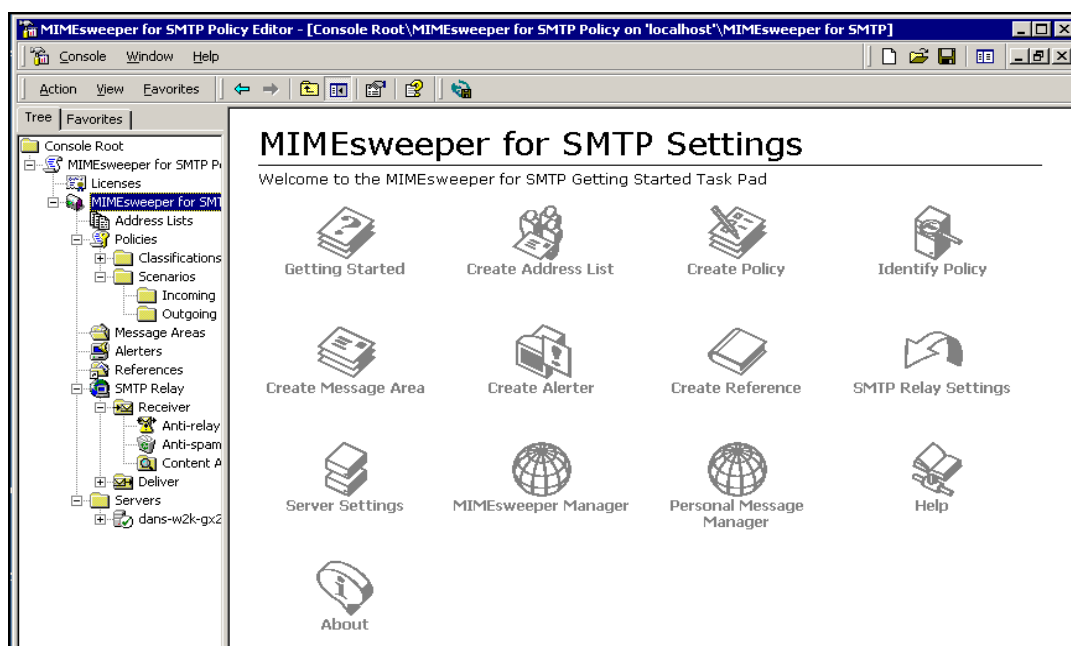


Figure 7: Task Pad

The Task Pad is designed to help you 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. 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, from the **Action**, or a context menu from an item in the MIMESweeper Policy Editor. For more information on the Policy Editor's components, see *Using the New Policy Wizard to create new policy items* on page 43.

Modifying your policy

You can use the Create Policy Wizard to easily create new policy items. The wizard takes you through the process of creating the policy components that you require. For information about using the Create Policy wizard, see *Using the New Policy Wizard to create new policy items* on page 43.

Configuring SMTP mail routing and relay policy

You also use the Policy Editor to configure mail routing and relay policies.

MIMESweeper for SMTP routes and relays the processed email messages passing through your domain according to the routing and relay policies you configure. Whenever you add an additional email domain to the SMTP routing and relay properties, you should:

1. Add the domain and responsible mail server to the Routing options under each enabled server.

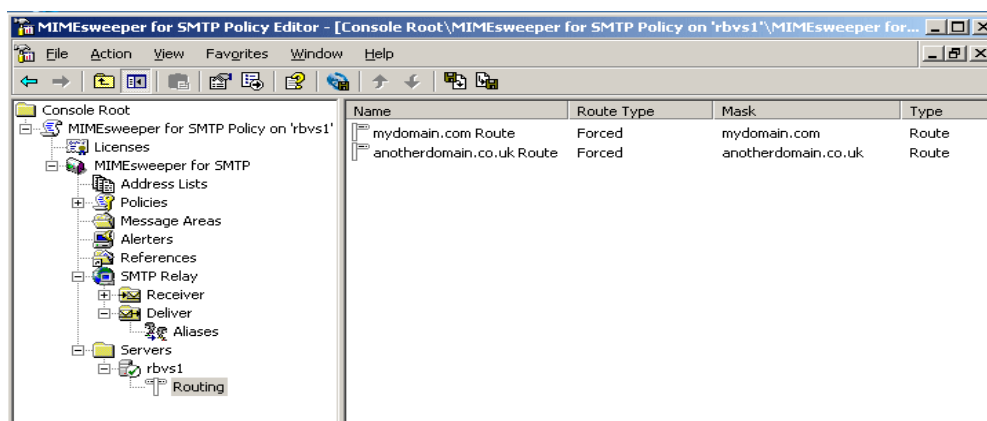


Figure 8: Routing Options

More information on the available types of SMTP routes can be found in the *MIMESweeper for SMTP Reference*.

2. Ensure the email domain is listed under the Relay Targets and the responsible mail server is listed under the Relay Hosts section. These configuration options are accessible from the SMTP Relay / Receiver / Anti-Relay Policy Editor options. Alternatively, you can access them from the Getting started taskpad under SMTP relay settings, and then from the Anti-relay Properties option.

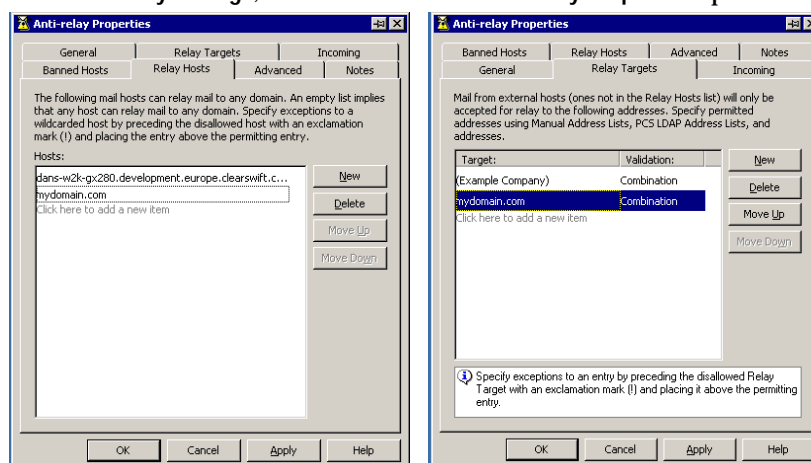


Figure 9: Anti-relay Properties

3. The new domain should be added to at least one of the existing address lists. Typically, you can add it to the default address list for your organization which is automatically created at the time of installation.

