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 Administrator's Guide, which are available from Trend Micro's Web site at:

`www.trendmicro.com/download/`

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 reviewed on an annual basis at Trend Micro's then-current Maintenance fees.

Trend Micro, the t-ball logo, ActiveAction, IntelliScan, InterScan Messaging Security Suite, InterScan VirusWall, OfficeScan, and ScanMail are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

This product includes software developed by the following third parties:

Apache Software Foundation. Copyright (c) 1995-2005. All rights reserved.

`http://www.apache.org/licenses/LICENSE-2.0`

Copyright© 2002 - 2005 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. SMEM72242/50408

Release Date: July, 2005

Protected by U.S. Patent No. 5,951,698

The Administrator's Guide for Trend Micro ScanMail 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.

For technical support, please refer to Contacting Trend Micro in this Administrator's Guide. 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.

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: Welcome to Trend Micro™ ScanMail for Microsoft™ Exchange

Features and Benefits 1-2
What's New 1-3
  Version Comparison 1-5
ScanMail Technology 1-6
  The Trend Micro Scan Engine 1-7
    Scan Engine Updates 1-7
  The Trend Micro Virus Pattern Files 1-8
    Pattern file numbering 1-9
  How the Scan Engine Works with the Virus Pattern File 1-9
  About ActiveUpdate 1-10
    Incremental updates of the virus pattern file 1-10
    Using ActiveUpdate with ScanMail 1-10
  Trend Micro IntelliScan™ 1-11
  Trend Micro ActiveAction™ 1-11
  Spam engine and spam pattern files 1-12
  System Watcher 1-12

Chapter 2: Installing and Removing ScanMail

System Requirements 2-2
Before you Begin 2-3
  Pilot installation 2-3
  Testing your installation 2-4
  Deployment Strategy 2-6
    Deploying ScanMail to multiple servers 2-7
    Deploying ScanMail to multiple Local Area Network (LAN) segments 2-9
Preparing to Install 2-9
  Pre-Installation Checklist 2-10
  Overview of the Installation Process 2-11
Performing a Fresh Install 2-13
    Installing on a cluster 2-13

Upgrading to ScanMail 7.0 2-13
Upgrading on clusters 2-16
Running the Setup Program 2-17
Cluster installation 2-33
Post-Installation 2-34
Set Up Spam Prevention 2-34
Verifying a Successful Installation 2-34
Removing ScanMail 2-36
Removing ScanMail using the Trend Micro™ Enterprise Solution CD 2-36
Removing ScanMail Using the Windows Control Panel 2-37
Removing ScanMail from Clusters 2-38

Chapter 3: Activating and Updating ScanMail

Registering and Activating ScanMail 3-2
Activation Codes 3-2
Activating ScanMail 3-4
Updating ScanMail 3-5
Updating Components on Clusters 3-6
Setting your proxy server 3-6
Manually updating your components 3-7
Setting a scheduled update 3-8
Download Source 3-9
Rolling Back a Component Update 3-11

Chapter 4: Managing ScanMail Servers

Using the Web Management Console 4-2
Management console main view 4-2
The Web management console elements 4-3
Getting Help While Using the ScanMail Web Management Console 4-5
Viewing Servers from the Web Management Console 4-5
Viewing Virtual Servers on a Cluster 4-6
Understanding the Real-time Monitor 4-7
Understanding the Server Management Console 4-8
Using Server Management to Replicate Configurations 4-9
Manually Creating a ScanMail Resource for Virtual Servers 4-10

Chapter 5: Understanding Threats to an Exchange Environment

What do the terms mean? 5-2
- Viruses 5-2
- Worms 5-4
- Trojan horse programs 5-4
- Joke Programs 5-4
- About Mass-Mailing Attacks 5-5
- About Compressed Files 5-5
- About Macro viruses 5-6
- Spyware and other Grayware 5-7

How Can these Things Affect the Exchange Environment? 5-9
How ScanMail Protects the Exchange Environment 5-10

Chapter 6: Establishing and Maintaining Security for your Exchange Servers

Establishing a Security Baseline 6-2
Maintaining Security 6-3
Updating ScanMail 6-4
Managing Outbreak Situations 6-5

