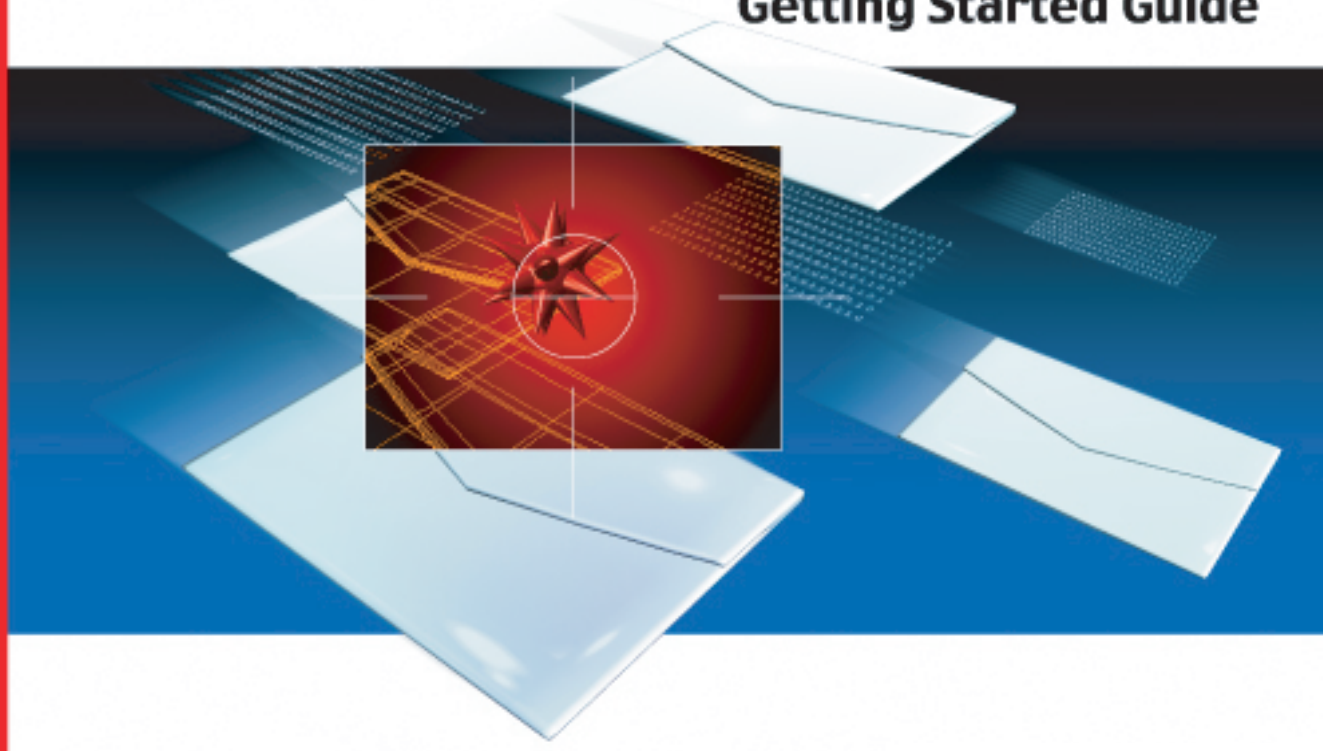
TREND MICRO™

ScanMail™ 5

eManager™ for Microsoft™ Exchange

Content Security for your Microsoft™ Exchange and Exchange 2000 Messaging and Collaboration Platforms

Getting Started Guide



TREND MICRO™

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

http://www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

http://www.trendmicro.com/license

Document Part No. SEEM50893/11101

Release Date: January 2003

Protected by U.S. Patent No. 5,951,698 and 5,889,943

The Getting Started Guide for Trend Micro™ ScanMail™ eManager™ for Microsoft Exchange is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and online Solution Bank at Trend Micro's Web site.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at **docs@trendmicro.com**. Your feedback is always welcome. Please evaluate this documentation on the following site:
http://www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 3: Spam Filtering

Chapter 4: Content Filtering

Chapter 5: Rule, Import, and Log Files

Chapter 6: Quarantine Directory, Spam Information, and Technical Support

Appendix A: Control Manager Agent for ScanMail eManager

Index

Chapter 1

Introducing Trend Micro™ ScanMail™ eManager

Trend Micro ScanMail eManager for Microsoft Exchange works to reject spam mail bound to or sent from users of the corporate LAN. Rejected spam mail is not processed by the Exchange server and it does not end up in your clients' mailboxes. As new spam is written and released onto the public, Trend Micro monitors and collects telltale blocking information and incorporates it into new Anti-Spam Rule and Import files.

In addition, ScanMail eManager lets the administrator create their own anti-spam filter Rules. Rules can be created based on the message header fields, subject, and/or attachment file name. In addition, rules can be configured to block or include messages based on message body or attachment size. Any number of rules can be created. A message that matches a rule can be blocked (Deleted, Archived, or Quarantined) or designated as a Global Exception.

ScanMail eManager also supports content filtering, which allows you to check inbound and outbound mail for content deemed to be offensive or otherwise objectionable. A content filter Policy represents a group of conceptually related words and phrases that are matched against messages. You can have attachment text filtered for content violations as well. You can use the included content filter policies and also define policies of your own.

ScanMail eManager is comprised of one module that can be installed on any server that is running the ScanMail for Microsoft Exchange core module (ScanMail main program).

This chapter provides an introduction to ScanMail eManager and describes how eManager interfaces with ScanMail for Microsoft Exchange. The topics include:

- Content Management
  - Spam Filtering based on message header, body, and/or attachments
  - Content Filtering based on a more detailed analysis of the message text
  - User-definable keyword lists and anti-keywords
- Tracking Spammers
- Rule and Import Files, which can be updated regularly from Trend Micro
- Anti-Spam Rules
- Content Filter Policies
- Boolean Expressions
- ScanMail for Microsoft Exchange and ScanMail eManager Processing Order
- Summary of New Features

Content Management

ScanMail eManager is completely user-configurable and allows you to filter out spam mail and check inbound and outbound messages for content deemed to be sensitive, offensive, or otherwise objectionable.

Spam Filtering

ScanMail eManager's spam filter quickly evaluates the header and/or content of messages. In particular, it checks the origin of messages to assess whether they are spam (unsolicited commercial email, or UCE), by comparing the header information to a set of user-defined rules. Messages that are found to match the filter rules can be **deleted** or **quarantined** and are not passed to ScanMail for Microsoft Exchange for virus checking. Alternatively, messages can be **archived** (copied to the archive directory), and passed to ScanMail for Microsoft Exchange for virus checking.

Spam rules are completely user-definable and there is no limit to the number of rules you can employ. Trend Micro also provides a comprehensive list (called the Rule File list) of the most flagrant spammers, identified by subject and sender. This list can be updated manually or at scheduled intervals.

Content Filtering

A second function of eManager is the content filter. It performs a more sophisticated analysis of the actual message text. Like the spam filter, the content filter evaluates messages on the basis of user-defined rules. These rule-sets, or *policies*, can be created to check for the use of inappropriate or offensive language, etc. In fact, you can screen for any content *before* it is delivered.

What is Spam Mail?

Spam, (also known as unsolicited commercial email (UCE), and bulk mail) is email, unrequested and unwanted, that is sent to multiple users for the purpose of promoting a business or idea.

Email address lists can readily be bought for as little as $50.00 for 50,000 to 100,000 "verified" addresses, including the service of sending the spam.

Of course, one person’s "spam" may be another person’s "business opportunity" (or the valued chance to "earn a college degree in just two weeks!") Broadly speaking, however, "spam" is used to describe the unwanted and unsolicited commercial email messages promoting tacky Internet sites, products of dubious quality, and get-rich-quick schemes.

The messages are bulk-mailed to hundreds of thousands of people at a time, with the cost of delivery borne largely by the recipient (through the uninvited use of their SMTP servers, Exchange servers, client machines, and, in some cases, a delivery fee charged by the ISP).

Why is Spam Mail Bad?

On the corporate level, where the problem is multiplied by hundreds and thousands, spam is more than a nuisance. It’s a theft of resources, it's costly, and it wastes employee time—for the end user to read and/or delete it, and for the MIS staff to

support the additional burden. By some estimates, currently 15 percent of all Internet email is spam.

- Spam mail is at the very least annoying, but it can also be offensive, wasteful, and illegal.
- Spam blasts can bog down your network, as bandwidth is consumed in the delivery of hundreds of unwanted email messages.
- Spam mail wastes time and is distracting. Just to delete spam, email clients must first identify who the messages are from and what they are about. Even careful users risk deleting legitimate messages while trimming spam from their inbox.
- Spam mail serves no corporate interest, yet uses the corporate Exchange server(s) for processing and delivery. It uses CPU, takes up space on the server hard drive, and on the hard drives of countless end-users. Even when the messages have been deleted, it can take weeks before the messages are permanently deleted by the user when they empty their trash mail, and months for server backups to cycle through.
- Spam mail multiplies the risk of widespread virus attacks by simultaneously exposing many people to the same infected file or URL containing a malicious Java or ActiveX application.

Tracking Spammers

All email from spammers must enter the Internet from somewhere. Part of constructing a good spam filter is identifying where the spam originated from and other telltale bits of information which you can use to construct broad, solid anti-spam rules and profiles.

Rule and Import Files

As new spam is written and released onto the public, Trend Micro monitors and collects telltale blocking information and incorporates it into new **Rule** and **Import** files.

- The **Vendor-provided rule file** is used by the spam filter and contains numerous predefined anti-spam rule-sets.
- **Import files** are used by the content filter and can augment existing policies.

Clearly, it is very important to keep these files up-to-date. New Rule and Import files are published regularly by Trend Micro.

Anti-Spam Rules

Anti-Spam Rules can be defined by entering criteria in any one or all of the following fields:

- To
- From
- cc
- Subject
- File size
- File name

Generally speaking, it is best to create spam-filtering rules by defining only one or two criteria. For example, if you are defining spam-filtering rules that are based on actual spam mail, define the rule using only the mail's **Subject** field, or only the **From** field. The more criteria you specify for any given rule, the less chance there is of stopping similar, but not identical, violations.

Anti-Spam Rules Strategy

When specifying multiple rules in the Current Rules list, we recommend that you employ an inverted pyramid model, wherein you put rules with the broadest reach, or highest probability of matching, at the top of the list. Those that are more narrowly defined (less likely to trigger a match) should be placed towards the bottom of the list. This is the most efficient arrangement because in this way, the filter eliminates the greatest proportion of traffic with the fewest number of evaluations.

Content Filter Policies

A content filter **Policy** represents a group of conceptually related words and phrases that are matched against inbound and outbound messages.

Policies can be created to check mail for any type of content. Examples include:

- Inappropriate language (four letter words, etc.)
- Racial slurs
- Pornography

Only the email message text and non-encoded text/Word attachments are included in content filter comparisons; binary email attachments are not considered. You can create content filter policies to screen for any content.

Example "Free offer" Policy

In this example, three different rules comprise the "Free offer" policy, which is designed to block spam mail purporting to offer ways to make money fast.

> ***Rule 1)*** *money, $$$*
> ***Rule 2)*** *Free offer, hot deal, cash*
> ***Rule 3)*** *free offer, dollars, earn*

The following paragraph matches the rule-sets above:

> *Free Offer — Hot Deal. Make cash fast with a 60 day no-risk money-back guarantee.*

It does not match the first rule. Although it contains the word **money**, it does not also contain the symbol **$$$**.

This paragraph triggers a match because it matches the second rule (it contains the phrase **free offer**, and the phrase **hot deal**, and the word **cash**).

Because it matches the second rule, the third rule is not evaluated. It does not match the third rule. Although it contains the phrase **free offer** and the word **dollars**, it does not also contain the word **earn**.

Since the paragraph is found to match at least one of the three rules that make up the policy, it triggers a match.

Boolean Expressions Implied in the Content Filter

The OR operator is always implied as the connector *between* Keyword lines within a content filter policy. Included synonyms are also implicitly connected via the OR operator. For example, "bargain" is a synonym for the word "deal". Any mail with the term "deal" OR the term "bargain" is a match.

The AND operator is implied *within* a given keyword list. In other words, all keywords on the same line, delimited with a comma, are connected. For example, the entry:

```
"a, b, c"
```

means "a AND b AND c". In the ScanMail eManager Content Filter, you do not use the literal operators "AND", "OR", but rather the placement of the keywords in single versus multiple fields and keyword lists is what dictates their connection.

ScanMail for Microsoft Exchange and ScanMail eManager Processing Order

On a network where both ScanMail for Microsoft Exchange and ScanMail eManager are installed, the processing order is as follows:

1. ScanMail for Microsoft Exchange receives inbound mail and redirects it to ScanMail eManager. This action occurs before virus scanning.
2. In a quick operation, a spam/not-spam evaluation is performed.
3. Message information is compared to the user-defined list of current rules. Mail that is found to match any one of the specified criteria is **Deleted, Archived,** or **Quarantined**, as defined in the matching rule. The message is not compared further. Deleted and quarantined messages are not forwarded to ScanMail for Microsoft Exchange. Archived messages are copied to the archive directory and then forwarded as usual to ScanMail for Microsoft Exchange.

4. The processing order is shown below:

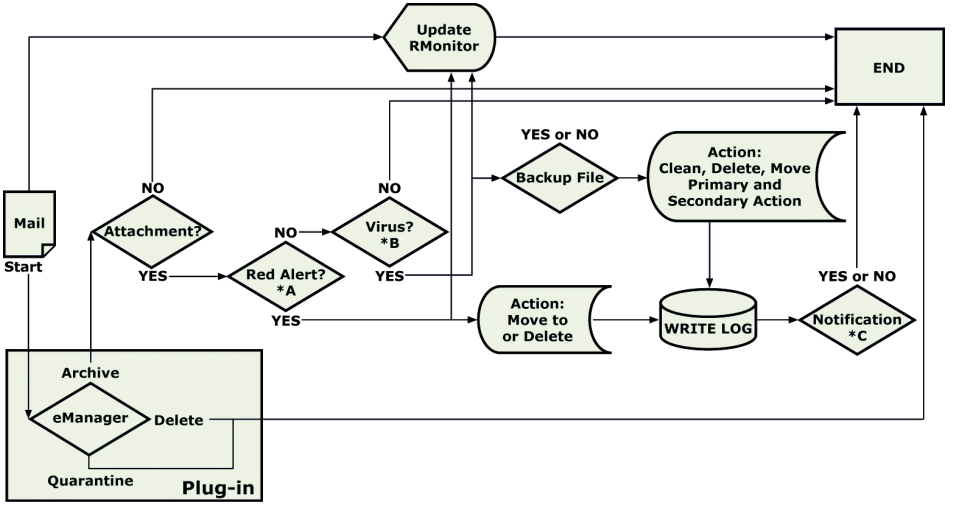


FIGURE 1-1. Email process flow through ScanMail eManager to ScanMail for Microsoft Exchange

5. Next, the message text of all mail found not to be spam is evaluated against active user-defined policies in the content filter. Mail that is found to match any one of the specified criteria is **Deleted, Archived,** or **Quarantined**, as defined in the policy.
6. Mail that has not matched any of the content filter policies or spam filter rule-sets is forwarded to ScanMail for Microsoft Exchange, where it is checked for viruses.
7. Infected email attachments are either **Cleaned**, **Quarantined**, **Deleted**, or **Passed** (delivered without cleaning), according to what is specified in the ScanMail configuration. Cleaned and uninfected messages are passed to the Exchange server for processing as usual.
8. The Exchange server delivers the email and any uninfected attachments to the intended recipient(s).

