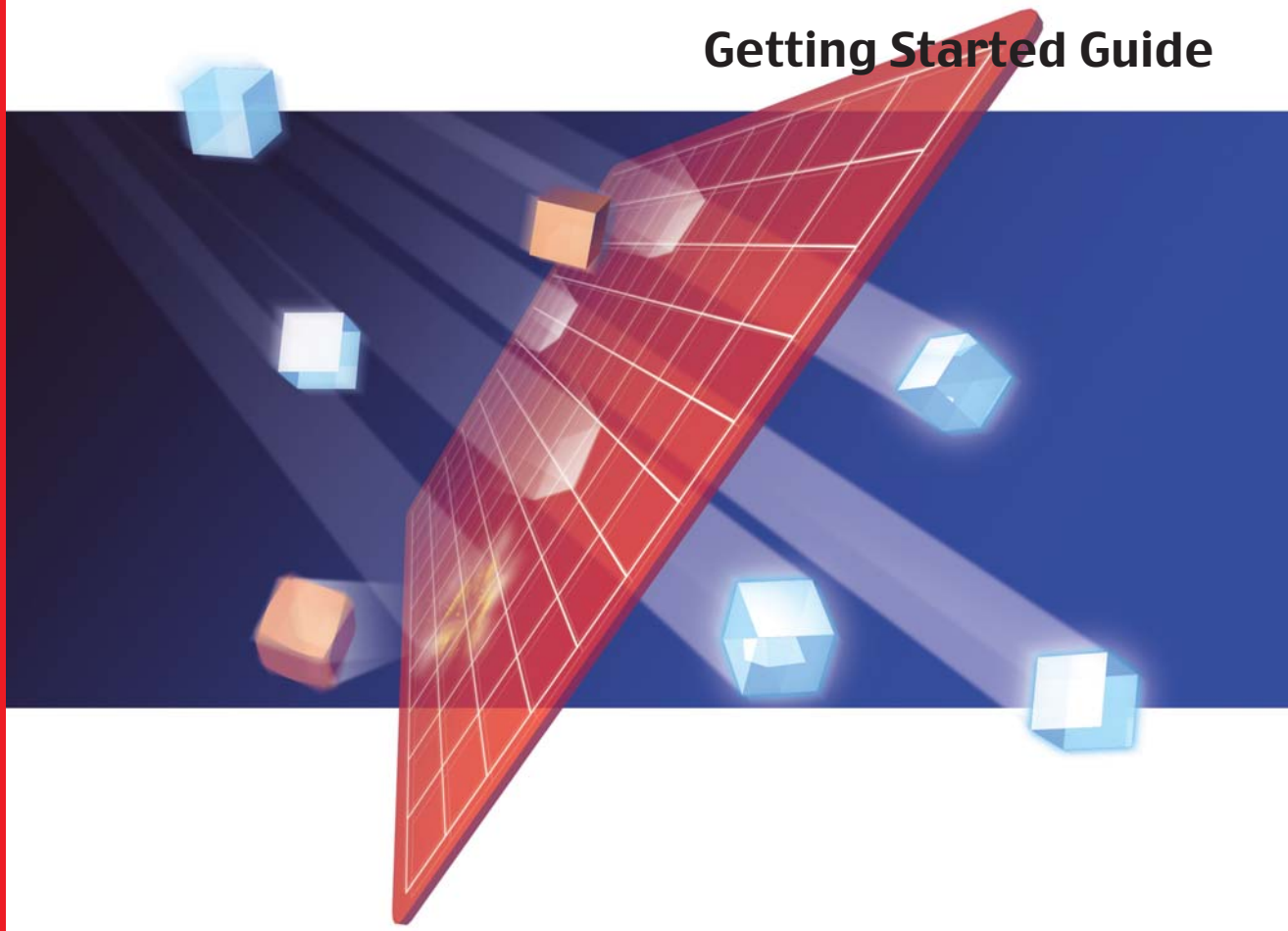
TREND MICRO™

InterScan™ 3 eManager™

for Unix

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 usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Document Part No. IMEM31514/30529

Release Date: August 2003

Protected by U.S. Patents

The Getting Started Guide for Trend Micro InterScan eManager for Unix 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 Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its 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:

www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 1

Introducing Trend Micro™ InterScan eManager™

Trend Micro™ InterScan eManager™ is a part of the InterScan suite of products. Used in conjunction with InterScan VirusWall, eManager provides additional security and management features to an Internet gateway security solution. InterScan VirusWall scans SMTP traffic passing between the corporate network and the Internet. eManager adds the ability to filter out spam mail and inappropriate content.

This chapter introduces InterScan eManager and describes how eManager interfaces with InterScan VirusWall™. The topics include:

- Content Management
  - Spam Filtering
  - Content Filtering
  - Specialized Filtering
- How InterScan eManager processes mail

Content Management

InterScan eManager filters spam mail and checks user messages for content considered sensitive, offensive, or against company policy. Configure eManager to fit your business needs.

InterScan eManager provides **Content Management**, which includes spam, content, and specialized filters.

Spam Filtering

Content Management's **spam filter** quickly evaluates the header fields of messages en route to the SMTP server. 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 anti-spam rules. Content Management can **delete**, **archive**, or **quarantine** spam messages. InterScan eManager does not pass them to the SMTP server for delivery.

Spam rules are user-definable and there is no limit to the number of rules you can employ.

Use the Trend Micro Trend$RF, also called the Vendor-provided Rule File, as part of the current spam filter rules. Trend$RF provides a comprehensive list of spammers, identified by subject, routing domain, or sender.

Content Filtering

Content Management's Content Filter performs an analysis of the message header and body. The content filter evaluates messages based on Trend Micro Bg_AntiSpam (also known as Vendor-provided Import file) and user-defined content filter policies.

Create content filter policies to check for the use of inappropriate language, to guard against the loss of proprietary information, or to scan for resumes.

Content filter policies can check inbound or outbound mail for any type of content. Examples include:

- Sensitive, or restricted business information
- Inappropriate language (for example, "four-letter words")
- Racial slurs
- Indications of job hunting

- Pornography traffickers

InterScan eManager can Quarantine, Archive, or Delete messages that match a spam filter rule.

Specialized Filtering

Content Management's **Specialized Filtering** removes attachments with a particular filename or MIME content-type from email messages and replaces them with a configurable text message. Specialized Filtering uses policies to filter messages based on message headers and attachments. You can configure a specialized filter policy to notify the sender, recipient, or administrator.

InterScan eManager takes the Quarantine action for messages that match a specialized filter policy.

Mail Processing

InterScan eManager components are applicable to incoming (inbound) or outgoing (outbound) SMTP traffic. **Incoming SMTP traffic** refers to mail or Internet traffic originating outside the network that will pass the Internet gateway and into the

network. **Outgoing SMTP traffic** refers to mail or Internet traffic originating inside the network that will pass through the Internet gateway and leave the network.

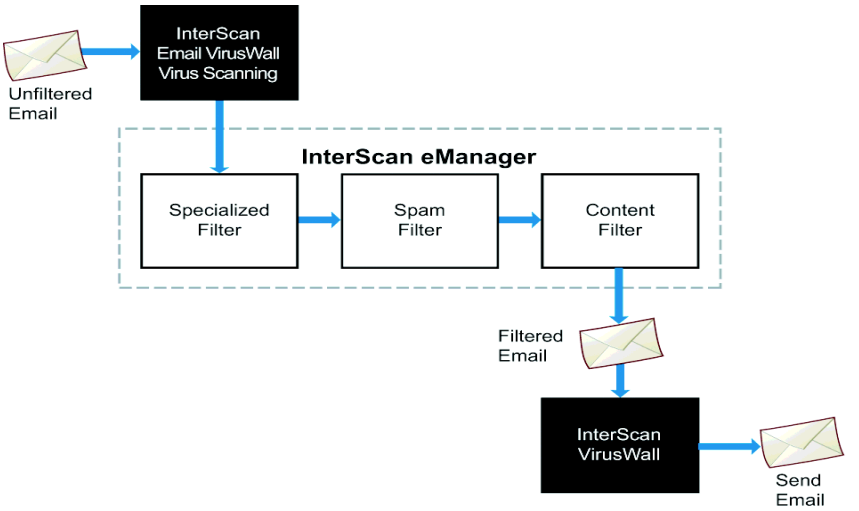


FIGURE 1-1. A graphic overview of the processing order of an incoming email.