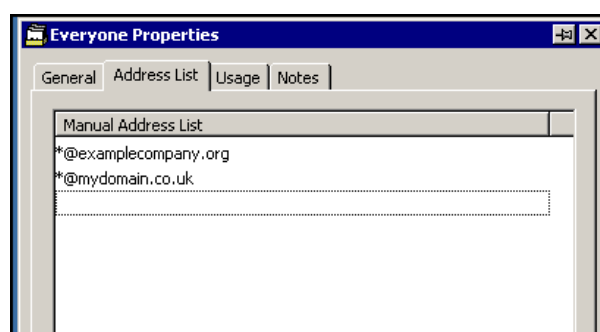


Figure 10: Address List Tab



In order to apply policy to messages to or from the email domain, the domain must be listed on at least one of the configured address lists. Refer to *Appendix H: Testing*, of the *MIMEsweeper for SMTP Reference* for testing and evaluation of the configured policy and address lists.

After modifying the SMTP relay properties, you must save and apply the policy changes.

Saving and applying your policy



The Policy Save button is located on the MIMESweeper for SMTP toolbar, as shown in the following figure. Take care not to confuse the MIMESweeper for SMTP Save button with the Management Console Save button. The Management Console Save button saves the console settings only, and does not save and apply your policy.

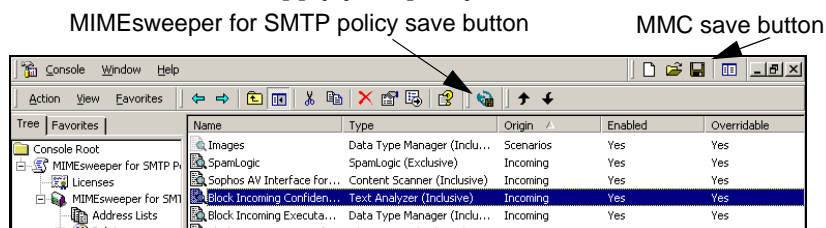


Figure 11: Policy Editor Save button

When 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. Click the **Save** button to save your policy. When you save your policy:

- Click **Yes** to save the policy on the PCS and then apply the policy to the Policy Servers. This now becomes your active policy at the SMTP gateway.
- Click **No** to save the draft policy on the PCS only. The policy is not applied to the policy servers until the next automatic replication time, usually half-hourly. Use this command as you build up your policy.



If you do not save before closing down the MIMESweeper Policy Editor, your changes will be lost.

Testing your policies

MIMESweeper provides a number of email accounts that you can use when testing policies and mail routing for the MIMESweeper for SMTP system. These are known as echo accounts.

You can send a message from your organization to any of the echo accounts, and an automatic message reply is sent from the MIMESweeper server to the sending address.

Each Echo account sends back a text message. This test can simulate an incoming message containing a data type that needs to be blocked by your organization. The available Echo accounts are shown in Table 1:

Table 1: : Echo account references

Send an email to this account	To receive
echo@clearswift.com	A plain text message detailing the other echo accounts available.
doc.echo@clearswift.com	A UUE encoded Microsoft Word document.
exe.echo@clearswift.com	A UUE encoded small exe file.
image.echo@clearswift.com	A UUE encoded image file.
virus.echo@clearswift.com	A UUE encoded EICAR virus false positive.
encrypt.echo@clearswift.com	A UUE encoded password protected zip file.
vbs.echo@clearswift.com	Trigger text for VBS script checking.
threat.echo@clearswift.com	The trigger text only of the Sircam virus.
spam.echo@clearswift.com	A test spam message.

To use the echo accounts to test your system:

- Send a message to an echo account from your email address.
For example, echo account echo@clearswift.com returns an email that:
 - Tests that messages can be sent to a remote system and that an automated Response is generated.
 - Offers a list of threats to test against.

Depending on your configured policy, it can be useful to use a combination of the above accounts as part of your daily validation processes.



All message attachments are sent from the MIMESweeper server using the UUE format.

Testing your policies

Managing your installation

MIMESweeper Manager is used to configure, control, and monitor your system as it processes messages. The Installation Wizard creates a desktop icon to start MIMESweeper Manager.

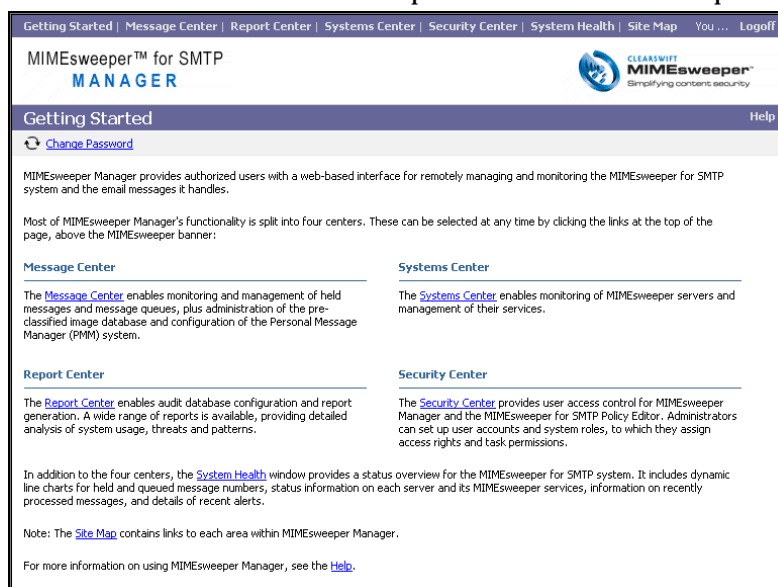


Figure 12: MIMESweeper Manager

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 processing and quarantining messages and how messages are tracked and managed by the content security policy.
- **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.

MIMESweeper Manager authenticates the user name and password before providing access to the application containing the Message, System, Report and Security Centers.



You must supply the name and password of a MIMESweeper user account with assigned permissions to access the areas of MIMESweeper Manager.

Enabling message tracking

To use message tracking in the Message Center area of the MIMESweeper Manager, enable the message tracking features of MIMESweeper for SMTP. Tracking is disabled by default:

1. Logon to the MIMESweeper Manager interface, with the administrator username and the password you specified as part of the software installation. Click on the **Message Center** option from the main screen.
2. Click the **Configure Tracking** button. A wizard starts to guide you through the process of setting up the tracking database. Follow the on-screen wizards to create a new database with a name of your choice.

The screenshot shows the MIMESweeper Manager interface. On the left, under 'Message Tracking', the 'Configure Tracking' button is highlighted with a red circle. The main area displays two tables: 'Held Messages' and 'Queued Messages'.

Held Messages	Count	Size
Parked messages	0	0 bytes
Quarantined messages	3	9 KB
Problem messages	0	0 bytes

Queued Messages	Count	Size
Waiting for analysis (Analysis)	0	0 bytes
Approved for delivery (Checked)	0	0 bytes
Ready for dispatch (Delivery)	0	0 bytes

Below the tables are buttons for 'Parking Areas', 'Quarantine Areas', 'Problem Messages', and 'Queues'.