Results may vary greatly, but the spam and content filters can substantially reduce the volume of email that is delivered to the Exchange clients.

Control Manager™ Agent for ScanMail eManager

Trend Micro Control Manager (formerly known as Trend Virus Control System or Trend VCS) is a centralized management console which coordinates, tracks, and maintains the antivirus software products that are installed on a local area network (LAN) or wide area network (WAN). Because Control Manager allows one administrator to unify and manage all the different antivirus products on a network—regardless of platform or physical location—it is especially useful for large and complex networks.

For example, from the Control Manager console, the administrator can configure antivirus programs on the network to behave in the same way, view aggregate virus logs for virus events network-wide, and update the virus pattern files for all programs. Install the Control Manager agent for ScanMail eManager on your ScanMail for Microsoft Exchange server, and use Trend Micro Control Manager to centrally manage your ScanMail eManager server.

Trend Micro Control Manager is sold separately. Once you have purchased and installed the Control Manager server software, you can install the Control Manager agent for ScanMail eManager for Microsoft Exchange. Control Manager allows you to configure groups of ScanMail servers from one convenient Web console. For more information on Trend Micro Control Manager, see *Introducing Trend Micro Control Manager* starting on page A-2.

Summary of New Features

Trend Micro ScanMail eManager for Microsoft Exchange includes many new features and enhancements, including:

- Inbound and outbound Spam and Content Filtering
- Global exceptions can be applied so that a message that matches a global exception filter rule does not have any of the other filter rules applied. The global exception filter rules are based on the same conditions as the anti-spam filter rules, which can be text contained in message header fields, the message/attachment size, or the attachment name.

  For example, global exception rules can be configured so that specified users do not have any of the anti-spam filter rules applied to their email. As another example, a global filter rule can be set so that any inbound or outbound message

that is less than one megabyte is allowed to pass through even if it matches the conditions of another filter rule.

- Attachment content scanning for inappropriate text content can be enabled
- Attachment filtering based on the attachment file name is now available and supports the wildcard character '*'. Any attachments with names that match a filter rule can either be blocked (deleted, quarantined, or archived) or designated as a global exception to enable passing through.
- Message filtering based on user-specified rules for the message header fields now supports the wildcard character '*' in the To, From, CC, Subject, and File name fields. Messages whose header fields match one of the filter rules can either be blocked (deleted, quarantined, or archived) or designated as a global exception to enable passing through.
- Message filtering now accepts multiple entries in the To, From, and CC fields.
- Message filtering can be enabled based on message body size or size of any of the attachments passing through. If the message body or any of the individual attachments is a specified size, it can be blocked or designated as a global exception.
- Anti-spam filter can send separate notifications for user-defined rules versus Trend Micro or Vendor-Provided Rule Files. In either case, separate notification messages can be sent to the sender, recipient(s), and/or administrator(s)
- Quarantined mail can now be sent to a quarantine directory rather than a quarantine mailbox. Archived mail can be sent to a separate archive directory. The quarantine and archive directory locations are now configurable from the ScanMail eManager Configuration console
- User Interface has been enhanced to provide the ability to minimize the ScanMail eManager Configuration console and keep it open on the Windows task bar.
- Supports Outbreak Prevention Service (OPS) with Trend Micro Control Manager 2.5. Upon detection of a new, fast-spreading email-borne virus in the wild, Trend Micro will release an outbreak prevention policy which can be automatically downloaded and deployed by ScanMail eManager. By leveraging eManager's content filtering capability, the policy blocks the new virus at the gateway, shielding your network while a new virus pattern file is developed.

ScanMail Management Console (SMMC)

- ScanMail eManager can now be enabled or disabled from the ScanMail Management Console, Virus Scan Options (ScanMail for Microsoft Exchange 2000) or Real-time Scan Options (ScanMail for Microsoft Exchange) screen.

WARNING! *In ScanMail for Microsoft Exchange 2000, if you enable eManager on the Virus Scan > Options screen, eManager is enabled for all types of scans, i.e., real-time scan, scheduled scan, and manual scan. However, in ScanMail forMicrosoft Exchange, you can separately enable or disable eManager for real-time scan, scheduled scan, and manual scan.*

Chapter 2

Installing Trend Micro™ ScanMail™ eManager

This chapter provides information on installing Trend Micro ScanMail eManager and describes how eManager interfaces with ScanMail for Microsoft Exchange. The topics include:

- System Requirements
- Installing ScanMail eManager
- Starting and stopping eManager
- Starting the eManager console
- Viewing the ScanMail eManager processes
- Registering
- Installing ScanMail eManager Cluster Server
- Removing ScanMail eManager

System Requirements

To use ScanMail eManager for Microsoft Exchange, you need the following hardware and software:

ScanMail™ eManager™ for Microsoft™ Exchange 2000

Target Servers

- Microsoft Exchange 2000 Server with Service Pack 1 (or above)
- Windows 2000 Server or Windows 2000 Advanced Server with Service Pack 1 (or above)
- Intel™ Pentium™ 200MHz or higher processor (or equivalent)
- 128MB RAM minimum (256MB or more recommended)
- 30MB free disk space for the program files
- 100-500MB of free disk space for swap and temporary files
- A monitor with 800x600 or higher resolution

For Microsoft Cluster servers, you also need:

- Microsoft Windows 2000 Advanced Server

Setup PC

- Windows 2000 Server / Windows 2000 Professional Workstation
- LAN connection

ScanMail™ eManager™ for Microsoft™ Exchange

Target Servers

- Intel™ Pentium™ 200MHz or higher processor (or equivalent)
- 128MB RAM minimum (256MB or more recommended)
- 30MB free disk space for the program files
- Windows NT Server version 4.0 (English) with Service Pack 6 (or above); Windows 2000 Server; Windows 2000 Advanced Server
- Microsoft Exchange Server 5.5 with Service Pack 2 (or above)

For Microsoft Cluster servers, you also need:

- Microsoft NT 4.0 Enterprise Edition; Windows 2000 Advanced Server
- Microsoft Exchange 5.5 Enterprise Edition

Setup PC

- Windows NT 4.x Server / Windows NT 4.x Workstation with Service Pack 5 (or above); Windows 2000 Server / Windows 2000 Advanced Server/ Windows 2000 Professional Workstation
- LAN connection

Upgrading ScanMail eManager

Note: You must stop the ScanMail for Microsoft Exchange services temporarily in order to upgrade ScanMail eManager (ScanMail_Monitor, ScanMail_Web, and ScanMail_RealTime Scan).

1. Stop the ScanMail for Microsoft Exchange services (ScanMail_Monitor, ScanMail_Web, and ScanMail_RealTime Scan).
2. Follow the installation prompts described in the "Installing ScanMail eManager" section below. The installation program automatically saves your registry settings and upgrades ScanMail eManager.
3. Restart the ScanMail for Microsoft Exchange services.

Installing ScanMail™ eManager

ScanMail for Microsoft Exchange must be installed on your server first before you can install ScanMail eManager. ScanMail eManager should be installed on the same server as the ScanMail for Microsoft Exchange core module (ScanMail main program). It does not need to be installed on the same machine where the ScanMail Management Console (ScanMail Windows interface) is installed.

Use a Windows **Administrator** account to install ScanMail eManager. For Windows NT, this account should be assigned the additional advanced user privileges to **Log**

on as a service and **Act as part of the operating system**. For Windows 2000, the account should also have **Domain Admin** privileges.

1. If you have the Trend Micro Enterprise Solution CD, run **go.exe** by inserting the CD into the CD-ROM drive or by running the program from the Start menu. Select the language you want to use and then on the next screen click **Install**. Select **ScanMail eManager** from the list at the right and then click **Install**.

   -or-

   If you downloaded the installation files from the Trend Micro Web site, double-click the file **setup.exe** to begin installation.

2. The ScanMail eManager Welcome screen appears. Click **Next** to continue, then **Yes** to agree to the terms of the License Agreement (required to proceed).

3. The Serial Number screen appears. Enter your name, company name, and the product's serial number (the serial number can be found on the front cover of the ScanMail eManager Getting Started Guide and on the product registration card).

   -or-

   If you are installing the free 30-day trial version, click **Enter** without providing a serial number. The trial version is fully functional but "times-out" after 30 days. Click **OK**.

   Click **Next** to display a confirmation screen. Click **Next** to continue or **Back** to modify the displayed values.

4. The Select Target Servers screen appears.

   From the list in the left pane, select the servers you want to install ScanMail on. You can either highlight the target server names individually or highlight the Domain name to install ScanMail on all servers in a Domain. Double-click a Domain name if you want to view the servers within.

   Then click **Add**. The selected server(s) appear in the **Server Name** list at the right. If you are installing ScanMail on selected servers within a Domain only, repeat this process until you have added all the servers you want.

   To remove server(s) from the **Server Name** list, select them and then click **Remove** or **Remove All**.

   Click **Next** to continue.

5. The Server Logon screen appears. In the **User name** text box, enter the account the displayed server is currently logged on under.

   In the **Password** text box, enter the password for the specified administrator account.

   Keep the default temporary **Share** directory, C$, or specify a different share name for which the specified User has **Full Control** access rights. This share is used for copying the temporary installation files and is accessible by the administrator only.

   Click **Logon**.

   For servers that require different logon credentials, Setup displays the Server Logon screen again.

6. After the logon process, Setup displays a list of the selected servers. Click **Next** and the **Next** again on the following screen.

7. In the next screen, enter the destination directory and program folder name for the ScanMail eManager installation. Taking note that the settings you specify on this screen apply to all servers in the group, accept or modify the proposed destination directory and folder name. The default values are:

   `Destination directory:` **`c:\Program files\Trend\SMCF`**

   `Subfolder name:` **`Trend Micro ScanMail eManager`**

   If you are upgrading from a previous version of ScanMail eManager, the path box is grayed out and ScanMail eManager is installed to the same directory that you used previously.

8. Click **Install** to start installing ScanMail eManager on the selected servers. The Installing Program screen displays the installation status. Installation may take several minutes.

   The system displays an error message for those servers using accounts with incorrect or insufficient rights.

9. When the ScanMail eManager installation program finishes for all selected server(s), click **Next**.

You then see the Installation Summary screen that shows which of the ScanMail eManager installations were successful. Click **Finish** to complete the ScanMail eManager Setup process.

Note: After installation, make sure that the target folder for ScanMail eManager has been shared with Administrator privileges. By default, the target folder is `...\Program Files\Trend\SMCF.`

Starting and Stopping eManager

Starting/Stopping eManager from the ScanMail Management Console

ScanMail eManager can now be conveniently stopped and started directly from the ScanMail Management Console.

To enable ScanMail eManager:

1. Start the ScanMail Management Console (go to Windows **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > ScanMail Management Console**).
2. Enable real-time virus scanning.
3. After you have installed the ScanMail eManager plug-in, you can select **Enable eManager**. This option does not appear if you have not installed the eManager plug-in.

Note: In ScanMail for Microsoft Exchange 2000, if you enable eManager on the Virus Scan > Options screen, eManager is enabled for all types of scans, i.e., real-time scan, scheduled scan, and manual scan. However, in ScanMail for Microsoft Exchange, you can separately enable or disable eManager for real-time scan, scheduled scan, and manual scan.

Restarting ScanMail™ for Microsoft™ Exchange and eManager™

ScanMail eManager only processes messages while ScanMail Exchange is running. If ScanMail has stopped, you must restart it to reactivate ScanMail eManager.

To restart the ScanMail for Microsoft Exchange services:

1. Open Control Panel and click **Services**.
2. From the list of services that appears, select **ScanMail_RealTimeScan**, then click **Start**. If you use the Web interface for ScanMail, you must also restart the Web service—select **ScanMail_Web**, then click **Start**.

Note: Stopping the ScanMail_RealTimeScan service also stops the ScanMail_Web service, but starting ScanMail_RealTimeScan does not automatically start the Web service.

ScanMail eManager services start along with ScanMail Exchange.

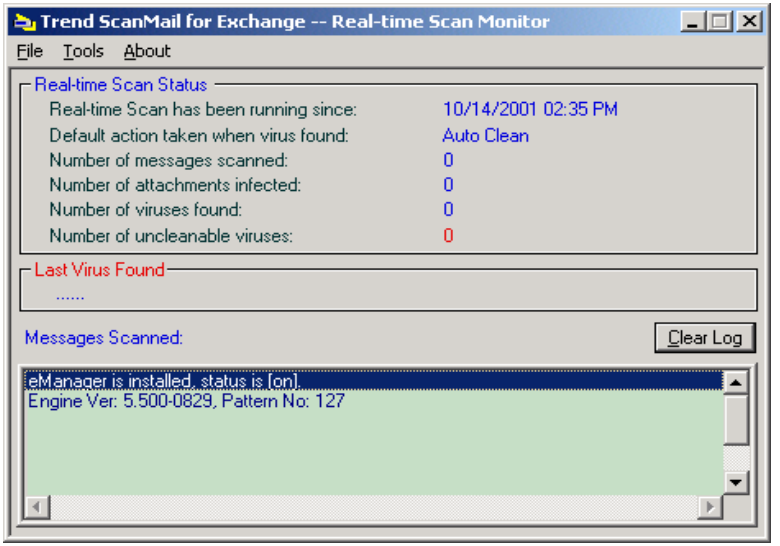


FIGURE 2-1. Real-time Scan Monitor, Messages Scanned section shows that the ScanMail eManager Content Filter has been loaded.

You can view the status of ScanMail eManager using the ScanMail Real-time Scan monitor. If Real-time Scan Monitor is not already open, go to **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Real-time Scan Monitor**.

Stopping ScanMail™ for Microsoft™ Exchange and eManager™

1. Open Control Panel and click **Services**.
2. From the list of services that appears, select **ScanMail_RealTimeScan**, then click **Stop**. If you use the Web interface for ScanMail, it stops automatically as well. **ScanMail eManager** services stop along with ScanMail for Microsoft Exchange.

Note: Stopping ScanMail_RealTimeScan service also stops the ScanMail_Web service and ScanMail eManager.

---

3. You can view the status of ScanMail eManager using the ScanMail Real-time Scan monitor. If the Real-time Scan Monitor is not already loaded, go to **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Real-time Scan Monitor**. It reports "ScanMail Real-time Scan Service Stopped!" under **Real-time Scan Status**.

Starting the ScanMail™ eManager Console

The ScanMail eManager Console is loaded separately from the ScanMail Windows or Web consoles. To open the ScanMail eManager Console, go to the server where you have the ScanMail for Microsoft Exchange core module installed.

1. Click **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Trend Micro ScanMail eManager > ScanMail eManager Configuration** to bring up the Server Logon screen.
2. Enter your **User name** and **Password**, then click **Logon**. The ScanMail eManager Console appears.

Note: You must use a Windows Administrator account.

