

---

# MAILsweeper 4.2 for SMTP Reviewer's Guide

---

February 2001



**For more information, contact:**

Anne Marshall  
Public Relations Manager  
Baltimore Technologies  
(425) 460-6018  
[Anne.Marshall@baltimore.com](mailto:Anne.Marshall@baltimore.com)

---

---

# Contents

<a href="#">Introduction</a> .....	3
<a href="#">Product Background</a> .....	4
<a href="#">The MIMESweeper Product Family</a> .....	4
<a href="#">Potential Security Threats Resulting From Corporate E-mail Access</a> .....	4
<a href="#">How MAILsweeper Works</a> .....	5
<a href="#">Design Goals and Key Features</a> .....	5
<a href="#">Basic System Requirements</a> .....	10
<a href="#">Installation and Setup Instructions</a> .....	12
<a href="#">Installation from CD</a> .....	12
<a href="#">Installation via Web Download</a> .....	12
<a href="#">Setup Instructions</a> .....	12
<a href="#">License Key Installation Instructions</a> .....	13
<a href="#">Policy Setup, Editing and Creation Instructions</a> .....	13
<a href="#">Downloading and Applying Sample Policies</a> .....	14
<a href="#">Editing a Policy</a> .....	15
<a href="#">Creating a Policy from Scratch</a> .....	16
<a href="#">How to Test a Policy</a> .....	18
<a href="#">Support / Customer Help</a> .....	19
<a href="#">Appendixes</a> .....	19

---

# MAILsweeper 4.2 for SMTP Reviewer's Guide

## Introduction

This guide is designed to allow users to evaluate MAILsweeper 4.2 for SMTP. MAILsweeper is a member of the Baltimore Technologies MIMESweeper family of content security solutions.

In recent years, electronic messaging has become critical to internal and external business communications, and the volume of e-mail sent has grown exponentially. International Data Corporation (IDC) predicts that daily e-mail traffic worldwide will grow from 2.1 billion messages in 1998 to 7.9 billion in 2002. IDC also predicts that 35 billion e-mail messages will be sent every day by 2005.

The ubiquity of e-mail messaging has enormous network security and legal implications for any enterprise. Large organizations are particularly vulnerable to network-based threats, due to the size of their networks and the number of employees capable of sending out or receiving damaging e-mail. Recent cases such as BubbleBoy, Melissa and LoveBug have highlighted the damage that virus infection can cause to e-mail networks. Other high-profile cases, such as the circulation of pornography at Dow Chemical (Computerworld), have demonstrated that improperly used e-mail could cause damage to a company's reputation.

MAILsweeper 4.2 for SMTP is the latest release of Baltimore Technologies' flagship content security product. It is the premier solution for mission-critical e-mail security both for large-scale corporate networks as well as for smaller businesses.

Three primary attributes describe why MAILsweeper 4.2 is the most comprehensive, reliable and powerful e-mail security solution on the market today.

- **Scalability.** MAILsweeper is designed from the ground up for enterprise-level performance, increased resilience, compatibility with Windows 2000, and comprehensive reporting and auditing features.
- **Manageability.** MAILsweeper is easy to administer regardless of a network's size, thanks to a design based on policy management, integration with LDAP directories, remote management capabilities and simplified installation.
- **Flexibility.** MAILsweeper is the most comprehensive and flexible content security solution available. No other package provides so many solutions to security issues facing e-mail networks. MAILsweeper provides extremely granular analysis via advanced tools, increased resistance to "Denial of Service" attacks, multiple-language support and additional functionality for image analysis, policy-based encryption and message archiving.

This reviewer's guide explains the design goals and key features of MAILsweeper 4.2, and provides simple instructions for exploring its capabilities and benefits.

## Product Background

MAILsweeper 4.2 for SMTP is a member of the Baltimore Technologies MIMESweeper family of products. Baltimore Technologies is a global leader in e-security. MIMESweeper, launched in 1995, was the first product on the market to scan e-mail and attachments for content threats. MIMESweeper products address the full range of security threats posed by e-mail and Internet systems.

### The MIMESweeper Product Family

MAILsweeper is the MIMESweeper solution for content security of e-mail. It is available in specific versions for SMTP, Microsoft Exchange and Lotus Domino. The MIMESweeper family, including WEBSweeper for Web-transmission security, covers the broad range of content security threats faced by organizations today.

Baltimore also makes add-on modules that extend MAILsweeper's functionality. The modules are PORNsweeper, which analyzes messages for inappropriate images, SECRETsweeper for policy-based encryption, and Archivist, which enables policy-based message archiving.

### Potential Security Threats Resulting From Corporate E-mail Access

The dangers resulting from corporate e-mail access fall into two primary areas: network integrity threats and business integrity threats.