The 'Configure Message Tracking Wizard' is open, showing 'Step 1: Enable Tracking'. It asks to 'Define whether to create a new database or connect to an existing one.' with two radio buttons: 'Create new database' (selected) and 'Use existing database'. Navigation buttons 'Cancel', '< Back', and 'Next >' are at the top right.

Figure 13: Configure Tracking.



As with the audit database, for the purposes of evaluations, and for small installations, you can select the same SQL Server 2005 Express installation that was installed on the PCS for storing the operations database. For larger deployments, you should consider using a dedicated database server. You can use the **Configure Tracking** button to modify the message tracking properties at any time.



Ensure that the specified database server you specify is available and online and that the account you configure has permissions to create the appropriate database structure.

- After entering the database name of your choice, on the next two pages, configure the retention period and the rollover period. The retention period is the length of time that the system retains tracking data, and the rollover period is the frequency at which information is consolidated from the various information sources into the Report Center database.

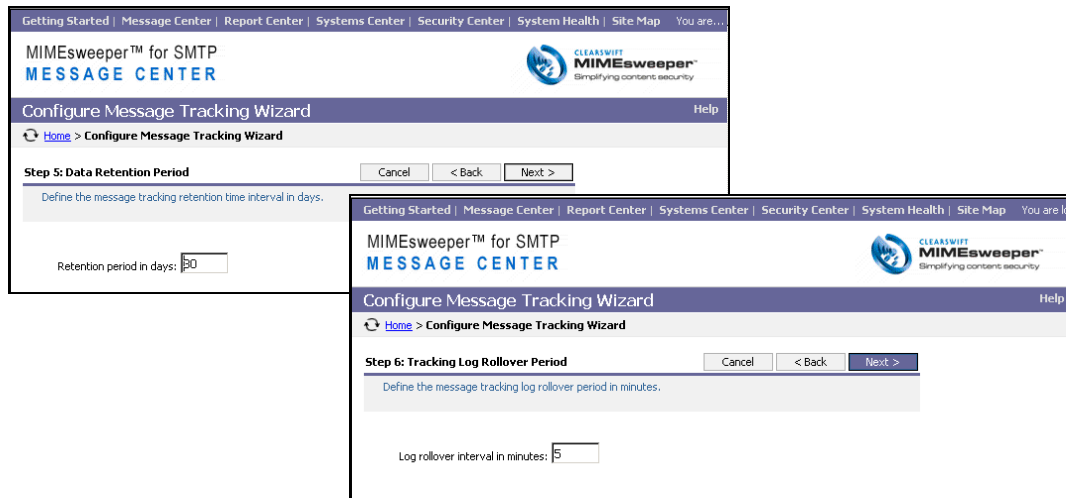


Figure 14: Retention and Rollover periods

The retention period is set to 30 days by default. If you need to track older messages, increase the number of days. The database will grow to a larger size the longer you retain records. If you use a large data retention period, regularly check the database server to check that it does not run out of free disk space.

The rollover period is set to 30 minutes by default. If you require the information reflected more frequently, reduce this number. The more frequent the rollover period, the more frequently system resources will be utilized by this process.

- Complete the Wizard to create the tracking database and enable tracking.

With tracking configured, all message tracking data can be accessed from the Message Center and reported on through the Report Center option. There are no tracking records in the database until the system has processed some messages, and the tracking data has been rolled over to the database.

Configuring administrator access

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 a user starts the MIMESweeper Policy Editor, he or she is prompted to enter a user name and password, and 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 logon 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 the sections of MIMESweeper Manager and the 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. A user's permissions can also control which domains within the organization he or she can manage

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.

Managing your installation

MIMESweeper for SMTP automatically creates a super-user account, called Administrator, which always has full access permissions to all areas of MIMESweeper for SMTP. Initially, your evaluation is likely to be performed using this administrator account, but the following questions must now be considered;

Question Which users will be required to administer some area of the MIMESweeper for SMTP?

Action Manually create a user account in the Security Center for each nominated user.

Question How can the users administration rights be grouped into roles?

Action Assign the newly created user accounts to the designated roles.

Question What features of MIMESweeper for SMTP should each role have access to?

Action For the newly created roles assign the appropriate permissions for the message areas, message operations and other areas of the system.

A number of sample roles have already been defined in the default MIMESweeper for SMTP installation which should be suitable for involving other users to assist in the evaluation process.

Table 2: Default roles

Role	Permissions
Domain Mail Administrator	Manage messages only to or from a specific domain in your organization
Help Desk Operator	Able to view mail and manage queues. Also has basic access to other parts of the system.
MIMESweeper Administrator	Access-all-areas. Allowed to perform all tasks associated with both the MIMESweeper Manager and the Policy Editor.
Network Administrator	Allowed to configure the network elements of the system. Can manage queues, configure auditing and restart services.
Network Operator	Very basic access to the system. Allowed to access and manage the queue areas.
Policy Administrator	Full access to the Policy Editor. Able to view all areas within the Policy Editor, make amendments and save and apply changes.
Security Manager	Full access to the Security Center. Able to define users and roles and assign access rights.

Specific details about the permissions available for these roles is available in the *Reference* document. Alternatively, you can review them directly through the Security Center in the MIMESweeper Manager interface.



Where possible, try to avoid assigning permissions to specific user accounts unless required by specific circumstances. It will be easier to change permissions later if they are applied to roles representing multiple individual accounts.



You only need to create accounts for those users who will perform some MIMESweeper for SMTP administration role. PMM user accounts, to enable users to manage their spam messages, are automatically created by the system.

Configuring auditing and producing reports

In order to generate any of the management information in the Report Center area of the MIMesweeper Manager, you must first enable the auditing features of MIMesweeper for SMTP. These are disabled by default:

1. Logon to the MIMesweeper Manager interface, with the administrator username and the password you specified as part of the software installation. Click on the **Report Center** option from the main screen.
2. Click on the **Configure Auditing** option and follow the on-screen wizards to create a new database with a name of your choice.

The screenshot displays the MIMesweeper for SMTP Report Center interface. The top navigation bar includes links: Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health | Site Map | Logoff. The main header shows 'MIMesweeper™ for SMTP REPORT CENTER' and the Clearswift logo. Below the header, the 'Report Center Home Page' is visible with links: Home, Configure Auditing, and Purge Options. The 'Configure Auditing Wizard' is the active window, showing 'Step 2: Database Connection'. The wizard includes a description: 'Define the database server type, name and administrator login details. The SQL Server instance name and port number can also be optionally entered.' The form fields are: Server type (SQL Server), Server name (Pick server: ALID, Specify server:), Instance name (Optional), Port number (Optional), Administrator, and Password.

Figure 15: Configure Auditing Wizard



For the purposes of evaluations, and for small installations, you can use the Microsoft SQL Server 2005 Express software that you installed on the PCS for storing the operations database. For larger deployments you should consider using a dedicated database server. You can modify these auditing properties using the **Configure auditing Wizard** option at any time.