Selecting the Server to Administer

When you originally start eManager, you log onto the local server. The server you are currently logged on is displayed in the **Current server** line. To log on another server:

1. Scroll down and double-click a server name in the **Logon Server** List or type a server name.

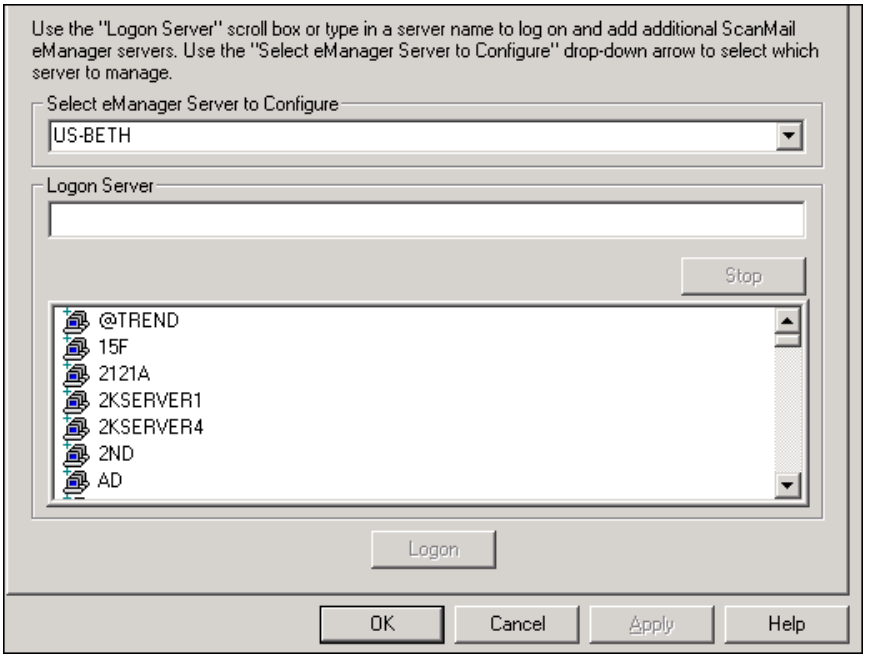


FIGURE 2-2. ScanMail eManager Select Server screen

2. Click **Logon**.

Note: Although you can administer any remote server that is part of your network, you can only administer one server at a time using the ScanMail eManager console.

3. Select which server you want to administer using the drop-down arrow under **Select eManager Server to Configure**.

You can administer any server you have already logged on without needing to re-enter your user name and password. Just select the server name and it becomes the current server to configure.

Viewing the ScanMail™ eManager™ Processes

You can view the status of ScanMail eManager using the ScanMail for Microsoft Exchange Real-time Scan monitor. If the Real-time Scan Monitor is not already open, go to **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Real-time Scan Monitor**. If ScanMail eManager is loaded, the message "eManager installed, status is [on]" is displayed.

Alternatively, you can view whether the eManager process is loaded by opening the Windows Task Manager:

1. Press the **Ctrl-Alt-Delete** keys simultaneously.
2. Select **Task Manager**.
3. Select the **Processes** tab.

The process **Cm_smex.exe** should be listed.

Note: The process ContScan.exe is listed only if the ScanMail eManager console is open.

Registering eManager

Serial numbers can be found on the front cover of the ScanMail eManager Getting Started Guide and on the product registration card. There are two ways to register ScanMail eManager: (1) by filling out and mailing the Registration Card included in the ScanMail eManager package, or (2) by entering your serial number in the Registration screen from the Windows Start Menu.

Note: You must register eManager in order to obtain updated Rule and Import files from Trend Micro.

Register ScanMail eManager from the Windows Start menu ScanMail eManager Registration screen by following these steps:

1. Go to Windows **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Trend Micro ScanMail eManager > ScanMail eManager Registration** to bring up the serial number screen.
2. Type your ScanMail eManager serial number and click **OK**.
3. Restart the real-time scan service.

You are now able to download new rule and import files from Trend Micro's Web site.

Installing ScanMail™ eManager on a Cluster Server

Following are the instructions to install ScanMail eManager on a cluster server. In ScanMail eManager, you must install all nodes of the server in the same installation session.

Use a Windows **Administrator** account to install ScanMail eManager. For Windows NT, this account should be assigned the additional advanced user privileges to **Log on as a service** and **Act as part of the operating system**. For Windows 2000, the account should also have **Domain Admin** privileges.

1. If you have the Trend Micro Enterprise Solution CD, run **`go.exe`** by inserting the CD into the CD-ROM drive or by running the program from the Start menu. Select the language you want to use and then on the next screen click **Install**. Select **ScanMail eManager** and then click **Install**.

   .-or-

   If you downloaded the installation files from the Trend Micro Web site, double-click the file **setup.exe** to begin installation.
2. The ScanMail eManager Welcome screen appears. Click **Next** to continue, then **Yes** to agree to the terms of the License Agreement (required to proceed).
3. The Serial Number screen appears. Enter your name, company name, and the product's serial number (the serial number can be found on the front cover of the

Trend Micro ScanMail eManager for Microsoft Exchange Getting Started Guide and on the product registration card).

-or-

If you are installing the free 30-day trial version, click **Enter** without providing a serial number. The trial version is fully functional but "times-out" after 30 days. Click **OK**.

4. When the Select Target Servers screen appears, from the list in the left pane, select all of the cluster server's physical nodes. Do not select the cluster server's virtual name.

   Then click **Add**. The selected server appears in the **Server Name** list at the right.

5. In the Server Logon screen, **User name** text box, enter the account the displayed server is currently logged on under.

   In the **Password** text box, enter the password for the specified administrator account.

   Keep the default temporary **Share** directory, C$, or specify a different share name for which the specified User has **Full Control** access rights. This share is used for copying the temporary installation files and is accessible by the administrator only.

   Click **Logon**.

6. After the logon process, Setup displays a list of the selected nodes. This step differs for Windows NT and Windows 2000:

   a. For Windows NT cluster servers, the directory must be on the shared storage space. For example:

   ```
   e:\smcf
   ```

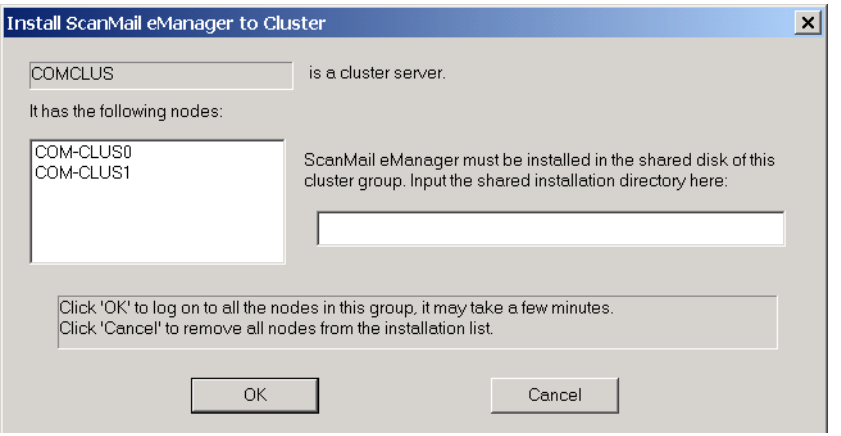


FIGURE 2-3. Input the shared directory name for Windows NT Cluster servers.

b. For Windows 2000 cluster servers, the cluster server is listed with its physical nodes. The shared directory option is not presented because ScanMail will be installed on a local directory of each node, as specified in Step 7 below.

The cluster logon screen as it appears in a Windows 2000 cluster environment is shown below:

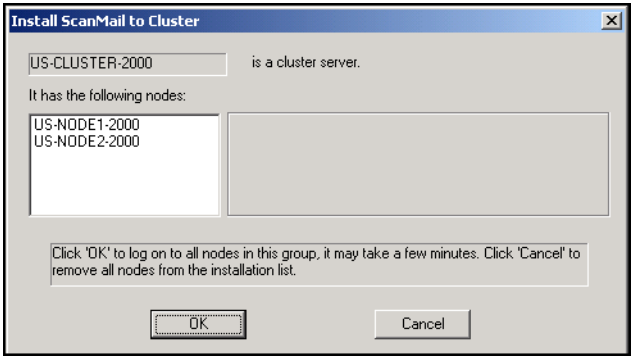


FIGURE 2-4. ScanMail eManager will be installed on all the Windows 2000 nodes listed.

7. Depending on whether you are using Windows NT or Windows 2000, enter the destination directory and program folder name to install ScanMail eManager to:

   a. For Windows NT servers, this option is grayed out because ScanMail is installed on the shared storage directory specified in Step 6.

   b. For Windows 2000 servers, taking note that the settings you specify on this screen apply to all nodes in the group, accept or modify the proposed destination directory and folder name. The default values are:

   `Destination directory:` **`c:\Program Files\Trend\SMCF`**

   `Subfolder name:` **`Trend Micro ScanMail eManager`**

   If you are upgrading from a previous version of ScanMail eManager, the path box is grayed out and ScanMail eManager is installed to the same directory that you used previously.

8. ScanMail eManager is installed on the selected nodes, as shown below for a Windows 2000 environment.

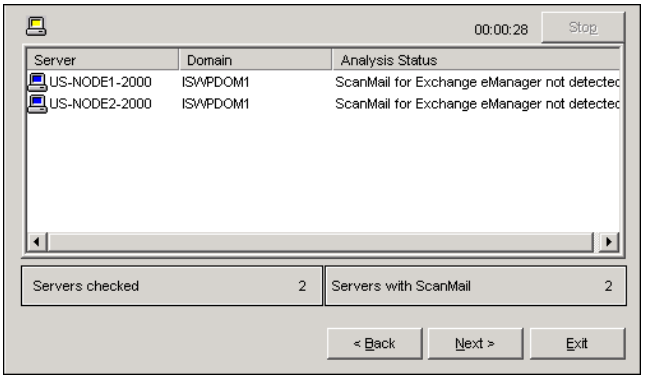


FIGURE 2-5. ScanMail eManager has not been installed previously.

9. The Installing Program screen displays the installation status. Installation may take several minutes. When the ScanMail eManager installation program finishes for all selected nodes, click **Next**.

You then see the Installation Summary screen that shows which of the ScanMail eManager installations were successful.

Note: After installation, make sure that the target folder for ScanMail eManager has been shared with Administrator privileges. By default, the target folder is: `...\Program Files\Trend\SMCF.`

Removing ScanMail eManager

To remove ScanMail eManager, you must first stop the ScanMail for Microsoft Exchange real-time scanning services (ScanMail_Monitor, ScanMail_RealTimeScan, and ScanMail_Web). You can remove ScanMail eManager directly from the local server console, or by using the Trend Micro Enterprise Solution CD or the `uninstall.exe` program.

Removing ScanMail eManager Using the Windows™ Start Menu

The simplest way to remove ScanMail eManager is directly from the local server's Windows Start menu.

1. On the ScanMail eManager server, go to **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Trend Micro ScanMail eManager > Uninstall ScanMail eManager**.
2. Click **Yes** on the Confirm File Deletion screen.
3. When the program finishes, click **OK**.

Removing ScanMail eManager using the Trend Micro™ Enterprise Solution CD or the Uninstall.exe Program

1. From the Trend Micro Enterprise Solution CD, run the **`uninstall.exe`** program located in the **`\Programs\Smeman5`** directory.

   -or-

   If you downloaded ScanMail eManager from the Trend Micro Web site, run **`uninstall.exe`** to uninstall.

2. Click **Next** on the Welcome screen.
3. The Select Target Servers screen appears. From the list at the left-hand side of the screen, select the server you want to remove ScanMail eManager from by highlighting the target server and clicking **Add**. The selected server appears in the **Server Name** list at the right. Repeat this process until you have added all the servers you want to remove ScanMail eManager from.

   To remove a server from the **Server Name** list, select it and then click **Remove**.

   Click **Next** to continue.

4. The Server Logon screen appears. In the **User name** text box, enter the account the displayed server is currently logged on under.

   In the **Password** text box, enter the password for the specified administrator account.

5. Click **Logon** to log on the server(s).

Setup checks whether or not ScanMail eManager is installed on each server and then displays the results on the next screen. For servers that require different logon credentials, Setup displays the Server Logon screen again.

6. After the logon process, Setup displays the Analyze Selected Server(s) screen. Click **Next** and then **Uninstall** on the next screen to start removing the program from the selected servers.
7. On the next two screens, click **Next** and **Finish** to complete the removal process.

Removing ScanMail eManager from a Cluster Server

The instructions to remove ScanMail eManager from a cluster server are nearly the same as the regular removal instructions. Type or select all of the cluster physical nodes to remove ScanMail eManager completely.

ScanMail™ eManager Files

By default, ScanMail eManager installs its executable files to the `...\Program Files\Trend\SMCF` directory. The following folders are created in the same location:

```
SpamRule, Tempdir, Quarantine, Archive
```

ScanMail eManager also adds the following entry to your registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\
ScanMail for Exchange eManager
```

Chapter 3

Spam Filtering

All email from spammers must enter the Internet from somewhere. Part of constructing a good spam filter is identifying where the spam originated and other telltale bits of information that you can use in constructing anti-spam rules. Trend Micro provides a ready made rule-set that contains hundreds of rules for filtering out many of the most common spam types. In addition, you can create an unlimited number of your own anti-spam rules.

When creating spam rules, it is important to bear in mind that many spammers add bogus header information to their messages in an effort to make tracking back to the source difficult. The most flagrant bulk emailers often reuse the same bogus header information because it's just too much work to create a unique fake for each spam-blast. This is actually good news when it comes to creating anti-spam rules, because you can use this bogus information like a "signature," to identify and safely block whole classes of spam rather than creating rules on a one-rule-one-spam basis.

Global exceptions can now be applied as Anti-Spam rules. Messages meeting the criteria specified do not have any of the other rules applied to them. For example, you can specify certain users to have all their messages delivered, whether the messages match your anti-spam rules or not.

File attachment blocking can be used during virus outbreak conditions to temporarily block all attachments with a particular file name. To use this option, simply specify the file names to block. You can select case-sensitive and/or exact matches for the file names, or use the "*" wildcard character.

This chapter provides information on spam mail detection and configuration to ward against spam. The topics include:

- Rules strategies
- Creating anti-spam rules
- Creating global exception rules
- Operators
- Using vendor-provided rule files
- Notification messages
- Action on unwanted email

Viewing Email Headers

Many mail clients support viewing the header information of email messages, usually through a **Properties** item on the menus, an **Options** tab on the open message, by saving the message as ASCII text, or opening the message using an ASCII editor such as Windows Notepad.

Header information is often not available on forwarded messages. To preserve the header information on second-hand messages, have users copy the message (as a file) and include it as an attachment in the email they are forwarding to you. Check the on-line help that came with the mail client for instructions on reading message header data.

In ScanMail for Microsoft Exchange, you can view the Internet Headers as follows:

1. Open the message.
2. Go to **View > Options**.
3. At the bottom of the Message Options screen, you will see an **Internet headers** section.

Example Message Header

Return-Path: <dgq7@botmail.ro>
Received: from *rly-yes01.mx.aol.com* (rly-yes01.mail.aol.com [123.18.144.193])
by air-yes05.mx.aol.com (v47.2) with SMTP; Fri, 07 Aug 1999 07:20:53 -0400
Received: from mail1.starfordnet.com (mail1.staffassoc.com [123.10.128.47]

(may be forged)) **by** *rly-yes01.mx.aol.com* (8.8.8/8.8.5/AOL-4.0.0) with ESMTP id HAA20159; Fri, 7 Aug 1999 07:20:41 -0400 (EDT)
From: dgq7@botmail.ro
Received: from abanks (ip77.washing11.dc.pub-ip.psi.net [123.30.47.77])
by mail1.starfordnet.com (8.8.5/SCA-6.6) with SMTP id LAA12458; Fri, 7 Aug 1999 11:26:05 GMT Date: Fri, 7 Aug 1999 11:26:05 GMT
Message-Id: <199908071126.LAA12458@mail1.starfordnet.com>
To: prs1000@botmail.ro
Subject: FREE Adult XXX Pix
Mime-Version: 1.0
Content-type: text/plain; charset=US-ASCII
Content-transfer-encoding: 7bit

Note: All text appearing above is header information, read by the spam filter. Text appearing below is body information, read by the content filter. The content filter also reads the header information.

This paragraph and the last, representing email message text, are read by the content filter but not the spam filter. MIME, UUencode, and other encoded binary files are not included in the content filter's comparison. Non-encoded text files and Word documents are included.

Configuration Files

All configuration settings for the spam and content filters are stored in the following files:

```
\Program Files\Trend\SMCF

       contscan.ini
       csconfig.dat

\Program Files\Trend\SMCF\spamrule

       contscan.txt
       spamrule.txt
       AntiSpam.###
       Trend$RF.###
```

Using the Spam Filter

The spam filter starts and stops with ScanMail for Microsoft Exchange, and cannot be run independently. You can view the operational status of the spam filter (i.e., eManager) in one of several ways:

1. Open the ScanMail Management Console and go to the **Virus Scan > Options** (Exchange 2000) or **Real-time Scan > Options** (Exchange 5.5) screen. **Enable eManager** should be selected.
2. Open the Real-time Scan Monitor on the ScanMail eManager machine to see real-time virus and filter processing. The Real-time Scan Monitor, Messages Scanned section should list that eManager is loaded.
3. Alternatively, you can open the Windows task manager and make sure that the process **Cm_smex.exe** is loaded.

See Chapter 2, "Installing Trend Micro ScanMail eManager", for more details on stopping and starting ScanMail for Microsoft Exchange and ScanMail eManager.

Creating Anti-Spam Rules

Anti-Spam rules can now be individually created to either block mail based on specified conditions or let selective mail pass through. For example, you can create rules to block mail that exceeds a size limit and then set up a global exception rule so that the CEO can send messages of any size.

The two types of rules are:

- Regular rules
- Exception rules

The same configuration options are used for each type of rule. The only difference is the action taken when a message matches the conditions. A message matching a regular rule condition can be Deleted, Quarantined, or Archived (sent through, but a backup copy of the mail is also made). Exception rules allow messages matching the condition to pass through completely, rather than being Archived as well.

Select the Anti-Spam tab to create rules, as shown in the figure below.

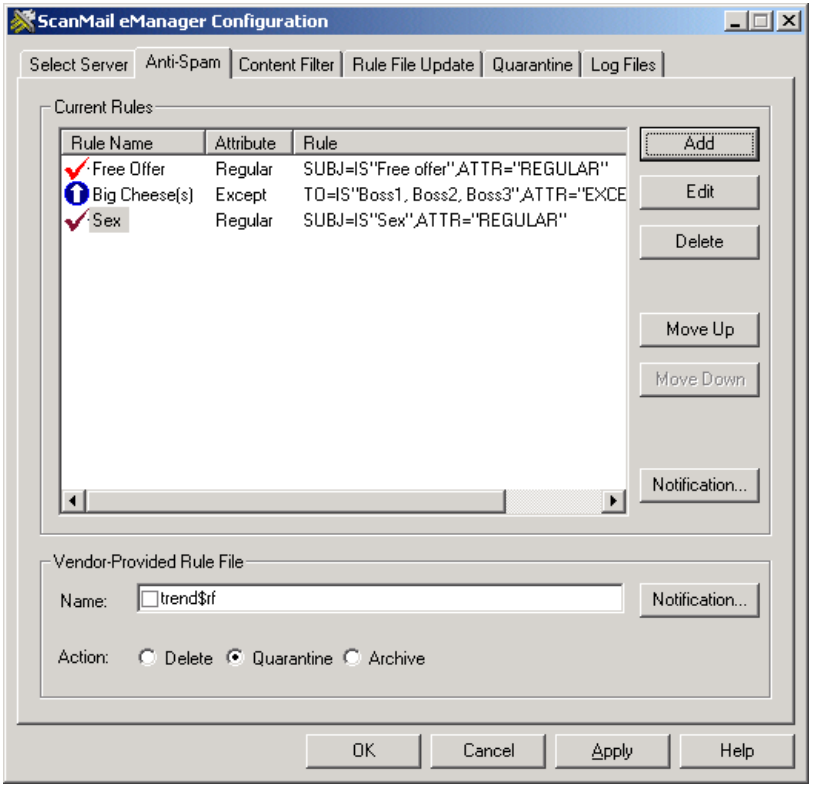


FIGURE 3-1. This eManager spam filter shows anti-spam and exception rules in effect.

The Attribute field shows whether each rule is a Regular or an Exception rule. In addition, the Rule Name field has a check mark in front if it is a Regular rule or an up-arrow if it is an Exception rule.

Current Rules Strategy

When specifying multiple rules in the Current Rules list, we recommend that you employ an inverted pyramid model, wherein you put rules with the broadest reach, or

highest probability of matching, at the top of the list. Those that are more narrowly defined (less likely to trigger a match) should be placed towards the bottom of the list. This is the most efficient arrangement wherein the filter eliminates the greatest proportion of traffic with the fewest number of evaluations.

To change the placement order of a rule, select it and click **Move Up** or **Move Down**.

Rules Strategy Example

Let's say that you have created the four spam filter rules shown below in an effort to reduce the amount of spam processed by your Exchange server and arriving in your users mailboxes:

1. Delete any mail sent from *SpamKing*.
2. Quarantine any mail being sent to *SpamLover.*
3. Delete any mail containing the phrase "Free Offer" in the subject line.
4. Quarantine any mail containing the term "SeXXX" in the subject line.

Let's further say that you have analyzed your incoming messages and know that for every 10,000 messages processed by the Exchange server, 42 are sent by *SpamKing*, 500 contain the phrase "Free Offer" in the subject line, 18 are sent to *SpamLover*, and 196 contain the term "SeXXX" in the subject line.

In this case, the optimal ordering of the rules appearing in the Current Rules list is as follows:

1. Free Offer (500 instances)
2. SeXXX (196 instances)
3. SpamKing (42 instances)
4. SpamLover (18 instances)

When ordered as above, 500 of every 10,000 incoming messages can be eliminated in the first round of evaluation because they match the "Free Offer" rule. If, on the other hand, the order were reversed and "SpamLover" was the first rule and a "Free Offer" message arrived, the message would be evaluated four times (1. check for "SpamLover," 2. check for "SpamKing," 3. check for "SeXXX," 4. check for "Free Offer") before finally matching on "Free Offer" and being rejected.

User-defined Current Rules

The **Current Rules** table shows the individual rules by which inbound and outbound messages are evaluated.

Messages found to match all the criteria specified in any one of the rules trigger the action (**Quarantine, Archive,** or **Delete**) specified within the rule, and a notification message is automatically sent to the administrator or other specified party.

For the spam filter, the header information of messages (for example, *From:*, *To:*, *CC:* and *Subject:* lines) is evaluated. For the content filter, the contents of the message text are considered in addition to the header data.

Note: Binary attachments encoded using MIME, UUencode, or other encoding schemes are not evaluated. Non-encoded text and Word attachments are included in the evaluation.

The evaluation of Exchange traffic against the rules starts from the first, or top rule, and proceeds down through to the end. There is no limit to the number of Current Rules you can set.

Add-Edit Rule Options Screen

Use the **Add/Edit** screen to specify the criteria by which email messages are evaluated. Each Add/Edit screen represents a distinct rule, represented by the **Rule Name** specified at the top.

For each rule, only when *all* of the conditions defined on the screen are true is the action specified in the **Action on Unwanted Mail** field taken. Blank fields are ignored.

Note: The **Routing domain** and **Reply-to** fields are not available in this version and are grayed out, as shown below.

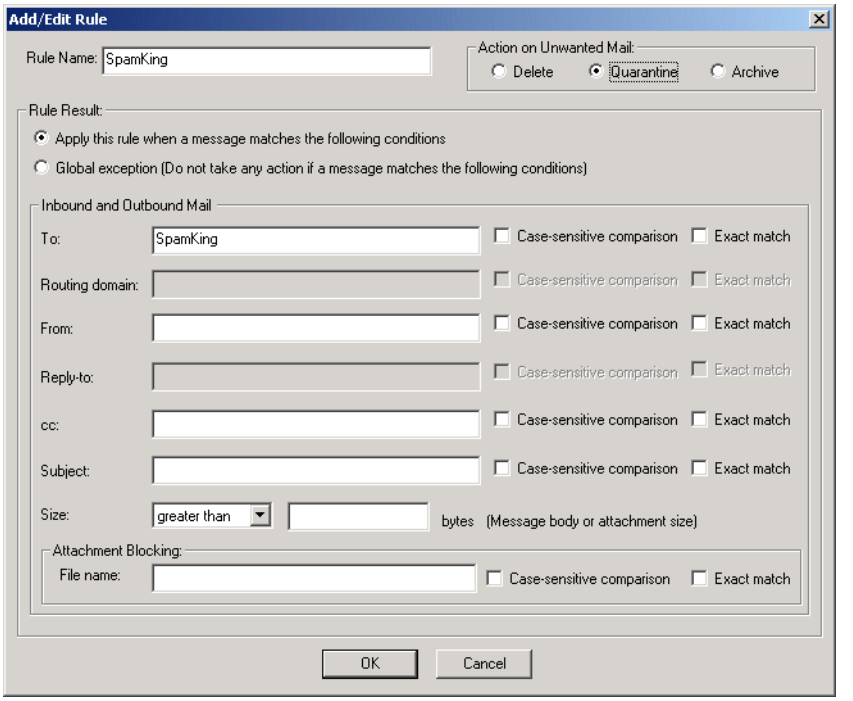


FIGURE 3-2. This rule blocks inbound messages sent to SpamKing.

For the spam filter, only the email header information is compared against the rules defined in the Add/Edit screen. Identical information appearing in the message text of a forwarded message does not trigger a match. To evaluate message text, use the content filter.

Rule Name

Use the **Rule Name** field to create mnemonic names for the rules you create. The name, which appears in the **Current Rules** list, is not evaluated against the content of the message.

Action on Unwanted Mail

Messages that are found to match the filter rules can be deleted or quarantined and are not passed to ScanMail for Microsoft Exchange for virus scanning. Alternatively, messages can be copied to the archive directory, and then passed to ScanMail for Microsoft Exchange for virus checking.

All blocked actions are recorded in the log file.

Quarantined email messages are moved to the quarantine directory, specified on the Quarantine screen.

Archived email messages are forwarded to the intended recipient, but are also renamed and moved to the archive directory, specified on the Quarantine screen.

We recommend that you **Archive** messages for the first few weeks following the creation or modification of your spam filter rules. You can then check these messages to evaluate the efficacy of your rule. The original header information is attached to the message.

Rule Result

Rules can be designated as Regular rules or Exception rules based on the rule result. By default, rules are considered Regular, wherein the rule is applied to any email message when the condition specified is matched.

Alternatively, you can create a Global Exception rule that takes effect regardless of what other rules you have configured. This rule is also applied when an email message matches the conditions you specify. However, if a message matches the Global Exception conditions, it is exempted from any further comparisons with other rules and is passed to ScanMail for Microsoft Exchange for virus scanning.

Address and Subject Fields

You can configure the spam filter to filter out mail based on information contained in any of the following fields:

To, From, cc, Subject

Except for the Subject field, you can use a comma as to delimit multiple entries.

Blind Carbon Copies (email addresses appearing in the **bcc** field), are not included in the header information and so cannot be used as a basis for filtering spam.

Case-Sensitive Comparisons

By default, capitalization is not considered when evaluating the spam-filter rule-sets. For example, "Free Offer," "Free offer," and "free offer" are considered equivalent.

For the spam filter, case-sensitivity can be applied on a field-by-field basis, by individually selecting the Case-sensitive comparison check boxes for the To, From, cc, and Subject fields.

Exact Matches

Anti-Spam keywords are considered a match if the specified word matches any part of the mail header, i.e., To, From, cc, and Subject fields. For example, if "Free" is specified as the keyword in the Subject field, an occurrence of "Freezer" in the mail header, specifically the Subject field, is considered a valid match.

To prevent such generalizations and reduce the likelihood of false positives, select **Exact match** in the appropriate spam filter Add/Edit rule field. It is a good idea to avoid very short rules or keywords, such as "AOL."

Note: Accepting partial words as a valid match can increase the incidence of false positives.

Message or Attachment Size

Messages can be filtered according to what size the individual part of the message being filtered is — the message body or the attachment size. You can filter messages according to the size in bytes, using the following conditions:

- greater than
- less than
- equal to
- not equal

For example, you can select to block the mail body or the attachment if it is greater than 100,000 bytes by filling in:

```
Size: "greater than" 100000 bytes
```

Attachment Blocking

File attachment blocking is usually used during virus outbreak conditions to temporarily block all attachments with a particular file name. To use this option, type the file name of the attachment to block in the File name text box under Attachment blocking. You can use the wildcard "*" in specifying the file name. Note that you can only specify one attachment file name to block in each rule.

Select **Case-sensitive comparison** if you only want to block files if the case matches exactly what you typed. Normally, you should not select this option.

Select **Exact match** if you only want to block files that have the exact file name with no additional characters. We recommend that you do not select this check box because additional spam messages may use the same file name, with a few characters added. For example, TROJ_MTX also catches files named:

```
TROJ_MTX_II.DLL, TROJ_MTX_IlI.DLL, etc.
```

Vendor-Provided Rule Files

The **Vendor-Provided Rule File** contains hundreds of predefined anti-spam rule-sets for blocking unsolicited and unwanted email originating from a number of known spammers or containing popular spam subjects. It is typically used in conjunction with the customized list of rules you develop to address specific occurrences of spam.

Select the **Vendor-Provided Rule File** check box to have eManager include the individual rules in the analysis of inbound and outbound mail. Rules included in the rule file do not appear in the Current Rules table.

The **Vendor-Provided Rule File**, which is encrypted, can be found in the `\Program Files\Trend\SMCF\spamrule` directory. The file name takes the form of `Trend$RF.###`, where ### represents the version number of the file. The file is not user-editable.

This rule file is provided by Trend Micro and can be updated automatically.

Anti-Spam Notifications

You can configure separate notifications for the user-defined Current Rules section and the Vendor-Provided Rule File section. Just select the corresponding **Notification** option.

Current Rules Notification

To set notifications to the administrator(s), sender, and/or recipient(s) when email meets a rule, click **Notification**, then select any or all of the following:

- Notify the following administrator(s) — enter the Administrator(s) email addresses in the "Mail to" text box. Multiple email addresses should be delimited with semi-colons. Then enter the message text to send, for example:

  "Note: ScanMail eManager spam filter blocked an email."

- Notify sender — enter the message text to send.
- Notify recipient(s) — enter the message text to send.

Vendor-Provided Rule File Notification

To create a notification message to be sent when one of the vendor rules is met, click the lower **Notification** option. Configure your vendor-rule notifications as described above in the Current Rules Notification section for the administrator(s), sender, and/or recipients(s).

Chapter 4

Content Filtering

The content filter provides a means for the administrator to evaluate and control the delivery of email on the basis of the message text itself. It can be used to monitor inbound and outbound messages to check for the existence of harassing, offensive, or otherwise objectionable message content.

There is no limit to the number or type of content policies that can be created and policies can be individually enabled or disabled. The content filter also provides a synonym checking feature which allows you to extend the reach of your policies.

You can, for example, create policies to check for:

- Sexually harassing language
- Racist language
- Offensive language, e.g., "four-letter" words
- Spam that is found in text in the mail body
- Spam that is found in text in the attachment

Any number of policies can be created, regarding any subject.

This chapter includes information on configuring the content filter to ward against harassing and other objectionable messages.

The topics include:

- Trend Micro ScanMail eManager content filter policies
- Creating content filter policies
- Creating keyword lists
- Creating anti-keywords
- Synonym checking
- Global Settings for exact matches, case-sensitive comparisons, and scanning the content of attached files
- Action on unwanted mail

Using the ScanMail™ eManager Content Filter

The ScanMail eManager Content Filter starts and stops with ScanMail for Microsoft Exchange, and cannot be run independently. Chapter 2, "Installing Trend Micro ScanMail eManager" describes starting and stopping ScanMail eManager for Microsoft Exchange.

To view the operational status of eManager, open the Performance Monitor (which shows ScanMail's real-time virus and filter processing) on the ScanMail for Microsoft Exchange machine. Go to **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Real-time Scan Monitor** and view the **Messages Scanned** text box.

About Content Filter Policies

A content filter **policy** represents a group of conceptually related words and phrases that are matched against inbound and outbound messages. The message text, or body, of email (including the header) is compared against the list of policies and whenever *any* policy is found to match the contents of a given email, the **Action** specified in the matching policy is taken. The message can be **Archived**, **Quarantined**, or **Deleted**.

Only the email message text and non-encoded text/Word attachments are included in content filter comparisons; binary email attachments are not considered.

Messages are checked first for the keywords specified in the first policy on the list, then the second policy, third, and so on.

Policies can be individually enabled by selecting them in the Policies list. There is no limit to the total number of policies that can be engaged by the content filter. One rule of thumb, however, is that the more active policies there are, the longer it takes to evaluate a given email message.

The Content Filter screen is displayed in the figure below.

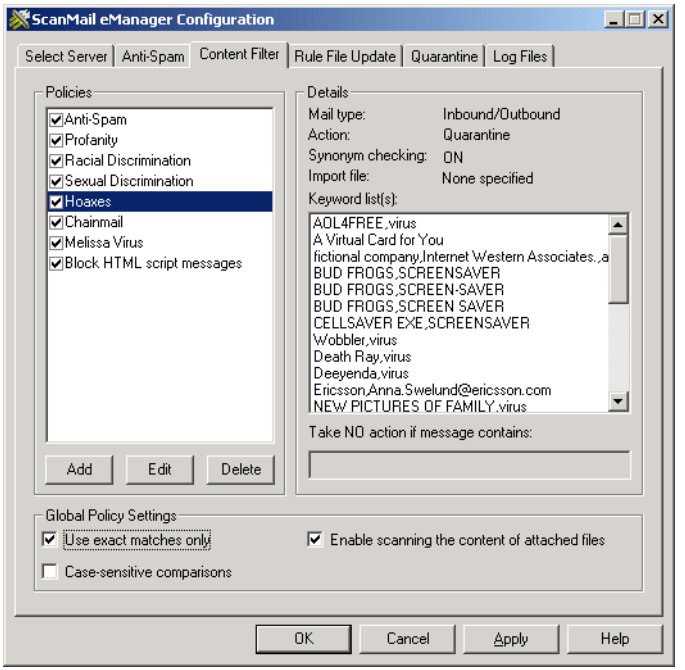


FIGURE 4-1. Content filtering is policy-based and user-configurable.

Keyword Lists

The **Keyword List** for a given **Policy** contains the words and phrases that the content filter uses to check email message contents. When multiple keywords are included on the same line of a policy, a match is made only when the message being evaluated

contains *all* of the keywords on that line. For example, you can add the following keywords to the list (perform four separate **Add**s).

Example 1:

sex, bare
sex, nude
sex, naked
sex, buff

Notice that in this example, four related words are used instead of just one. Basing the policy solely upon the word *sex* is not likely to produce reliable results because *sex*, i.e., sexual intercourse, has a different meaning than *sex*, i.e., the category male vs. female. To minimize the chance of such false positives, it is a good idea to qualify the primary word, *sex*, with additional words typically associated with it in a spam sex message: *buff*, *bare*, *nude*, and *naked*. Including several keyword groups increases the reach of the filter.

As configured in the example, messages that contain any of the keyword pairs are considered a match.

Example 2:

Alternatively, you can have the filter trigger an action only when all five words are encountered in a single message. Do this by including all the keywords on a single line (perform a single **Add**).

sex, bare, nude, naked, buff

Obviously, the likelihood of detecting every sex message on the basis of this filter is much less than for a policy that contains several rule-sets bases upon the word *sex*, as shown in Example 1 above.

Example 3:

In this example, a policy is constructed wherein the occurrence of any one of the related words in Example 2 triggers a match.

nude
sex
buff
bare
naked

This technique can be used to filter out other offensive content—not every four-letter word in the dictionary need appear in a message to qualify as a match. Instead, you may deem the occurrence of any one of the words on your offensive list to be sufficient to warrant tracking (**Archive** option), further investigation (**Quarantine** option), or immediate deletion.

The words listed above probably do not qualify for exclusion on their own. We'll leave it up to the reader's imagination what words might be offensive enough individually to warrant exclusion.

ScanMail™ eManager's Content Filter Policies

ScanMail eManager comes preconfigured with a list of content filter policies. You can create your own content filter policies to complement this list.

The preconfigured content filter policies include keyword lists for topics such as Anti-Spam, Profanity, Racial Discrimination, Sexual Discrimination, Hoaxes, Chain mail, and an option to block HTML script messages.

Anti-Spam

The Anti-Spam policy is read from the Import File that you can download from Trend Micro. The Import File is updated periodically. It is stored in the ...\SMCF\spamrule directory. The Import File is of the form Anti-Spam.###, where ### is the number of the current import file, for example, Anti-Spam.17. ScanMail eManager always checks and uses the latest Import File when evaluating email.

See *Automatic Update* starting on page 5-3 for more information on updating the Import file.

Profanity and Discrimination Lists

The Profanity list includes keywords such as "four-letter words" and other keywords which can be used in offensive ways. This is just an example list and you can edit the list to add or delete terms.

The Racial Discrimination list is used to store words that are considered to be racist and offensive. This is just a starter list of words that are commonly considered offensive and do not have alternate meanings that are not offensive. You can add as many terms to this list as you like.

The Sexual Discrimination list is used to store words that are considered to be sexually harassing and inappropriate. This is also just a starter list of words that are considered offensive and is intentionally brief. The keywords listed are words that generally do not have alternate meanings that are not offensive.

Hoaxes and Chain Mail Lists

The Hoax list contains keywords that in combination can be used to identify some of the most common hoaxes on the Internet. These warning messages often describe fantastical or impossible virus or Trojan program characteristics, but appear to be real or forwarding these hoax warnings to friends and co-workers only perpetuates the problem. Other hoaxes offer bogus free gifts or other items not appropriate for a corporate environment.

The Chain mail list contains several keyword phrases that can be used to identify chain letters. Chain letters are sometimes "get rich quick" schemes. A typical chain letter includes names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then eliminate that name and add yours to the bottom. You are then instructed to mail copies of the letter to a few more individuals.

There are several problems with chain letters. They're illegal if they request money or other items of value and promise a substantial return to the participants, even when delivered on the Internet. Chain mail that does not request request money can also bog down networks and contribute to a spam mail problem. Chain mail can be offensive and may contain threats that if you do not forward them, bad luck will come your way. You can edit the Chain mail list to add chain letter phrases that are prevalent at your organization.

Blocking HTML Script Messages

The HTML script block list contains several entries that are generally found in all HTML scripts. Some HTML scripts have been known to contain code that executes destructive commands on the user's computer. Be careful when using this option if HTML scripting is an important part of your company's business.

Customizing the Trend Micro™ ScanMail™ eManager™ Content Filter Policies

You can customize any of the Trend Micro ScanMail eManager policies by clicking **Edit** and adding or deleting items. See the next section for more information on creating and editing content filter policies.

The Anti-Spam policy is the only policy that does not allow customization, because it is based on the Import File downloaded from Trend Micro. However, all of the policies are set by default to **Quarantine** messages that match the stated criteria and you can change the action to **Archive** or **Delete** matched items instead.

Creating Content Filter Policies

Generally speaking, keywords linked on the same line should not include more than four or five values or they risk being overly restrictive. On the other hand, if only one keyword is included on any given line, the policy risks being too permissive—too many email messages will be found to match. Of course, a lot depends upon what you are filtering for.

The criteria you specify are evaluated exactly as they are entered, including any quotes, spaces and punctuation. Phrases, delimited by commas, are treated as a single unit. Only when each word, space, etc. in the phrase is found to appear in the message, and it appears in the order entered, is a match triggered.

Note: Do not use quotes to signify a phrase. Use commas to delimit multiple words entered in a single Keyword field.

Step-by-Step Example

In this example we create a policy to check email messages for the word "floozy".

Since we are creating a new policy, set the **Action** to **Archive** at first as a safeguard against errors. Neither the **Sender,** nor the **Recipient** will be informed of the message evaluation. Edna Brokaw, the human resources manager, will be automatically notified. Additionally, if the message being sent contains Edna's name (as appears in her signature at the end of her email), the message will be ignored even if a match is made.

1. In eManager, click the **Content Filter** tab, then the **Add** option that appears below the Policies list.
2. In the **Policy name** field, enter a name for the policy, in this example, **Sex**.
3. Define the **Action** to take whenever a match is detected.
   - Choose **Archive** to save a copy of the email in the archive directory, but also deliver the original to the intended recipient.
   - Choose **Quarantine** to move, without delivering, the message to the quarantine directory.
   - Choose **Delete** to remove the message from the server without saving or delivering it.
4. Click the **Add** option that appears below the Keyword lists field and enter the word or phrase you want to scan for. **Add** (i.e., create) a new keyword for each word or phrase that you want the content filter to check for. For example, *Floozy.*
5. To check for synonyms of the word or phrase:
   a. Select **Check Synonyms** to have the content filter suggest additional words with a similar meaning. By default, these suggested words are not considered.
   b. In the **Synonyms** list box, highlight the keyword you want to check for synonyms, and click the word or words in the **Exclude** list to move them to the **Include** list.
   c. Click << or >> to move a word from one column to another.
6. In the **Take NO Action if Message Contains** field, enter the name of Edna Brokaw, the HR manager, to exempt her email from the policy. (Do this to allow Edna to reply to any messages that contain sex messages sent to the HR department.)
7. Configure the **Notifications** so that Edna is automatically sent an email whenever a violation of the sex policy is detected. Select **Notify the following administrator(s)** and enter Edna's email address. The message sent is as follows:

   Edna: I am forwarding an email to you for review. Please determine whether this individual is receiving messages about sex. The email was delivered, but if the behavior continues you may want to discuss policy with him or her.

Because of the sensitive nature of this policy, neither the message sender or intended recipient are informed of the action. Alternatively, you can have a mild warning automatically sent to the **Recipient**:

A message you received appears to violate the company email policy. We do not condone the use of company time and equipment for viewing sexual material; please refrain from this behavior in the future. If you feel that you've received this message in error, email your concerns to the following address: admin@yourcompany.com.

Click **OK** to add the policy to the **Policy list**.

8. Back on the **Content Filter** tab, select the policy name if it is not already selected.
9. Select **Use exact matches only**.
10. Click **Apply** to save the Policy and stay in eManager or click **OK** to save the Policy and exit eManager.

Using the Content Filter to Block Spam

You can use the content filter to block spam, especially spam mail which appears to comply with anti-spam legislation. Legislation requires that bulk emailers provide a means of removal from the spamming list. This requirement provides a convenient way to exclude email based on the placement of the word "remove" or the legislation reference itself.

For example, create a new Policy and add keywords such as the following to cover a wide range of "remove" phrasings:

remove in the subject line
"remove" in the "SUBJECT"
"remove" in the subject line
remove in the "subject" line
remove list
Per Section 301, Paragraph (a)(2)(C) of S. 1618

Disable **Case-sensitive comparisons** in the **Content Filter** screen to have the filter trigger a match for *remove, REMOVE, ReMove*, etc.

Content Filter Options

The Content Filter screen displays all the current policies and is where you can enable and disable policies. You can also set the Global Policy Settings which apply to all policies listed.

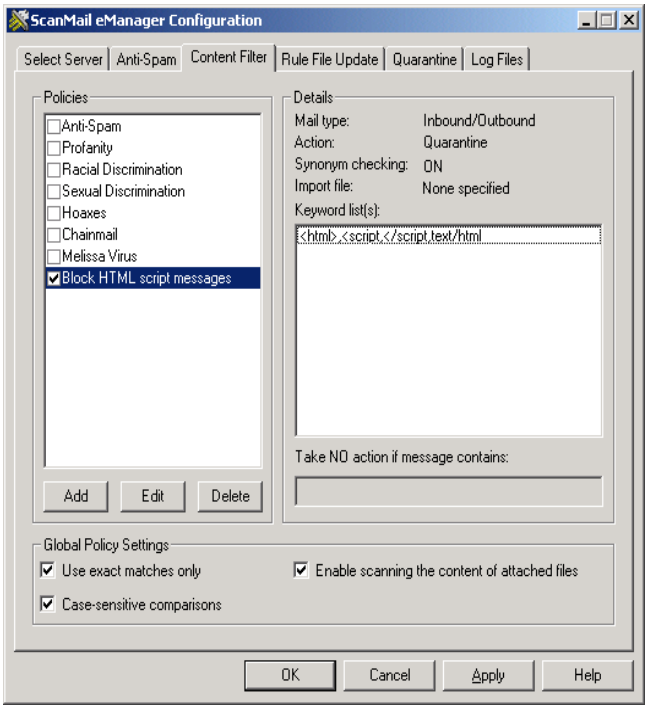


FIGURE 4-2. Content filter policies can include multiple keyword sets, synonyms, import files, and anti-keywords.

Policies

The **Policies** list shows the individual rules by which inbound and outbound messages are evaluated.

Messages found to match all the criteria specified in any one of the policies trigger the action (Quarantine, Archive, or Delete) specified. A notification message is then automatically sent to the administrator or other specified party.

The AND operator is implied within any given keyword-set, whereas the OR operator is implied between keyword-sets.

Note: Binary attachments encoded using MIME, UUencode, or other encoding schemes are not evaluated. Non-encoded text files and Word documents are included in the evaluation.

The contents of the message text are considered in addition to the header data. The evaluation of mail traffic against the policies starts from the first, or top rule, and proceeds down through to the end. As such, it is advisable to place policies with the broadest reach at the top of the list, and those that are more narrowly defined at the bottom.

There is no limit to the number of policies you can create.

Details

The content filter **Details** area provides a detailed summary of the currently highlighted policy. The data represents the **Add/Edit Policy** screen and serves as an extension of the policy name, offering more information on the make-up of a given policy.

To change the values that appear in the Details area, click **Edit** below the Policies list. Make your edits and then click **OK**. The Details area reflects the currently highlighted policy name.

Available fields include: **Mail type**, **Action**, **Synonym Checking**, and whether the **Import file, Keyword list(s):** and the **Take NO action if message contains** settings are in use for a given policy.

Keyword Lists

The Keyword list(s) box on the main Content Filter tab displays the keywords used in whatever policy is highlighted in the Policies list box.

Add/Edit Policy Options

The criteria you specify for content filter policies are evaluated exactly as they are entered, including any quotes, spaces and punctuation. Phrases are treated as a single unit. A match is triggered only when each word, space, comma, etc. in the phrase is found to appear in the message.

Note: Do not use quotes to signify a phrase, or commas to delimit multiple words entered in a single field. Instead, create separate rules. Wildcard characters such as * are not supported in the content filter. If included in a rule, this character is taken literally.

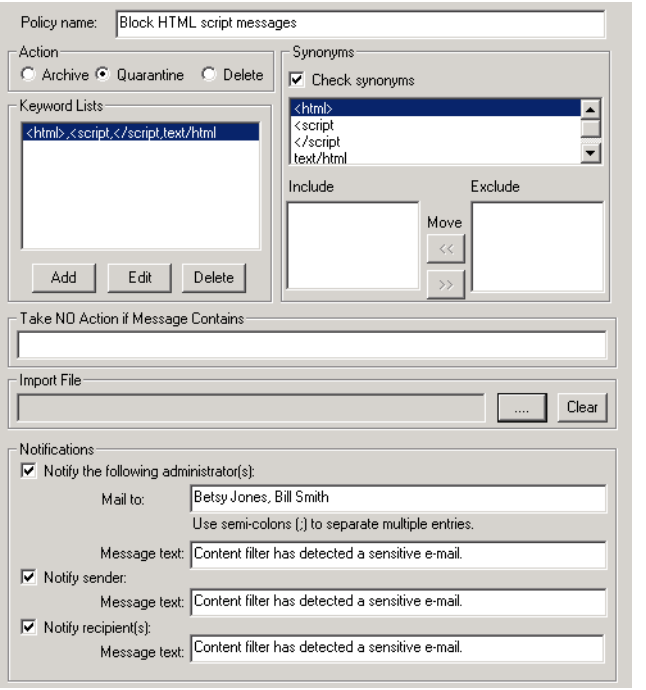


FIGURE 4-3. Add/Edit Policy Screen

Add/Edit Policy options are individually configured for each policy you create. Each of the options are explained below.

Policy Name

Use the **Policy Name** field to create mnemonic names for the policies you create. The name, which appears in the **Policies** list, is not evaluated against the content of the message.

Messages are evaluated first against all the conditions in the first policy, and if no match occurs, against the second rule, the third, etc.

Action

Messages found to match the criteria specified in a given content filter policy can be **Archived**, **Quarantined**, or **Deleted**.

We recommend that you **Archive** messages for the first few weeks following the creation or modification of your content filter policies. You can then check these messages to evaluate the efficacy of your policy. The original message header is attached to the message.

For example, if you inadvertently created a policy where one of the policies consisted of the keyword "the", every email message passing through the Exchange server would match. If the **Action** is set to **Delete**, the error is unrecoverable. If the action is set to **Archive**, however, no harm would be done and you could easily modify or delete the errant keyword after discovering the error.

Archived mail is delivered normally, but also renamed and copied to the specified archive directory. The **Archive** option is set on a policy-by-policy basis.

Quarantined email messages are not delivered to the intended recipient. Instead, they are renamed and moved to the specified quarantine directory.

Keyword List(s)

Whenever a policy is highlighted in the **Policies** window, all keywords associated with a given policy appear in the **Keyword list(s)** window. Keywords appearing on the same line are implicitly connected by the AND operator (the message must contain all the words to trigger a match). Keywords appearing on different lines are

implicitly connected by the OR operator (the message can contain any of the words from the various lines).

The following is an example to illustrate the relationship within a policy between multiple keywords contained on the same list-line vs. keywords listed on multiple lines. It shows a content filter rule-set.

Keyword List (to add in the **Add/Edit Policy** screen):

> ***Rule 1)*** *free offer, hot deal, dollars*
> ***Rule 2)*** *dollars, $$$*
> ***Rule 3)*** *free offer, dollars, earn*

In this rule-set, a match occurs for only those emails that contain [the phrase "free offer", *and* the phrase "hot deal", *and* the word "dollars"], ***or*** [the word "dollars" *and* the term "$$$"] ***or*** the phrase ["free offer", *and* the word "dollars", *and* the word "earn"] anywhere in the contents of the message text.

The following paragraph matches the rule-set above:

> *Free Offer — Hot Deal. Make dollars fast with a 60 day no-risk money-back guarantee.*

This paragraph triggers a match because it corresponds to the first rule (it contains the phrase "*free offer*", and the phrase "*hot deal*", and the word "*dollars*"). Because the first rule matched, the second and third rules are not evaluated.

The second and third rules would not match if they were evaluated. Although the paragraph contains the word "*dollars*", it does not also contain the term "$$$." Nor does it not match the third rule. Although it contains the phrase "*free offer*", and the word "*dollars*", it does not also contain the word "*earn*".

Since the paragraph is found to match at least one of the three rules that make up the policy, it triggers a match and the action specified for the policy is carried out.

Using Synonym Checking

Synonyms are an extension of the content filter's **Keyword list** and can be used to broaden the reach of a keyword to include conceptually related topics. Synonym suggestions for a given word or phrase must be added to the **Include** list to be considered by the content filter.

Note: Global property settings for both **Case-sensitive comparisons** (enabled on the **Content Filter** tab) and **Exact Match** are also applied to synonyms.

As previously noted, multiple keywords appearing on the same line of the list are implicitly connected by the **AND** operator. Individual lines of the list are implicitly connected by the **OR** operator.

When synonym checking is engaged, a combination of the two is applied.

Keyword List Example

Case 1. Keywords appear on a single line