**Network integrity threats** affect the IT infrastructure in a way that compromises system operations or performance. Administrators must be on continual alert to protect against e-mail content that can affect the availability of IT systems, including:

- Viruses and malicious scripts
- Bandwidth-hogging oversized attachments
- Unauthorized e-mail relay
- E-mail-based denial-of-service attacks

**Business integrity threats** damage a company's bottom line and ability to compete. In order to maintain business integrity, corporate executives and administrators must be vigilant for e-mail threats that can affect an organization's business viability. These can include:

- Unauthorized distribution of confidential information and trade secrets
- Lawsuit-inducing offensive or harassing e-mail messages
- Productivity loss from network downtime, spam, games, jokes and other nonbusiness uses
- Damage to reputation from inappropriate e-mail use

## How MAILsweeper Works

MAILsweeper provides for extensive policy-based management of e-mail. Policies can be configured to specify who is allowed to send and receive what content, as well as what happens when a rule is violated. This allows granular control of this vital business tool and gives administrators the flexibility they need to deal with today's e-mail-related business issues.

At the most fundamental level, policy implementation depends on who is sending and receiving a given message. Policies can be further refined according to the content of messages, file type or keyword phrases. A policy itself is composed of scenarios, which perform the content security operations. Scenarios categorize messages into Classifications, which then determine how the messages are each dealt with.

MAILsweeper processes e-mail messages in four phases:

1. When MAILsweeper first receives the message, the policy is identified by the sender/recipient route, and the appropriate policy is applied.
2. Next, the message is broken down into its components. For instance, if you receive an e-mail message with a Microsoft Excel spreadsheet that has a Microsoft Word file embedded in it, MAILsweeper breaks down the document until all the data is in its basic state. *This recursive disassembly of a message can occur up to 50 layers deep if necessary.*
3. Each data component is analyzed according to policy.
4. After analysis, viruses are cleaned using the organization's configured third-party anti-virus tool, and the parts are reassembled.
5. Finally, the message is classified, meaning that the appropriate classification actions are applied to that message, whether it is delivery, quarantine, notification, archiving, or a number of other possible actions. MAILsweeper also gives organizations the option to append legal disclaimers to e-mail, automatically archive e-mail messages and attach informational messages.

## Design Goals and Key Features

**Design goal: MAILsweeper is the premier enterprise-level solution for e-mail security.**

MAILsweeper 4.2 for SMTP is designed to address the e-mail security needs of large-scale enterprises as well as smaller networks. One important new modification is that MAILsweeper for SMTP can now be installed in a clustered configuration that shares a single policy. If there is a failure in any of the three services in any MAILsweeper system, the services continue to run on other MAILsweeper systems within the same array, ensuring that mail can still be safely processed and delivered. MAILsweeper clustering is highly scalable, enabling e-mail servers to be easily added as a network grows. This means both that administrative costs are reduced and that high availability is achieved.

This latest version of MAILsweeper has been designed to work with Windows 2000 Professional and Windows 2000 Server. The Windows 2000 operating system provides a more manageable, robust and scalable platform.

Finally, comprehensive real-time reporting and scalable auditing features have been built into MAILsweeper. Graphical reporting menus give you up-to-the-minute reports on potentially destructive e-mail content and attachments by type, number, data volume, date and time. Administrators can see at a glance the types of incoming and outgoing e-mail content flowing through the network based on the rules that have been set in the easy-to-configure templates. This information can be used to:

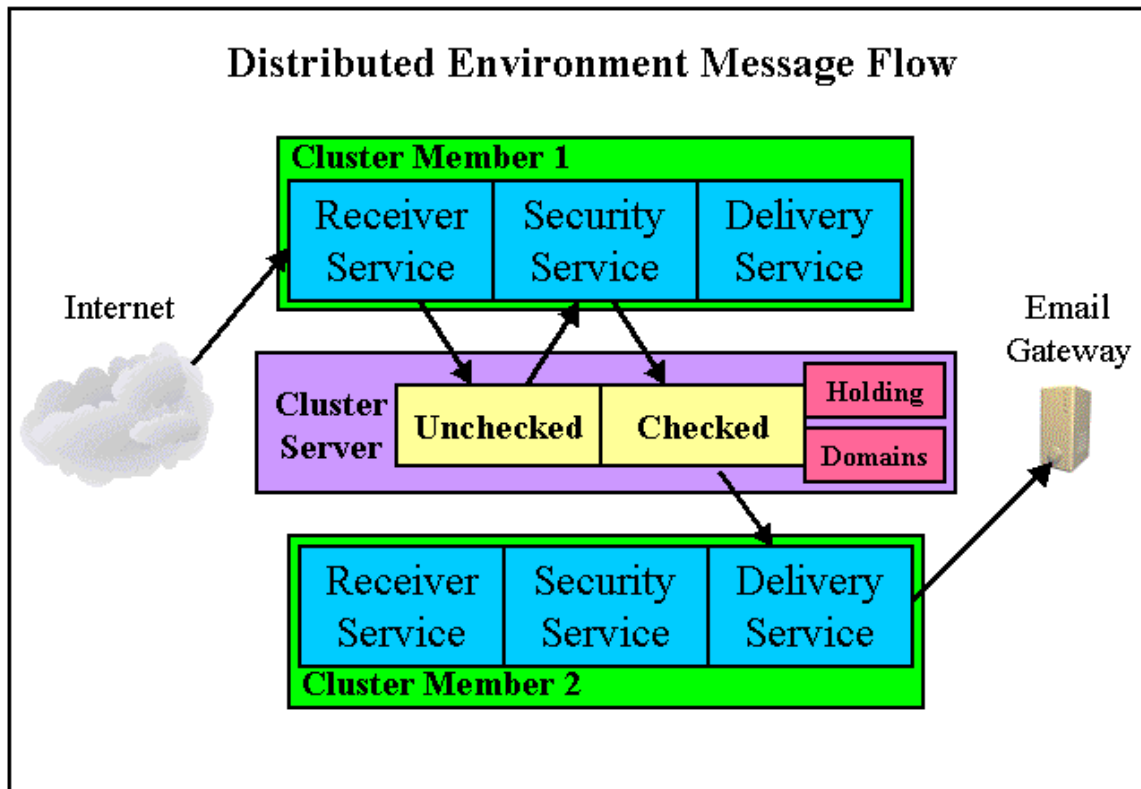
- Monitor threatening e-mail content in order to establish a sound company e-mail policy for optimal network performance and minimal legal exposure.
- Fine-tune filtering scenarios to achieve the most effective defense against the kinds of e-mail content that threaten a network.
- Quickly demonstrate MAILsweeper's return on investment with graphical illustrations of the volume of potentially destructive e-mail content entering and leaving the network.

**Key features:**

- **Scalability and increased resilience via clustering.** Message processing can be distributed across multiple systems, but still operate as a single system enforcing a single policy. This provides resilience through automatic failover between servers and transparent load sharing. The configuration consists of one server with multiple cluster members, each running identical Receiver, Security, and Delivery services. Because the cluster members are configured identically, a message is processed in the same way regardless of which cluster member does the processing.

The machines work cooperatively to process a large volume of message traffic, providing a more efficient system than a single machine, and enabling enhanced scalability. As many servers can be deployed as needed to cope with normal and peak server loads.

The scalability, resilience and ease of management provided by a distributed configuration result in higher availability, less network downtime, lower administrative costs and increased flexibility of deployment. This ultimately saves IT/MIS departments time and money, and safeguards mission-critical e-mail.



*Figure 1. An example of mail flow through a MAILsweeper clustered environment.*

- **Compatibility with Windows 2000 Professional and Windows 2000 Server.** Administrators can reduce the total cost of ownership for MAILsweeper by taking advantage of new hardware and the performance improvements of Windows 2000.
- **Enterprise-level message auditing.** Message auditing has been redesigned to scale to the needs of larger customers. Auditing using the Auditor for Reporting feature enables logging to a Microsoft SQL Server 7 database via ODBC. A processing summary is available through the management interface and/or as a notification to administrators.
- **Comprehensive reporting.** There are 23 preset reporting formats, including traffic volumes, top 10 senders or recipients, e-mail classifications and types of attachments. The reports can be exported to a number of formats, including e-mail, HTML, various spreadsheets and raw data. Some examples of report types are:
  - Policy Usage: Summarizes the volume of incoming and outgoing messages detected by the MAILsweeper policy scenarios.
  - Message Throughput: Shows the average number of messages and the average volume of message data processed by MAILsweeper per hour.
  - Data Type Summaries: Show which data subtypes of e-mail-borne content and attachments are being detected by the MAILsweeper policies. Users can drill down for summaries of specific data types (e.g., documents or images) or track data types detected by date or hour.

- **Message Classification:** Shows the number of e-mail messages of various classifications (e.g., encrypted, profanity, spam) detected over a specified time period. Shows the volume of data in the detected messages of various classifications.
- **Processing Performance:** Shows the average time that it takes for receipt of a message, and the time for MAILsweeper to analyze incoming and outgoing message content.

### **Design Goal: MAILsweeper is easy to administer.**

MAILsweeper's design is based upon the concept of policy-based management, whereby network administrators have tight control over who uses the e-mail system and for what purposes. Policy management has been improved with version 4.2 as a result of the new clustering capability. Previously, MAILsweeper could only work with separately managed copies of a policy on separate servers, whereas MAILsweeper for SMTP 4.2 can share one policy among several servers. The multiple systems can be managed from a single management console, reducing the duplication of administrative effort. Furthermore, MAILsweeper has now been integrated with LDAP directories. This prevents the additional administrative overhead of re-creating group address lists.