Chapter 7: Configuring and Performing ScanMail Tasks

About ScanMail Configurations 7-2
- Optimizing your ScanMail configurations 7-2
- Trend Micro default actions 7-3

About Virus Scanning 7-5
- ScanMail filtering strategy 7-5
- About Notifications 7-10
  - Setting up Notifications 7-10
  - Windows Event Logs 7-11
- Enabling and Disabling Scans 7-12
- Configuring Virus Scanning 7-13
- Selecting files to scan 7-14
  - File types eligible for scanning 7-14
  - About Scannable Files 7-15
  - About IntelliScan 7-16
  - True file type 7-16
  - Scan restrictions for large attachments and compressed files ... 7-18

Setting Scan Actions 7-20
About ScanMail actions 7-20
Types of Security Threats 7-21
Using ActiveAction 7-22
Using customized actions 7-22
About Uncleanable Files 7-24
Using Advanced Scanning Options 7-27
Using advanced macro scanning 7-27
Running Manual Scans 7-29
Managing Scheduled Scans 7-30
Virus Scanning on Clusters 7-32
About Blocking Attachments 7-33
Selecting blocking targets 7-34
Attachment Blocking actions 7-35
Filtering Undesirable Content 7-37
Viewing Content Filtering Rules 7-37
Enabling Content Filtering Rules 7-38
Adding Content Filtering rules 7-39
Specifying global directories 7-48
Modifying Content Filter rules 7-48
Changing the Rule Order 7-51
About Filtering Keywords 7-51
Using keywords effectively 7-51
Formatting keywords that use operators 7-53
Using Regular Expressions 7-55
Content Filtering Actions 7-61
Screening Out Spam 7-62
Using Approved and Blocked Senders 7-64
Setting the spam detection level 7-66
Setting Anti-spam action 7-66
Detecting and Taking Action against Phish 7-67
Managing the End User Quarantine Tool 7-68
End User Quarantine housekeeping feature 7-68
Setting Up and Managing the Quarantine Folder 7-69

Chapter 8: Configuring and Sending Alerts and Notifications

Setting Notifications 8-2

About Outbreak Alerts and System Events 8-2
Configuring System Event Notifications 8-3
Configuring Outbreak Alerts 8-6

Chapter 9: Managing Reports, Logs, and the Quarantine Folder

Managing Reports 9-2
Types of reports 9-2
Contents of a report 9-3
Generating, Viewing, and Sending Reports 9-4
Deleting Reports 9-5
Managing Logs 9-6
Setting up and running log queries 9-6
Deleting Logs 9-7
Managing the Quarantine Folder 9-8
Making Quarantine queries 9-9
Resending quarantined messages 9-10
Deleting Quarantined Messages 9-11

Chapter 10: Administrative Tasks

Setting the Proxy Server 10-2
Notification Settings 10-2
Setting up the Spam Folder 10-4
Understanding Product License Information 10-6
Maintenance Agreement 10-6
When your License Expires 10-7
Renew ScanMail Maintenance Agreement 10-8
Reactivating an Activation Code 10-8
Participating in World Virus Tracking 10-8
Generating Debugger Reports 10-10

Chapter 11: Getting Support and Contacting Trend Micro

Contacting Trend Micro 11-2
Contacting Technical Support 11-2
Before contacting Technical Support 11-3
TrendLabsSM 11-4
Known Issues 11-5
Frequently Asked Questions (FAQ) 11-11

Appendix i: Windows Event Log Codes

Appendix ii: Glossary of Terms

Chapter 1

Welcome to Trend Micro™ ScanMail for Microsoft™ Exchange

Trend Micro designed Trend Micro™ ScanMail™ for Microsoft™ Exchange version 7.0 to protect your Exchange 2000 and 2003 mail servers. Once installed, ScanMail immediately begins to protect your servers, in real time, against viruses, Trojans, worms, spyware, and other grayware. ScanMail also sustains business and network integrity by screening out spam mail and messages containing undesirable or unwanted content. ScanMail notifications send timely alerts to administrators or other designated individuals whenever significant system events or outbreak activities occur.

