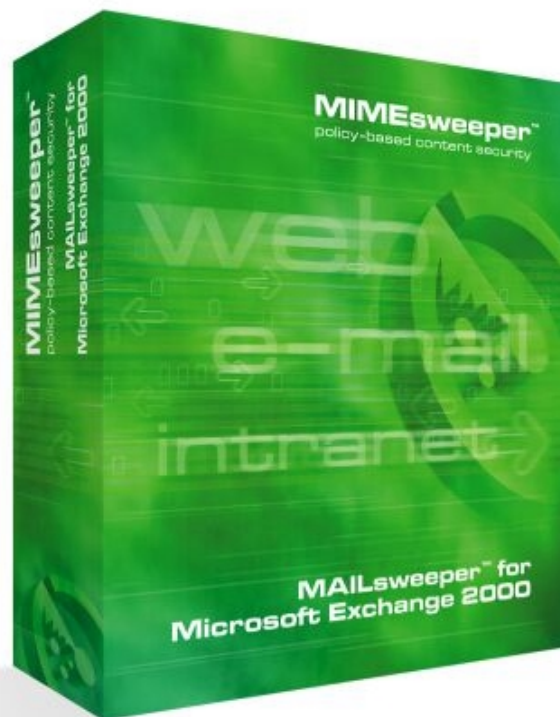

MAILsweeper for Exchange 2000

Reviewer's Guide

January 2002



MIMESweeper™
policy-based content security

For more information, contact:

Chris Witeck
Senior Product Marketing Manager
MIMESweeper Group
Chris.Witeck@baltimore.com

Contents

Introduction	3
Product Background.....	3
The MIMESweeper Product Family	3
Configuring MAILsweeper for Exchange 2000	4
Potential Security Threats to an Exchange 2000 Mail System	5
Network Integrity Issues	6
Business Integrity Issues	6
The MAILsweeper Approach to E-Mail Content Security.....	7
Policy-Based Content Security	7
How It Works.....	7
An Unmatched Feature Set for E-Mail Content Security.....	8
Detection of System-Threatening Content.....	8
Enforcement of E-mail Usage Policies	8
Reporting and Monitoring	9
Optimizing Bandwidth.....	9
New Features	10
Installation and Product Walk-Through.....	10
Installing MAILsweeper for Exchange 2000.....	11
Installing the Intercept Module	11
Configuring the MAILsweeper Security Service	14
Creating and Modifying Policies.....	15
Scenarios and Classifications	16
Corporate Crime: Scanning for Red-Flag Terminology.....	16
Legal Liability: Using MAILsweeper to Deter Workplace Profanity.....	21
Workplace Productivity: Blocking AVI Attachments	23
Network Degradation: Parking Large E-Mail Messages	23
Forcing a New Policy to Load Immediately.....	25
Testing the New E-Mail Policies	25
Downloading and Applying Sample Policies.....	26
Support / Customer Help	27
Appendixes	27

Introduction

IT managers today are diligent to secure their enterprises from Internet threats — primarily viruses and other potentially damaging code — but the idea of content security has expanded substantially in recent years. More than ever, businesses are concerned about the exposure to liabilities such as lawsuits and confidentiality breaches resulting from malicious, inappropriate or unintentional use of e-mail and the Web.

Even so, a security loophole remains. Although the Internet gateway may be well protected and monitored, the internal use of enterprise e-mail systems is largely unregulated, and has the potential of costing organizations a bundle. Threats range from the relatively benign, such as the erosion of employee productivity, to damaging, such as the introduction of virus-laden files through local disk drives, to malicious, including the transmission of confidential or inappropriate content via e-mail. Some of these threats can compromise system infrastructure, while others can result in legal liability for the business, loss of reputation or leaks of intellectual property.

MAILsweeper for Exchange 2000 protects organizations from these threats through a highly flexible content-security policy for monitoring Exchange e-mail traffic. MAILsweeper's policy-based structure gives IT managers complete control to build a customized set of e-mail usage policies that can be applied globally or to specific groups.

This latest edition of MAILsweeper for Exchange is a new product — not an upgrade — which builds upon the powerful MIMESweeper V4 engine. This change, resulting from Exchange 2000's use of SMTP as its transport mechanism, makes possible a more robust feature set in MAILsweeper for Exchange 2000.

This reviewer's guide lays out some of the key features and benefits of MAILsweeper for Exchange 2000, and gives you a starting point for testing the service yourself. The MIMESweeper Group is committed to maintaining its leadership in the content-security category, and you'll see how with this product, along with the entire MIMESweeper product family, we're giving organizations the most comprehensive content-security service on the market today.

Product Background

The MIMESweeper Product Family

MAILsweeper for Exchange 2000 is a member of Baltimore Technologies' MIMESweeper family, which has been expanding to address the full range of content security challenges faced by companies today. Based on the same policy-based content-screening approaches, the MIMESweeper family has since become a leading solution for content security, providing organizations with defenses against business and network integrity threats — whether transmitted over internal e-mail systems, Internet mail or the Web. Today, over 10,000 customers and 10 million users are protected by MIMESweeper products. Other solutions in the MIMESweeper family include MAILsweeper for Domino, MAILsweeper for SMTP, and WEBSweeper.

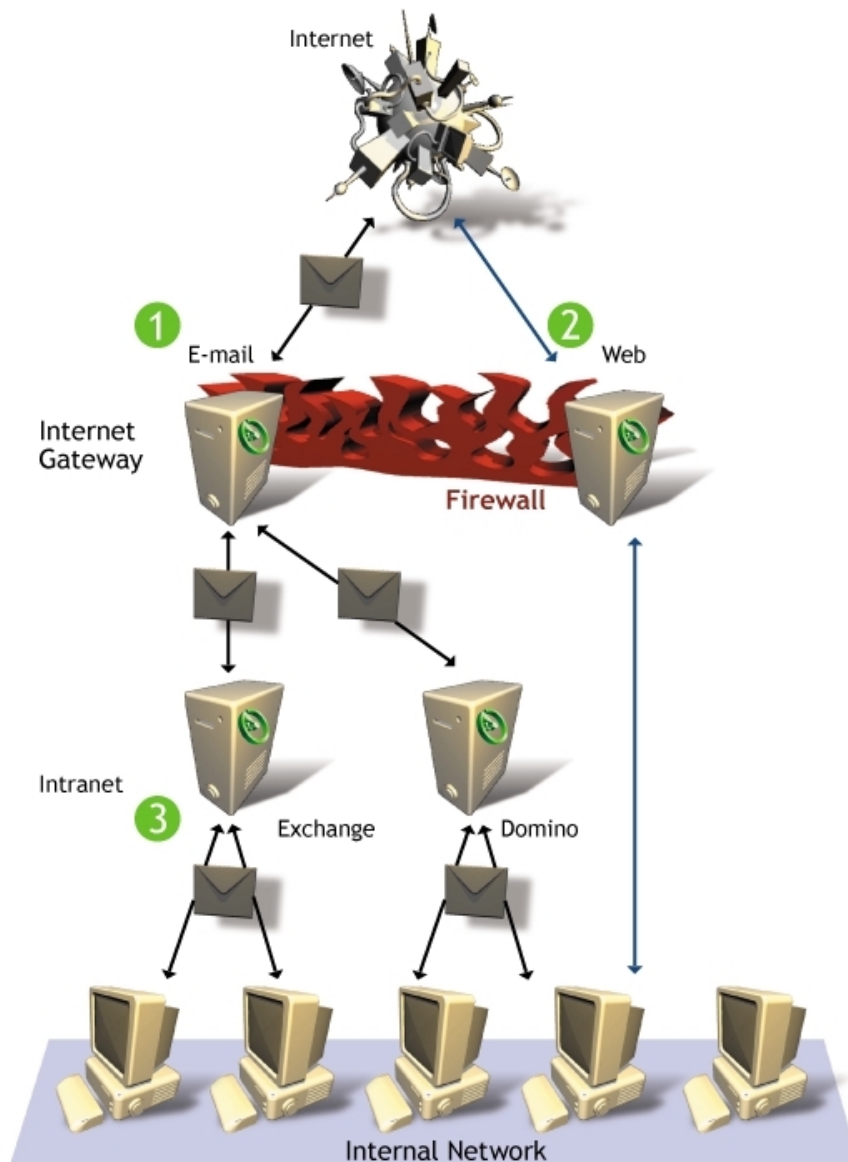


Figure 1. MIMESweeper products provide enterprisewide protection from external threats. (1) MAILsweeper for SMTP prevents damaging e-mail from entering or leaving the network at the firewall. (2) WEBSweeper provides content security for Web downloads and uploads. (3) MAILsweeper for Domino and MAILsweeper for Exchange protect against threats that are introduced and propagate within an organization's e-mail system.

Configuring MAILsweeper for Exchange 2000

MAILsweeper supports three deployment configurations. The optimal configuration depends largely on the number of users in the enterprise and the volume of e-mail generated.