The ability to set up multiple quarantine areas for data carrying viruses, inappropriate content, confidential information or unwanted information is essential to content security. Equally important is a means to dispose of such threats easily and reliably, with minimal involvement from the e-mail system manager. Sixty-four quarantine areas are now supported in MAILsweeper. Quarantine areas are secured by Windows NT user permissions and are accessed via the management console, simplifying and distributing message area management.

MAILsweeper also now provides processing information to Windows NT Performance Monitor. This greatly reduces the day-to-day management overhead and enables administrators to react more swiftly to changes in activity and trends. Finally, version 4.2 has been designed to be easy to install and configure with sample policies. These policy templates let administrators experience the benefits of MAILsweeper for SMTP in minutes, instead of starting from scratch.

#### **Key features:**

- **Improved policy-based management.** Policies can be created and implemented by group, department and/or individual, for both incoming and outgoing messages. Policies can be defined for message classification, quarantine and disposal. Subgroups or individuals automatically inherit policies created at a higher level.
- **Integration with LDAP directory servers.** MAILsweeper can query LDAP servers to obtain lists of e-mail addresses used in defining the content security policy. MAILsweeper keeps a cached copy of these lists and updates them as often as the user specifies. Filtering expressions can be used to further specify the address lists a policy uses. Different legal disclaimers can be sent out on messages based on functional groups (e.g. Human Resources, sales, marketing, etc.) by creating a separate policy folder for each group, defined by an LDAP query or a manual user list.
- **Remote Management Capability.** Version 4.2 has been designed as a Microsoft Management Console snap-in. This allows management of services and message areas, and is secured by Windows NT security.

- **Windows NT Performance Monitor Support.** Operation functions can be observed, including alerts of abnormal conditions (e.g. overload, failed messages), and improved visibility of abandoned or stuck messages.
- **Easy policy setup using sample policies.** Sample policies are free, preconfigured policy templates that system administrators can download and set up using a simple utility. Several common policies are available to establish immediate protection, or to provide a baseline on which customized policies can be built.

### **Design Goal: MAILsweeper is the most comprehensive content security solution available.**

MAILsweeper for SMTP 4.2 is much more than an anti-virus or text-analysis tool. It provides a single, easy-to-manage, cost-effective solution that performs at an enterprise level. MAILsweeper extends anti-virus functionality of scanners and goes beyond them to address key business issues such as legal liability, confidentiality and obscenity. Text-based e-mail analyzers cannot compete with the comprehensive protection offered by MAILsweeper for network integrity issues, or provide the same level of in-depth analysis.

MAILsweeper deconstructs data by “recursive disassembly,” breaking down complex data into its basic form in order to analyze it for threats. This is particularly important for e-mail attachments, where viruses can be disguised. This design boosts the power of a company’s anti-virus software, allowing virus scans to catch hidden viruses. Furthermore, by analyzing words, syntax, sentence and document structure in e-mail attachments, MAILsweeper is designed to stop junk e-mail, loss of confidential or proprietary information, and prevent inappropriate content and loss of productivity from e-mail misuse. Additional data types are now recognized, including MP3, AIFF, WAV and graphics file formats.

Because the number and sophistication of malicious “Denial of Service” attacks has grown substantially, this version of MAILsweeper has been reinforced against such attacks. Non-U.S. characters are now supported. In fact, MAILsweeper is the only full content security solution currently available for the Japanese market. Word and expression lists are now configurable by language, and legal disclaimers can now use language-specific characters. Finally, MAILsweeper has been designed as a platform to which modules providing additional functionality can be added, including PORNsweeper for image analysis, SECRETsweeper for encrypted e-mail and MAILsweeper Archivist for SMTP.

### **Key Features:**

- **Recursive disassembly boosts anti-virus power.** Other anti-virus solutions tend to scan messages for known viruses in top-level attachments. No other solution successfully deconstructs multiply compressed and embedded files to discover the viruses inside messages to the level of MAILsweeper. By providing full disassembly, decoding and decompression, MAILsweeper boosts the power of third-party anti-virus software. Administrators can continue to use their installed anti-virus software or even integrate several products for maximum protection.
- **Enhanced analysis tools.** Improved data type recognition has been implemented for the scenarios, improving speed, resilience, recognition and extraction of embedded objects. Advanced features such as Pattern Matcher and Filename Blocker detect inappropriate attachments by name, type and binary pattern. Pattern Matcher is user-configurable for specific files or types, e.g., confidential computer-aided design files. It allows administrators to block almost any type of file by searching for a binary “fingerprint.” Filename Blocker detects files by name, type or partial name.