Ensure that the database server you specify is available and online and that the account you specify has permissions to create the appropriate database structure. See the *Getting Started Guide* for a discussion of database authentication options.

3. After entering the database name of your choice, select the reporting elements to be recorded. For the purposes of evaluation, it is recommended that you enable all the available options.

Getting Started | Message Center | Report Center | Systems Center | Security Center | System Health

MIMESweeper™ for SMTP
REPORT CENTER

Configure Auditing Wizard

Home > Configure Auditing Wizard

Step 4: Audit Settings Cancel < Back Next >

Define the auditing settings.

☒ Classifications

☒ Threats

☒ Formats

Figure 16: Audit Settings Page

4. Enter the log rollover period. The rollover period is the frequency at which information is consolidated from the various information sources into the Report Center database. This is set to 1 hour (60 minutes) by default. If you require the information more frequently, reduce this number. The more frequent the rollover period, the more frequently system resources will be utilized by this process.

The screenshot shows the 'Configure Auditing Wizard' interface for MIMESweeper™ for SMTP Report Center. At the top, a navigation bar includes links for 'Getting Started', 'Message Center', 'Report Center', 'Systems Center', 'Security Center', and 'System Health'. Below this, the title 'MIMESweeper™ for SMTP REPORT CENTER' is displayed. The main heading is 'Configure Auditing Wizard', with a breadcrumb trail 'Home > Configure Auditing Wizard'. The current step is 'Step 5: Audit Log Rollover', which includes 'Cancel', '< Back', and 'Next >' buttons. The instruction reads: 'Define the audit data log roll over time interval in minutes.' At the bottom, a text field shows '50' minutes, with the label 'Roll over the audit data log after' and 'minutes.'

Figure 17: Audit Log Rollover

Now we have configured auditing, all future message transactions can be reported on through the Report Center option. It is unlikely that there will be any auditing information in the database now – although we will refer back to the Report Center over the next few days.

Managing spam and personal messages

Personal Message Manager (PMM) allows end users to manage their own withheld messages. For example, for spam messages, PMM:

- Notifies users when messages sent to them are probably spam, and have been withheld.
- Provides users with a link to access and check their withheld messages.
- Enables users to either release the withheld messages into their Inbox, or delete them.

You can configure any message area to be managed by PMM. Messages in any PMM-enabled area have been withheld because the policy in place on the system has resulted in a classification that has directed them there. It is up to the recipient to check them to determine whether they are legitimate mail.

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, 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.

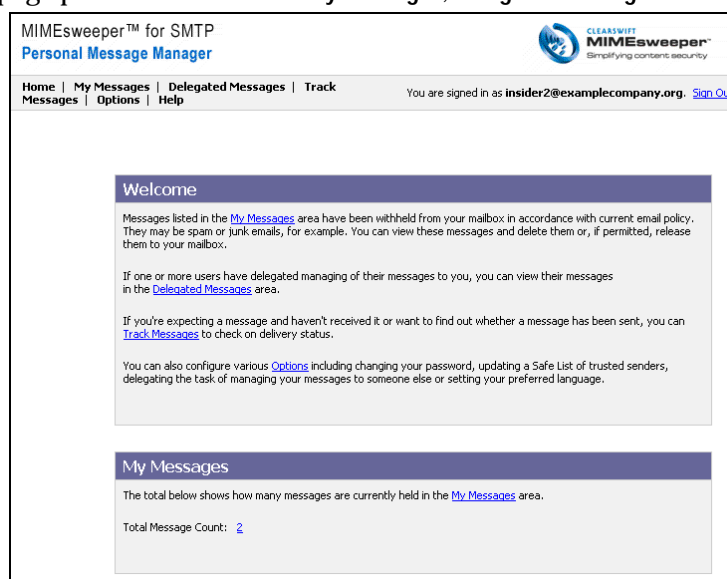


Figure 18: Personal Message Manager

How to disable / enable Personal Message Manager (PMM) features

With MIMESweeper for SMTP the PMM features are installed and enabled by default.



By default, only the Personal Messages area is selected for management by PMM.

This means that, on a daily basis, all users who have at least one retained message will receive a summary email notification. This notification includes the details of messages in any quarantine areas which are configured to be managed using the PMM. Until you are confident with the management of your MIMESweeper deployment, you may want to temporarily disable this feature.

Message areas can be configured for PMM management through the MIMESweeper Policy Editor, under the properties settings for each message area.

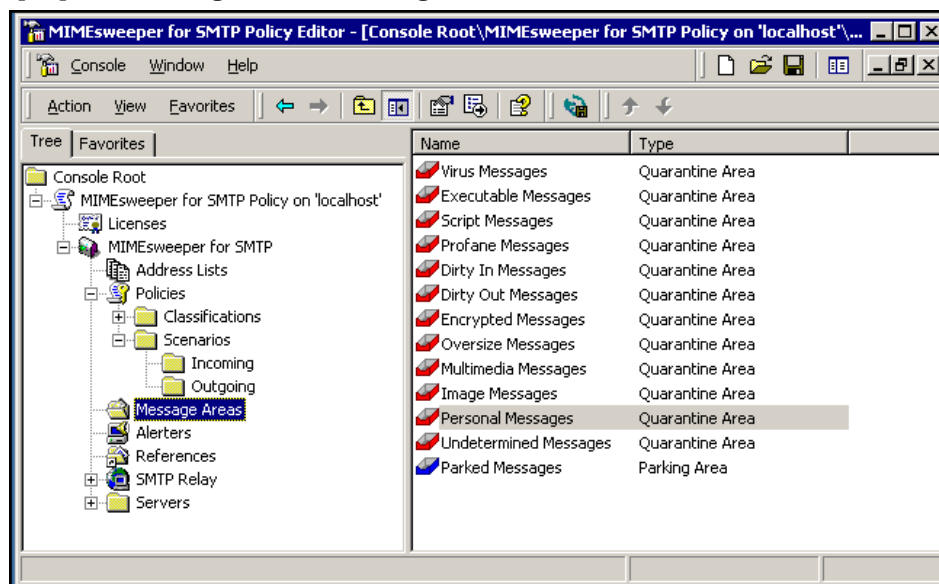


Figure 19: Personal Messages Area

Only message areas that are selected for management by PMM are included in the daily summary emails to users.

To disable or enable a message area for PMM management:

1. In the Policy Editor, in the left hand pane, select Message Areas, and in the right hand pane, select and right-click the message area to configure.
2. From the pull-down menu, select Properties to display the Message area's Properties dialog box.

3. Under the Management tab, select or de-select the **Allow area to be managed by PMM** option, and click **OK** to apply the change.