- **Stand-alone deployment.** MAILsweeper services can be installed on the same PC as Microsoft Exchange 2000. This configuration may be economical and appropriate for the smallest Exchange environments, but typically is not recommended because of the extra load created by the MAILsweeper security service.
- **One-to-one deployment.** MAILsweeper is usually installed on a dedicated, networked PC capable of accessing a shared folder on the Exchange 2000 server.
- **Distributed deployment.** For high-volume sites, MAILsweeper can be installed on multiple PCs if the load exceeds the capacity of a single MAILsweeper services PC.

A small company with a single Exchange 2000 server might choose to install MAILsweeper for Exchange directly on the Exchange server, to avoid the cost of additional hardware. But in most cases, MAILsweeper is best hosted on a separate system, for the highest level of protection and performance. There is no client-side component, which keeps administrative costs low.

Unlike previous versions of Exchange, Exchange 2000 does not have its own SMTP message queue, or "stack," of messages being transmitted through the server. Instead the SMTP stack is managed by Windows 2000 through Microsoft Internet Information Services (IIS). MAILsweeper for Exchange 2000, then, includes an Intercept Module that is installed on the Exchange server, which acts as a "transport sink" on the SMTP stack, detouring e-mail messages for content analysis before they are processed by Exchange for normal delivery. Because MAILsweeper operates outside of Exchange 2000, messages do not enter the Exchange environment until they have been scanned, typically on a separate server, by MAILsweeper.

MAILsweeper for Exchange 2000 is capable of providing content security for all sources of e-mail within the Exchange environment. For a comprehensive e-mail security solution, however, organizations should deploy MAILsweeper for SMTP at the Internet gateway, to screen external e-mail before it enters the system, and use MAILsweeper for Exchange 2000 to manage the content security of typically higher-volume internal e-mail (Figure 1).

Potential Security Threats to an Exchange 2000 Mail System

Content security protects enterprises from two broad types of dangers: network integrity threats and business integrity threats. Network integrity threats are what most people think of when they consider security issues — any e-mail message, file attachment or piece of code that can compromise system operations. Business integrity threats, on the other hand, involve the intentional or unintentional transmission of confidential or inappropriate content via e-mail, which could expose the organization to any number of liabilities.

A complete content security service, MAILsweeper for Exchange 2000 protects against both kinds of threats — allowing administrators to define and enforce policies to ensure that e-mail in the workplace is used appropriately and for legitimate business purposes by individuals, groups and departments.

MAILsweeper Content Security

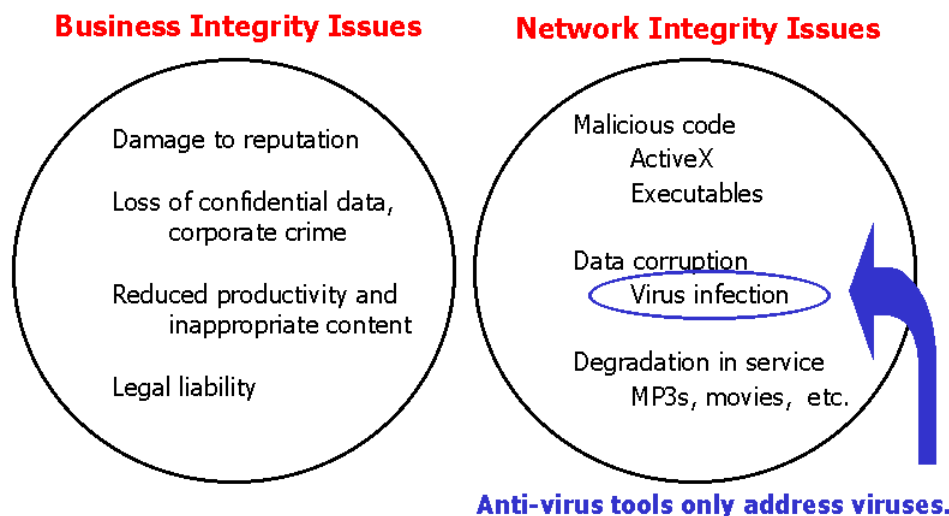


Figure 2. MAILsweeper protection extends well beyond that of anti-virus applications.

Network Integrity Issues

An Exchange mail system or an entire network can be compromised by unprotected and inappropriate use of the system. Viruses or damaging code can be introduced via Web download or floppy disk and then distributed via e-mail, and system performance can be damaged by large, but otherwise benign, attachments in e-mail sent to a large group of recipients.

- **Degradation of service.** Network throughput can be compromised or even suspended entirely as a result of employees sending very large files through e-mail. A 10 MB presentation sent to a company's global sales force, for example, could bring down a mail server.
- **Data corruption.** Viruses can infiltrate the internal mail system in several ways: via Internet e-mail, the attachment of files downloaded from the Web, or by employees bringing infected files in on disk and attaching them to a message.

Business Integrity Issues

Many organizations have learned hard lessons about the circulation of inappropriate content in e-mail messages within their internal messaging systems. The results are often well-publicized lawsuits and employee dismissals that cost millions of dollars and create public relations nightmares, all stemming from internal threats.

- **Breaches in confidentiality.** International Data Corp. research suggests that over two-thirds of all security threats originate from internal sources, and e-mail is an incredibly easy mechanism for confidential content to be spread — intentionally or inadvertently — to people not entitled to the information. Furthermore, the stakes of privacy breaches have increased for some organizations because of legislation around the world that controls the treatment of electronic consumer information.

- **Legal liability.** Likewise, unlicensed software or other copyrighted materials are also easily spread among employees over e-mail, potentially exposing the organization to copyright infringement lawsuits. If the unlicensed content is on an internal system, the company is liable.
- **Lost productivity.** E-mail can be a source of distraction and inappropriate use of time in the workplace. Through the sharing of music files, video clips, jokes and other non-work-related content, workplace productivity can be significantly compromised.
- **Offensive content.** The poor judgment of one employee can result in substantial harm to an organization. Racist, sexist, pornographic or other offensive content distributed via e-mail can create a negative, antagonistic work atmosphere and potentially open an organization to harassment lawsuits.

The MAILsweeper Approach to E-Mail Content Security

MAILsweeper helps organizations protect themselves from all these threats, based on e-mail-usage policies defined by the organization. With MAILsweeper for Exchange 2000, all internal e-mail transmissions are disassembled, evaluated against the governing security policy and scrutinized at the binary level before being allowed to pass through to recipients' mailboxes.

Policy-Based Content Security

Content security for Exchange is much more than protection against viruses. It's a tool for defining an e-mail usage policy that covers what is and is not acceptable content, and then monitoring the system and enforcing the policy through a software solution. Instead of attempting to be a one-size-fits-all solution, MAILsweeper allows system administrators to build a highly customized e-mail policy, tailored to any number of groups or individuals based on their business needs.

For example, an organization might use MAILsweeper for Exchange 2000 to ensure that a task team working on a highly confidential new product refrains from sharing any relevant details with colleagues through e-mail. Or it might log the volume of multimedia files transmitted across the network to assess the system load and productivity implications of nonwork-related use of e-mail. Or it might filter out spam by blocking messages from a running list of junk-mail senders or via a policy that identifies and blocks "get rich" messages using text analysis.

It's up to the IT manager and business decision makers to determine the content-security policy that best fits the organization — MAILsweeper provides the level of scrutiny and protection required.

How It Works

To implement a content-security policy, MAILsweeper scrutinizes e-mail in four stages:

1. **Policy identification.** When an e-mail message is sent, MAILsweeper retrieves the policy parameters for all recipients as well as the sender. It then applies the security operation to each message.

2. **Content disassembly.** MAILsweeper then identifies the primary components of the message, breaking down messages and attachments — such as compressed files, executable files and documents — to reveal their primary elements. MAILsweeper identifies content by its file architecture, rather than simply the file extension, and the pattern matcher feature allows file types to be identified by their binary sequence, giving administrators the ability to block any file type.
3. **Content analysis.** Once the content has been disassembled, MAILsweeper analyzes and evaluates it according to the policy as it applies to the message sender and recipients. MAILsweeper screens out designated file types or sizes, analyzes text to identify potential confidentiality breaches or prohibited content, and initiates a virus scan. MAILsweeper integrates with the leading virus scanners, and supports multiple, concurrent anti-virus solutions.
4. **Classification.** Once the content has been fully disassembled and analyzed, MAILsweeper implements the policy by allowing the message to be delivered, archiving the message for administrator review, adding a legal disclaimer to the message, deleting the attachment(s), or blocking the transmission altogether. A configurable message informs users when their e-mail has been blocked, and automatic notification to appropriate parties can be configured.

An Unmatched Feature Set for E-Mail Content Security

MAILsweeper offers the most comprehensive content-security service for the Exchange environment, including the full range of protections from detecting and purging malicious code to enforcing proper e-mail practices across an organization.

MAILsweeper for Exchange 2000 allows for combinations of these parameters to be built into highly detailed, customized, evolving policies — designed as the organization sees fit to encourage safe, productive and efficient use of e-mail.

Detection of System-Threatening Content

- **Virus detection and cleaning.** MAILsweeper for Exchange 2000 integrates with the leading anti-virus solutions — including products from Trend Micro, Command Software Systems, Norman, F-Secure, Symantec and McAfee — to detect and block or disinfect messages with virus-laden attachments. Multiple anti-virus packages can be deployed alongside MAILsweeper.
- **Protection against malicious code.** MAILsweeper protects against Trojan horses, document “bombs,” or potentially damaging code written in JScript, Buttons, Actions or Java. If the policy so dictates, MAILsweeper can block the transmission of executable files altogether.