In this chapter, you will find information about:

- *Features and Benefits* on page 1-2
- *What's New* on page 1-3
- *ScanMail Technology* on page 1-6
- *About ActiveUpdate* on page 1-10

Features and Benefits

ScanMail features provide the following benefits:

Fast and simple installations

- Install to a single or multiple Microsoft Exchange servers using a single installation program
- Install to cluster environments

Powerful and creative antivirus features

- SMTP scanning for Exchange 2000 and 2003 servers
- Leverage Microsoft VSAPI to scan messages at a low-level in the Exchange store
- Quickly scan messages using multi-threaded in-memory scanning
- Detect and take action against viruses, Trojans, and worms
- Detect and take action against spyware and other grayware
- Use true file type recognition to detect falsely labeled files
- Use Trend Micro recommended actions or customize actions against viruses
- Detect all macro viruses and remove them or use heuristic rules to remove them

Attachment blocking

- Block named attachments or block attachments by file type

Content filtering

- Use rule-based filters to screen out message content deemed to be harassing, offensive, or otherwise objectionable

Anti-spam rules

- Use anti-spam filters with adjustable sensitivity levels to screen out spam while reducing falsely identified messages
- Server-side rules control approved sender lists that are maintained by clients

Quarantine

- Set ScanMail to quarantine suspect email messages
- Query logs for quarantine events and resend quarantined messages when you decide they are safe

Web based management console

- Use SSL to access remote servers through a secure Web management console

Notifications

- Alert administrators about ScanMail actions using customizable notifications
- Set Alerts to notify selected recipients whenever a virus outbreak or significant system events occurs

Informative and timely reports and logs

- Keep up-to-date using activity logs that detail system events, viruses, and program update events, send or print graphical reports

Updates

- Receive scheduled or on-demand component updates, customize your update source

What's New

The following new features are available in ScanMail version 7.0:

Integrated anti-spam and content filtering features

Integrated anti-spam and content filtering features. Manage all anti-spam and content filtering from one Web management console with new enhanced scanning capability. Spam management for Exchange users is provided in EUQ 1.1 and rule-based filters are used to screen out messages that contain undesirable content.

SMTP scanning

For better scanning capability, ScanMail delivers a new SMTP scanning technology for Microsoft Exchange 2000 and 2003. You can now scan message traffic with full mail information available at the mail transport level on both platforms, preventing unsolicited messages from entering Exchange store databases on back-end servers.

Server Management

Server Management allows you to replicate configurations from one server to another.

Cluster support

ScanMail 7.0 uses Exchange Virtual Servers (EVS) management model for managing clusters. Each virtual server owns independent ScanMail configuration information and keeps the data consistent even when performing a failover to another node, thus supporting increased availability on clusters.

Keyword matching

Use keyword matching to search for logs and quarantined email messages.

Real-time monitor Web console

Monitor real-time scanning activity on remote and local servers from the convenient Web management console on one single machine.

Web management console

All scanning configurations are available from one single Web management console, including logs and reports.

Comprehensive and graphical reports

Generate a comprehensive and graphical report of the scanning result summary on demand or by scheduled task. The report is available by mail or from the Web management console.

Customizable notifications

Customizable notifications for system events and outbreak alerts. ScanMail can send alerts when the period or the number of notification occurrences exceeds a user-configured number.

Version Comparison

The following table lists all versions of ScanMail and the features for each:

Support	ScanMail 3.53	ScanMail 3.82	ScanMail 6.2	ScanMail 7.0
OS Version	•Windows 3.51 with SP5 •Windows NT 4.0 with SP3 •Windows 2000 with SP1	•Windows NT 4.0 with SP3 •Windows 2000, with SP1	•Windows 2000, with SP1 •Windows 2003	•Windows 2000, with SP2 •Windows 2003
Minimum Exchange Version	•Exchange 4.0, 5.0, and 5.5 (to use VSAPI, store.exe must be at least version 5.5.2652.42)	•Exchange 5.5 SP2	•Exchange 2000 SP1 •Exchange 2003	•Exchange 2000 SP3 •Exchange 2003
Scan mechanism	•MAPI •VSAPI	•ESEAPI	•VSAPI 2.0 •VSAPI 2.5	•VSAPI 2.0 •VSAPI 2.5
Exchange Information Store scanning	•Yes	•Yes	•Yes	•Yes
SMTP scanning	•No	•Yes	•Yes	A new SMTP scanning technology
Quarantine Manager	•No	•Yes	•Yes	•Yes
Active Message Filter	•No	• Mailstore level (outbound) • SMTP level (inbound and outbound messages)	•Inbound and outbound messages	•Integrated as delete function for inbound and outbound messages
Notification	•Dependent on ScanMail profile	•Dependent on ScanMail profile	•Collaborative Data Object	•Collaborative Data Object