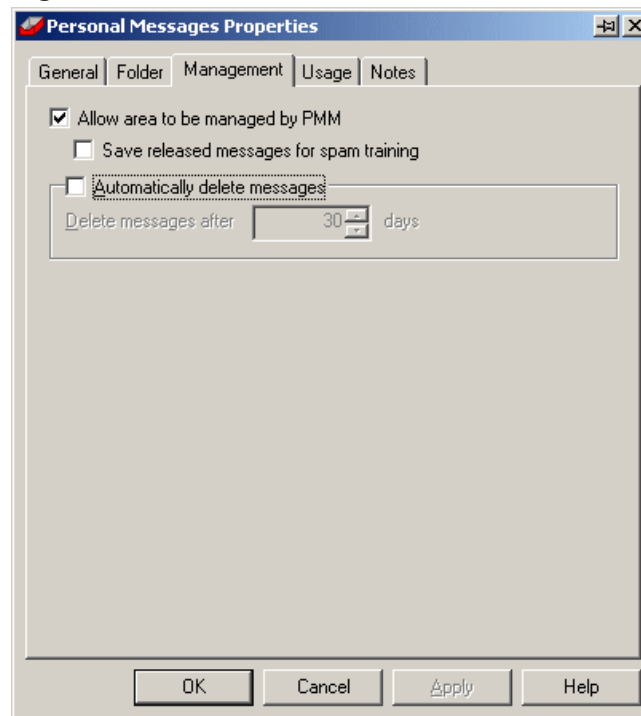


Figure 20: Personal Messages Properties

4. Save and apply your new policy.

Monitoring 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. It is an important tool to provide a status display of the current MIMESweeper for SMTP installation and all of its critical components.

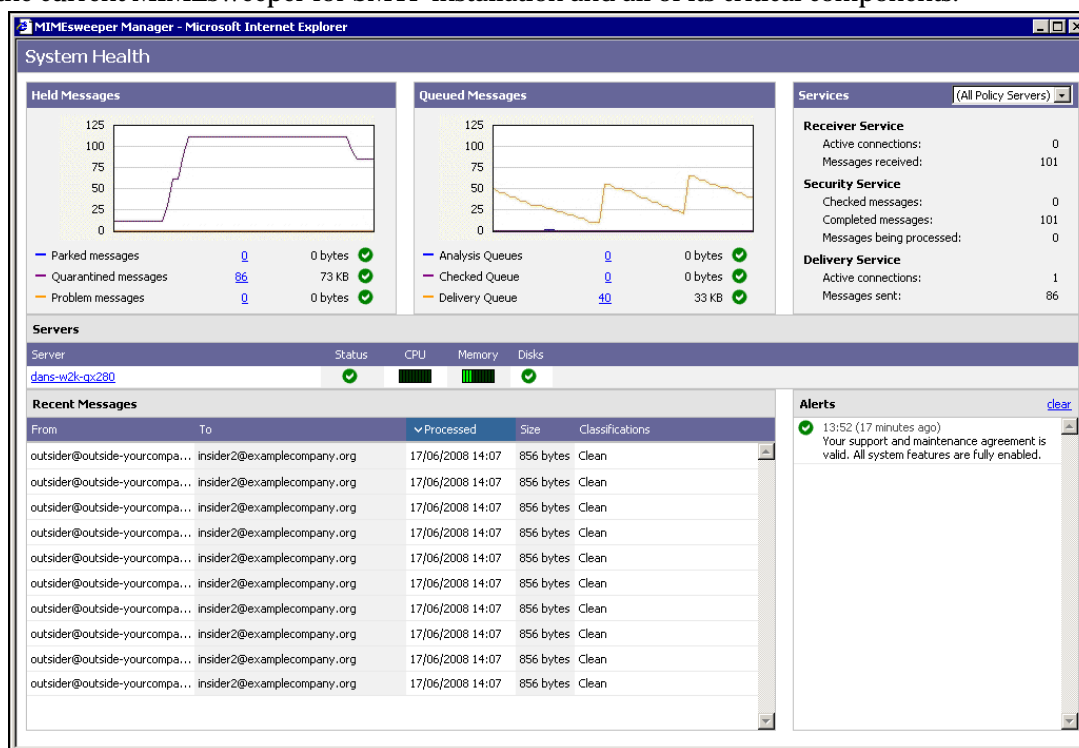


Figure 21: System Health

Access to the System Health window is provided from the site navigation bar of the MIMESweeper Manager and the following level of data is provided:

- **Held messages**

Held messages are messages that MIMESweeper for SMTP has parked or quarantined, or placed in the problem messages area.

A graphical display plots a trace for each type of held message. The trace indicates the current volume of held messages.

Below the plot area the actual number of messages and the disk space occupied by them is displayed. The message numbers provide links to the relevant areas of the Message Center.

- **Queued messages**

Queued Messages are those that are awaiting either analysis or delivery by the system. Queued messages are grouped in analysis queues, checked queues or delivery queues.

A graphical display plots a trace for each type of queued message. The trace indicates the current volume of queued messages.

Below the plot area, the actual number of messages and the disk space occupied by them is displayed. The message numbers provide links to the relevant areas of the Message Center.

Icons indicate: System healthy

Alert - The Alert pane displays short messages indicating the nature of the alert.

- **Services**

This pane displays the status of the Receiver, Security and Delivery services. The data shown applies to the server selected in the drop-down list. The drop-down list provides an option to select all servers:

- Receiver service

Active Connections - The number of currently active connections in the service. Indicates current service activity.

Total Messages Received - The number of messages which have been received by the service since it was last restarted.

- Security service

Processing Messages Count - The number of messages being processed by MIMESweeper for SMTP.

Checked Messages Count - The number of messages that the service has checked.

Completed Messages Count - The number of messages that have been processed by MIMESweeper for SMTP.

- Delivery service

Active Connections - Outgoing SMTP connections that are currently open.

Total Messages Sent - The number of messages that have been sent by the service since it was last started.

- **Servers**

This pane displays the status of all the active servers in the MIMESweeper for SMTP deployment.

Services for a specific server are managed on the **Services** page, which is accessed by selecting the server name.

The icon in the **Status** column indicates the status of a server's associated services.

Managing your installation

A server's performance is indicated by graphic displays, which show the percentage of CPU or memory usage. To display a percentage value on a Tooltip hover the mouse over a graphic display.

The server's free disk space values are also displayed.

- **Recent messages**

This pane shows summary information for messages recently processed by all the mail servers in your deployment. Messages are sorted by process date and time with the most recent message at the top of the list.

- **Alerts**

The Alert pane displays system alert messages that are associated with alert icons displayed in other system health panes.

To clear the Alerts panel, select the **Clear Alerts** command.

Performing backups and other system tasks

System maintenance tasks are performed by the System Maintenance wizard which is accessed from the **Start** menu. System maintenance tasks may only be performed by system administrators and for all tasks you need the administrator username and password.