Enforcement of E-mail Usage Policies

- **Attachment screening.** E-mail attachments can be screened based on file size, type or name. For example, system administrators can prevent known files — whether they be video clips or executable files — from being distributed. Very

large files can be blocked, to prevent system degradation. And sharing certain types of attachments, such as MP3 files, can be prohibited.

- **Text analysis.** Text-based analysis of e-mail messages and attachments can be used to prevent the distribution of content that could be damaging to the business, worker productivity or the professionalism of the workplace. Types of undesirable content might include confidential business documents or sensitive intellectual property, discriminatory content, pornography, or any other content that can be identified using keywords or phrases.
- **Legal disclaimers.** With MAILsweeper, an organization might choose to add a legal disclaimer to certain kinds of transmitted e-mail, to protect the company and help prevent e-mail content from being used to support a lawsuit.
- **Spam reduction.** MAILsweeper for Exchange 2000 can filter out unsolicited junk mail — generated from within or outside of the Exchange network — to prevent it from distracting, annoying or otherwise reducing the productivity of employees.
- **Encryption management.** Organizations can implement encryption policies with MAILsweeper for Exchange 2000. While encrypted messages cannot be disassembled and analyzed, MAILsweeper can control which employees have the authority to use encryption.

Reporting and Monitoring

- **Notification messages and logging.** Any MAILsweeper event can be set to trigger specified notification actions, such as alerting the system administrator or a department head. MAILsweeper can also make entries into an event log, to record a history of content security operations. Employers can get a profile of individual users, departments, message types and frequencies from an internal as well as external perspective.
- **System monitoring.** MAILsweeper can be used to monitor the performance of the Exchange system. By monitoring internal as well as external e-mail traffic, customers can identify areas of their mail system that are underused and reallocate resources appropriately, substantially increasing their return on investment.
- **Regulatory auditing and tracking.** Regulated industries and individual organizations are increasingly being directed, through legislation and court orders, to monitor, audit and store their e-mail communications. E-mail can also be called upon as evidence in court. MAILsweeper allows organizations to fully comply with these directives.
- **E-mail quarantines.** MAILsweeper has the ability to quarantine messages containing specific threats or prohibited content. A system administrator can then review and, if appropriate, release messages that triggered the action.

Optimizing Bandwidth

- **Reducing nonwork-related traffic.** An effective set of e-mail policies will automatically relieve stress on an Exchange system by blocking large audio and

video files, jokes and other inappropriate, nonwork-related messages. Such policies can save significant amounts of space on Exchange 2000 server databases.

- **Parking oversized messages.** Parking enables a message to be held in a holding area until a time specified by the administrator. For example, large messages can be parked during normal working hours and then released when there is less traffic on the network.

New Features

The differences in Exchange 2000 over Exchange 5.5 have removed several restrictions on MAILsweeper for Exchange. With this version of MAILsweeper, users can take advantage of the following:

New Feature	Benefit
MAILsweeper V4 technology	More powerful and flexible protection against the full spectrum of content security threats
User interface	Seamless integration with Microsoft Management Console (MMC), with no need to edit configuration files
Active Directory support	Full access to user and group information stored in the Windows 2000 Active Directory
MAILsweeper clustering	No limit to the number of users supported
Choice of anti-virus tools	Flexibility to work with customer's choice of anti-virus tools
Powerful reporting	Up-to-the-minute reports of internal e-mail use
Sample policies	Quick-start content security protection
Attachment stripping	Ability to block offensive attachments while allowing the recipient to receive the body of the message
Full compatibility with Exchange and Outlook features	The Inbox Assistant and Out of Office Assistant in Outlook are fully functional

Installation and Product Walk-Through

Now that you've read about the capabilities of MAILsweeper for Exchange 2000, let's take a look at the product itself. This brief walk-through will familiarize you with the MAILsweeper interface using Microsoft Management Console and give you an understanding of how a content security policy is implemented. While this guide only gives you a glimpse of the features in MAILsweeper for Exchange 2000, it provides step-by-step installation instructions and a straightforward introduction to the product. We hope you will continue on to review and test the many features that set MAILsweeper apart as an end-to-end content security service.

In addition to this reviewer's guide, we've provided an evaluation CD and Administrator's Guide. To review MAILsweeper for Exchange 2000 and take the following guided tour,

you will need to install MAILsweeper's e-mail Intercept Module on an active Exchange 2000 server, and install MAILsweeper on a networked Windows 2000 or Windows NT system with Outlook. Make sure that the administrator mailbox is configured, in order to test MAILsweeper's e-mail inform capabilities.

The following technical requirements apply:

Hardware

- 500MHz (800MHz recommended) Pentium III or higher processor
- At least 256 MB of RAM (512 MB or more for a stand-alone deployment)
- 500 MB of free disk space on an empty NTFS-formatted partition (20 GB recommended).
- 500 MB of free disk space in the \temp directory
- Network interface card, with access to CD-ROM or network for installation
- VGA or better display resolution

Software

- Microsoft Windows 2000 Server or Advanced Server with Service Pack 1, configured as a domain controller
- Microsoft Exchange 2000 Advanced Server with Service Pack 1
- Microsoft Outlook XP as the messaging client, only required for the system on which the security service is installed
- Microsoft data access components (MDAC) 2.6 and Service Pack 1 (MDAC 2.6 is not compatible with a SQL Server cluster)
- Microsoft Jet 4.0 with Service Pack 3
- Microsoft SQL Server 7 for reporting

Installing MAILsweeper for Exchange 2000

This walk-through assumes a one-to-one deployment configuration — one MAILsweeper system connected to one Exchange 2000 server — which is appropriate for most enterprises. To configure MAILsweeper, you'll first install the MAILsweeper Intercept Module on the Exchange server, then install the MAILsweeper security service on the Windows 2000 and Outlook XP system.

Installing the Intercept Module

Insert the evaluation CD into the Exchange 2000 server. The installation program loads automatically. Click **Next** several times until Windows Installer begins installing the MIMesweeper technology and MAILsweeper for Exchange components on the Exchange server. Click **Next** to begin the installation, and **Next** again to install the second component.

Accept the license agreement and choose the destination folder. For this walk-through, select **One-to-one** and click **Next**.

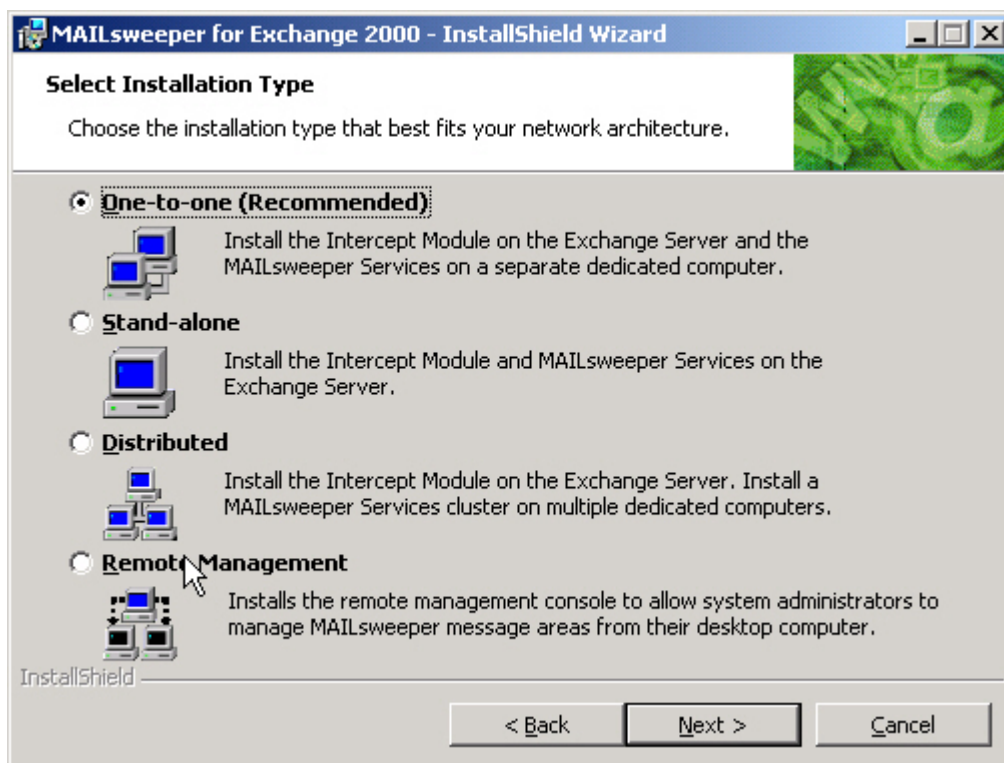


Figure 3. MAILsweeper for Exchange 2000 supports several deployment configurations.

Choose **MAILsweeper Intercept Module Only**, and **Next**.