TABLE 1-1. ScanMail version comparison

Note: Previous versions of ScanMail offered eManager as a separate module add-on. ScanMail 7.0 has fully integrated eManager features so that it is no longer necessary to install eManager separately.

ScanMail Technology

The following diagram gives an overview of the key components of ScanMail and shows their relationship to each other.

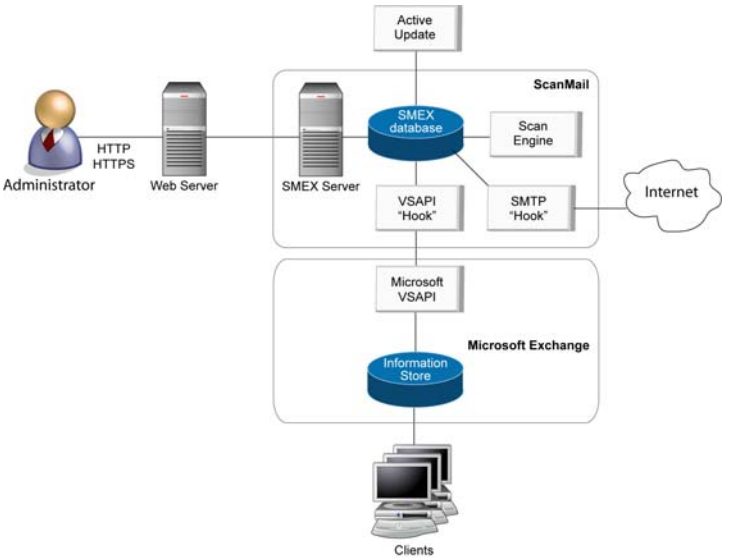

FIGURE 1-1. ScanMail components overview

The ScanMail administrator uses the Web management console to configure ScanMail. This can be done locally or remotely from another Web management console on the same domain.

The ScanMail VSAPI (Virus Scanning Application Interface) "hook" works with the Microsoft Virus Scanning API (Application Interface) to deliver all email messages to the Trend Micro scan engine for scanning.

The Trend Micro scan engine and spam engine detect viruses and other security threats and screen out spam messages. These two engines rely on the most up-to-date pattern files supplied by TrendLabs and delivered through ActiveUpdate servers or a user-configured update source.

The Trend Micro Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. This engine has a long history in the industry and has proven to be one of the fastest.

The ScanMail scan engine is designed to work closely with the Virus Scanning Application Programming Interface (VSAPI) 2.0 and 2.5 available from Exchange.

- VSAPI provides a virus-scanning implementation with high performance and guarantees that scanning occurs before a client can access a message or attachment. This low-level access facilitates the elimination of viruses that file-level scanners cannot eliminate.
- VSAPI enables message scanning once before delivery, rather than multiple times as determined by the number of intended recipients, reducing processing time. This single-instance scanning also prevents re-scanning when a user copies a message.

The scan engine provides:

- Real-time multi-threaded scanning

  ScanMail performs all scanning in memory and is capable of processing multiple scan requests. When it receives multiple scan requests, it prioritizes and queues the requests that it cannot run immediately and runs the requests when resources become available. When a manual or scheduled scan is running and a client attempts to access an email message, ScanMail performs an immediate real-time scan on the requested message.

  ScanMail supports SMTP real time mail scanning. It supports this for both Exchange 2003 and Exchange 2000.

- Non-redundant scanning

  When ScanMail completes a scan of a message, it logs the message as scanned. If you access the message again, ScanMail checks to see if it has already scanned the message and does not scan the message a second time.