In order to perform certain advanced functions (including performing a system restore) you may also require the username and password to access your SQL Server or Microsoft SQL Server 2005 Express operations database.

In the event of a system failure there are a number of recovery procedures that can be used to ensure that your system is available as soon as possible (for example, the promotion of a regular Policy Server to become a permanent replacement for the PCS). These are discussed in more detail in the *Reference* documentation.

The complete loss of all infrastructure components and servers will of course require an offline backup to recover the MIMESweeper for SMTP systems. The System Maintenance wizard provides varying levels of system backups to allow the recovery of system configuration data through to including the data held on the policy servers. As an introduction to best practice, you should regularly take backups of the system configuration throughout the first few days, but ultimately the frequency and level of system backups will be dependent upon your organization's recovery requirements.



It is recommended that you perform a system backup at content security policy level (1) every time you change your policy configuration.

Creating a backup

A level (2) system backup includes the following system components:

- Your content security policy (scenarios, classifications, domains and routing information).
- The configuration of your deployed MIMESweeper for SMTP server components.
- The configuration of your Personal Message Manager (PMM) system. (e.g. mail server to use, the period to send out digest messages, the templates for digest messages and password reminders).



Although the system automatically performs a two-hourly emergency backup on the PCS at this level, a regular offline backup will facilitate disaster recovery situations where the currently running systems are not available.

Performing backups and other system tasks

To create a backup:

1. Launch the System Maintenance wizard from the Windows Start / Programs / MIMESweeper for SMTP menu, enter the Administrator login details, and click **Next**.
2. Select **System Backup** from the available options, and click **Next**.

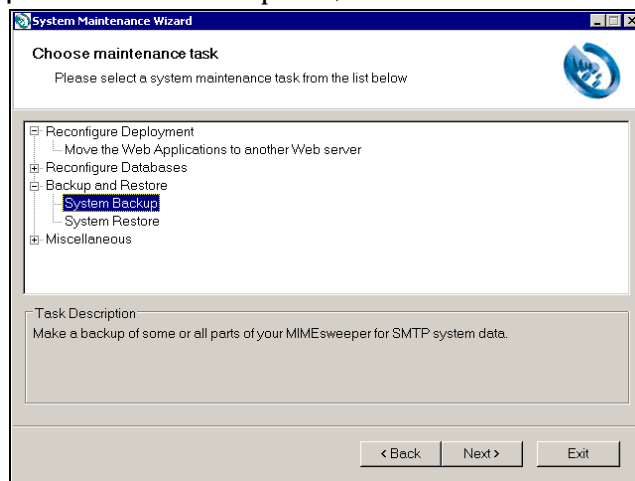


Figure 22: System Maintenance Wizard - Chose Task

3. Click **Next** on the opening System Backup screen. Select the second level of backup and use the **Browse** button to specify the appropriate location for the backup file.

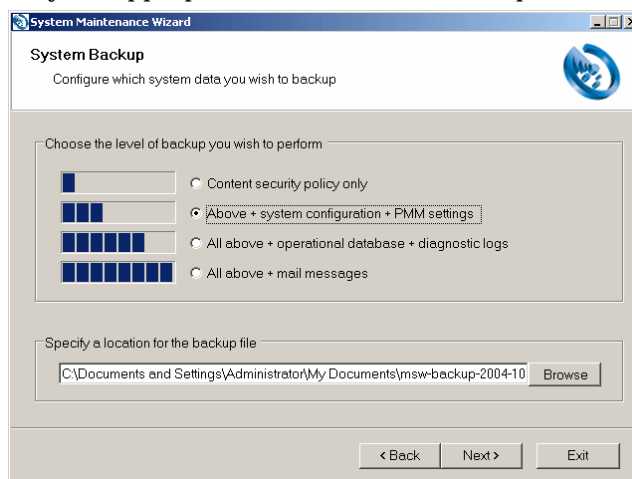


Figure 23: System Maintenance Wizard - System Backup

4. Enter the database server login details and click **Next**.

5. Once the backup has been completed, move the backup file to an offline location so that the backup remains accessible in the event of a complete system failure.

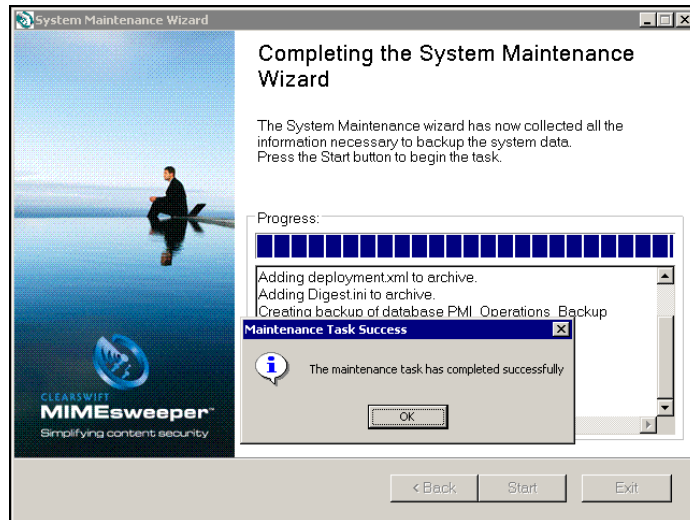


Figure 24: System Maintenance Wizard - Completion

Performing backups and other system tasks

APPENDIX

Working with MIMESweeper for SMTP policies

This appendix provides additional information on creating and modifying your policies.

Using the New Policy Wizard to create new policy items

MIMESweeper for SMTP uses the Microsoft Management Console (MMC) to host the Policy Editor user interface. The MIMESweeper Policy Editor snap-in provides the interface to manage licenses and to configure your MIMESweeper for SMTP email policy implementation.

MIMESweeper provides two primary functions in an SMTP email network:

- SMTP mail routing and relay
- Content security.

Creation of additional policy items

The easiest way to create additional policy items is to use the Create Policy Wizard from the Getting Started Taskpad. Double-click the Create Policy icon to start the wizard.