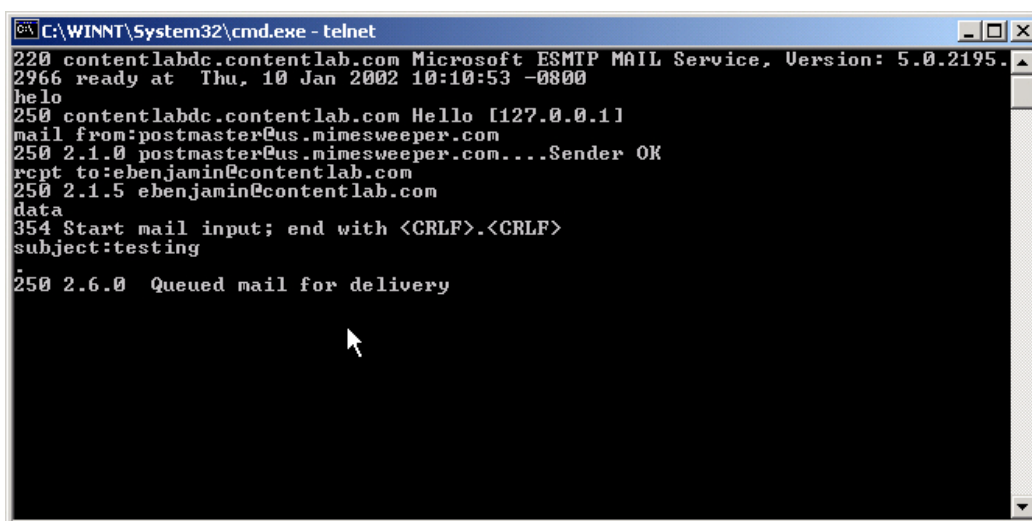
Enter the IP address of the MAILsweeper server, which we'll configure next, and click **Add**.

To set the service logon account, set the user as the domain administrator, with user name and password. Click **Next** again to begin the installation, and **Finish**.

Stop the Exchange System Attendant and reboot the system when prompted.

Now the Intercept Module needs to be enabled. This is done through either the command line or Exchange System Manager Extension. In this case, we'll enable the Intercept Module by creating a manual message. Enter the following commands:

```
telnet
set local_echo
open localhost 25 [The mail system will answer.]
helo
mail from:postmaster@yourdomain.com [Enter the postmaster e-
mail address.]
rcpt to:user@yourdomain.com [Enter your user address on the domain
that the installation is configured for.]
data
subject:testing
```

A screenshot of a Windows command prompt window titled "C:\WINNT\System32\cmd.exe - telnet". The window shows a telnet session with a mail server. The user enters "telnet", "set local_echo", "open localhost 25 [The mail system will answer.]", "helo", "mail from:postmaster@us.mimesweeper.com", "rcpt to:ebenjamin@contentlab.com", "data", and "subject:testing". The server responds with "220 contentlabdc.contentlab.com Microsoft ESMTMP MAIL Service, Version: 5.0.2195.2966 ready at Thu, 10 Jan 2002 10:10:53 -0800", "250 contentlabdc.contentlab.com Hello [127.0.0.1]", "250 2.1.0 postmaster@us.mimesweeper.com... Sender OK", "250 2.1.5 ebenjamin@contentlab.com", "354 Start mail input; end with <CRLF>.<CRLF>", and "250 2.6.0 Queued mail for delivery".

```
C:\WINNT\System32\cmd.exe - telnet
220 contentlabdc.contentlab.com Microsoft ESMTMP MAIL Service, Version: 5.0.2195.
2966 ready at Thu, 10 Jan 2002 10:10:53 -0800
helo
250 contentlabdc.contentlab.com Hello [127.0.0.1]
mail from:postmaster@us.mimesweeper.com
250 2.1.0 postmaster@us.mimesweeper.com... Sender OK
rcpt to:ebenjamin@contentlab.com
250 2.1.5 ebenjamin@contentlab.com
data
354 Start mail input; end with <CRLF>.<CRLF>
subject:testing
250 2.6.0 Queued mail for delivery
```

Figure 4. Enabling the intercept module.

You can verify that MAILsweeper interception has been enabled correctly by opening the Properties dialog box on the Exchange server and clicking the MAILsweeper tab.

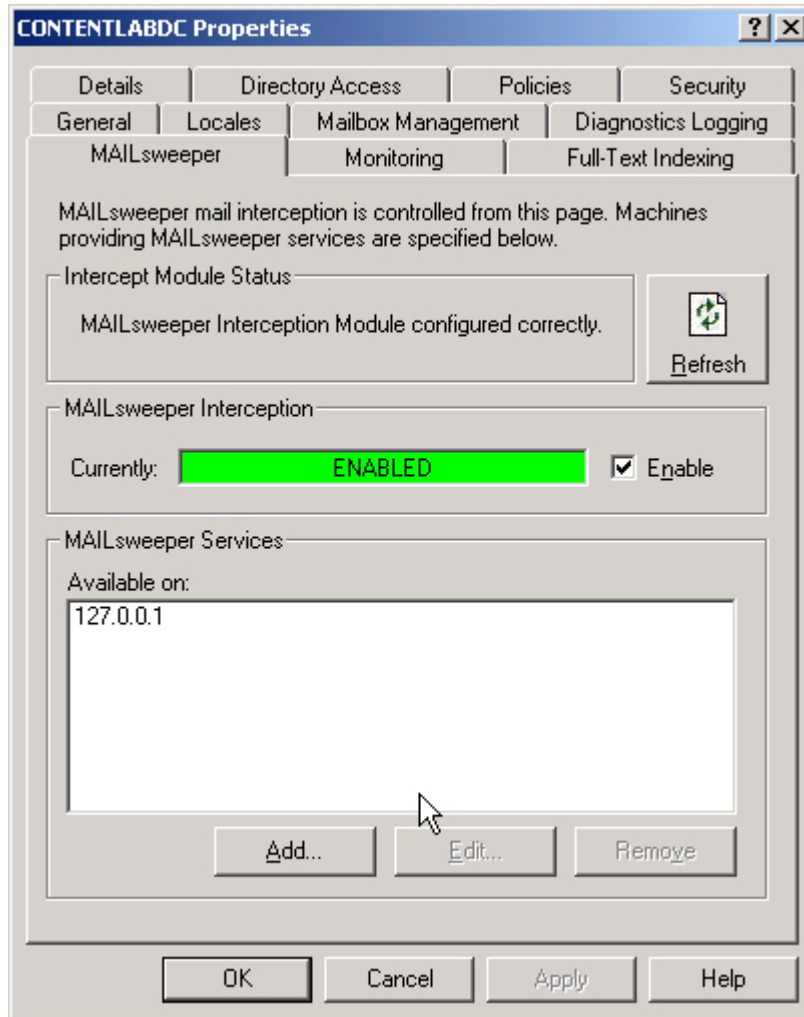


Figure 5. The Properties dialog box indicates that the Interceptor Module is enabled.

Configuring the MAILsweeper Security Service

On the Windows 2000 and Outlook XP system, insert the evaluation CD. The installation program loads automatically.

Click **Next** several times until Windows Installer begins installing the MIMESweeper technology and MAILsweeper for Exchange components. Click **Next** to begin the installation, and **Next** again to install the second component.

Accept the license agreement, choose the destination folder.

Select **One-to-one** and click **Next**. This time, select **MAILsweeper Only**, and **Next**.

At the Company Configuration screen, enter the company and domain names. Click **Next**.

Again, set the user as the domain administrator, with user name and password.

Enter the computer name or IP address of the Exchange 2000 server in the next window. Click **Next**, then **Install** to begin the installation. Click **Finish** when the installation is complete. Click **Finish** again to reboot the system.

The MAILsweeper installation is now complete. **Note:** in a typical deployment, we would install an anti-virus solution at this point, in order to integrate it with MAILsweeper as part of the overall e-mail security solution. MAILsweeper supports all of the leading anti-virus applications.

The next step is to install the MAILsweeper license.

Bring up the MAILsweeper for Exchange 2000 console which, with this version of MAILsweeper, uses the Microsoft Management Console interface.

Expand the MAILsweeper Policy Editor in the left navigation tree, right-click **Licences**, and select **New > MAILsweeper for Exchange 2000 Licence**. Click **Next**, and enter your company name and the license key and serial number provided with your evaluation kit. Click **Next**.

Enter "Evaluation" as the name of your license, and click **Finish**.

Now we're ready to explore MAILsweeper's capabilities. But first, let's make sure the MAILsweeper system is up and running.

From the MAILsweeper Console, expand the Local MIMESweeper Manager in the navigation tree and select **Services**. Select all of the services that appear in the right panel and right-click to open the shortcut menu. Select **Start service**. MAILsweeper is now running, although no policies have yet been configured.