On a network with an SMTP server, InterScan VirusWall, and one or more instances of Content Management installed, the mail processing is as follows:

1. InterScan VirusWall receives inbound or outbound mail, scans, and cleans mail for viruses. If the email is clean of viruses, InterScan VirusWall directs the mail to InterScan eManager.
2. InterScan eManager performs spam detection. Content Management compares message header information to the user-defined list of current spam rules and specialized filter policies. Content filter policies filter message content and attachments. Mail that violates a spam filter rule or content filter policy is **Deleted, Archived**, or **Quarantined**; specialized filter policy **quarantines** spam mail. When Content Management takes one of these actions, InterScan eManager stops comparing the message to the remaining criteria.
3. Next, InterScan eManager logs the action taken on the mail. If a violation occurs, the Content Management component logs the violation and stops filtering.

4. Infected email attachments are **Cleaned**, **Quarantined**, **Deleted**, or **Passed**, according to InterScan VirusWall configuration. InterScan passes uninfected and cleaned messages to the SMTP server for processing, as usual.
5. The SMTP server delivers the email to the intended recipient(s).

Chapter 2

Installing Trend Micro™ InterScan eManager™

This chapter provides information on how to install Trend Micro InterScan eManager. The topics include:

- Installing InterScan eManager
- How to get started using eManager
- Enabling Inbound and Outbound filtering
- Upgrading InterScan eManager
- Removing InterScan eManager

System Requirements

Install InterScan eManager 3.8 on a system with InterScan VirusWall 3.6 or above present and at least the configuration indicated below:

Solaris Version

- Solaris™ 2.7 or later on Sun™ SPARC™ platform
- 256MB main memory (DRAM)
- Swap space should be 2 to 3 times the main memory
- 50MB disk space for InterScan and eManager plug-in installation
- Minimum 9GB disk space for processing email messages during operation

Linux Version

To run InterScan eManager version 3.7 for Linux™, you must install to a computer that has InterScan VirusWall 3.7 or above. You need the following minimum configuration:

- IBM/AT™ compatible PC with Intel Pentium™ 133MHz or faster
- Memory: 128MB or more
- Swap space should be 2 to 3 times the main memory
- 20MB disk space for InterScan
- At least 9GB disk space for operation (processing email messages)
- OS: Linux kernel 2.2.12 or above, glibc 2.1.2 or above
  Trend Micro tested on these Linux distributions.
  - RedHat™ Linux 6.1
  - RedHat™ Linux 6.2
  - TurboLinux™ Server 6.1 Japanese version (*)
    * Install C++ standard shared library (libstdc++) package. For more details about its installation, refer to the manuals of your OS.
- Package name: libstdc++-compat

Installing InterScan eManager

InterScan eManager is a plug-in for InterScan VirusWall. Install it on the same machine as E-Mail VirusWall. The current version works with the *Standard Edition* of InterScan. It does not work with the *CVP (Content Vector Protocol) Edition.*

Before Installing InterScan eManager

Important: Before installing eManager, you must have InterScan VirusWall installed on the same machine. The machine should have the following InterScan VirusWall components: the SMTP, ISADMIN, and ISBASE packages. If you do not have these packages installed, install them before continuing with the eManager installation.

Installing InterScan eManager

The eManager setup includes scripts requiring superuser permission — log on as **root** before installing eManager.

To install InterScan eManager:

1. Do one of the following to navigate to the install script:

   If you are installing from a CD-ROM:

   a. Mount Disk #3 of the Trend Micro Enterprise Protection CD into the CD-ROM drive.

   b. Change to directory where the installation package is located. For example, `programs/InterScan eMan Solaris/English` directory.

   c. Locate and copy the distribution file to your local directory.

   d. Run the `gzip` and then the `tar` commands to extract the distribution file.

   ```
   gzip -d {distribution file}.tar.gz
   tar -xvf {distribution file}.tar
   ```

   Where the `{distribution file}` is:

   - `emux_en_sol_v38` for InterScan eManager 3.8 for Solaris
   - `isem_en_linux_38` for InterScan eManager 3.8 for Linux

   If you are installing from a downloaded `gzip` file:

a. Change to the directory that contains the InterScan eManager software.

b. Run the `gzip` and then the `tar` commands to extract the distribution file.

```
gzip -d {distribution file}.tar.gz
tar -xvf {distribution file}.tar
```

2. Locate and execute `install.sh`. The **Main Menu** appears, displaying the installation options.
3. Choose **Option 1** to start the installation.
4. Type a valid 16-digit serial number. Press **Enter** without typing in a serial number to install the 30-day evaluation copy. This version of eManager is fully functional but will expire after 30 days, at which time you should upgrade or remove it. For information on how to buy the product, refer to the following URL:

   `http://www.trendmicro.com/buy/us/enterprise.asp`

Note: You can find serial numbers on the front cover of the InterScan eManager manual and on the product registration card.

   By default, eManager will scan the file system and install under the directory where you installed InterScan. If you installed InterScan into the default `/opt/trend` directory, `install.sh` will install eManager into the `/opt/trend/Plug-Ins/EM` directory.
5. Continue to follow the screen prompts to complete the installation.
6. After installation finishes, `install.sh` displays "InterScan eManager has been installed. Enable eManager from the InterScan VirusWall console." Select **Exit** to close the Main Menu.

Starting InterScan eManager

After installing eManager, configure InterScan VirusWall to recognize and enable eManager. Perform the following tasks in the sequence shown to enable eManager.

To start InterScan eManager:

1. Using a Web browser, open the InterScan VirusWall Web console (by default, user name and password are **admin)**.
2. Click **Configuration** from the menu options. The Scan Configuration page appears.
3. Select **Configuration: E-Mail Scan** check box.
4. Click **Configuration: E-Mail Scan** button.
5. Scroll down to the bottom of the page and select the **Enable Plug-Ins** check box.
6. Click **Apply.**
7. In the menu, click **Turn On/Off**. The Turn On/Off page appears.
8. Click the **Mail** button **OFF**, and then click **ON** to turn it back on.

InterScan eManager is now up and running.

Accessing the Web Console

The eManager installation adds an eManager Web Console link to the InterScan VirusWall Web console. You can access the eManager Web console by clicking this link in the InterScan VirusWall Web console, or typing the URL directly in the browser as shown below.

To access the InterScan eManager Web console:

1. Open a Web browser, then type the eManager URL followed by the port (**:1812)**. The URL can be either the domain name or IP address of the eManager machine. The port used for the Web Console is also user-configured. For example,

   ```
   http://domain:port/eManager/eManager.html
   http://isvw.widget.com:1812/eManager/eManager.html
   http://123.12.123.123:1812/eManager/eManager.html
   ```

2. Use the InterScan VirusWall Web console password to access the eManager Web console. The eManager Web console password is the same as the InterScan

VirusWall Web console password. If you change the InterScan VirusWall Web console password, the eManager Web console password will change accordingly.

Note: The default InterScan VirusWall Web console password is **`admin`**.

Inbound Filtering

Enable the **Inbound mail processing** check box in E-Mail VirusWall to scan and filter unwanted emails bound to recipients inside your organization.

To enable inbound mail processing:

1. Open the InterScan VirusWall Web console.
2. Click **Configuration** from the menu. The Scan Configuration page appears.
3. Select the **Configuration E-mail Scan** check box.
4. Click **Apply** to save changes.

Outbound Filtering

Select the **Enable Outbound Mail Processing** check box in E-Mail VirusWall to perform outbound SMTP traffic content and spam filtering.

Note: Outbound mail processing is a separate operation from outbound mail scanning. Select **Enable outbound mail virus scanning** to turn outbound virus scanning on.

To enable outbound mail processing:

1. Open the InterScan VirusWall Web console.
2. Click **Configuration** > **Configuration E-mail Scan**. The E-Mail Scan Configuration page appears.
3. Click **Additional Email Options** at the end of the page. The Additional Email Options page appears.
4. Under the **Local domain** group:

a. Type your **local domain** (required). Use a space to separate multiple domains.

b. Select the **Enable outbound mail blocking and disclaimer processing** check box.

5. Click **Apply** to save changes.

Refer to the *Additional Email Options* topic of the InterScan VirusWall Administrator's Guide for details on disclaimer processing.

Removing InterScan eManager

The `install.sh` file automatically removes InterScan eManager from your system. You must use a root account to automatically or manually remove InterScan eManager.

To automatically remove InterScan eManager:

1. To remove eManager, type `./install.sh` from the directory where your eManager files are located.
2. Choose **Option 2** and follow the on-screen prompts to remove eManager.

Note: During uninstall, `install.sh` provides an option to keep the eManager configuration files. Doing so makes the current configuration available when you reinstall eManager.

Upgrading from the Evaluation Version

Upgrading from the evaluation version is simple. Open the InterScan eManager Web console and go to the **Register Software** page. Type the serial number in the provided field and click **Save**.