International computer security organizations, including the International Computer Security Association (ICSA) annually certify the Trend Micro scan engine.

Scan Engine Updates

Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- Trend Micro incorporates new detection technologies into the software
- A new, potentially harmful, virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:
`http://www.trendmicro.com`

To view the version of the scan engine that ScanMail is currently using on an Exchange server, open the Web management console and view **Summary > System**. Trend Micro recommends frequently updating your scan engine.

The Trend Micro Virus Pattern Files

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses and other Internet threats.

You can view the most current version, release date, and a list of all the new viruses definitions included in the file from the following Web site:
`http://www.trendmicro.com/download/pattern.asp`

To view the version of the pattern file that ScanMail is currently using on your ScanMail server, open the Web management console and view **Summary > System**. Trend Micro recommends frequently updating your pattern file.

Pattern file numbering

To allow you to compare the current pattern file in your software products to the most current pattern file available from Trend Micro, pattern files have a version number.

The pattern file numbering system uses 7 digits, in the format *xx.xxx.xx*.

For the file pattern number 1.786.01:

- The first digit (1) indicates the new numbering system. (The second of two digits in this segment of the pattern file identifier will not be utilized until the number increases from 9 to 10.)
- The next three digits (786) represent the traditional pattern file number.
- The last two digits (01) provide additional information about the pattern file release for Trend Micro engineers.

Note: The anti-spam pattern file does not use this numbering system.

Be sure to keep your pattern file updated to the most current version to safeguard against the most current threats.

How the Scan Engine Works with the Virus Pattern File

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique "signature" or string of tell-tale characters that distinguish it from any other code, the virus experts at TrendLabs capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match. When it finds a match, it sends a notification through an email message to the system administrator.

Note: The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space).

About ActiveUpdate

ActiveUpdate provides up-to-date downloads of all ScanMail components over the Internet. ScanMail components include pattern files for viruses, spam, and additional threats; and components for the scan engine and spam engine.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. ScanMail can receive updates on a regularly scheduled interval or through manual updates.

Incremental updates of the virus pattern file

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software.

Configure ScanMail to use ActiveUpdate and incremental updates to decrease the time spent updating.

Using ActiveUpdate with ScanMail

You can configure ScanMail to use the ActiveUpdate server as a source for manual and scheduled component updates. When it is time for the component update, ScanMail polls the ActiveUpdate server directly, ActiveUpdate determines if an update is available, and ScanMail downloads it.

Tip: For a more efficient download in a multi-server environment, designate a single ScanMail server to act as a hub server for downloading updates and then have your spoke ScanMail servers pull in the update using replication. Another efficient method is to set ScanMail to duplicate the update package on a server; making it a virtual ActiveUpdate server for any other servers that receive incremental updates.

Trend Micro IntelliScan™

IntelliScan optimizes performance by examining file headers using true file type recognition and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by using a harmless file extension type. The following are just a couple of the benefits IntelliScan offers to administrators:

- **Performance optimization**: Server system resources allotted to scan will be minimal, thus using IntelliScan will not interfere with other crucial applications running on the server.
- **Time saving**: Since IntelliScan uses true file type identification, the scan time for running IntelliScan is significantly less than the time required for **all scannanble files** (this means that only files with a greater risk of being infected are scanned). This time difference is noticeable when you use IntelliScan with Manual scan.

Trend Micro ActiveAction™

ActiveAction identifies virus types and recommends actions based on how each type invades a computer system or environment. ActiveAction categorizes malicious code, replication, and payload types as viruses. When ScanMail detects a virus, it takes the recommended action (clean, quarantine, delete) on the virus type to protect your environment's vulnerable points.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- **Time saving and easy to maintain** — ActiveAction uses scan actions recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- **Updateable scan actions** — Virus writers constantly change the way viruses attack computers. Trend updates ActiveAction settings in each new virus pattern file to protect clients against the latest threats and the latest methods of virus attacks.

Spam engine and spam pattern files

ScanMail uses the Trend Micro Spam engine and Trend Micro spam pattern files to detect and take action against spam messages. Trend Micro updates both the engine and pattern file frequently and makes them available for download. ScanMail can download these components through a manual or scheduled update.