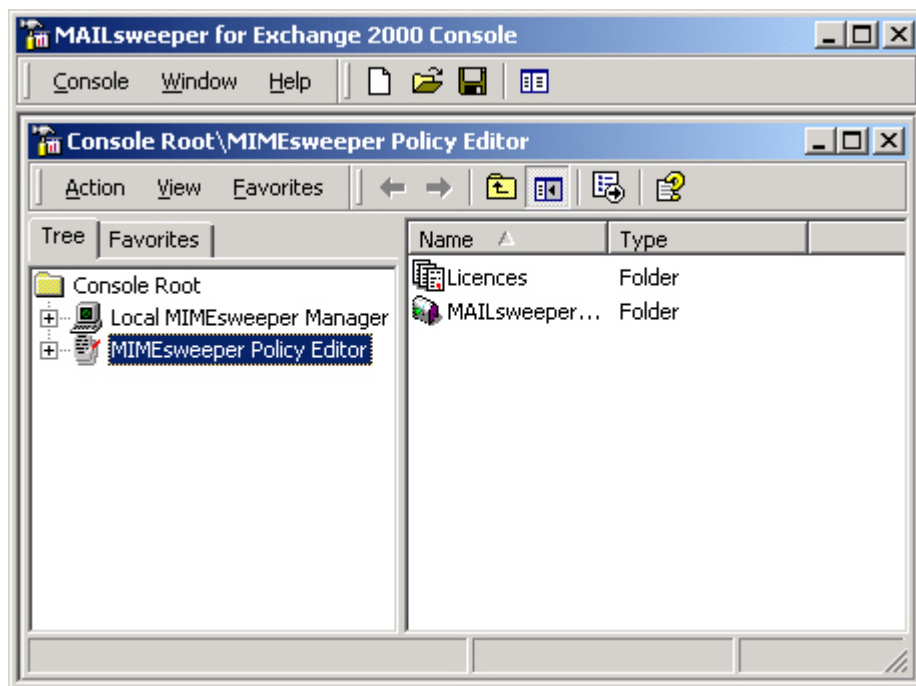


Figure 4. The MAILsweeper for Exchange 2000 console.

Creating and Modifying Policies

With this walk-through, we'll be configuring a content security policy from scratch, and then give you an opportunity to test the results. Let's say we're a medium-size company that

has concerns about confidentiality leaks, liability from harassment and inappropriate language in e-mail, employee productivity, and system degradation from users sending very large e-mail messages. To address these concerns, we'll implement four policies.

Scenarios and Classifications

MAILsweeper policies are essentially built around two elements — scenarios and classifications. Scenarios define the types of things MAILsweeper screens for under specified conditions, and classifications define the actions MAILsweeper takes once it detects an offending transmission. Scenarios are the *rules*, and classifications are the *consequences*.

Scenarios are applied to users or groups of users. And while an organization's policy will have a default set of scenarios, any user or group can be exempted from any scenario, or have custom scenarios created to fit specific circumstances.

Corporate Crime: Scanning for Red-Flag Terminology

Companies that deal with highly sensitive information may want to implement an e-mail policy that prevents employees from sending confidential material — intentionally or inadvertently — via e-mail.

At the console, expand the MAILsweeper Policy Editor in the left panel, and expand MAILsweeper for Exchange 2000 and click **References**.

Right-click **References** and select **New > Expression List for Text Analysis**.

The New Reference wizard appears. Click **Next** to create a new list. Select **English** and **Next**.

In the Expressions window, click directly under the Expression bar and type "Sausage", our new-product code name.

Use the **Tab** key to drop down to the next entry. Note that the weighting, which defines an acceptable frequency of use of the term, defaults to Detected, in other words, zero tolerance for that word.

Enter "Confidential" and any other words you want MAILsweeper to scan for. [Remember some of these words. You'll have the opportunity to test MAILsweeper's ability to scan for them in e-mail and attachments later.]

Click **Next**. Enter "Corporate Crime" as the name of the list. Click **Next**, and **Finish**.

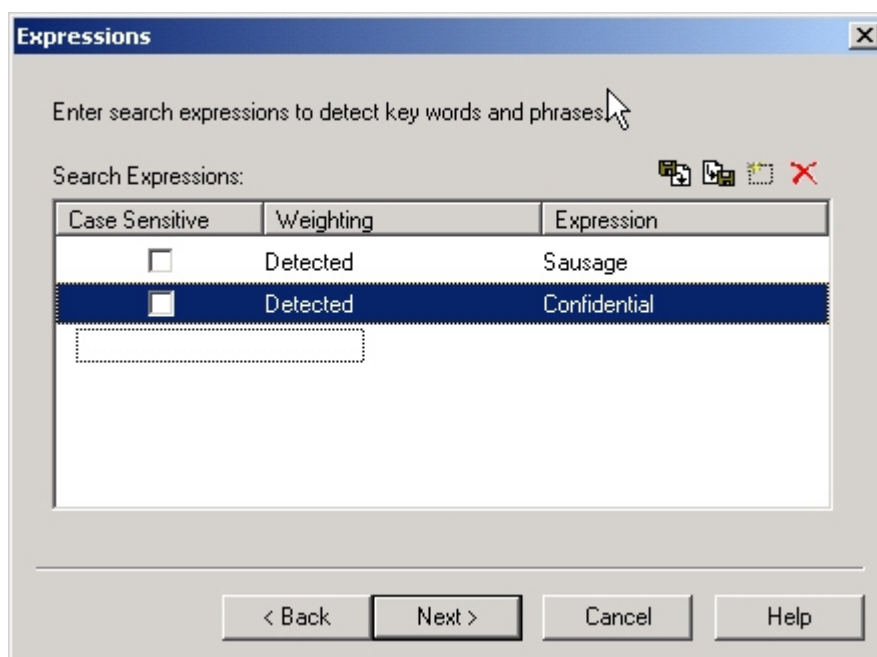


Figure 5. To scan for restricted content in e-mail, companies can build a policy around a custom word list.

Now that the list of restricted words has been established, we have to set up the classification — the action that takes place after restricted words have been detected. In this case, we want to quarantine any suspected messages and then send an e-mail alert, or “inform,” to the system administrator.

Back at the console, expand **Policies** under MAILsweeper for Exchange 2000 in the left panel. Highlight and right-click **Classifications** to open the shortcut menu. Select **New > Classification**.

The New Classification wizard appears. Click **Next**. Default to Exclusive and click **Next**.

Name the classification “Corporate Crime.” Click **Next** and **Finish**. The Corporate Crime classification appears in the classification tree.

Select and right-click **Message Areas** under MAILsweeper for Exchange 2000 in the navigation tree. Select **New > Quarantine Area** from the shortcut menu.

The New Message Area wizard appears. Click **New Folder** to create a quarantine area called “Corporate Crime” within MAILsweeper’s Message Areas directory.

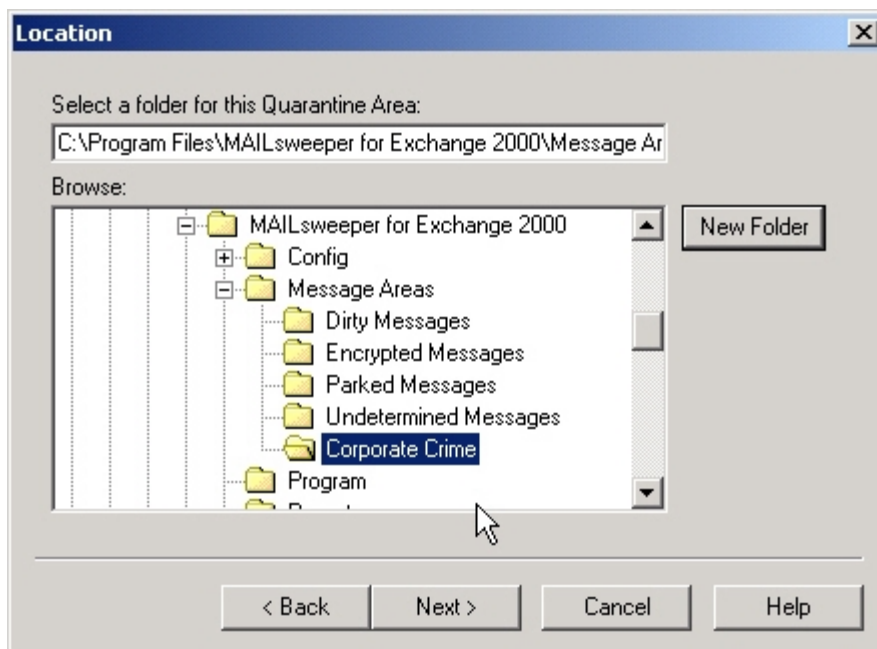


Figure 6. Creating a quarantine area, or holding area, for messages that contain restricted terms.

Click **Next**. The Permissions window appears. This is where we determine who has the right to release messages from quarantine.

Click the **Add User** icon in the upper right corner.