Evaluation version users who want to remove the time limit can contact Trend Micro via email at:

support@trendmicro.com or sales@trendmicro.com

Chapter 3

Using the Spam Filter

This chapter presents a number of tasks that take you through the basic processes and functions of the Spam Filter. The tasks presented in this chapter provide a comprehensive understanding of how the Spam Filter works. Refer to the online help for detailed information on each eManager function.

This section includes the following topics:

- Creating a spam filter based on problem spam mail
- Using user-defined anti-spam rules to stop spam

Creating a Spam Filter Rule

Trend Micro provides a ready made rule-set that contains hundreds of rules for filtering out many of the most common spam types. These are available in `Trend$RF`. Create spam filter rules, which InterScan eManager saves in `/opt/trend/Plug-Ins/EM/spamrule/spamrule.txt`.

When creating spam rules, it is important to know that many spammers add false header information to their messages in an effort to make tracking back to the source difficult (see detailed information on spam in the online help topic About Spam). Bulk emailers often reuse the same false routing domains and other header information because it is 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 these false domains like a "signature," to identify and safely block many spam messages rather than creating rules on a one-rule-one-spam basis.

Some ISPs do not have adequate anti-spam rules. They can easily become hosts to spammers. Identifying these domains and adding them to your rules can have a significant impact on the amount of spam your organization receives.

Viewing Email Headers

The header information from known spam is an excellent source of data for defining anti-spam rules. Many mail clients support viewing the header information of email messages. In a Windows-based mail client (for example, Microsoft™ Outlook™), you can view header information by:

- Opening the **Properties** option on the mail client menu
- Opening the **Options** tab on the open message
- Saving the entire message as ASCII text

Header information of the original message is usually not available on forwarded messages. To preserve the header information of forwarded messages, have users copy the message (as a file) and include it as an attachment in the email they are sending you. Check your mail client online help for instructions on reading message header data.

Spammers' Email Lists

These are some ways in which spammers generate lists of email addresses:

- Culling the addresses from postings to UseNet
- Using special Web-crawlers to harvest them from Web sites, and collecting them from false contests, drawings, surveys, and other Internet gimmicks
- Legitimate marketing outfits and business also put together lists, and sell and resell these lists countless times

Lists of email names are easily available for purchase over the Internet and through other channels, with prices as low as $50.00 for 100,000 "verified" names. The following UCE example shows a current price list.

An Example of Unsolicited Commercial Email

Return-Path: *<123@123.com>*
Received: from *<1a2a3.123.com>* (1a2a3.123.com [123.221.129.28])
by xyz.com (8.8.5/8.8.5) with ESMTP id AAA12130
for <xyz@xyz.com>; Mon, 12 Apr 2000 00:09:52 -0700
Message-Id: <199910120709.AAA12130@xyz.com>
Received: from 1a2a3.123.com ([123.37.75.162]) by 1a2a3.123.com
(Post.Office MTA v3.1.2 release (PO203-101c)
ID# 629-49361U15000L15000S0) with SMTP id ACJ2386;
Mon, 12 Apr 2000 00:12:00 +0500
To: user1@domain.com
Date: Sun, 11 Apr 00 21:54:54 EST
From: 123@xyz.com
Subject: Hi
Reply-To: *user1@domain.com*
X-UIDL: 440bb61acc12ec0536991b3a41132b1f
Status: RD

Do you know what the number one factor is, (sic) that will determine whether your business is a success or not? ADVERTISING! Effective conventional advertising is quite expensive. So what do you do? Direct email is one of, if not thee(sic) most effective method of advertising in the 90's. You can get your ad out to hundreds of thousands, even millions, for only a fraction of the cost of traditional advertising. The wave of future advertising is here, (sic) don't miss it. We will send your advert for you. We have gone through painstaking methods to insure(sic) that we have the the(sic) most (sic) quality lists on the Internet. We send your ad for your (sic), all you have to do is create it.

250,000 addresses - $199
350,000 addresses - $250
500,000 addresses - $350

Anti-spam Rules

Create spam-filtering rules by only defining one or two criteria on the **Add/Edit Rule** page.

For example, if you are defining spam-filtering rules based on actual spam mail, define the rule using only the mail's **Subject** field, or only the **Sender** field. The

more criteria you specify for any given rule, the less chance there is of stopping similar spam.

eManager evaluates the criteria you create exactly the way you specified, including any quotes, spaces, and punctuation. eManager treats phrases as a single unit. Content Management triggers a match only when it finds each word in the phrase, and it appears in the order entered.

Do not use quotes to signify a phrase, or commas to separate multiple words entered in a single field. Instead, create separate rules.

Step-by-Step: Creating the Rule

In this example, create a spam filter rule to block all email messages originating from a fictitious organization that sends advertisements soliciting business for their bulk emailing service (such as the example in the previous page).

To create a rule to block email messages:

1. Open the eManager Web console, and click **Anti-spam** > **Set Rule**. The Set Rule page appears.

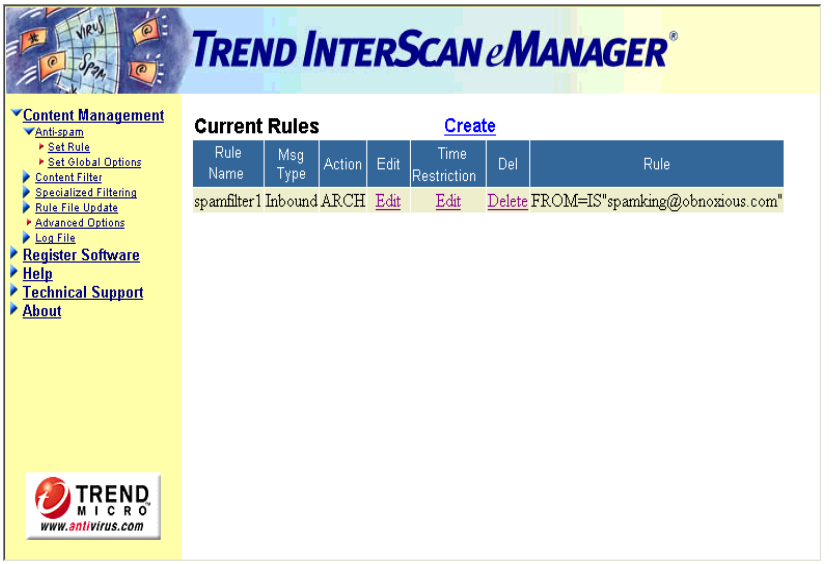


FIGURE 3-1. The Set Rule page shows the currently available policies. All policies shown on this page are active.

2. Click **Create** to open the **Add Rule** page.
   a. Type the spam rule name in the **Rule Name** field, for example, *Bulk Mail Solicitation, 05-01-00.*
   b. Select the **Inbound** check box, for the SMTP flow direction.
   c. Under **Action on unwanted mail**, click one of the following:
      - **Delete**: InterScan VirusWall or the SMTP server does not process deleted mail
      - **Quarantine**: SMTP server does not send quarantined mail to the recipient. It is renamed and moved to the `/EM/Quarantine` directory of the local machine

- **Archive**: SMTP server delivers archived mail to the intended recipient, however InterScan eManager keeps a copy of the message, including header information in the `/EM/Archive` directory

  You can change the destination directory using the **Advanced Options** page.

For new rules, click **Archive** to save rather than delete matching messages, at least for the first week. This way, recipients will still get email while you fine-tune your policies.

d. Check the header of the spam message to identify the criteria by which you can best block this and similar messages.

Because the Subject line is "Hi," it is too broad and would not make a good filter. Perhaps the spammer knew this. The routing domain, however, is clear: *1a2a3.123.com* and there is no evidence of forgery (as may be indicated by numerous routing domains). Other possible candidates for the filter are the forged **To** field and the **Reply to** field, which also appears to be forged (it does not match the domain of origin).

3. Create a second anti-spam rule to cover two filtering criteria.

a. In the **Edit Rule** page, type only *1a2a3.123.com* in the **Routing domain** field.