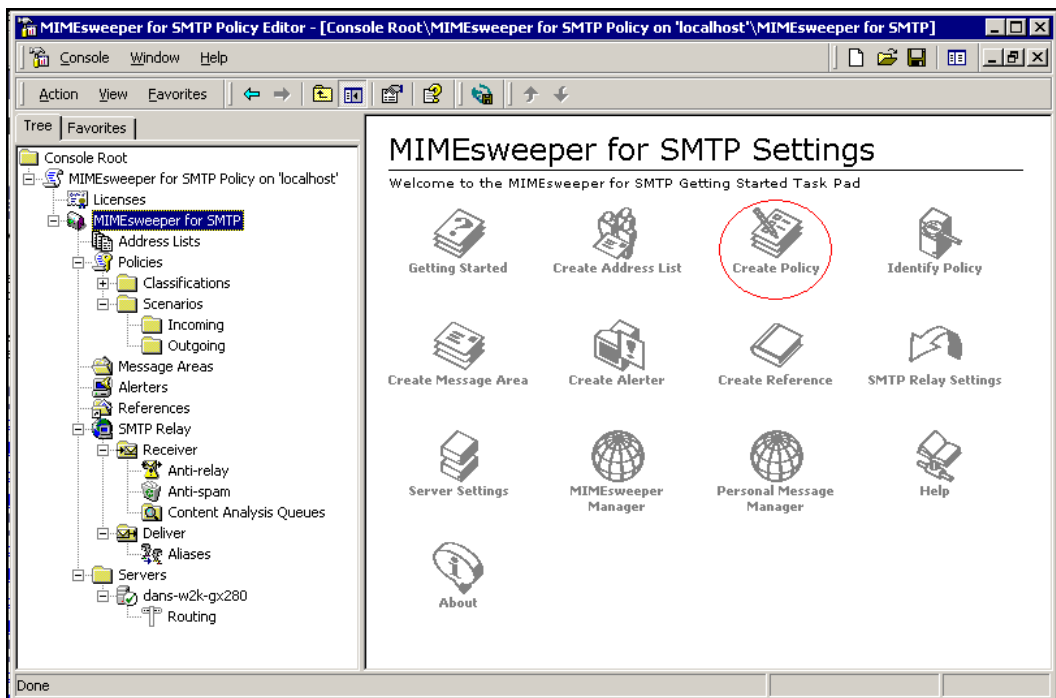


Figure 25: Create Policy

The Policy Wizard takes you through the tasks required to create a policy item. The Policy Wizard provides information on the policy creation process, and lets you know where you are up to in the process. It provides context-sensitive links to the online help, so that you can find more information if required.

You can use the Policy Wizard to create all of the policy component, for example the scenario, classifications and actions that you require,

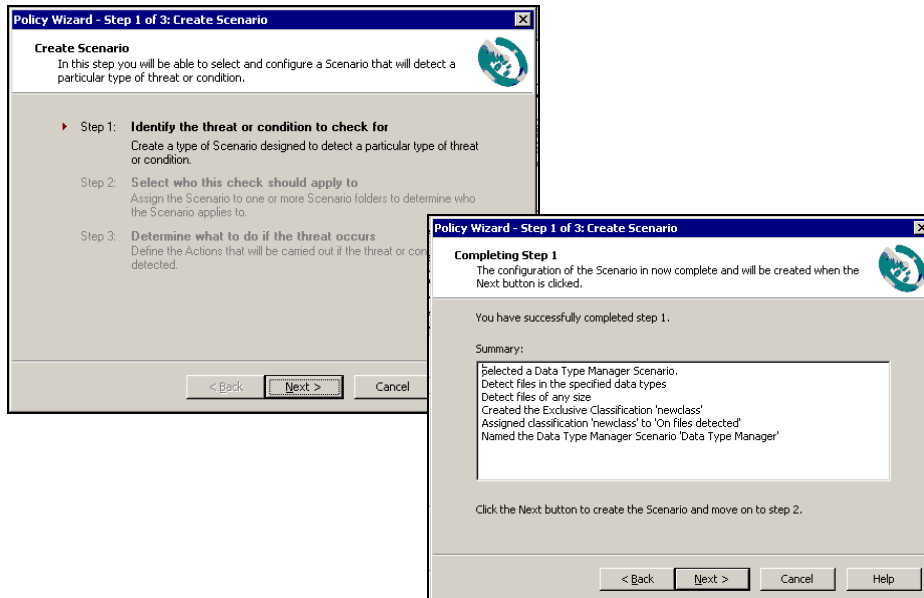


Figure 26: Policy Wizard steps

The Policy Wizard creates policies in three stages, or steps:

- In Step 1, you select the scenario to use, configure the types of messages that the scenario detects, and define how the message is classified. You can use existing classifications, or create a new one to use.
- In Step 2, you define the message direction (incoming or outgoing), and the senders and recipients that the scenario is to apply to. For example, you could apply the scenario to all messages incoming to your organization, or to messages incoming to specific sections within your organization only.
- In Step 3, you define what happens to detected messages.
 - If you selected an existing classification in Step 1, you can add additional actions to the classification.



Any changes you make affect all scenarios that use the classification, and not just the ones for your new scenario.

- If you created a new classification in Step 1, you can configure the actions for the classification.

You can also configure notifications and alerts in this step, for example sending a reply to the message sender advising that their message contained a virus.

Configuring a Managed Downloads password

You can configure a new, or change an existing Managed Downloads password after you have installed the MIMESweeper for SMTP software. For information on obtaining a Managed Downloads password, see *Configuring and using Clearswift Managed Downloads* on page 1-4.

When you have obtained a password, you can then store the password with your license key. This enables Managed Downloads functionality, and your managed references are updated automatically from the Clearswift website.

To configure your Managed Downloads password, double click the MIMESweeper for SMTP license item in the policy editor to open the License Properties dialog box, enter the password, click on **Apply**, and then save the policy to apply this change.

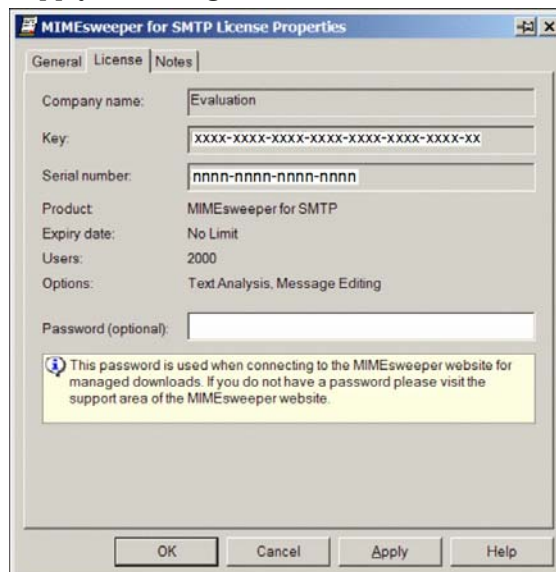


Figure 27: Licence Properties page

Your MIMESweeper for SMTP server is now ready to authenticate with Clearswift's website to receive our Managed Services.

Re-setting the password

If you need to re-set your Managed Services password at any time, you can repeat the process above for the website registration and then set the password for your MIMESweeper for SMTP server.

Testing your Managed Downloads password

You can test that your Managed Downloads password is registered and recognized by the Clearswift website.

1. In MIMESweeper Manager, access the System Center, and under the System Center Home Page heading, select **Licensing**. The licensing page displays the license details that are registered for your installation.
2. At the bottom of the page, click the **Validate** button. A message appears: **The license has been successfully validated.**

Creating a scenario that uses a managed reference

The following procedure describes how to create a **Text Analyzer** scenario that uses a **Managed Expression List**. For example, you could use the procedure to create a scenario that detects messages with attachments that contain internet banking phishing attack expressions.