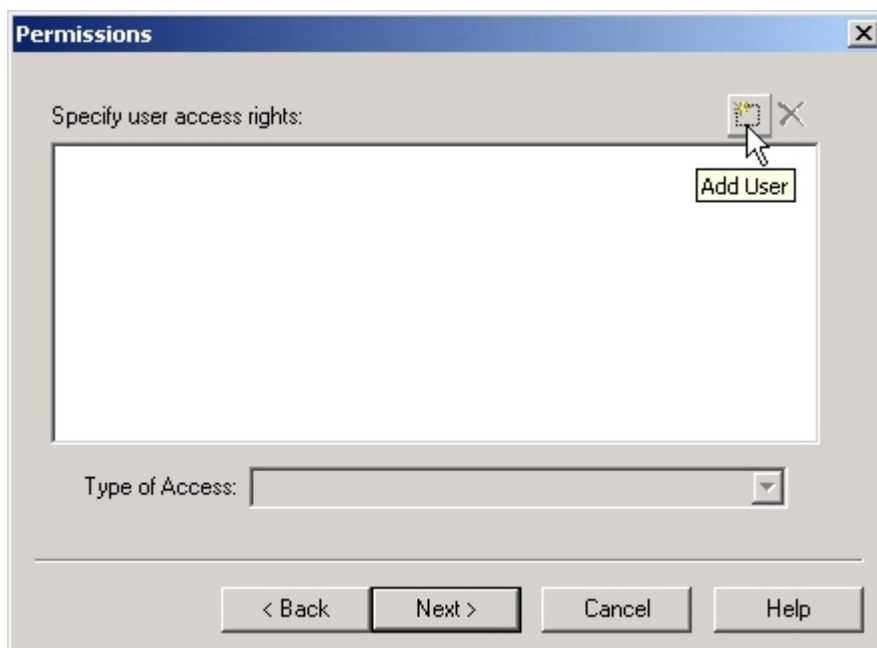


Figure 7. The Add User icon is in the upper right corner of the Permissions window.

The user groups appear. Click **Show Users**. Select **administrator** from the Windows 2000 Active Directory user list. Click **Add**, and give the administrator **Full Control**. Click **OK** and **Next**.

Determine how long a message can exist in quarantine before being automatically deleted, and click **Next**.

Name the Message Area "Corporate Crime" and **Finish**. Note that Corporate Crime has been added as a message area.

Highlight the **Corporate Crime** classification (not the message area) in the navigation tree. Right-click within the right panel (which is empty), and select **New > Notification** from the shortcut menu. Tick **Inform**.

The New Notification wizard appears. Click **Next**. Tick **Administrator** as the e-mail account from which inform messages will be sent. Click **Next**.

Under the Address bar, define the recipients of the inform message. Add the administrator's e-mail address, and under Type, click the down arrow to select how the message will be addressed. Underneath the administrator's e-mail address, enter "%SENDER%", which is the token for the person who sent the original message with restricted language. And, to the left, have them appear on the "To" line of the inform message.

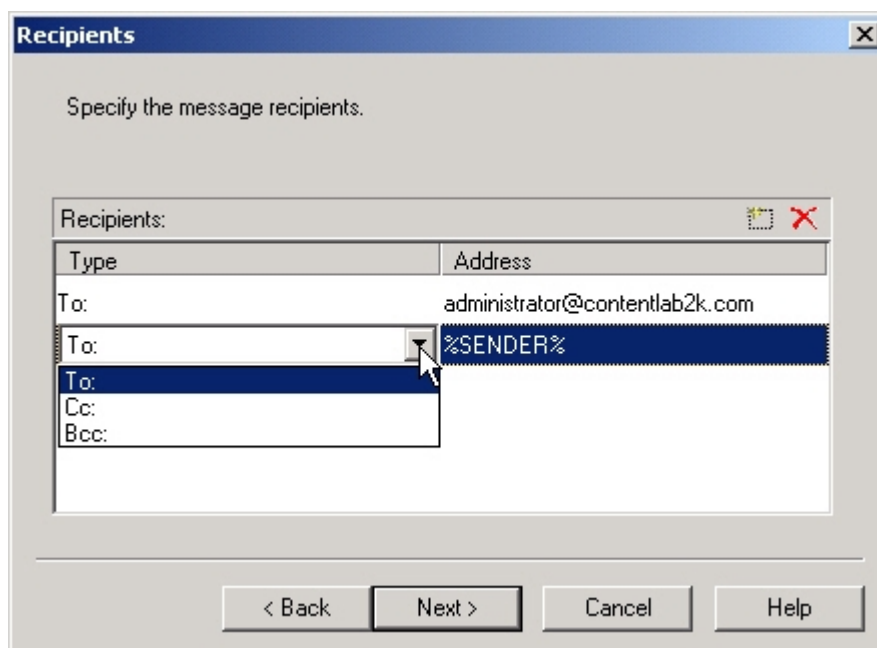


Figure 8. Determining who will receive the inform message.

For the subject line of the inform message, enter "Potential Security Breach (%SUBJECT%)". Click **Next**.

For the body of the message, enter "This message has been quarantined for violating the confidentiality policy." Click **Next**. And **Next**.

In the Attachments window, select "Include results from Text Analysis." Click **Next**.

Name the notification "Corporate Crime." Click **Finish**.

Right-click once again in the right panel of the Corporate Crime classification, and select **New > Action > Quarantine**. The New Action wizard appears. Click **Next**. Select **Corporate Crime** from the list. In the next window, tick **in original form**, since this policy is not dealing with messages that have been infected with viruses or attachments. In the next window, name the action "Corporate Crime Quarantine". Click **Next** and **Finish**.

The last step in creating the policy is to define the scenario, that is, defining which circumstances trigger the Corporate Crime classification we just created.

Expand **Scenarios** in the MAILsweeper navigation tree. The scenario can be applied to incoming, outgoing and/or internal e-mail. In this case, we want to screen for restricted terms in internal and outgoing e-mail, but not incoming e-mail.

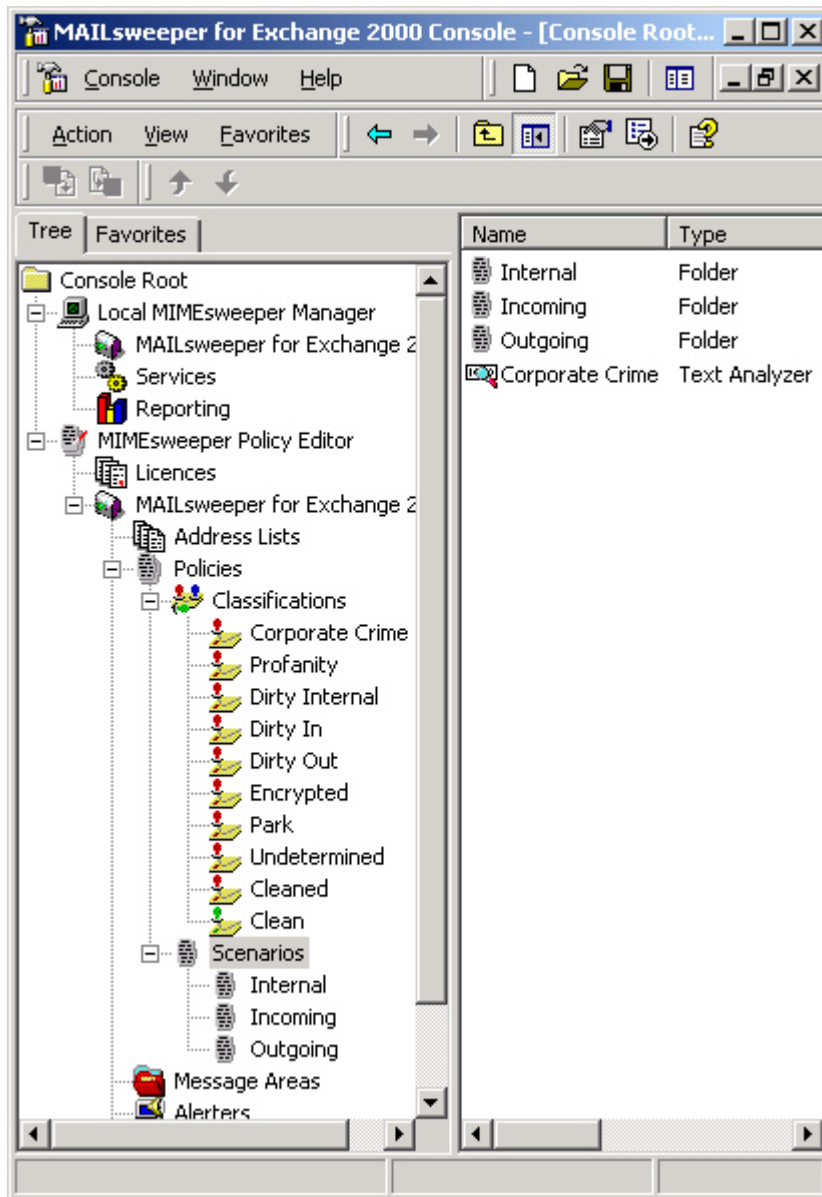


Figure 9. The expanded navigation tree in the MAILsweeper console.

Highlight **Scenarios**, and right-click. Select **New > Scenario > Text Analyzer**. The New Scenario wizard appears. In the next window, make sure that both boxes are checked. We will want to override lower levels of the scenario in this case.

In the next window, select the **Corporate Crime** expression list, and click **Next**.

Set the threshold level at 1 and leave the proximity setting at 10. This essentially sets the scenario to trigger at any single use of any word or phrase on the expression list. Click **Next**, and **Next** again to scan all areas of the message.

Select **Corporate Crime** as the classification (or action) that the scenario triggers.

Name the scenario "Corporate Crime". Click **Next** and **Finish**.