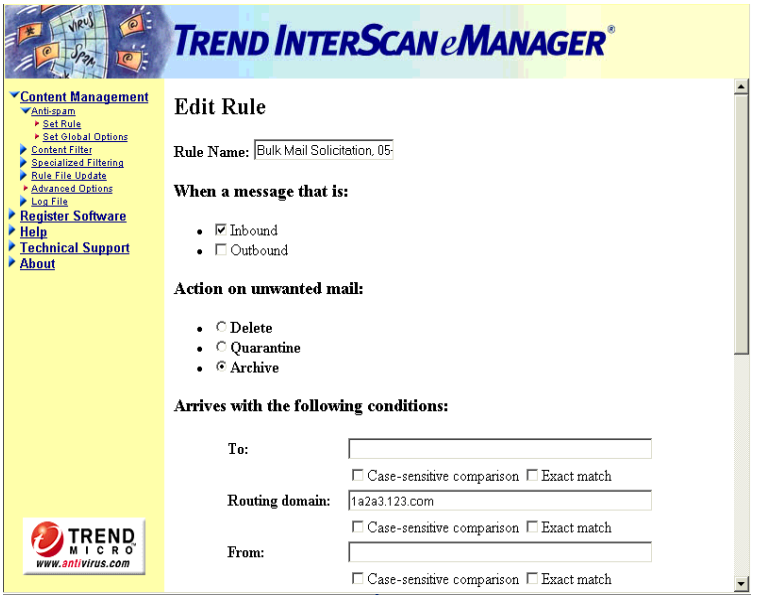


FIGURE 3-2. The Add Rule page showing the routing domain used to block spam.

b. Click **Set Rule**, and under the **Time Restrictions** column click the **Edit** link.

c. Select the times when you want the rule to be in effect. In this case, select the morning hours from 12:00 A.M. to 7:00 A.M. and the evening hours from 7:00 P.M. until 12:00 A.M for all days.

Red time cells indicate the times when the rule is in effect. If you do not set any time restriction, Content Management applies the rule 24 hours a day.

FIGURE 3-3. The dark squares show times when the spam filter rule is in effect.

d. Click **OK** and return to the **Set Rule** page.

4. Click **Anti-spam** > **Set Rule** to create another rule. This time type *user1@domain.com* in the **Reply to** field.

You can use both criteria to create a single rule. The decision to create one rule with multiple criteria or several rules, each with single criteria, depends on whether you trust the routing domain. If the routing domain was AOL.COM, or HOTMAIL.COM, for example, you would probably want to narrow the scope of the rule by including an email address in the **From** or **Reply to** fields.

Click **Save** to save the rule. A screen with the message appears confirming you that the rule is active. Click **Back** to display the **Set Rule** page.

5. Click **Anti-spam** > S**et Global Options**, and type the email address of the person(s) you want eManager to automatically notify whenever one of your current rules matches a message.

   Include a brief message in the **Message text** field. For example,

   Anti-spam filter has blocked a junk mail.

   If you type multiple email addresses in the **Notifications** field, separate them with commas.

6. Click **Save**.

   Notifications are global. InterScan eManager sends the same notification regardless of which spam filter rule actually triggers the match.

Current Rules Strategy

When specifying multiple rules in the Current Rules list, Trend Micro recommends that you employ an inverted pyramid model, where you put rules with the broadest reach, or highest probability of matching, at the top of the list. Place those that are more narrowly defined (less likely to trigger a match) towards the bottom of the list. This is the most efficient arrangement because in this way the filter will eliminate the greatest proportion of traffic with the fewest number of evaluations.

Spam Filter Strategy Example

The following example further explains the inverted pyramid rule strategy. For example, you have created the five spam filter rules shown below:

- Delete any mail originating from the domain *SPAM.COM*
- Delete any mail sent from *SpamKing*
- Quarantine any mail sent to *SpamLover@company.com*
- Delete any mail containing the phrase "*Free Offer*" in the subject line
- Quarantine any mail containing the term "*SeXXX*" in the subject line

Let us also assume that you have analyzed your incoming messages and know for every 10,000 messages processed by the SMTP server, *SpamKing* sends 42 messages, 150 originate from the *SPAM.COM* domain, 500 contain the phrase "*Free*

Offer" in the subject line, SMTP server delivers 18 to *SpamLover@company.com*, and 196 contain the term "*SeXXX*" in the subject line.

In this case, the optimal rule order appears in the Current Rules list as the following:

1. "Free Offer" (500 instances)
2. "SeXXX" (196 instances)
3. *SPAM.COM* (150 instances)
4. *SpamKing* (42 instances)
5. *SpamLover@company.com* (18 instances)

When ordered as above, eManager can eliminate 500 of every 10,000 incoming messages in the first round of evaluation because they match the "*Free Offer*" rule. In a reverse order, *SpamLover@company.com* is the first rule. When a *Free Offer* message arrives. InterScan eManager evaluates the message five times (1. check for *SpamLover@company.com*, 2. check for *SpamKing*, 3. check for *SPAM.com*, 4. check for *SeXXX*, 5. check for *Free Offer*) before matching on *Free Offer* and rejected.

However, because Free Offer mail occurs at a relatively high frequency, placing it first on the list will trigger the largest number of matches with the least amount of searching.

Blocking Attachments with the Spam Filter

The Internet is offering more and more material to promote the music and film industry. Users can easily download audio and video files. Unfortunately, these types of file are usually big files. They take up a large amount of bandwidth during the download process and can slow down the delivery of business communications. MP3 files are popular downloads and users can share them through email. In this example, create a spam filter rule that will block these types of audio files transferred through email during normal business hours.

Step-by-Step: Creating the Rule

In this example, create a spam filter rule to block all email messages containing **.mp3* attachments coming from outside the company.

To create a rule to block mp3 files:

1. Open the eManager Web console and click **Anti-spam** > **Set Rule**. The Set Rule page appears.
2. Click the **Create** link to open the **Add Rule** page.
   a. Type a name for the spam rule in the **Rule Name** field. For example, *Audio_Files*.
   b. Select the **Inbound** check box for the SMTP flow direction.
   c. Under **Action on unwanted mail**, click **Delete, Quarantine,** or **Archive**.

      Because this is a new rule, select **Archive** to save rather than delete matching messages.
   d. Scroll to the bottom of the screen and type *mp3* in the **Extension type** field.

      To block only **.mp3* files, you do not need to fill in any of the other information on the screen.

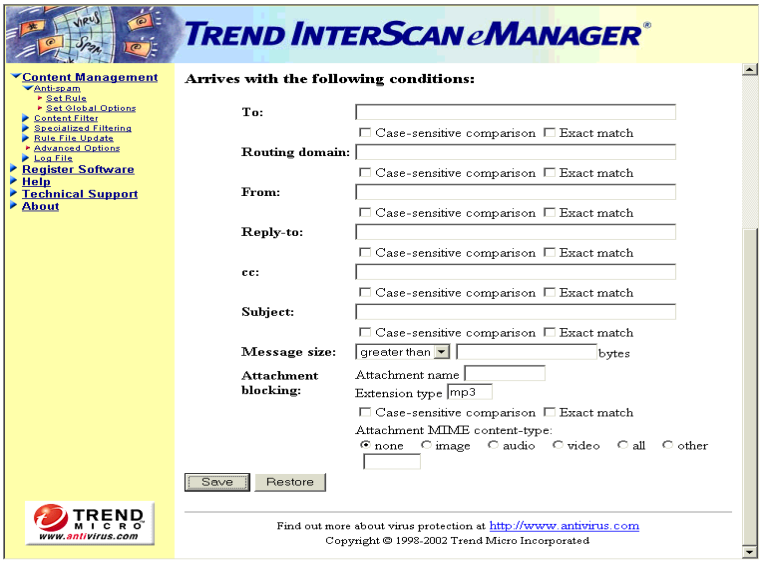


FIGURE 3-4. Do not put a wildcard character in the Attachment type field. The Attachment Blocking rule does not support wildcards.

e. Click **Save**. A message page will notify you that the rule has been saved. Click **Back** to return to the **Current Rule** page.

3. Click **Set Rule**, and under the **Time Restrictions** column, click the **Edit** link for the *Audio_Files* rule.
4. Select the times that you want the rule to be in effect. In this case, select the standard work hours for your company: for example, from 8:00 A.M. to 5:00 P.M.

   Red time cells indicate the times when the rule is in effect. If there is no time selection specified, the rule is applied 24 hours a day.
5. Click **OK** to save the Rule.

Testing the Rule

After creating the rule, you will need to test the rule. Configure an email client to send an email with an **.mp3* attachment to the InterScan SMTP server. You can use any email client to send the message.

To test the *Audio_Files* rule:

1. Set the **Outgoing mail (SMTP):** field in the server properties of your email client to point to InterScan.
2. Send an email to any address that includes an **.mp3* file as an attachment.
3. Refer to *Viewing Log Files* for instructions on how to view the log files.

See *Using Telnet* to test a rule or policy using Telnet.

Chapter 4

Using the Content Filter

This chapter presents a number of tasks using the Content Filter. Refer to the InterScan eManager online help for detailed information on the Content Filter options.

This chapter discusses the following:

- Using the content filter to stop spam
- Using the content filter to block a specific file type
- Using the content filter to block greeting cards

Creating Content Filter Policies

The content filter allows administrators to evaluate and control the delivery of email based on the message text itself.

Create content filter policies to monitor both inbound and outbound messages to check for sensitive, offensive, or otherwise objectionable message content sent to customers, competitors, or others. Content Management enables or disables individual content filter policies.