```
Apple Juice, Pear, Orange
```

Case 2. Keywords each appear on their own individual lines

```
Apple Juice
Pear
Orange
```

Case 3. Keywords appear on a single line and synonym checking is enabled for the word Orange,

```
Apple Juice, Pear, Orange
orangish
red
yellow
```

where the words *orangish*, *red*, and *yellow* are included from the synonyms list.

- In **Case 1**, only messages containing all items, *Apple Juice*, *Pear*, and *Orange* (in any order, anywhere in the message text) are considered a match.
- In **Case 2**, all messages containing the phrase *Apple Juice* are considered a match, all messages that contain the word *Pear* are considered a match, and all messages that contain the word *Orange* are considered a match.
- In **Case 3**, with synonym checking on, messages that contain the phrase *Apple Juice*, and the word *Pear*, and also contain any of the word(s) *Orange*, *orangish*, *red*, or *yellow* are considered a match.

Notes:

Apple Juice is a phrase because the words *Apple* and *Juice* are not delimited with a comma; even if the words *Apple* and *Juice* both appear somewhere in the message, no match is triggered unless they occur together, as *Apple Juice*.

The capitalization and exact-match properties of synonyms are consistent with those defined on the Content Filter tab. In other words, if the word *red* appears in the synonyms list , it only triggers a match with the word ***red****undant* if **Exact Match** is not selected; likewise, the word *red* only triggers a match with the word *Red* in the message text if **Case-sensitive comparison** is not selected.

Take NO Action if Message Contains

The **Take NO Action if Message Contains** option allows you to define exceptions or "anti-keywords" that apply to all the rule sets.

Even if all the values specified in a given keyword list are detected in a message, no action is taken if any of the words or phrases appearing in this field are also found.

Like a keyword list, individual words and phrases are delimited with a comma and connected with an **OR** operator. A message that matches on two keywords or phrases (for example, *free offer* and *hot deal*) that would ordinarily be blocked, would not be blocked if the message also matched *any* of the words or phrases specified in the **Take No Action if Message Contains** field.

Unlike the keyword list, where multiple rule sets are possible, multiple **Take No Action if Message Contains** lists cannot be created for a single policy.

Example

You may want to set a policy to block *Free Offer* email, but do not want to block email that includes the option for users to take themselves off the mailing list. To set up this exclusion, type a phrase such as "*To remove yourself from this list*" in the **Take No Action If Message Contains** field.

Use a comma as a delimiter if you want to enter multiple phrases.

Note: It may not be a good idea to accept mail containing the phrase "*To remove yourself from this list*". Some Spammer's take any reply as just confirming that they have reached a valid email address. It could be safest to block messages containing this phrase.

Import File

Trend Micro provides special keyword lists that are designed to efficiently filter out certain types of spam and other unwanted email based on message content. Contained in "Import files", these policies go beyond the quick header checking used by the spam filter, and instead filter messages based on an analysis of the actual message content. Import files, like the Rule-file, are updated monthly by Trend Micro and can be downloaded "on demand" or scheduled for automatic downloads.

Additionally, Import files can be developed by the user to augment an existing content filter policy. These files might include an existing list of keywords exported from a database or spreadsheet program, from the U.S. Federal Trade Commission's "dirty-dozen" list of the worst spam scams, or from keyword lists solicited from department heads and other concerned individuals in your organization.

Import File Format

Entries must be ASCII characters only. Edit an Import list using an ASCII editor (for example, Notepad) and disable the Word Wrap feature, if any. Quotes should not be used.

Delimit individual words and phrases within a policy using commas. Multiple words and/or phrases within a line are implicitly connected by an AND operator.

Define individual rules within a policy with a carriage return (line break). Multiple rules (i.e., multiple lines containing line breaks) within a policy are connected by an OR operator.

Notifications

Whenever the content filter acts upon an email message, the email administrator and others can be automatically notified of the action.

Content filter notifications are policy-based to allow different people to be notified depending on which policy registers the rule violation. For example, you may want to notify your HR department whenever the **Sexual Harassment** or **Racial Harassment** policy triggers a match.

You can set policy specific notifications as follows:

1. With eManager running and the **Content Filter** tab active, click the **Add** or **Edit** option that appears below the Policies window.
2. Select **Notify the following administrator(s)**, **Notify sender**, and/or **Notify recipient(s)**.
3. If you selected to notify the administrators, specify the email addresses of the parties to whom you want a notification sent in the **Mail to** field.

   Multiple email addresses should be delimited with semicolons.
4. In the **Message text** field, enter the message text you want the notification recipient to receive, for example:

   ScanMail eManager content filter archived an email thought to contain offensive text.

Global Policy Settings

Three options on the **Content Filter** tab are global, i.e., not Policy-dependent:

- Use exact matches only
- Case-sensitive comparisons
- Enable scanning the content of attached files

When enabled, the global options are applied to the keyword list(s) that are defined in the **Add/Edit** screen of every policy and any included **Synonyms**.

Exact Matches

By default, words included in the **Keyword list(s):** are considered a match if the specified word matches any part of the message text.

More specifically, only when the total number and order of letters in the two words being compared are the same, is a match valid. Accepting partial words as a valid match can increase the incidents of false positives.

For example, if "*Free*" is specified as a keyword, an occurrence of the work "***Free****zer*" in the message text is considered a valid match.

For content filtering, the **Use exact matches only** field applies to all policies. Therefore if you do not select exact matches, every keyword or phrase used in every list for every policy is considered for partial matches. We recommend that you enable **Use exact matches only** for content filtering.

Case-Sensitive Comparisons

By default, capitalization is not considered when evaluating the content filter policy keywords. Unless **Case-sensitive comparisons** is selected, "*Free Offer*", "*Free offer*", and "*free Offer*" are considered a match for "***free offer***".

Enable Scanning the Content of Attached Files

You can select **Enable scanning the content of attached files** if you want to evaluate the text in attachments for content violations in addition to the message subject and body text. Non-encoded text files and Word documents can be scanned for their contents.

Note: Scanning the content of attached files takes longer than just scanning the message subject and message body.

Chapter 5

Rule, Import, and Log Files

As new spam is written and released onto the public, Trend Micro monitors and collects telltale blocking information and incorporates it into new Rule and Import files. The Rule File Update screen provides configuration choices for these two types of files:

- The Vendor-Provided Rule File is used by the spam filter and contains numerous predefined anti-spam rule-sets.
- Import Files are used by the content filter and can augment existing policies.

Clearly, it is very important to keep these files up-to-date. New Rule and Import files are published regularly by Trend Micro. This chapter includes information on configuring automatic Rule and Import file updates from Trend Micro.

The Log Files screen provides viewing and configuration choices for ScanMail's logs. Log Files are kept whenever ScanMail eManager takes action on an email message. View log files, for example, to evaluate new rules and policies created for the spam and content filter.

This chapter includes information on the log files provided by eManager and how to set up automatic log deletion.

Rule and Import File Formats

The rule and import files are kept in the following directory:

```
\Trend\SMCF\spamrule
```

Rule files are named according to the following convention:

```
Trend$RF.###
```

The Anti-Spam Import files are named according to the following convention:

```
AntiSpam.###
```

where **###** represents the file version. When multiple rule and import files exist in the directory, only the one with the most recent extension (the highest number) is read.

Updates are available free to registered ScanMail eManager customers for a year; they can be scheduled for automatic download over the Internet, or updated "on demand."

Rule File Information

The following information is available on the Rule File Update screen:

- **Version of last rule file (Trend$RF):** Used by the spam filter, represents the current rule file version.
- **Date of last rule file (Trend$RF) update:** Used by the spam filter, represents the current rule file date.
- **Version of last imported Anti-Spam policy:** Used by the content filter, represents the current import file version.
- **Date of last imported Anti-Spam policy update:** Used by the spam filter, represents the current import file date.

Click **Refresh** after adding a new rule file to display the most current settings.

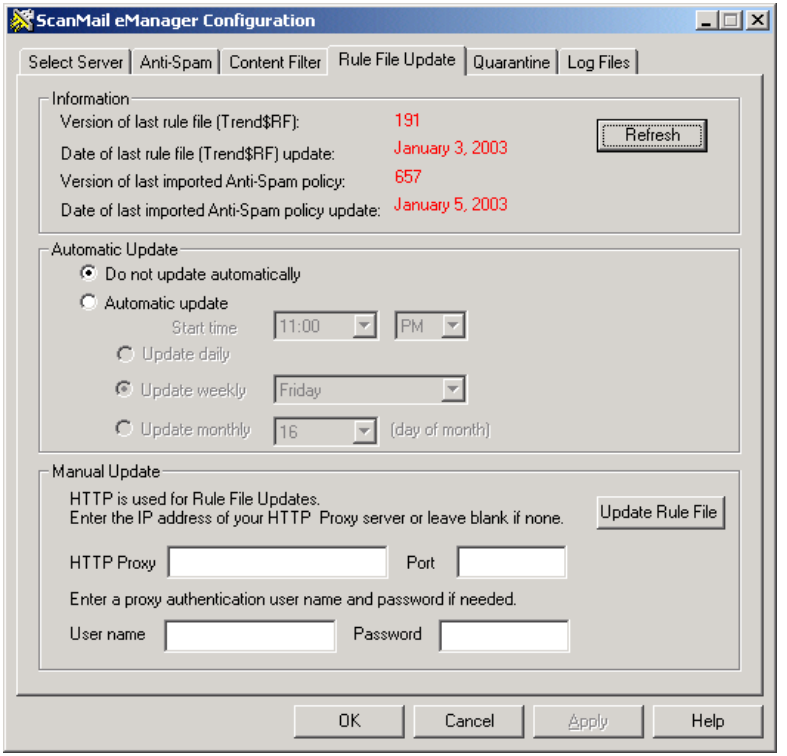


FIGURE 5-1. Existing anti-spam rule-sets, called the Rule File, can be automatically downloaded from Trend Micro.

Automatic Update

When **Automatic update** is selected in the **Rule File Update** tab, the content filter automatically updates the Rule and Import files from Trend Micro at the interval specified.

New files are published regularly and special releases are occasionally made to address new spam issues that are likely to pose an immediate problem for customers. We recommend that you schedule automatic Rule and Import file updates.

Updating the Rule File Automatically

To schedule automatic updates:

1. Choose **Automatic update**, which enables the schedule options. Select a suitable **Start time** for downloads and then select from the **Update daily, Update weekly,** or **Update monthly** update options.
2. Enter the IP address or domain name and port of your HTTP proxy server if one is required for eManager to contact Internet addresses.
3. Enter the appropriate logon credentials (proxy user name and password) if they are required.
4. Test your proxy information by clicking **Update Rule File** to perform an immediate download of the pattern files.
5. Click **Apply** to save your settings and stay in eManager or click **OK** to save your settings and exit eManager.

Manual Update

To perform an immediate update of the Rule and Import files:

1. If an HTTP Proxy server is used on the network, enter its IP address/domain name (name or number) and Port number in the fields provided.
2. Enter the appropriate logon credentials (proxy user name and password) if they are required.
3. Click **Update Rule File** in the Manual Update section at the bottom of the Rule File Update screen to initiate the update.

   If the current Rule and/or Import file on your server is already up-to-date, you receive a message such as "your rule file is already up-to-date." Otherwise, you may see a progress bar informing you of the download progress. Rule and Import file downloads are usually completed within a few seconds.

   After the files have been downloaded, a status confirmation message appears. There is nothing more that you need to do; the new files are automatically installed and take effect immediately.

Note: You must register eManager before you can download new Rule and Import files.

4. Click **Apply** to save your settings and stay in eManager or click **OK** to save your settings and exit eManager.

Log Files

Logs are kept whenever ScanMail eManager takes action on an email message. You can view logs files for all policies, or select a policy to view its entries. All records meeting Anti-Spam conditions can be viewed by selecting the Anti-Spam policy. Each of the Content Filter policy log records can be viewed individually.

Viewing Logs

To view eManager log files:

1. Start the eManager configuration and make the **Log Files** tab active.
2. In the **Time Period** section, select the log dates you want to view:
   - Select **All dates** to view the log files for all the dates.
   - Select **One month** to view the log files generated over the past 30 days.
   - Select **One week** to view the log files generated over the past seven days.
   - Select **Today** to view the log file generated since midnight of the current day.
   - Select **Range** to view a range of dates, and specify the start and end dates for the log files.

The Log Files screen is shown below:

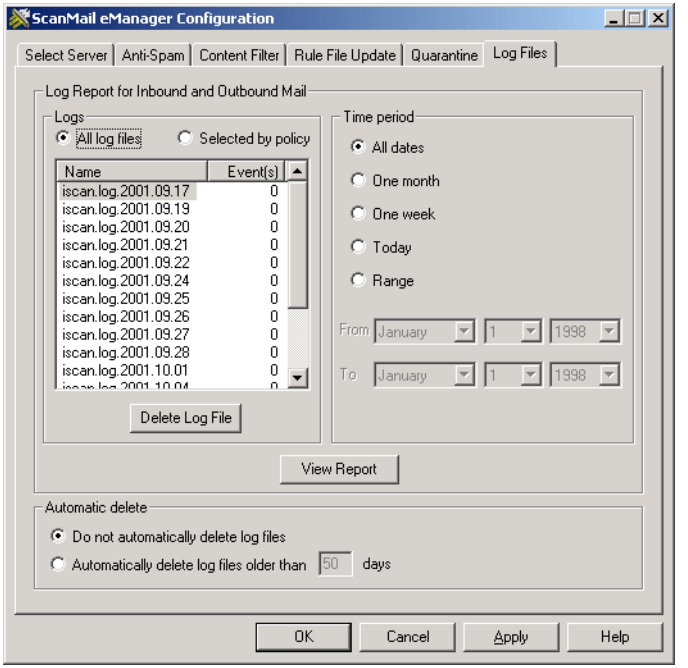


FIGURE 5-2. View all or selected log files from the Log Files screen.

3. Click **View Report**. eManager displays all the logs that fit the criteria you specified.

   The Log Reports popup box displays the Content Filter **Policy** or Anti-Spam **Rule Name**, as well as **From**, **To**, **Action** on matched files, and **Date & Time** the file was scanned.

4. Alternatively, you can view the logs directly from the Logs section:

   a. Select **All log files** to view the logs by date. Then double-click a log file name to view the details, for example:

   ```
   iscan.log.2002.12.04
   ```

   shows the logs produced on December 4, 2002.

b. Click **Selected policy** to view the logs by policy type. Double-click the policy you are interested in: Anti-spam, Profanity, Racial Discrimination, Sexual Discrimination, Hoaxes, Chain mail, or Block HTML script messages.

5. Click **OK** to close the screen and return to the **Log Files** tab.

Deleting Logs

Spam and content filter logs can be automatically deleted after a specified number of days or deleted only at the times you choose.

Automatically Deleting Logs

To schedule ScanMail eManager to automatically delete log files more than a certain number of days old:

1. Open the ScanMail eManager configuration and make the **Log Files** tab active.
2. In the **Automatic Delete** section, click **Automatically delete all logs older than __ days**.

   Enter a value in the **days** field. The maximum is 180 days, meaning that files older than 180 days are deleted if they are left in the default directory. The default value is 30 days.
3. Click **Apply**.

Manually Deleting Logs

To manually delete individual log files:

1. Open the ScanMail eManager configuration and make the **Log Files** tab active.
2. In the **Logs** section, highlight the individual log you want to remove and click **Delete Log File**.
3. Click **OK** to close the configuration window.

Chapter 6

Quarantine Directory, Spam Information, and Technical Support

ScanMail eManager now sends quarantined mail to a quarantine directory rather than a quarantine mailbox. In addition, archived mail is now stored separately in an archive directory. The quarantine and archive directories are user-configurable from the Quarantine screen.

Trend Micro's Web site has a wealth of information on the latest security threats, such as spam and offensive email that can interfere with your companies' productivity. Visit the Virus Information Center to find information on spam, viruses, and malicious code threats. Also on the Web site, visit "SolutionBank", Trend Micro's online Knowledge Base of common answers to technical questions.

This chapter contains information on:

- Quarantine and Archive directories
- Trend Micro's Virus Information Center
- Contacting Technical Support
- SolutionBank
- TrendLabs™

Quarantine Screen

The Quarantine Screen is used to set the quarantine and archive directory locations. The default settings are:

Quarantine directory:

```
…\Program Files\Trend\SMCF\Quarantine
```

Archive directory:

```
…\Program Files\Trend\SMCF\Archive
```

You can edit the directories listed or click **Browse** to locate other directories to use instead.

Quarantine and Archive Directory Structure

ScanMail for Microsoft Exchange and ScanMail eManager back up files sent to Quarantine or Archive under the directory setting specified in eManager. ScanMail for Microsoft Exchange and ScanMail eManager create files in the subdirectories with the following format:

```
/yyyy-mm-dd/HH-MM-SS.counter/
```

The "yyyy-mm-dd" represents the date information, and "HH-MM-SS" represents the time information. Since there is a "counter" in the directory path, no two scanning messages are stored in the same directory.

Trend Micro's Virus Information Center

The Trend Micro Web site has a wealth of information on the latest security threats, such as spam and offensive email that can interfere with your company's productivity. Visit the Trend Micro Virus Information Center to find information on spam, viruses, and malicious code threats. Comprehensive security information is available over the Internet at our antivirus center:

```
http://www.trendmicro.com/vinfo
```

Use the **Virus Information Center** to find out about:

- Which viruses and malicious mobile code are currently "in the wild" or active
- A list of computer virus trigger dates
- Computer virus hoaxes and determining whether a detection is actually a false alarm
- Trend Micro's Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- A basic guide to computer viruses
- A safe computing guide

Contacting Technical Support

A license to Trend Micro antivirus software includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

If you need help, or just have a question, contact us. We also welcome your comments. Trend Micro can be reached by telephone, fax, email, mail or through our Web site at:

```
http://www.trendmicro.com/support
```

- Our main U.S. phone and fax numbers are:

```
Toll free: +1-800-228-5651 (sales)
Voice: +1-408-257-1500 (main)
Fax: +1-408-257-2003
```

- To reach us outside the U.S., call:

```
+1-408-257-1500 (main)
```

- Our U.S. headquarters are located in Silicon Valley at:

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014

Accessing Technical Support from the ScanMail™ for Microsoft Exchange Windows Console

1. Select **Help.**
2. Select **Technical Support**.
3. You are linked to the Trend Micro Technical Support Information screen. Select the country and office you desire support from.

Speeding Up Your Support Call

When you contact tech support, to speed up your problem resolution, ensure that you have the following details available:

- ScanMail product versions for the ScanMail Management Console, ScanMail core module, and ScanMail Web console
- ScanMail pattern file and scan engine versions
- ScanMail eManager Rule and Import file versions
- Microsoft Windows and Service Pack versions
- Microsoft Exchange server and Microsoft Exchange Service Pack versions
- Number of mailboxes
- Network type
- Computer brand, model, and any additional hardware connected to your machine
- Amount of memory and free hard disk space on your machine
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

SolutionBank Knowledge Base

On the Trend Micro Web site, you can visit SolutionBank, Trend Micro's online database of common answers to technical questions, at:

`http://solutionbank.trendmicro.com/solutions/solutionsearch.asp`

In the ScanMail Management Console, access it by choosing **Help > ScanMail SolutionBank**, or open a Web console and go to:

`http://solutionbank.trendmicro.com/solutions`

You can find this resource under **Knowledge Base**. After signing up, under **Knowledge Base** in the left navigator pane, click **Search Solutions**. In the Product list box, use the drop-down arrow to select **ScanMail for Exchange**.

Alternatively, you can select **FAQs** to view a list of the most frequently asked questions.

The SolutionBank contents are being continuously updated. If you are unable to find an answer, however, click **Submission Wizard** and fill out the requested information. A Trend Micro support engineer will investigate the issue for you.

TrendLabs™

TrendLabs is Trend Micro's global complex of antivirus research and support centers. It's located on three continents, with a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Free email access to antivirus engineers
- SolutionBank, Trend Micro's online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Appendix A

Control Manager Agent for ScanMail eManager

Trend Micro Control Manager delivers powerful centralized management of antivirus and content security strategies deployed throughout a network. With single point-of-contact administration, monitoring, and deployment, corporations can more effectively manage their antivirus and content security strategies enterprise-wide. Control Manager provides a framework for the Outbreak Prevention Service that assists in collectively addressing the antivirus concerns of the business.

The Control Manager server communicates with its managed products through applications called agents. Trend Micro ScanMail eManager for Microsoft Exchange uses a Control Manager agent specifically designed for the product. Through Control Manager, you can remotely configure groups of servers to perform the same tasks and use the same configuration settings. If you have a large network, Control Manager can greatly reduce the time you spend configuring your servers.

This chapter includes information on:

Introducing Trend Micro Control Manager

Control Manager builds on the centralized management concept Trend Micro pioneered with Trend Virus Control System (Trend VCS). If you are currently running Trend VCS, you can purchase an upgrade to obtain all the new benefits of Control Manager. For more information on upgrading your management server from Trend VCS to Control Manager, see the *Trend Micro Control Manager Getting Started Guide*.

Key features of Control Manager include:

- Centralized management, which allows administrators to configure, monitor, and maintain Trend Micro software installed on the network from a single console — regardless of location or platform.
- Flexible and scalable configuration, which simplifies the administration of a corporate virus and content security policy.
- A hierarchical structure for job delegation so administrators can determine access control. Different operators can be assigned separate access to individual branches of the hierarchy.
- Outbreak Commander provides a proactive attack protection service. It blocks malicious code, by file name or specific file details, while new pattern files are being developed that can detect and clean the new threat.

Control Manager uses a new communications infrastructure called the Trend Micro Management Infrastructure (TMI) that is built on the Secure Socket Layer (SSL) protocol. TMI protects communication between the Control Manager server and

managed product with a combination of encryption and authentication, depending on the security settings.

What is the Outbreak Prevention Service?

The Outbreak Prevention Service (OPS) allows enterprises to take proactive steps against new virus threats before the necessary virus pattern file update becomes available. By bridging the gap between threat notification and virus pattern delivery, enterprises can quickly contain virus outbreaks, minimize system damage, and prevent undue downtime.

OPS provides you with outbreak prevention policies — product setting recommendations designed to secure your network during outbreaks. These policies are applied to the products managed by Control Manager using Outbreak Commander. Outbreak Commander applies policies in the following stages:

1. Prevention — threat information delivery and deployment of precautionary content security policies (anti-spam rules) while a new virus pattern file is being developed.
2. Notification — notifications are automatically sent to the individuals and groups configured.
3. Scanning — real-time scanning on antivirus products is enabled.
4. Updates — a new virus pattern file is deployed to the antivirus product. If the threat requires development of a new scan engine, the scan engine can be automatically deployed as well.

What are the Components of the Agent Installation Program?

The agent package is composed of two parts:

- The Communicator
- The agent program

The Communicator is the managed product-side component of the Trend Micro Management Infrastructure (TMI) — the communications backbone of the Control Manager network. Control Manager agents have their own local Communicator, which is shared by all the agents on that server. Though there can be as many agents on a server as there are managed products, only one Communicator is required for

each server. The TMI uses the same encryption key and message routing settings for all agents installed on a server.

The Communicator can be upgraded and released independently, without upgrading the agent itself.

Control Manager agents serve two primary purposes:

- Receive command inputs from the Control Manager server and apply them to the managed product
- Collect logs from the product, and report them to the Control Manager server

System Requirements

To install the Control Manager agent for ScanMail eManager, you need the following minimum hardware and software on your Exchange server:

- Intel™ Pentium™ 300MHz processor (or higher recommended)
- 128MB RAM minimum (256MB or more recommended)
- 50MB free disk space for the agent program files
- Microsoft Windows NT 4 with Service Pack 3; Microsoft Windows 2000 Server or Advanced Server
- Must be installed on an NTFS partition

Control Manager Agent Installation Notes

The agent that is installed depends on the version of the Trend Micro product that you are using. With Control Manager, ScanMail eManager for Microsoft Exchange has its own agent. Trend Micro ScanMail for Microsoft Exchange has its own agent that displays the ScanMail configuration screens. To manage both ScanMail eManager and ScanMail running on the same server, you install the Control Manager agent for ScanMail for Microsoft Exchange and the Control Manager agent for ScanMail eManager.

The Control Manager agent for ScanMail eManager for Microsoft Exchange installation files are included on the Trend Micro Enterprise CD.

Information Needed Before Starting Agent Installation

You will need the following information before deploying the agents:

- Fully Qualified Domain Name (FQDN) or IP address of the Control Manager server
- Administrator privileges on the Exchange servers where agents are to be installed
- Presence of shared drives on the target server. There must be at least one shared drive on the remote server to install an agent
- A Control Manager User ID with an Administrator, Power User, Operator, or root account type

Note: It is very important to maintin this account. If the Control Manager User ID is deleted, the agent won't be able to re-register with the Control Manager server.

- The location of the public encryption key of the Control Manager server with which you intend to register the agent

Note: Do not install the Control Manager agent using Terminal Services.

Installation Steps

Installation consists of the following steps:

- Obtain the Public Encryption Key
- Obtain the Remote Install program
- Loading the agent package on the Control Manager server
- Install the agent

Obtaining the Public Encryption Key

To obtain the public encryption key needed for installation:

1. Open the Control Manager console at:

```
http://computer name/ControlManager
```

where “computer name” is the IP address or host name of the Control Manager server.

2. Enter a **User ID** and **Password**. The User ID can be a Control Manager Operator, Power User, Administrator, or root.
3. Select **Products**.
4. Select **Add/Remove Product Agents**.
5. Right-click the **Public encryption key**, then select **Save Target As**. Save the public encryption key in a location that is accessible to the server upon which the agent will be installed.

Obtaining the Remote Install Program

To obtain the setup program:

1. Click **Products** on the menu.
2. Click **Add/Remove Product Agents** on the left-hand menu.
3. On the Add/Remove Product Agents screen, click **Use this** for the Control Manager agent update packages.
4. At the File Download screen, select **Save** to save the program to disk.
5. At the Save As screen, select a location for the program, and then click **Save**.

Loading the Agent Installation Package

To load the agent package on your Control Manager server:

1. Using Windows Explorer, double-click **`RemoteInstall.exe`**.
2. At the Control Manager Agent Setup screen, click **Add/Update packages**.
3. In the Add/Remove Agent Packages screen, enter the following information:
   a. Type the IP address or host name of the Control Manager server to be updated in the **Host** field.
   b. Type the UNC path of the agent package for eManager (`RemoteInstall.xml`) in the **File** field.

Alternatively, click the ellipsis button (". . .") to locate the package, and then click "Open".

Note: The agent files are located on the Trend Micro Enterprise Solution CD.

c. Click **Next**.

4. In the Agent Package Information screen, compare the package to be uploaded with the package currently on the Control Manager server. To continue with the upload, click **Upload**.
5. After completing the upload, click **OK**.

Installing the Control Manager Agent

Log on the setup machine using a Windows Administrator account with Domain Administrator privileges.

To install the Control Manager agent:

1. Click **RemoteInstall.exe** to start the installation process. The Control Manager agent setup screen opens.
2. Click **Install**.
3. In the **Welcome** screen, click **Next**. Read the License Agreement screen; you must agree to the license conditions to proceed with Setup.
4. Specify, and provide logon credentials for, the Control Manager server that contains the agent package. Type the following information:
   - **Host name** — IP address or host name of the Control Manager server
   - **User name** — use domain\user name format
   - **Password**
5. In the list of products that appears, choose eManager for ScanMail for Microsoft Exchange and click **Next.** If the required agent is not on the Control Manager server, either select another server, or obtain the necessary agent package. See *Loading the Agent Installation Package* starting on page A-6 for more information.

6. When the **Select Target Servers** screen appears, select the servers on which you want to install the Control Manager agent for ScanMail eManager. From the list in the left pane, you can highlight each target server name or highlight the Domain name to install the agent on all servers in the Domain. Double-click a Domain name to view the servers in that domain. After you have finished making your selections, click **Next**.
7. Provide Administrator-level logon credentials for the selected servers:
   - **a.** Type an Administrator account or the Administrator account preceeded by the Domain name for the **User name**.
   - **b.** Type the **Password** for the specified administrator account.
   - **c.** Keep the default temporary **Share** directory, C$, or specify a different share name for which the specified User has **Full Control** access rights. This share is used for copying the temporary installation files and is accessible by the administrator only.
   - **d.** Leave the check box "Retain user name and password after logging on" selected if you want to log on multiple servers with the same account.
   - **e.** Click **Log on**.

   For servers that require different logon credentials, Setup displays the Server Logon screen again.
8. After the logon process, Setup displays a list of the selected servers. Click **Next** and then **Next** again on the following screen.
9. Type an Administrator, Power User, Operator, or the root account on the Control Manager server for the **User ID**. Be sure to maintain this account. If the account used here is deleted, either deliberately or accidentally, you are no longer able to manage the agent.

Note: Trend Micro recommends that you use the root account when installing agents.

This **Entity name** is used to identify the product agent in the Control Manager server console directory.

10. When the Message Routing Path configuration screen appears, set the path for incoming and outgoing messages.

    a. Incoming messages can be received using any of the following methods:

    - Any host — accept message from any source (the default)
    - IP port forwarding — enter the IP address and port numbers that have been mapped for Control Manager communication
    - Proxy server — click **Proxy Server Configuration** to specify the proxy server IP address, port number, and type (HTTP or SOCKS 4/5). If your proxy server requires, select **Authentication required** and specify the **User name** and **Password**

    b. Outgoing messages can be sent either directly or via a proxy server:

    - Direct to server (the default)
    - Proxy server — click **Proxy Server Configuration** to specify the proxy settings.

11. To set up secure communications with the Control Manager server, click **Import**. Locate the public encryption key, `E2EPublic.dat`, of the Control Manager server you are registering the agent with.

12. Follow the installation prompts to complete the installation.

To verify that the Control Manager agent installation was successful, open the Control Manager console described in *Performing Tasks from the Trend Micro Control Manager Console* starting on page A-11.

Removing the Control Manager Agent

You can remove the Control Manager agent for ScanMail eManager for Microsoft Exchange locally on the Exchange server, or remotely from another server or workstation on the network.

Local Removal of the Control Manager Agent

To remove the Trend Micro Control Manager agent for ScanMail eManager for Microsoft Exchange locally:

1. Click Windows **Start > Settings > Control Panel > Add/Remove Programs**.

2. Click **Trend Micro Control Manager Agent for ScanMail eManager** and then click **Remove**.
3. At the prompt, select **Yes** to remove the Control Manager agent.
4. After uninstallation finishes, click **Close**.

Remote Removal of the Control Manager Agent

You can remove the Control Manager agent for ScanMail eManager remotely from another server or workstation using the Control Manager `RemoteInstall` program.

To remotely remove the Control Manager agent for ScanMail eManager:

1. Click **RemoteInstall.exe** to start the removal process.
2. Click **Uninstall**.
3. In the **Welcome** screen, click **Next**.
4. Specify, and provide logon credentials for, the Control Manager server that contains the agent package. Type the following information:
   - **Host name** — the IP address or host name of the Control Manager server
   - **User name** — use domain\user name format
   - **Password**
5. In the list of products that appears, choose **eManager for ScanMail for Microsoft Exchange** and click **Next**.
6. In the **Select Target Servers** screen, select the servers from which you want to uninstall the Control Manager agent. From the list in the left pane, you can highlight each target server name or highlight the Domain name to uninstall the agent from all servers in the Domain. Double-click a Domain name to view the servers in that domain. Click **Next**.
7. Type an Administrator account or the Administrator account preceeded by the Domain name for the **User name**.

   Type the **Password** for the specified administrator account.

   Click **Log on**.
8. Continue following the removal prompts.

Performing Tasks from the Trend Micro Control Manager Console

The ScanMail eManager agent accepts commands from the Control Manager server and instructs ScanMail eManager to perform them. For example, when you select **Tasks > Deploy virus pattern/spam rule** in the Control Manager console, the Control Manager agent instructs ScanMail eManager to deploy the latest spam rule file.

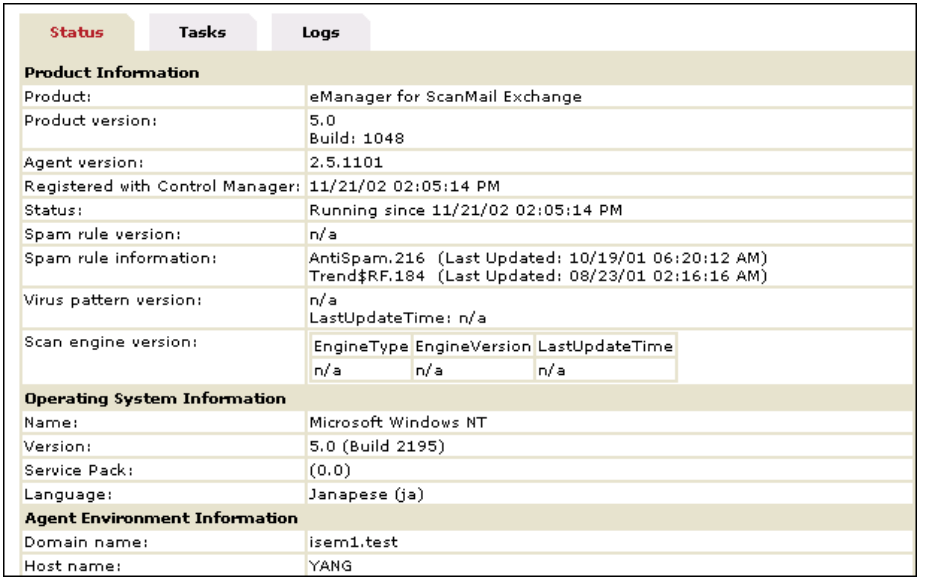
To manage ScanMail eManager from the Control Manager console:

1. Open the Control Manager console at:

   ```
   http://computer name/ControlManager
   ```

   where "computer name" is the IP address or host name of the Control Manager server.

2. Select **Products**.
3. Under the **Product Directory**, select the ScanMail eManager (EMAN) server to configure.
4. The following tabs are displayed:
   - Status
   - Tasks
   - Logs



Status | Tasks | Logs

Product Information	
Product:	eManager for ScanMail Exchange
Product version:	5.0 Build: 1048
Agent version:	2.5.1101
Registered with Control Manager:	11/21/02 02:05:14 PM
Status:	Running since 11/21/02 02:05:14 PM
Spam rule version:	n/a
Spam rule information:	AntiSpam.216 (Last Updated: 10/19/01 06:20:12 AM) Trend$RF.184 (Last Updated: 08/23/01 02:16:16 AM)
Virus pattern version:	n/a LastUpdateTime: n/a
Scan engine version:	EngineType: n/a, EngineVersion: n/a, LastUpdateTime: n/a
Operating System Information	
Name:	Microsoft Windows NT
Version:	5.0 (Build 2195)
Service Pack:	(0.0)
Language:	Janapese (ja)
Agent Environment Information	
Domain name:	isem1.test
Host name:	YANG

FIGURE A-1. Control Manager Management Console, Status Screen

Group Configuration

Using Control Manager, you can configure and perform tasks on multiple ScanMail eManager servers simultaneously. Control Manager requires only that the same ScanMail eManager version is used when performing group configuration and that the servers are listed in the same folder of the Control Manager Product Directory.

To configure a group of ScanMail eManager servers:

1. In the Product Directory on the left-hand menu, navigate to the desired folder that lists your ScanMail eManager servers.
2. Select the folder that contains the ScanMail eManager servers.
3. Select a configuration tab in the main menu. The controls in the **Status**, **Tasks** and **Logs** tabs affect all servers in the folder that use the same version of ScanMail eManager.

Status

By default, the **Status** screen is selected, as shown in Figure A-1. The following information is displayed:

- **Product Information**
  - Product name, product version, and build number
  - Agent version — Control Manager agent version installed
  - Registered with Control Manager — registration date and time
  - Status — date and time agent has been running since
  - Spam rule version and update information
  - Virus pattern version — not applicable for eManager
  - Scan engine version — not applicable for eManager
- **Operating System Information**
  This section includes information on the operating system, such as the version, service pack, and language.
- **Networking Information**
  This section includes network information such as the domain name, host name, IP address, and MAC address.

Tasks

The **Tasks** screen allows you to start a task remotely for individual ScanMail eManager for Microsoft Exchange servers or groups of ScanMail eManager servers. The **Tasks** screen contains the **Deploy virus pattern/spam rule** task.

To immediately download the latest spam rules:

1. Select **Deploy virus pattern/spam rule**.
2. The ScanMail eManager versions are displayed. The task is carried out on the server or folder selected in the left-hand menu. Click **Next**.
3. Click **Deploy Now**.

Viewing Task Results

To view the task details after you exit the Tasks screen:

1. Click **Administration** on the Control Manager Management Console's top menu bar.
2. Click **Command Tracking** to view the commands issued within the previous 24 hours.
3. Click the task status to view the **Command Details** screen.

Logs

In the Control Manager **Logs** screen, you can view the **Event Logs** and **Security Logs**. The Event Logs record events such as virus outbreak, module update, service on/off, and security violations. The Security Logs indicate the sources of virus infections, content security violations, and intrusions.

Event Logs

To view the Event Logs:

1. Select **Logs > Event Logs.**
2. Select the **Severity** of the logs to view (Critical, Warning, Information, Error, or Unknown).
3. Select the **Incident** (All events, Virus outbreak, Module update, Service ON, Service OFF, Security Violation).
4. For Product, select **eManager for ScanMail Exchange**.
5. Select the log period and sort order.
6. Click **View Logs** to view the Event Logs you selected.

   To save the results, click **Save Log as CSV** to save with Comma Separated Values.

Security Logs

To view the Security Logs:

1. Select **Logs > Security Logs.**
2. Select the type of query to perform on the security logs:
   - All virus log incidents
   - Content security violations — these are the log files that relate to ScanMail eManager specifically
   - Viruses found in download traffic (HTTP, FTP)
   - Viruses found in email
   - Viruses found in files
   - Web security violations (applicable for other Trend Micro products)
3. Click **Query**.
4. Select the log period and sort order.
5. Click **View Logs** to view the Security Logs you selected.

   To save the results, click **Save Log as CSV**.

Changing the Control Manager Agent Polling Interval

The Control Manager server polls the Control Manager agent for new information every minute. You can change the polling interval in the file `entity.cfg,` which by default is located in the C:`\Program Files\Trend\SMCF\Agent` directory.

To change the polling interval:

1. Open `entity.cfg` with a text editor, such as Notepad.
2. Edit the polling agent line:

   ```
   StatusLogPollingInterval=60
   ```

   The default value is 60 seconds. The minimum ScanMail eManager will accept is 60 and the maximum is 3600. If you input a value outside this range, it will be reset to the default.
3. Restart the Trend Micro Management Infrastructure Service.

Index

U

V

W

Trend Micro Incorporated
10101 N. De Anza Blvd.
Cupertino, CA., 95014 USA
www.trendmicro.com

For Sales:
Tel: +1 (800) 228-5651 (US and Canada)
Tel: +1(408) 257-1500 (outside US and Canada)
Fax: +1 (408) 257-2003

Item Code: SEEM50893/11101