Now that the scenario has been built, we need to determine which messages it applies to. In this case, the Corporate Crime scenario has been applied globally at the root level, so we need to deactivate it for incoming e-mail.

Highlight **Incoming** in the tree and right-click the scenario in the right panel. Uncheck **Active**.

NOTE: The classifications we create in this walkthrough must be organized at the highest priority level among the listed Classifications, and thus must be moved to the top of the list. To "promote" the item within the hierarchy of classifications, select the classification and click the up arrow in the toolbar continually until it is at the top.

Legal Liability: Using MAILsweeper to Deter Workplace Profanity

For the next policy, we want to scan for profanity in e-mail, and have MAILsweeper generate an inform message to the sender without blocking delivery of the original message.

First, we'll build the classification. From the Classifications shortcut menu, select **New > Classification** and name it "Profanity."

Only two actions are required for this classification — reply with an inform message to the sender and deliver the original message.

Select the **Profanity** classification, right-click in the right panel, and select **New > Notification > Reply**.

As you click through the wizard screens, select administrator as the account that the inform message is sent from, enter a subject of the message, and the body of the message as you like.

Default to the ISO character set, tick both boxes in the Attachments window, name the classification "Profanity Reply," and **Finish**.

To create the action to deliver the original mail, right-click once again in the right panel and select **New > Action > Deliver**. Click **Next** and enter "Deliver" as the name of the action and **Finish**.

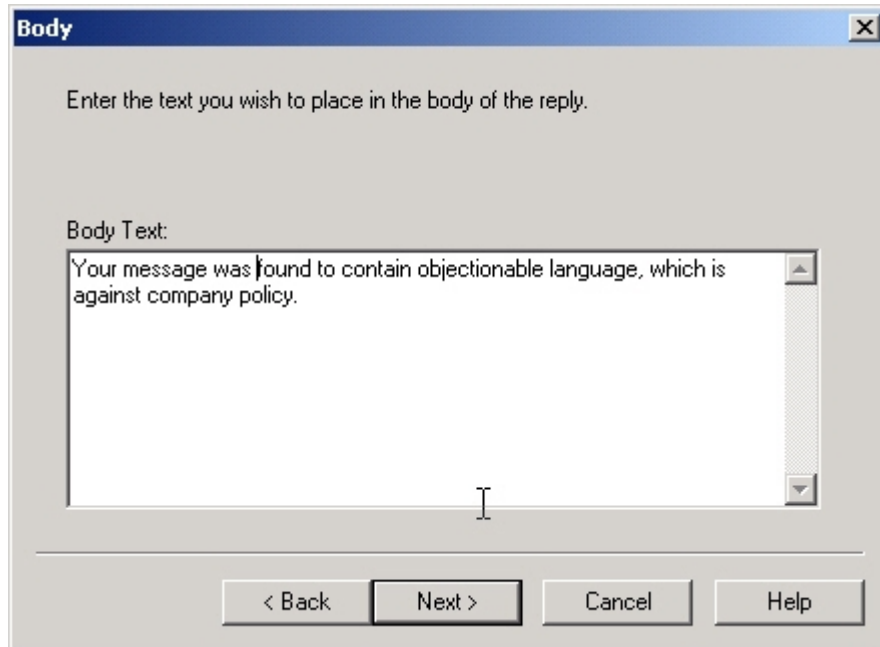


Figure 10. Creating a response to the use of profanity in e-mail.

Now let's build the scenario for this. Highlight **Internal** under Scenarios in the Policy Editor tree. Right-click and select **New > Scenario > Text Analyzer**.

Use the default settings on the next two screens. Choose the **Profanity** expression list, which is pre-existing in MAILsweeper (and can be modified).

Set the threshold and proximity to 1 and 10, respectively. Default to all scanned areas, and when the wizard screen appears, select the **Profanity** classification we just built.

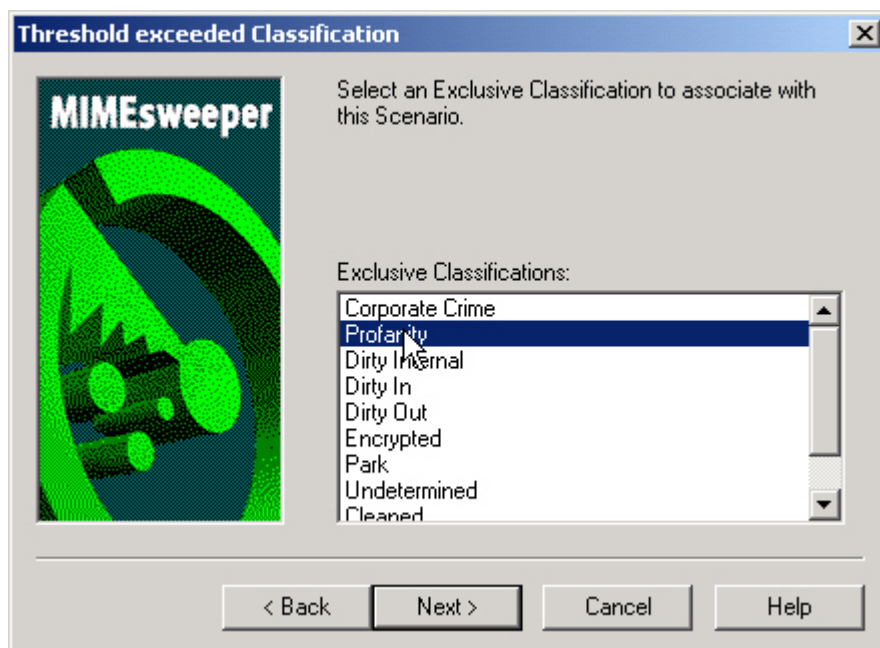


Figure 11. Selecting the Profanity classification for the Profanity scenario.

Choose **Next** and name the scenario "Profanity".

Workplace Productivity: Blocking AVI Attachments

Companies may choose to block certain types of e-mail attachments altogether. In this case, we'll block all AVI video files. NOTE: In this case, we're choosing to block attachments simply based on an AVI file extension. Administrators do have the option of configuring a similar policy that analyzes all attachments at the binary level to ensure complete blockage of AVI-format video clips.

Create a new classification called "Block AVI". Promote the classification so that it is under Profanity in the hierarchy of classifications.

Highlight the Block AVI Classification in the tree and right-click in the right panel. Select **New > Action > Deliver**.

Highlight the **Incoming** scenario, right-click within the right panel and select **New > Scenario > Attachment Stripper**.

Click through the wizard defaults until you reach the Format Types window. Tick "In selected formats" and select the **Video** check box to the left.

Click the **Change Option** button, and check the **AVI** box.

Click **OK** and **Next**. Default to AVI attachments of any size.

Annotate the message.

In the Detected Classification window, choose the **Undetermined classification** for attachments that cannot be stripped. In the Removed Classification window, choose **Block AVI**.

Name the scenario "Block AVI" and **Finish**.

Network Degradation: Parking Large E-Mail Messages

For our final policy, we want to delay the transmission of large e-mail messages, which bog down the Exchange 2000 environment during peak times. To do this, MAILsweeper "parks" messages in a holding area until a specified time.

Create a new classification called "Large Files". Promote the classification so that it is under Block AVI in the hierarchy of classifications.

Highlight the **Large Files** classification in the navigation tree and right-click in the right panel. Select **New > Action > Reply**.

Follow the wizard windows, select administrator as the account the reply message is sent from, enter a subject of the message, and the body of the message indicating that message delivery has been delayed until after hours to conserve network bandwidth.

Default to the ISO character set, leave both boxes in the Attachments window unchecked, name the classification "Large Files" and **Finish**.

Now we have to create the parking mechanism. First we have to build a parking area. Right-click **Message Areas** in the tree, and select **New > Parking Area**.

Create a "Large Files" folder in Message Areas.

Click the Add User icon in the upper right corner. The user groups appear. Click **Show Users**. Select **administrator** from the user list, and click **Add**. Give the administrator **Full Control**. Click **OK**. Click **Next**.

Decide which 30-minute windows to deliver messages with large attachments (say, 20:00 hours, or 8:00 p.m.) and decide how many of these messages to release for each selected half-hour period. Click **Next**.

Name the Message Area "Large File Parking".

Now we have to establish the action to park the large message during normal hours. Highlight the **Large Files** classification in the tree and right-click in the right panel. Select **New > Action > Park**.

When the Park window appears, select **Large File Parking** as the location. Choose to park messages in their original form.

Name the action "Large File Park" and **Finish**.

Now we have to build the scenario. Highlight **Internal**, right-click in the right panel and select **New > Scenario > Size Manager**.