Trend Micro provides Bg_AntiSpam Import file. The Import file is the source for keywords used by the default content filter policies.

Create content filter policies, which InterScan eManager saves in `/opt/trend/Plug-Ins/EM/CsConfig.dat`.

Depending on how you have InterScan VirusWall set up on the network, content filter only checks messages crossing the Internet gateway. It does not necessarily scan Internal email. Refer to the *Installation Topologies* section of the InterScan VirusWall Administrator's Guide for more details on different possible InterScan VirusWall installation.

Note: The content filter supports scanning double-byte messages, such as messages in Chinese and Japanese.

Content Filter Policies

A content filter **Policy** represents a group of conceptually related words and phrases that eManager uses to match against inbound messages, outbound messages, or both.

eManager compares the message text (including the header) against the list of policies. Whenever an email matches *any* policy, content filter takes the action specified in the matching policy. You can **Archive**, **Quarantine**, or **Delete** unwanted messages.

Content filter comparison only includes the email message text (and any non-encoded ASCII attachments); it does not consider binary email attachments.

eManager checks the messages for the keywords specified in the first policy on the list, then the second policy, third, and so on.

You can individually enable policies by selecting the check boxes preceding the policy name in the Policies list. There is no limit to the total number of policies that you can create. One rule of thumb, however, is that the more active policies there are, the longer it takes to evaluate a given email message.

Keyword Lists

The **Keyword List** for a given **Policy** contains the words and phrases that the content filter uses to check email message content.

When a policy has multiple keywords in the same line, eManager makes a match only when a message contains *all* of the keywords on that line. For example, you can

add the following keywords to the list (perform four separate **Add Keyword** procedures).

Example 1:

resume, position
resume, job
resume, experience
resume, enclosed

Note that this example uses four related words instead of just one. Basing the policy solely upon the word *resume* would not likely produce reliable results because *resume*, that is, curriculum vitae, shares the same spelling as *resume*, that is, to start again. To minimize the chance of such false matches, it is a good idea to qualify the primary word, *resume*, with additional words typically associated with it in a job-seeking letter: *enclosed*, *position*, *job*, and *experience*. Including several keyword groups will increase the reach of the filter.

InterScan eManager considers a match for messages that contain any of the keyword pairs. Another option is to have the filter trigger the configured action only if Content Management encounters all five words in a single outbound message. Do this by including all the keywords on a single line (perform a single **Add Keyword** procedure).

Example 2:

Resume, position, job, experience, enclosed

The likelihood of detecting every outbound resume based on this filter is much less than for a policy that contains several policies based upon the word *resume*, as in Example 1.

Example 3 is a policy wherein the occurrence of any one of the four words in Example 2 triggers a match.

Example 3:

job
resume
enclosed
position
experience

Although not applicable to the case of a resume filter, this technique is appropriate, for example, when filtering for offensive content — not every four-letter word in the dictionary need appear in a message to qualify as a match. Instead, you may decide that the occurrence of any one of the words on your offensive list is sufficient to warrant tracking (**Archive** option), further investigation (**Quarantine** option), or immediate deletion.

Keywords linked by the **AND** operator should not include more than four or five words or they risk being overly restrictive. On the other hand, if a policy includes only one keyword in any given line (**OR** operator), the policy risks being too restrictive — eManager will find many matching email messages. As shown above, a lot depends upon what InterScan eManager is filtering.

eManager evaluates the criteria you specify exactly as you entered, including any quotes, spaces, and punctuation. eManager treats phrases, separated by commas, as a single unit. eManager triggers a match only when it finds each word and space in the phrase in the message and it appears in the order entered.

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

More on Keyword Lists

Case 1. Keywords appear on a single line:

```
Apple Juice, [and] Pear, [and] Orange
```

Case 2. Keywords each appear on their own individual lines:

```
Apple Juice [or]
Pear   [or]
Orange [or]
```

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

```
Apple Juice, [and] Pear [and] Orange
[or] orangish
[or] red
[or] yellow
```

where the Synonyms list includes the words *orangish*, *red*, and *yellow.*

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

Note: *Apple Juice* is a phrase because the words *Apple* and *Juice* are not separated with a comma; even if the words *Apple* and *Juice* both appear somewhere in the message, eManager will not trigger a match 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 will only trigger a match with the word ***red****undant* if **Exact Match** is not checked; likewise, the word *red* will only trigger a match with the word *Red* in the message text if **Case-sensitive comparison** is not checked.

Step-by-Step: Creating the Policy

In this example, create a content filter policy to check outbound email messages for resumes.

Since this is a new policy, set the **Action** to **Archive** as a safeguard against errors. Inform neither the **Sender** nor **Recipient** of the message evaluation; notify Edna Brokaw, a fictitious human resources manager. If Edna's name appears in the message (as her signature at the end of her email), eManager should ignore the message even if content filter triggers a match.

To create a content filter policy to check outbound email messages for resumes:

1. From the eManager Web console, click the **Content Management** > **Content Filter** > **Set Policy**. The Set Policy page appears.

FIGURE 4-1. The Current Policies page shows some of the default policies that ship with eManager.

2. Click the **Create** link above the Policies list. When you click the **Create** link, eManager will assign the policy a number (for example, *Policy3*) and provide two links, **Options** and **Add Keyword**, which will allow you to create the new policy.
3. Click **Add Keyword**. The Add Keyword page appears.
   a. Type the word or phrase you want to filter. **Add** (that is, create) a new keyword for each word or phrase that you want the content filter to check. In the example, add *resume*.
   b. Click the **Synonym** link to create a synonym for resume. A new window will give list the synonyms for resume. By default, eManager excludes (does not scan) the words.
   c. Click **Edit**.

d. Select the synonyms that you want to check in the **Exclude Synonyms** list.

FIGURE 4-2. Use this page to add synonyms to keyword searches.

e. Click the << or >> button to move the word from one column to another. For this example, select *Curriculum Vitae* and move it to the **Include** list. None of the other synonyms applies.

f. Click **Save.**

4. Click **Content Filter** > **Set Policy**. The Set Policy page appears.

a. Click the **Edit** link of *Policy3*.

b. Click **Edit Options** to name the policy and set the scanning parameters. The **Edit Options** page allows you to complete the policy once you have defined the keyword list and the synonyms that eManager will scan.

c. Type a name for the policy in the **Policy name** field. In this example, type *Outbound Resumes*.

d. Select the **Enable policy** and **Check synonyms** check boxes.

e. In the **Take NO Action If Message Contains** field, type the name of Edna Brokow, the HR manager, to exempt her email from the policy. (Do this to allow Edna to reply to any inbound messages that contain resumes sent to the HR department.)

f. Select whether to monitor **Inbound** mail, **Outbound** mail, or Both.

g. Define the **Action** to take when eManager detects a match. In this case, choose **Archive** to save a copy of the email and deliver the original to the intended recipient.

h. Configure the **Notifications** so that eManager automatically sends notification to Edna whenever an email violates the *Outbound Resume* policy. Select the **Warning To user(s)** check box and type Edna's email address (use Internet email format, for example, *edna@company.com*, and separate multiple email addresses with a comma). The message sent is as follows:

> *Edna: I am forwarding an email to you for review. Please determine whether this individual is sending out resumes.*

Because of the sensitive nature of this policy, eManager informs neither the message sender nor intended recipient of the action taken. Alternatively, you could have a mild warning automatically sent to the **Sender**:

> *A message you sent appears to be an application for a job outside the company. We do not condone the use of company time and equipment to solicit employment.*

i. Click **Save** to add the policy to the **Policy list**.