- **Increased resistance to “Denial of Service” attacks.** This version of MAILsweeper is reinforced against the typical methods of overloading servers by the addition of user-configurable limits on the SMTP protocol. For instance, to prevent hackers from opening a number of MAILsweeper dialogs so large that it causes e-mail servers to be heavily loaded or crash, MAILsweeper can limit the number of connections it will accept. This results in higher availability and improved resistance to malicious attacks.
- **User-definable scenarios add flexibility.** Administrators can link other programs into MAILsweeper, add customizable analysis or actions to MAILsweeper’s comprehensive content security, add different anti-virus or mobile code scanners, and process e-mail according to user applications (e.g., SCRIPT.EXE Script Tool to detect malicious VBA and HTML scripts.)
- **Foreign language support, including Japanese.** Text analysis word and expression lists are now configurable by language, such as profanity lists in Japanese, English, Spanish, German and French. These lists can now be shared throughout the policy tree, which makes for easier management and less administrative overhead. In addition, legal disclaimers can now use language-specific characters such as Japanese kanji/kana characters instead of default disclaimers that support only US-ASCII characters.
- **Additional functionality with PORNsweeper, SECRETsweeper and MAILsweeper Archivist.** Organizations can now extend MAILsweeper’s scope with add-on modules:
  - PORNsweeper 1.1 allows organizations to analyze images for offensive material, control image distribution, deter circulation of inappropriate content, avoid sexual harassment lawsuits, avoid excessive file circulation.
  - SECRETsweeper provides secure site-to-site e-mail with policy-based encryption, enabling organizations to apply a content security policy to encrypted e-mail, validate digital signatures, manage the use of revoked or untrusted certificates, encrypt for particular recipients, and interoperate with other S/MIME gateways.
  - MAILsweeper Archivist enables messages to be preserved by policy-based archiving, long-term storage, tracing using a simple Web-search client, and filtering of mission-critical information as it passes through the e-mail system.

## Basic System Requirements

To deploy MAILsweeper 4.2 for SMTP, the following minimum requirements apply:

- Processor dependent on configuration and number of users; minimum recommendation Pentium II 400 MHz or equivalent
- 500 MB free space on NTFS partition for installation
- 500 MB free space in Temp directory
- 128 MB memory
- Microsoft Windows 2000 Professional or Server with Service Pack 1, or Windows NT Workstation or Server version 4.0 with Service Pack 5
- Internet Explorer 5
- Microsoft Management Console 1.2

- Outlook 98 mail client
- Microsoft data access components 2.1
- TCP/IP networking
- Access to CD-ROM or network for installation
- Microsoft SQL Server 7 for reporting

## Installation and Setup Instructions

**NOTE:** MAILsweeper cannot be installed on a system that is running any other MIMESweeper product. Other MIMESweeper products must be uninstalled before installing MAILsweeper.

### Installation from CD

1. Install the disk in your CD-ROM drive. If autoplay is disabled, then browse to  
install\msssmtp42\_1\setup.exe
2. From the initial display screen, click on the Products menu. Select MAILsweeper for SMTP. Click on Installation.
3. Click on Install MAILsweeper for SMTP Version 4.2.
4. Follow the Setup Instructions below.

### Installation via Web Download

1. Go to <http://www.mimesweeper.com/>. Choose the MIMESweeper server closest to you. Click on the **Download** menu item at the top of the page. On the page entitled "Download," click on **MAILsweeper for SMTP version 4.2 (18MB)**.
2. On the page entitled "Welcome to the MIMESweeper Membership Center", in the **Become a Member** box, follow instructions to create a new account. Fill in the form.
3. On the page entitled MIMESweeper Membership Center, under **Tools**, click **Download Software**.
4. From the Download page, under **E-mail content security**, check the box for **MAILsweeper for SMTP (Version 4.2\_1)**. Click **Download**.
5. On the page entitled "Thank you for choosing to download our MIMESweeper software," under **Download MAILsweeper for SMTP 4.2\_1 from:** choose the server nearest you. Follow the File Download instructions, saving the file to a local folder. Unzip the file (smtp42\_1.zip) to a new folder, preserving the directory structure. If you're using PKUNZIP, use the -d command line option. If you're using WinZip, use the Extract command, making sure that the Use Folder Names box is checked.

### Setup Instructions

1. Navigate to the folder and click on **setup.exe**. Follow the wizard instructions.  
**NOTE:** this setup requires the Windows Installer service. If you're running Windows 2000, you will already have this service. If you're running Windows NT 4, Windows Installer will automatically install itself and require a reboot before setup can continue.

2. Follow the Installation Wizard instructions.  
**NOTE:** the Destination Folder must be on an NTFS partition.  
Install the Full product.
3. On the "Network Layout" window, you have two options.
  - If you have an internal e-mail system you'd like to use to review this product: check the box under **Incoming Mail** to forward all incoming mail to a particular host. Enter the IP address for your internal mail SMTP gateway. You also have the option to forward mail to an outbound host by checking the box under **Outgoing Mail**.
  - If you do not have an internal e-mail system, leave the boxes unchecked.
4. Continue to follow the wizard instructions. You will need to reboot your system.