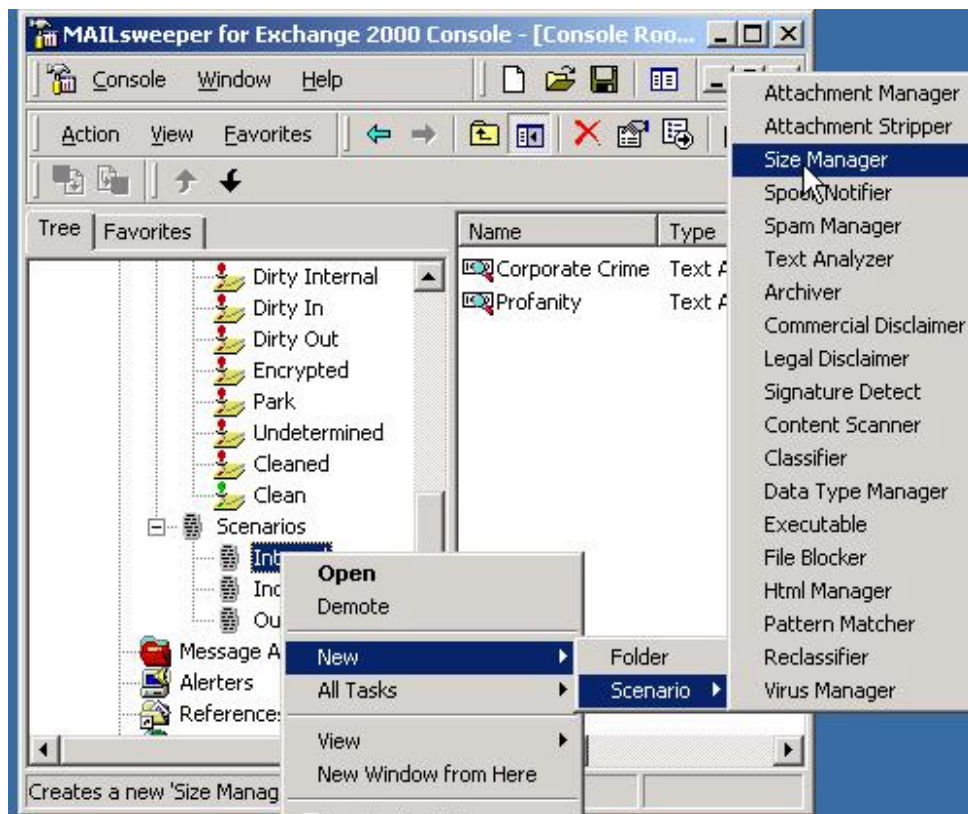


Figure 12. With MAILsweeper's Size Manager feature, companies can create a policy that delays the transmission of large e-mail messages during peak times.

Click through the default settings until you reach the Message Size window. Set the smaller threshold size to 2 MB. This will park messages with a total message size, including attachments, of greater than 2 MB.

Click **Next** through the Schedule to keep the policy in place at all times. Select the Large Files classification we created earlier. Name this scenario "Large File Park" and click **Finish**.

Forcing a New Policy to Load Immediately

To activate the policies we just created, you'll need to stop and restart the MAILsweeper services.

From the MAILsweeper Console, expand the **Local MIMESweeper Manager** in the left panel and click **Services**. Select all of the services in the right panel and right-click to open the shortcut menu. Select **Stop Service**.

Repeat these steps and select **Start Service**. All of our policies are now configured and active.

Testing the New E-Mail Policies

Now that the policies are activated, let's break the rules and see MAILsweeper for Exchange 2000 at work. For this evaluation, log in as administrator or as another user and simply send a piece of e-mail using Outlook.

Test the policies by sending some messages, such as the following:

- A message with attachments totaling more than 2 Mb
- A message that includes profanity, "Sausage" or "Confidential" in the body of the message or in an attachment
- A message with an AVI file attached

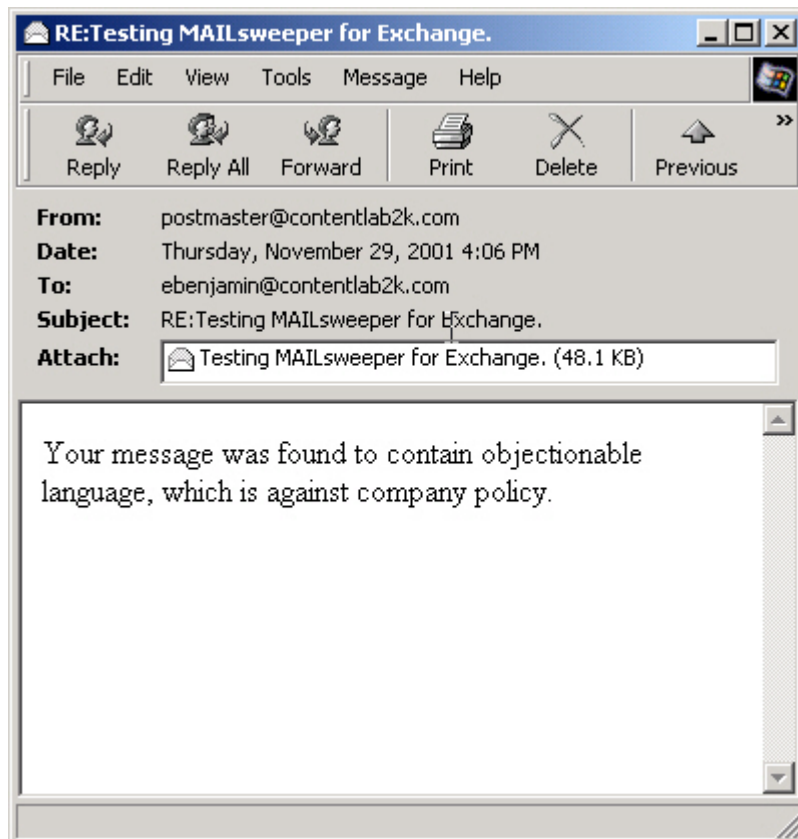


Figure 13. Inform messages can be used to warn users — or managers — of policy breaches.

This walk-through has given you just a glimpse at MAILsweeper for Exchange 2000. Now that you have a feel for the interface, we encourage you to spend more time exploring the modules and endless combinations of security parameters that can be implemented. We're confident you'll find that MAILsweeper for Exchange 2000 offers the deepest level of content security, the greatest policy flexibility and the richest administrative tools.

Downloading and Applying Sample Policies

If you would like to explore more of MAILsweeper's features and policy options, you might want to download a sample content security policy from the MIMESweeper Web site at <http://www.us.mimesweeper.com/>. Note that sample policies do not configure any anti-virus products.

Select **Download** from the menu at the top of the home page.

Click on **Support** then **MAILsweeper for Exchange 2000**.

Select **Sample Policies** on the left side of the page.

Click on the **Download** link.

Log in to Download.

Download the file from the Reading, UK, site and save the file to a temporary directory.

Extract the files to **c:\program files\MAILsweeper for Exchange 2000\policymate**, and run **PolicyMate.exe**.

The sample policies will install and configure the auditing tab. You must have access installed.

You will have a choice of installing one of the following policy sets:

- **Basic Policy**, which does the following:
 - Blocks image files by data type
 - Blocks executable files by data type (prevents renamed files from passing through)
 - Adds a template legal disclaimer on outbound messages
 - Parks outbound messages over 10 Mb
- **Comprehensive Policy**, which does the following:
 - Blocks executable files by data type (prevents renamed files from passing through)
 - Strips active file types such as VBS, BAT and CMD, and annotates the message
 - Blocks messages with English profanity
 - Adds a template legal disclaimer on outbound messages
 - Looks for inbound spam e-mail
 - Detects and blocks multimedia files being sent internally
 - Parks internal messages over 10 Mb
 - Detects outbound "company confidential" messages
- **Malware Policy**, which does the following:
 - Strips active file types according Microsoft security recommendations and annotates the message
 - Adds a template legal disclaimer on outbound messages

- Blocks virus worms
- Blocks virus hoaxes
- **US Policy**, which does the following:
 - Blocks executable files by data type (prevents renamed files from passing through)
 - Strips active file types such as VBS, BAT and CMD, and annotates the message
 - Blocks messages with English and Spanish profanity
 - Adds a template legal disclaimer on outbound messages
 - Looks for inbound spam e-mail
 - Detects nonproductive messages
 - Detects and blocks multimedia and images files sent internally
 - Parks internal messages over 10 Mb

Support / Customer Help

At Baltimore Technologies, our engineers work diligently to research, resolve and respond to customer inquiries through a combination of methods including telephone, e-mail, and voice-mail. Our team performs first-level problem resolution for delivery systems issues; acts as the front-line interface to customers, accepting trouble reports, and either resolves problems or dispatch/escalate them where appropriate. Our technical support team members ensure that all major technical support issues are properly addressed through proper training and a strong knowledge of the MIMESweeper product family.

Baltimore Technologies MIMESweeper customer support in North America will respond to all requests for phone support within 4 business hours; e-mail within 2 business days after receipt of such request. Customer support may respond via telephone or electronic mail. Telephone support hours are 5:30 a.m. to 6:00 p.m. PST at 425.460.6190; 24-hour support is also optionally available.

Appendixes

Additional information on MAILsweeper for Exchange 2000 is available through your sales representative (425.460.6000) or visit <http://www.mimesweeper.com/products> and select MAILsweeper for Exchange 2000.

MAILsweeper Fact Sheet
MAILsweeper Data Sheet
Reporting Data Sheet
Savings Analysis Tool – available at www.mimesweeper.com/roi
MIMESweeper Family Product Guide