5. Finally, click **Content Filter** > **Set Global Options**, and select the **Use exact matches only** check box.

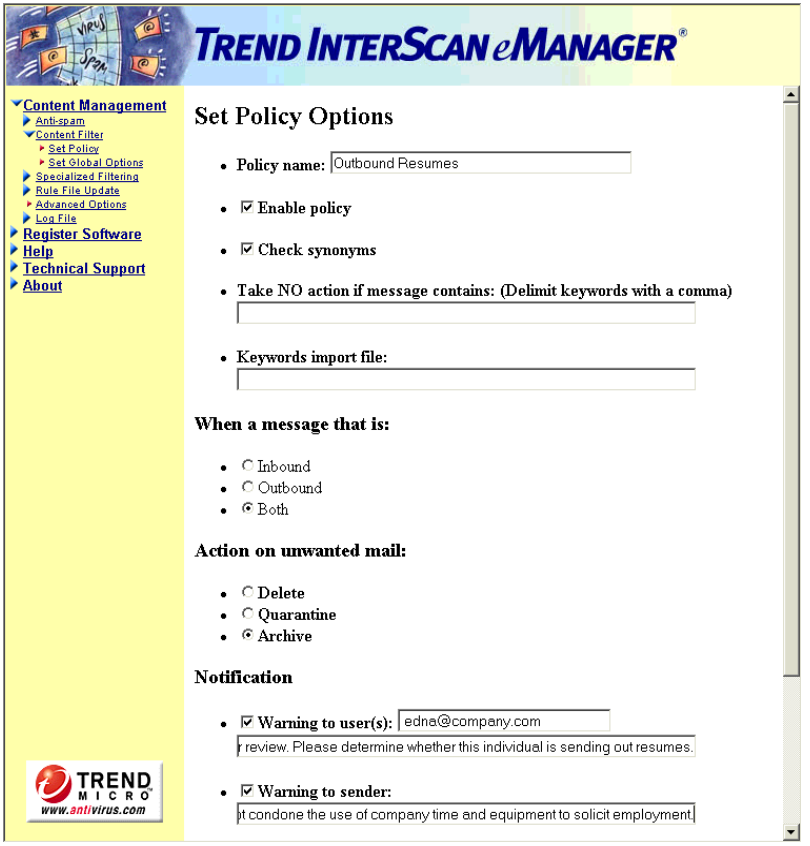


FIGURE 4-3. The Edit Options page shows many of the important scanning parameters.

6. Click **Save**.

Using Content Filter to Block Spam

You can use the content filter to block spam, especially the type of spam that complies, or attempts to comply, with legislation requiring that bulk emailers provide a means of removal from the spam list.

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

Clear the **Case sensitive comparisons** check box on the **Set Global Options** page to have the filter trigger a match for *remove, REMOVE, ReMove*, etc.

You can create additional policies like the one above according to actual samples taken from your own spam (or that of your users).

Blocking Greeting Cards with Content Filter

While electronic greeting cards are very popular, they tend to absorb valuable network resources. Volumes of business conducting over the Internet cause heavy network traffic during the Christmas season. Blocking greeting cards, along with spam and unwanted attachment types, can save you money and help your network run smoothly during the holidays.

`Bg_AntiSpam` includes a preset Content filter policy named *E-Greeting Card* to block unsolicited electronic greeting card messages. Create a new policy to enhance *E-Greeting Card* by including additional keywords as presented in the next example.

Step-by-Step: Creating the Policy

Create a policy to check inbound email messages for greeting card notifications.

Since this is a new policy, set the **Action** to **Archive** as a safeguard against errors. Inform neither the **Sender** nor **Recipient** of the message evaluation.

To create a policy to block unsolicited greeting cards:

1. In the eManager Web console, click the **Content Filter** > **Set Policy**, and then click the **Create** link above the Policies list.
2. Click the **Add Keyword** link.
   a. Add two keyword phrases to this policy. Type *free greeting card* and click **Apply**.
   b. Click the **Add Keyword** again and type *electronic greeting card.* Click **Apply**.

      Since each of the phrases is on their own line, eManager will scan for *free greeting card* or *electronic greeting card*.

FIGURE 4-4. Each time you create a keyword for a policy, it appears in a list under the policy name.

3. Click the **Edit Options** link.
   a. In the **Policy name** field, specify a name for the new policy. In this example, type *E-Greeting Card II.*
   b. Select the **Enable policy** check box.
   c. Clear the **Check Synonyms** check box.

d. Check that the **Take NO Action If Message Contains** field is blank.

e. Under **When a message that is**, click **Inbound**.

f. Define the **Action** to take whenever eManager detects a match.

- Choose **Archive** to save a copy of the email and 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.

g. Configure the **Notifications** to send notification of the blocked email to the appropriate recipients. Use Internet email format for the email address and separate multiple email addresses with a comma. For example,

manager@company.com,administrator@company.com

Note: When initially creating and testing policies, always include your email address for testing purposes. That way, when you send a text email, InterScan eManager sends a notification when a message violates a content filter policy.

---

4. Click **Save** to finish.

Refer to *Using Telnet* to test a rule or policy using Telnet.

Chapter 5

Using the Specialized Filter

This chapter includes information on how to create specialized filter policies to strengthen your defense against spam.

This chapter discusses the following:

- Using the specialized filter to stop spam
- Creating specialized filter policies to block a specific file type

Specialized Filter Policy

Specialized Filtering features the removal of attachments with a particular filename or MIME content-type from email messages and replaces them with a configurable notification text message. InterScan eManager can notify the sender, recipient, or administrator of the attachment removal.

Create a specialized filter policy that will block messages according to header (From, To, Reply-to, cc) or attachment (file name, file extension, MIME content type). InterScan eManager saves specialized filter policies in `/opt/trend/Plug-Ins/EM/spamrule/SFRule.txt`.

When you specify policy criteria according to **message header condition**, From, To, Reply-to, and cc fields support the wildcard character asterisk (*). Use commas (,) to separate multiple values — commas represent the OR operator. There is an AND

operator between the From:, To:, Reply-to:, and cc: fields. Similar to the other Content Management components, eManager triggers a match if an email meets the conditions of a specialized filter policy.

You can leave the Conditions fields empty and set specialized filter policy criteria according to **message attachment**. Configure a specialized filter policy to filter messages according to file name, extension name, or MIME content types.

Creating Specialized Filter Policy

Specialized filtering is off after a successful InterScan eManager 3.8 installation. Activate **Content Management** > **Specialized Filtering** > **Configuration** > **Enable Specialized Filtering** to instruct InterScan eManager to implement existing special filter policies.

You can create specialized filter policies the same way as content filter policies with some exceptions:

- The action on unwanted email is not configurable; the only action is Quarantine
- InterScan eManager strips (removes) all attachments from the message if it violates a specialized filter policy

Similar to creating spam filter rules, create specialized filter policies by defining only one or two criteria on the **Add Specialized Filtering Rule** page.

For example, if you are defining a specialized filter policy based on actual spam mail, define the policy using only the mail's **Subject** field, or only the **MIME content type** field. The more criteria you specify for any given policy, the less chance there is of stopping similar spam.

Applying Specialized Filter Policy Attribute

You can apply either one of two attributes for the specialized filter policy:

1. Include — apply the policy when it matched the conditions.
2. Exclude — apply the policy when it does not match the conditions.

Step-by-Step: Creating a Specialized Filter Policy

Create a policy to remove inbound or outbound message attachments whose MIME content types are `audio/x-mpeg`, `audio/wav`, and `application/zip` and replace them with texts. Configure Specialized Filter to send notification to sender and administrator.

To create a specialized filter policy:

1. Click **Content Management** > **Specialized Filtering** > **Set Policy**. The Attachment Removal page appears.
2. Click **Create**. The Add Specialized Filtering Rule page appears.
3. In the **Rule name** field, type a name for the specialized filter policy. For example, `block_all`.

   The maximum allowable length for a policy name is 80 characters. You can use both letters and numbers.
4. Select both the **Inbound** and **Outbound** check boxes for the SMTP traffic flow.
5. Under Attribute, click **Include**.
6. Under Attachment Removal, click **MIME content types** and type the following in the **MIME content types** field:

   ```
   audio/x-mpeg,audio/wav,application/zip
   ```

   There should be no spaces in between comma and the MIME content types.
7. Click **Save** to activate the specialized filter policy.
8. Click **Content Management** > **Specialized Filtering** > **Set Notification** and, type the message text that replaces the attachment in the **Replace attachment with the following text:** field. The default message is *"The attachment file in the message has been removed by eManager."*
9. Under Administrator[s] notification, enable and configure a notification for two **Administrators**:
   a. Select **inbound and outbound messages** from the list.
   b. Specify the email addresses of the administrators. Use a comma to separate one email address from the other. For example,

      ```
      mail_admin@company.com,network_admin@company.com
      ```

   c. In **Notification text**:, type

"To Administrator: eManager has removed an attachment file in the email."

10. Under Sender Notification, enable and configure a notification to **Sender**:

a. Select **inbound and outbound messages** from the list.

b. In **Notification text**:, type

"To Sender: eManager has removed an attachment file in the email."

11. Click **Save**.

Refer to *Using Telnet* to test a rule or policy using Telnet.

Notifications are global. InterScan eManager sends the same notification regardless of which specialized filter policy actually triggers the match.