1. In the Policy Editor, select the folder in which you want to create the scenario. For example, to create the scenario in the top-level **Scenarios** folder, right-click **Scenarios**, and from the list, select **New, Text Analyzer**, to start the Text Analyzer wizard.
2. On the Welcome screen, click **Next**, and on the Initial Scenario State screen, accept the defaults and click **Next**.
3. On the Data Types screen, select the data attachment types that your scenario is to process. For example, you can select **Documents** to check all documents, or you can expand the **Documents** section and select specific document types only. The scenario processes only the message attachments of the type that you select. Click **Next**.
4. On the Size screen, set any size restrictions to apply to scanned items. You can set size limitations for individual attachments, or for the total size of all attachments. Click **Next**, to display the Expression List screen.

The Expression List screen displays the static expressions that are available. These are lists of items that remain unchanged.

5. On the expression list screen, use the New pull-down list to select Managed Expression List.

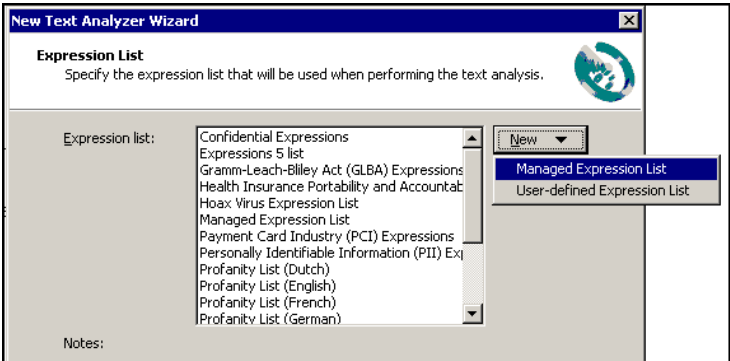


Figure 28: New Text Analyzer Wizard

The Managed Expression List.wizard starts.

6. Click Next to display the available managed expression lists. Items shown in gray are already associated with a reference, and cannot be used.

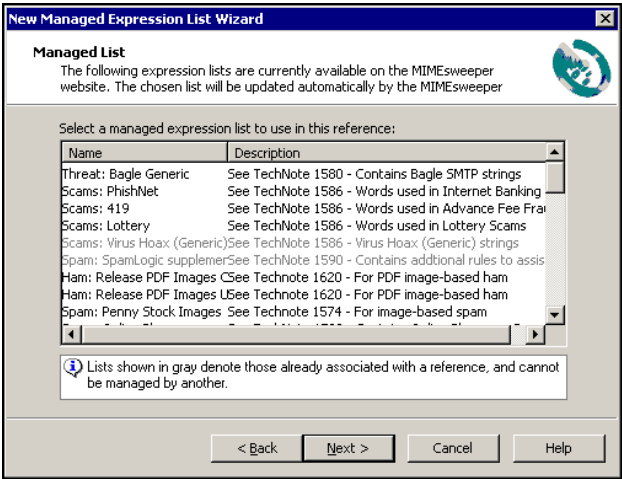


Figure 29: Available Managed Expression Lists

7. From the list, select the expression list that you want, and click Next. The expressions in the list are displayed. Click Next, and then enter a name for the list. Click Next, then click Finish to close the Managed List wizard and return to the Text Analyzer scenario wizard. The managed expression list that you created now appears in the list of available expressions.
8. In the list, select the managed expression list that you created, and click Next.
9. On the Thresholds screen, configure the Search threshold and the Proximity threshold, and click Next.

10. In the Scan Areas screen, select the parts of the message and attachments to scan for the expressions, and click **Next**.
11. Select a classification to assign to detected messages, and click **Next**.
12. Assign a name for the scenario, click **Next**, then click **Finish** to complete the process.

The wizard you have just run creates both a Scenario and a Reference. The update interval is set within the Reference properties. You must save and apply your policy in order that the managed reference can be updated automatically.

To adjust the update interval:

1. In the Policy Editor's **References** area, double-click the Reference and select the **Management** tab.
2. In the **Update Interval** field, either enter a value or use the arrow keys to set the update interval. Each time the update interval passes, your MIMESweeper for SMTP server checks for a new definition file. No download takes place if your current file is the latest available.
3. Click the **Update Now** button. Logging information appears, to verify that the download process is working correctly. If the update process fails, a message appears, and you can access information that tells you why the process failed.

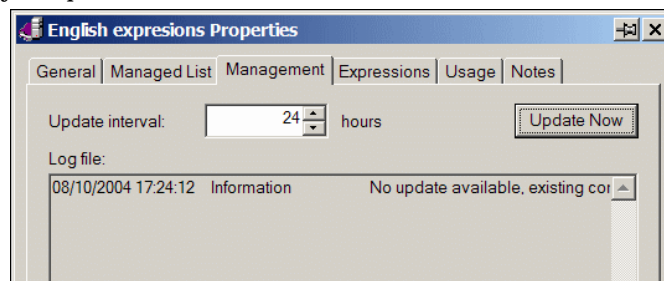


Figure 30: English Expressions Properties

Other Managed Lists and Clearswift's Anti-spam service

Other services available include:

- Checksum Matcher
- Script Manager
- SpamLogic

These services are setup in a similar way to the Managed Expression Lists above.

Note the following points:

- **Checksum Matcher:** This is primarily intended as a fast-response mechanism to detect threat signatures that Clearswift publishes in response to new threats as they are seen in the wild, for example virus signatures before they are available from Anti-virus software. For this reason, you should set the update interval to a low value, for example, to 1 hour.

- **Script Manager:** These Managed Lists require changes relatively infrequently, so a higher update value is appropriate, for example as much as 720 hours.

Policy Editor – Review and modify content security policy

After a policy has been implemented, you can modify the settings as part of a regular review process.

These modifications are likely to be either;

- **Modification of selection criteria**

Under the properties of the configured scenarios, it is possible to define exactly what the policy is detecting. In this case we can modify the Data Type manager scenario to select specific types of executables. To amend any existing policy item simply double-click, and navigate to the appropriate configuration tab.

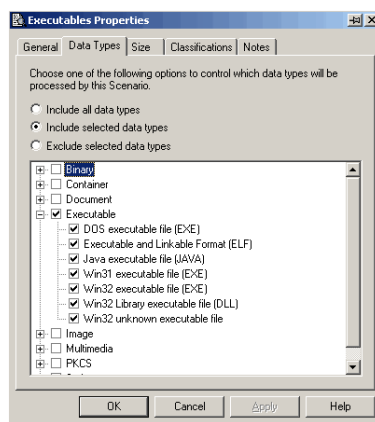


Figure 31: Executable Properties