## License Key Installation Instructions

You will need to have an evaluation license key in order to use this product.

To install your license key and start your services:

1. Launch the MAILsweeper for SMTP Console by clicking Start>Programs>MAILsweeper for SMTP>MAILsweeper for SMTP Console.
2. Under Console Root, expand the MIMESweeper Policy Editor. Right-click on **Licenses**. Select **New>MAILsweeper for SMTP License**.
3. Follow the New License wizard instructions. Enter Company name, Key and Serial number.
4. Name the license, giving it the name of your choice.
5. Once the license is installed, you can start the Services:  
under Console Root, expand Local MIMESweeper Manager. Select **Services**. On the right column, right-click on each service and select **Start Service**.

## Policy Setup, Editing and Creation Instructions

MAILsweeper now includes a simple way for you to get up and running quickly by using the free Sample Policy utility that you can download from our Web site. You can use it to apply one of a number of sample policies, which are templates created for general use. You can edit these policies to suit your own needs. Alternatively, you can create your own policies without using the sample policies. Following are instructions on how to do each one, followed by a section on how to test a policy.

Policies contain Classifications and Scenarios, each of which is customizable through the editing process.

**Scenarios** are the conditions that determine how the mail is filtered. For example, a scenario can detect a file of a specific size, or can detect text containing specific keywords or phrases.

**Classifications** determine what happens when a scenario's conditions are met. These events consist of *actions*, whereby a message is delivered, parked, quarantined or saved, or *notifications*, whereby a particular user is notified, a log entry written, or an alert is generated.

**NOTE:** each time you add or change a policy, you must stop and restart the security service.

## Downloading and Applying Sample Policies

1. Go to <http://www.mimesweeper.com/>. **NOTE:** this Web site is subject to change. Choose your closest MIMESweeper server. Click on the **Download** menu item at the top of the page. On the page entitled "Download," under **Extras, Utilities and Sample Policies**, click **Download**.
2. On the page entitled "Welcome to the MIMESweeper Membership Center," under Existing Members, enter your e-mail address and password. Click **Login**.
3. On the page entitled "Thank you for choosing to download our MIMESweeper software," choose the server nearest you.
4. Follow the File Download wizard instructions. Unzip the file to a temporary directory. Browse to the file and double-click **SPSetup.exe**.
5. Follow the InstallShield Wizard instructions.  
**NOTE:** if the MAILsweeper for SMTP Console is still open, close it.
6. After the wizard is finished, the PolicyMate 2.02 screen automatically comes up. You can also invoke it separately by clicking Start>Programs>MAILsweeper for SMTP>Sample Policies.
7. On the PolicyMate 2.02 screen, under Available Policies, select a policy that you'd like to apply. The description of each policy will appear on the Information Panel.
8. Click **Apply Policy**. Confirm by clicking **YES**.  
**NOTE:** Applying a policy overrides the current settings. If you'd like to revert back to your current settings in the future, first click **Save Current Configuration**.
9. You can now open the MAILsweeper SMTP Console by clicking Start>Programs>MAILsweeper for SMTP>MAILsweeper for SMTP Console. Under Console Root, expand MIMESweeper Policy Editor. Expand MAILsweeper for SMTP. Expand Policies. The policies that you have selected will appear under Classifications and Scenarios.

**NOTE:** In order for a Policy to take effect, you must restart the Security Service. Under Console Root, expand Local MIMESweeper Manager. Select **Services**. On the right column, right-click on the Security Service. Select **Stop Service**. Confirm by clicking **Yes**. Wait until the Status indicates "Stopped." Then, right-click again on Security Service and select **Start Service**.

## Editing a Policy

You can easily edit the sample policies or any existing policy. Policies can be customized by editing their scenarios and classifications. As an example, you will edit a scenario so that e-mail messages with attached images larger than 256K are blocked. You will then edit a classification to notify you by e-mail when a Scenario's conditions have been met, and forward the message as an attachment to the administrator.