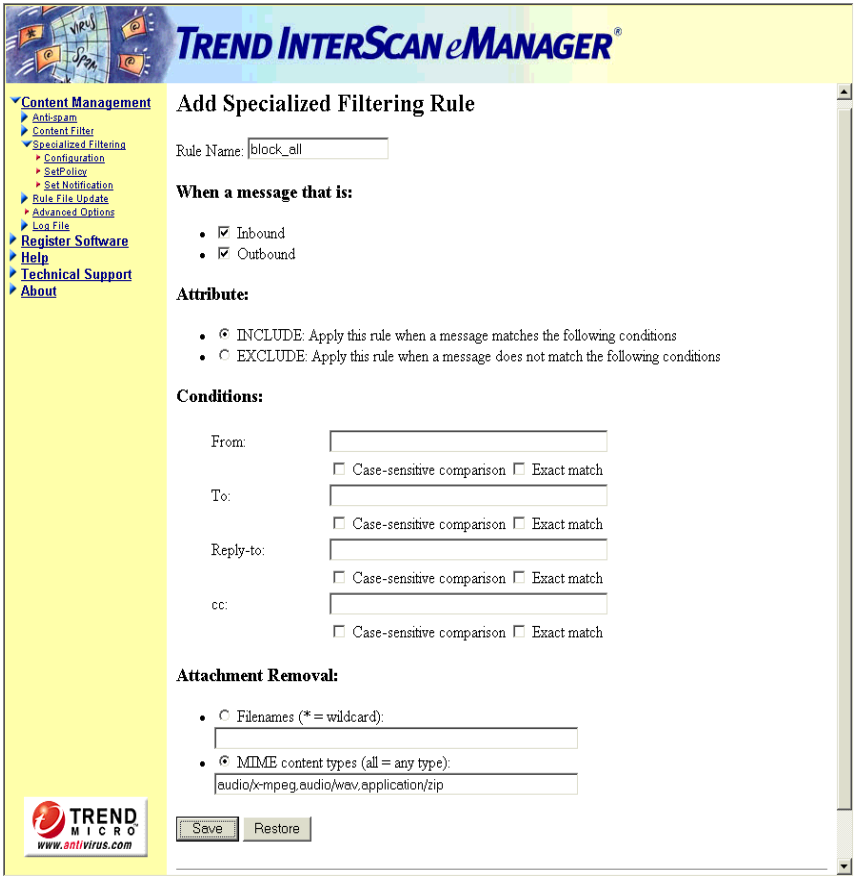


FIGURE 5-1. Use a comma (,) to separate values in the Attachment Removal MIME content types fields.

Chapter 6

Testing Rules and Policies

Use Telnet or any mail client to test your spam rules, content and specialized policies. Ensure that you are sending to the SMTP server that InterScan is scanning.

Using Telnet

To use Telnet when testing a rule or policy:

1. Connect to your SMTP server by typing the following at the UNIX command prompt:

   ```
   telnet {SMTP IP address} 25
   ```

   Where `{SMTP IP address}` is the IP address of your SMTP server.

2. When connected, type

   ```
   helo {domain name}
   ```

   Where `{domain name}` is the address after the @ sign. For example, `trendmicro.com`.

3. At the "ready" prompt, type the following:

```
MAIL FROM:{genuine From address}
RCPT TO:{genuine To address}

DATA
From:{type false email address}
To:{type false email address}
Subject:{type test subject}
Message text:{type the message text that you want the content
filter to check here}
```

Note: The **spam filter** filters only message header information that appears above **Message text** and below **DATA**. The **content filter** checks data appearing in both the message text and header areas.

Specify valid **MAIL FROM** and **RCPT TO** information.

4. End your test email with a period (.). Telnet displays *"250 Message accepted for delivery"* message.
5. If you have configured the notification to go to your mailbox, you will receive a notification. To view the InterScan eManager log files, go to *Viewing Log Files*.

Chapter 7

Using the Rule and Import Files to Stop Spam

This chapter discusses information about Trend Micro Rule and Import files, also known as the vendor-provided files. The topics include:

- Using `Bg_AntiSpam` and `Trend$RF`
- Updating the Rule and Import Files

Using the Rule and Import Files

InterScan eManager includes both Rule (`Trend$RF.####`) and Import files (`Bg_AntiSpam.####`) for the Content Management spam and content filter components. Trend Micro supplies Rule and Import files that contain predefined anti-spam criteria created by the Trend Micro engineering staff.

- Spam filter uses Trend Micro **Rule File** — `Trend$RF.####`, which contains numerous predefined anti-spam rules
- Content filter uses Trend Micro **Import File** — `Bg_AntiSpam.####`, which contains numerous predefined anti-spam policies. You can use these predefined policies to augment existing policies

`Trend$RF` and `Bg_AntiSpam` support 4-digit extension starting with version 1000.

eManager keeps log files for all rule or policy violations. Once you have established anti-spam rules and policies, Trend Micro recommends you review the log files to ensure the effectiveness of the criteria.

Both Trend Micro Rule and Import files are encrypted and are not user-editable.

Rule and Import Files Information

The following information is available on the *Rule File Update* page:

- **Version of last rule file** — used by the spam filter, represents the current Rule file version
- **Version of last imported Anti-spam policy** — used by the content filter, represents the current Import file version

Enabling the Rule File

You can enable the rule file from the **Anti-Spam Set Global Options** page.

To enable the rule file:

1. Click **Anti-spam** > **Set Global Options**. The Set Global Anti-Spam Rule Options page appears.
2. Select the **Enable vendor-provided rule file: "Trend$RF"** check box.

3. Click **Save**.

FIGURE 7-1. The Anti-Spam > Set Global Options page shows both the rule file and notification enabled.

Updating Bg_AntiSpam and Trend$RF

As spammers write and release new spam onto the public, and as they jump from one routing domain to another to cover their tracks, Trend Micro monitors and collects telltale blocking information and incorporates it into new **Rule** and **Import** files.

It is important to keep these files up-to-date. Trend Micro typically releases updated/new Rule and Import files every twelve (12) hours, and you should not wait much longer to update the files.

Updates are available free to registered InterScan eManager customers. You can schedule automatic download over the Internet, or update Rule and Import files "on demand" (click **Content Management** > **Rule File Update** > **Update Rule File**, and click **Update Now**).

Note: Registration uses HTTP to register. If you use a HTTP proxy, you need to know the host name (or IP address) and port. If the proxy requires a user name and password, you need to type them before updating the rule file.

The following directory contains `Bg_AntiSpam.####` and `Trend$RF.####:`

```
/EM/spamrule
```

Trend Micro names the Rule file according to the following convention:

```
Trend$RF.1
```

where **`.1`** represents the rule file version. When multiple rule files exist in the directory, eManager only reads the one with the highest number.

On Demand Update

If you use an HTTP proxy server on the network (that is, InterScan eManager server does not have direct Internet access),

To configure proxy settings and perform On Demand update:

1. Click **Rule File Update** > **Update Rule File** on the configuration menu.
2. Type the IP address (number) and port of this HTTP proxy in the fields provided.
3. Type the appropriate logon credentials.

Note: If you just installed InterScan HTTP VirusWall, your proxy information may have changed. Be sure to type the correct IP address and port.

4. Click **Update Now** to test the proxy connection and update the rule file.

If the current Rule and/or Import file on your server is already up-to-date, you will receive a message *"your rule file is already up-to-date"*. Otherwise, a progress bar informing you of the download progress appears. InterScan eManager completes Rule and Import file downloads within a few seconds (depending on your network speed).

After downloading the components, a status confirmation message appears. eManager immediately installs and implements the new Rule and Import files.

Note: You must register eManager before you can download new Rule and Import files. See *Upgrading from the Evaluation Version* for information on how to register InterScan eManager.

Automatic Update

When you enable **Automatic Update** on the **Set Automatic Update** page, the content filter will automatically update the Rule and Import files from Trend Micro at the interval specified.

Trend Micro typically releases new files every twelve (12) hours. However, special releases are occasionally made to address new spam issues that are likely to pose an immediate problem for customers. Trend Micro recommends scheduled automatic Rule and Import file updates at least daily.

Updating the Rule File Automatically

To schedule automatic Rule and Import files updates:

1. On the eManager Web console, click **Content Management** > **Rule File Update** > **Set Auto Update**. The Set Automatic Update page appears.
2. Choose one of the following:
   - **Update Daily** schedules InterScan to automatically update the files each day
   - **Update Weekly** to schedule InterScan to automatically update the files each week
   - **Update Monthly** and select a suitable date from the corresponding list

   If you do not want InterScan to automatically update the pattern file, clear the **Enable automatic update** check box.
3. Click **Rule File Update** > **Update Rule File**, and type the IP address and port of your HTTP proxy server (if required).

   Test your proxy information by clicking **Update Now** to start an immediate download of the pattern files.
4. Click **OK** to keep your settings, or **Restore** to display the last saved configuration setting.

Chapter 8

Maintaining InterScan eManager™

The tasks presented in this chapter focus on common eManager maintenance tasks. These tasks show you how to ensure that eManager files are up-to-date and the program is functioning properly. For detailed information on each of the functions in eManager, refer to the online help.

The topics include:

- Viewing the log files
- Troubleshooting Tips

Viewing Log Files

eManager keeps logs whenever it takes actions on an email messages. View log files, for example, to evaluate new rules and policies created for the spam, specialized, or content filter, to determine the file name of a quarantined email message, or to identify the sending party of a deleted message.

By default, the plug-ins write their logs to the `/Plug-Ins/EM` directory.

eManager logs follow this naming convention:

```
iscan.log.2003.05.09
```

Which describes an eManager log for May 09, 2003.

Logs include the following details:

Message Date & Time stamp
Message From:
Message To:
Message filename, if quarantined
Action (quarantined, archived, deleted)
Filter that performed the action
Policy/Rule that triggered the match

*__Date & Time stamp__ of the log entry
*__Service__ (Content Management, Email Management, etc.)
*__Process ID number__
*__Action/Message__
*__Service__ (Email, Web, etc.)
*__Error messages__

*The **Log Reports** dialog box does not display these details. Open the individual log with a text editor to view these details.

eManager also logs error messages.

Step-by-Step: Viewing Logs

You can view log files by the name of the individual policy or by all the policies grouped together. You can select a date range for either type of log report. The following example provides instructions on how to view a log report based on a specific policy. The same process applies to viewing all logs according to date.

To view eManager log files for a specific policy:

1. Start the eManager configuration menu and click **Log File > View Log by Policy**. The View Log by Policy page appears.
2. Under **Mail Type**, click the type of logs you want to view: **Inbound**, **Outbound**, or **Both**.

3. Under **Time Period**, click the log dates you want to view:

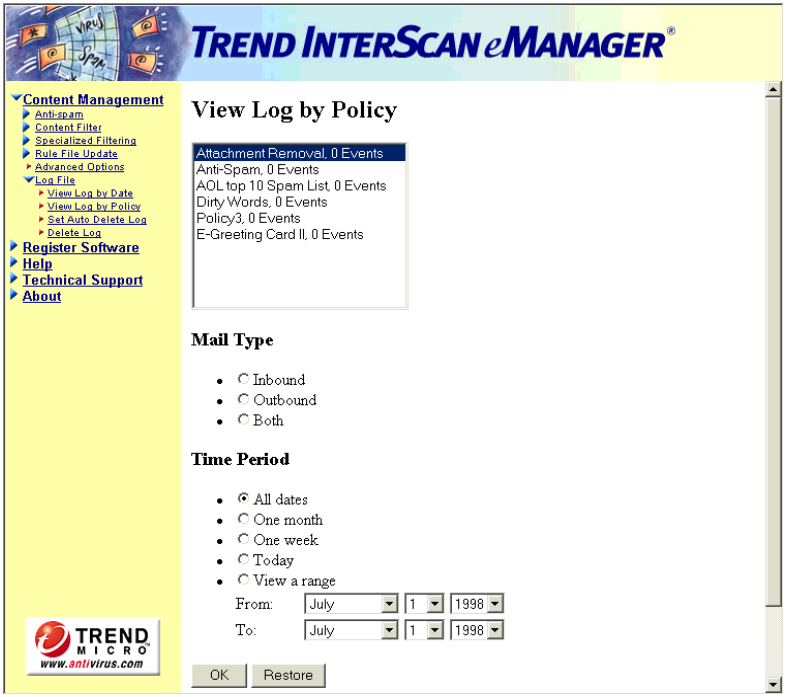


FIGURE 8-1. The View Logs by Policy page generates logs for individual policies.1

In this example, click **View a range** to view a range of dates. In the **From:** and **To:** boxes, specify the start and end dates for the log files.

4. Click **OK**. eManager displays all the logs that fit the criteria you specified in the **Log Reports** dialog box.

Troubleshooting Tips

1. What are the steps to enable and start InterScan eManager?

   Go to the InterScan Web console and click **Configuration: Email Scan**. Scroll down to the bottom of the page. Select **Enable Plug-Ins**. Click **Apply** and then go to the **Turn On/Off** page. Turn off the mail service and then turn it on again.

2. How can I check if eManager loaded successfully?

   You can view the plug-in value in the `intscan.ini` file. Check that it is set to **Yes**. The log file will also contain the following entry:
   "Returning from Initialize() of plug-in: eManager".

3. Why can't I update the rule file from the Internet?

   Before updating the rule file, you need to register eManager. Also, double-check if the network uses proxy settings.

4. After clicking **Back** or **Reload** on the browser, an error occurs or the browser exhibits unusual behavior.

   Back and **Reload** may affect the CGI program and cause it to rerun or lose the values you entered. Always click **Apply**, **Save**, or **OK** after making changes using the Web console before moving to another page.

5. eManager has been running for a long time, but it does not work consistently.

   Check to see if you are running an evaluation version. If so, you need to upgrade to a regular version.

6. eManager is running, but it does not block spam.

   Check the free space of `/opt` or the inode number of `/opt/trend/Plug-Ins/EM/Quarantine`(or `Archive`)

7. I can't install eManager.

   You must install InterScan VirusWall Standard Edition before installing eManager. If you have InterScan VirusWall installed, check that there is enough free space in the `/opt` directory for eManager to install.

8. How can you move the `quarantine`/`archive` folder to another folder (`/tmp` or `/var`), when space of `/opt` is full?

   From the command line, type the following:

   ```
   mkdir /var/quarantine [Enter]
   cd/opt/trend/Plug-Ins/EM [Enter]
   ```

```
mv quarantine  quarantine.orig [Enter]
ln -s /var/quarantine  /opt/trend/Plug-Ins/EM/quarantine [Enter]
```

This will create the new directory and move the files to the new directory.

9. How do I change the password for the eManager Web configuration program?

In the InterScan Web console, click **Configuration > Change Password**. The eManager password is the same as the one used by InterScan VirusWall and defined using the InterScan configuration.

Chapter 9

Getting Support

Trend Micro commits to providing service and support that exceeds our user's expectations regardless of their location. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter includes the following topics:

- Before Contacting Technical Support
- Contacting Technical Support
- Submitting Spam Messages
- TrendLabs™
- Other Useful Resources

Before Contacting Technical Support

Before contacting technical support, here are two things you can do to quickly find an answer to your problem:

- **Check your documentation**: the manual and online help provide comprehensive information about InterScan eManager. Search both documents to see if they contain your solution.

- **Visit our Technical Support Web site**: our Technical Support Web site contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

  To search the Knowledge Base, visit
  http://kb.trendmicro.com/solutions/solutionSearch.asp

Contacting Technical Support

In addition to phone support, Trend Micro provides the following resources:

- Email support
  support@trendmicro.com
- On-line help — Configuring the product & parameter-specific tips
- readme.txt — Late-breaking product news, install instructions, known issues, and version specific info
- Knowledge Base — technical information procedures provided by the Support team:
  http://kb.trendmicro.com/solutions/solutionSearch.asp
- Product updates and patches
  http://www.trendmicro.com/download/

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

http://www.trendmicro.com/en/about/contact/overview.htm

To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product serial number
- InterScan eManager, Import, and Rule file version
- Operating system version and Internet connection type
- Exact text of the error message, if any
- Steps to reproduce the problem

Submitting Spam Messages

You can recommend spam or content criteria for possible inclusion to Trend Micro Rule and Import files.

To submit spam messages:

1. Save the spam mail(s) and place them in a compressed file (for example, `tar`). Limit the size of the attachment to 3 MB.
2. Create a new mail message, address it to **spam@trendmicro.com**, and attach the compressed file containing the spam messages.
3. Send the message.

TrendLabs™

Trend Micro TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

www.trendmicro.com/en/security/trendlabs/overview.htm

Other Useful Resources

Trend Micro offers a host of services via its Web site, www.trendmicro.com.

Free Internet-based tools and services

- The World Virus Tracking Center - monitor virus incidents around the world.

- HouseCall™ - Trend Micro free online virus scanner.
- Free virus risk assessment - Trend Micro free online virus protection assessment program for corporate networks.

Appendix A

Document Conventions and Definitions

Document Conventions

The following table describes the type changes used in this manual.

TABLE 1-1. Typographical Conventions

Typeface	Description	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	`gzip -d emux_en_sol_v38.tar.gz`
AaBbCc123	The names of InterScan Web console menus and options	Click **Apply**.

Document Definitions

The IP addresses used in the InterScan eManager document set begin with 123. In addition, the domain names of all but Internet backbones have been altered.

Because the email examples presented here have been taken from actual unsolicited commercial emails (UCEs), and because of the continuously changing nature of the

Internet and the common use of "hijacked" domain names, SMTP servers, and IP addresses, the InterScan document set has taken this step to ensure that no one is improperly identified.

None of the domain names or IP addresses used in the examples of email headers are real.

Index

T

U