1. Follow the instructions 1 – 6 above for **Downloading and Applying the Sample Policies**.
2. On the PolicyMate 2.02 screen, under Available Policies, select **Basic**. Click **Apply Policy**. Confirm by clicking **Yes**. Click **Exit** to close PolicyMate 2.02.
3. Open the MAILsweeper Console by clicking Start>Programs>MAILsweeper for SMTP>MAILsweeper for SMTP Console. Under Console Root, expand MIMEsweeper Policy Editor. Expand MAILsweeper for SMTP. Expand Policies. Select **Scenarios**.
4. On the right column, right-click on **Block Images**. You will edit this scenario to apply only to images above 256K in size. Select **Properties**.
5. On the Block Images Properties screen, click on the **Size** tab. Under Block, select **On size**. Enter 256. Click **OK**.
6. Now you will edit a classification to add a notification to you that an image over 256K has been detected. Under Console Root, under Policies, expand Classifications. Select **Images**. Note that Quarantine Images is listed on the right column. This indicates that all images will be quarantined that meet the criteria of scenarios that reference this classification. In this case, all images greater than 256K will be quarantined.
7. Right-click on **Images**. Select **New>Notification>Inform**.
8. Follow the New Notification wizard. On the Sender screen, leave "Server" as the default selection. On the Recipients screen, under Type, click twice on the first line. Select **To**: if it is not selected.
9. Under Address, click twice. Enter your own e-mail address. (**NOTE**: you can also enter any standard token such as %ADMIN%, %SENDER%, %RCPTS%, etc.)
10. Hit Enter. Click **Next**.
11. On the Subject screen, put in a line of text such as "Large Image Detected." Click **Next**.
12. On the Body screen, under Body Text, put in a message such as "A message was received containing an image larger than 256KB. It will be quarantined." Click **Next**.
13. On the Character Set screen, leave the setting as is. Click **Next**.
14. On the Attachments screen, check the box marked Forward Attachments. Leave "In original form" selected. Click **Next**.

15. Name the Notification with a name such as "Notify Admin." Add a comment such as "This policy was added on 1/1/2001." Click **Next**. Click **Finish**. Notice that under Console Root, under Classifications, if you select Images, the new Notification is listed.

**NOTE:** In order for an edited or added scenario or classification to take effect, you must restart the security service. Under Console Root, expand Local MIMESweeper Manager. Select **Services**. On the right column, right-click on Security Service. Select Stop Service. Confirm by clicking **Yes**. Wait until the status indicates "Stopped." Then, right-click again on Security Service and select **Start Service**.

## Creating a Policy from Scratch

As an example of the flexibility and power of MAILsweeper, you will create a policy in response to external warnings about a special kind of virus we are calling the January worm, which is hidden in a Visual Basic Script file attached to an e-mail message. We will use two different methods (scenarios) to detect the worm: text analysis and filename block. Both methods will result in the same classification, or series of events taking place upon detection.

1. Open the MAILsweeper Console by clicking Start>Programs>MAILsweeper for SMTP>MAILsweeper for SMTP Console. Under Console Root, expand MIMESweeper Policy Editor. Expand MAILsweeper for SMTP. Expand Policies.
2. First, create a classification that quarantines the message and notifies the administrator and sender about the worm. Expand Classifications. You will see the default classifications listed for general use. (All messages fall into one of these classifications as they go through the system, with the default classification being "Clean." "Dirty In" is a general classification for inbound objects that have any kind of undesirable content. "Dirty Out" performs the same function for outbound content.) Create a classification by right-clicking on Classifications. Select **New>Classification**.
3. Follow the New Classification wizard. On the Type screen, make sure **Exclusive** is selected. An exclusive classification is one that is triggered by a scan. An Inclusive classification is an action that happens under all circumstances, such as Archiving.
4. On the Name screen, enter the name "January Worm." Enter the Comment "Created on January 9, 2001." Click **Next**. Click **Finish**.
5. On the Console screen, under Classifications, you'll see the new classification listed toward the bottom, above the default Classification "Clean." For any given message, the classifications are applied in the order that they appear in this list. The new classification needs to be moved to the top of the list so that it is followed first for any messages that meet the "January worm" scenarios we are about to create. Simply right-click on **January Worm** and select **Promote**. Repeat until January Worm is at the top of the Classifications list.
6. Select **January Worm**. Note that nothing appears on the right column. With such an empty classification, the default action is to delete the message. Instead, you will configure the classification to quarantine such messages in a quarantine area that you will create. (You can create up to 64 quarantine or park areas.)
7. First you must create a quarantine object. Under Console Root, under Policies, select **Message Areas**. Right-click on Message Areas and select **New>Quarantine Area**.

8. Follow the New Message Area wizard instructions. On the Location screen, click on **New Folder**. Name the folder "January Worm messages". Click **Next**.
9. On the Permissions screen, add a user by clicking on the grayed-out box on the same line as "Specify user access rights" (it has pop-up text "Add User.")
10. Now you will specify the permissions for who can view the message area. On the Add Users and Groups screen, select **Administrators**. Click **Add**. Click **OK**. Click **Next**. On the Delete screen, leave blank.
11. On the Name screen, enter the name "January Worm Messages." Enter the comment "Created on January 9, 2001 in response to January Worm warnings." Click **Finish**.
12. Now you are ready to add the quarantine object to the new Classification. Under Console Root, under Classifications, select **January Worm**. Right-click on January Worm and select **New>Action>Quarantine**.
13. Follow the New Action wizard instructions. On the Quarantine screen, select **January Worm Messages** from the Quarantine list.
14. On the Name screen, enter the name "Quarantine". Leave comment blank. Click **Next**. A new action has now been created. Click **Finish**.
15. Now you will create a notification object that will inform the administrator and sender of the worm intrusion. Select **January Worm**. Right-click on January Worm. Select **New>Notification>Inform**. Follow the New Notification wizard instructions. On the Recipients screen, click twice under Type so that **To:** is showing. On the same line, under Address, click twice. Enter "%ADMIN%". This is a token that will automatically reference the default administrator within MAILsweeper ([postmaster@<yourdomain.com>](mailto:postmaster@<yourdomain.com>)).
16. On the next empty line under Type, click twice so that **To:** is showing. On the same line, under Address, click twice. Enter "%SENDER%". Click **Enter**. Click **Next**.
17. On the Subject screen, enter "Worm detected". Click **Next**. On the Body screen, enter "A message containing the potentially dangerous January worm has been detected. The message has been quarantined." Click **Next**.
18. On the Character Set screen, leave as is. Click **Next**. On the Attachments screen, leave unchecked the box marked "Forward Attachments." Check the box marked "Include results from Text Analysis."
19. On the Name screen, enter the name Notify Admin and Sender. Click **Next**. Click **Finish**.
20. Now you will create two scenarios for text analysis and filename blocking. First you will create a text-analysis scenario. Under Console Root, Under Policies, expand Scenarios. To apply to both incoming and outgoing mail, you will create a scenario at the Scenario root level. Right-click on Scenarios. Select **New>Scenario>Text Analyzer**.
21. Follow the New Scenario wizard instructions. On the Options screen, leave all boxes checked. On the Expression List screen, select **Script Commands** from the Drop-down list. Click **Next**.
22. On the Thresholds screen, leave the figures as is. Click **Next**.

23. On the Scan Areas screen, leave All Areas selected. Click **Next**.
24. On the Threshold exceeded Classification screen, under Exclusive Classifications, select **January Worm**. Click **Next**. On the Name screen, enter the name **Detect January Worm via Text Analysis**. Click **Next**. Click **Finish**.
25. Now you will create a filename blocking scenario. Under Console Root, select Scenarios. Right-click on Scenarios. Select **New>Scenario>File Blocker**.
26. Follow the New Scenario wizard. Accept the defaults on the Options screen. On the File Name screen, under File Mask, enter "January.vbs." Click **Next**.
27. On the Blocked Classification screen, select **January Worm**. Click **Next**.
28. On the Name screen, enter the name "Detect January Worm via Filename block." Click **Next**. Click **Finish**.
29. Now you need to restart the Security Services to make the changes effective. Under Console Root, expand Local MIMESweeper Manager. Select **Services**. On the right column, right-click on the Security Service. Select **Stop Service**. Confirm by clicking **Yes**. Wait until the Status indicates "Stopped." Then, right-click again on Security Service and select **Start Service**.

## How to Test a Policy

This section describes how to test the functionality of a sample policy or one you have edited or created from scratch.

1. Configure an SMTP client such as Microsoft Outlook Express so that your outgoing mail server uses the MAILsweeper server IP address.
2. Compose a message containing content that you'd like to test.
3. Send the message.
4. Open the MAILsweeper for SMTP Console. Under Console Root, expand Local MIMESweeper Manager. Expand MAILsweeper for SMTP. Select **Recent Messages**. On the right hand side you will see a log of all messages that flow through MAILsweeper. Note the Classification column. If the message does not trigger a policy, its Classification entry will be "Clean." If the message triggers a policy, its Classification entry will be the name that has been defined for messages that trigger the policy.
5. If you'd like to view a message that has been quarantined, from the MAILsweeper Console, under Console Root, under Local MIMESweeper Manager, under MAILsweeper for SMTP, expand Message Areas. Select the Message Area you'd like to view. On the right hand side will be a list of messages contained in that quarantine area. Right-click on a message you'd like to view. Select **Open**.
6. On the Message tab, you can see the message itself. On the Analysis tab, you can see the scans that were applied to each piece of the message. On the Raw Data tab, you can see the actual message with all headers. On the Text Analysis tab, (this is

only there if text analysis triggered a policy) you can see the search expressions found in the message.

## 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 resolve problems or dispatch/ escalate them where appropriate. Our Technical Support team members insure that all major technical support issues are properly addressed through proper training and a strong knowledge of the MIMESweeper products 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

MAILsweeper Fact Sheet  
MAILsweeper Data Sheet  
Reporting Data Sheet  
Savings Analysis Tool – available at [www.mimesweeper.com/roi](http://www.mimesweeper.com/roi)  
MIMESweeper Family Product Guide