The spam engine makes use of spam signatures and heuristic rules to screen email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. ScanMail compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, ScanMail takes action against the spam.

For example: Many spammers use many exclamation marks, or more than one consecutive exclamation mark (!!!!) in their email messages. When ScanMail detects a message that uses exclamation marks this way, it increases the spam score for that email message.

Note: You cannot modify the method that the spam engine uses to assign spam scores, but they can adjust the detection levels used by ScanMail to decide what is spam and what is not spam.

System Watcher

When ScanMail is installed, a separate system watching program is installed with it. The System Watcher monitors ScanMail and logs when significant system events occur or when security outbreak conditions exist. You can configure ScanMail to send notifications when system events or outbreaks occur.

Chapter 2

Installing and Removing ScanMail

Install ScanMail locally or remotely to one or more servers using one easy-to-use installation program.

This chapter includes information about:

- *System Requirements* starting on page 2-2
- *Before you Begin* on page 2-3
- *Preparing to Install* on page 2-9
- *Performing a Fresh Install* on page 2-13
- *Upgrading to ScanMail 7.0* on page 2-13
- *Upgrading on clusters* starting on page 2-16
- *Removing ScanMail* on page 2-36
- *Removing ScanMail from Clusters* starting on page 2-38

System Requirements

To install ScanMail, you need the following minimum hardware and software:

Hardware/Software	Requirement	Recommendation
Processor	Intel Pentium or compatible 133MHz or higher processor.	Intel Pentium or compatible 733MHz processor
Memory	256MB RAM	512MB RAM
Disk Space	250MB free disk space	300MB free disk space
Java Virtual Machine	Version J2RE 1.4.1_02	Version J2RE 1.4.1_02

Platform/OS	Versions and Service Packs
Windows	Microsoft Windows 2003 Server or 2000 Server with Service Pack 2 or above
Exchange	Microsoft Exchange 2003 Server or 2000 with Service Pack 3 or above

Web server	• Microsoft Internet Information Services (IIS)
	  • Microsoft Windows 2003 Server requires IIS 6.0
	  • Microsoft Windows 2000 Server requires IIS 5.0
	• Apache Web server 2.0

Internet Explorer	A Java-enabled Web browser that supports frames, such as Microsoft® Internet Explorer® 5.5 with SP3
Netscape	7.2 or above

Note: For Web-based management, please download and install the latest version of the Java Virtual Machine, J2RE 1.4.1_02 or above. You can download the JVM from www.sun.com.

For cluster installation:

- Requires Microsoft Windows 2000 Advanced Server
- ScanMail also supports Windows 2003 Clusters.

Before you Begin

The following section contains some Trend Micro recommendations for installing ScanMail. Read this section before you begin your installation.

Pilot installation

Trend Micro recommends conducting a pilot deployment before performing a full-scale deployment. A pilot deployment provides an opportunity to gather feedback, determine how features work, and to discover the level of support likely needed after full deployment.

Tip: Monitor and test ScanMail in this test environment. When you are confident that ScanMail is working well in the test environment, use Server Management to replicate the settings to a live environment.

To conduct a pilot installation:

1. Create an appropriate test site.
2. Create a rollback plan.
3. Deploy and evaluate your pilot.

Create an appropriate test site

Create a test environment that matches your production environment as closely as possible. The test server and production servers should share:

- The same operating system, Exchange version, service packs, and patches
- The same Trend Micro and other third party software such as Trend Micro Control Manager™, Trend Micro OfficeScan™, and Trend Micro™ ServerProtect™
- The same type of topology that would serve as an adequate representation of your production environment

Note: Trial versions of most Trend Micro products are available for download from the Trend Micro Web site:
http://www.trendmicro.com/download/

Rollback plan

Trend Micro recommends creating a rollback or disaster recovery plan in case there are issues with the installation or upgrade process. This process should take into account local corporate policies, as well as technical specifics.

Install and evaluate your pilot

Install and evaluate the pilot based on expectations regarding both antivirus and content security enforcement and network performance. Create a list of successes and failures encountered throughout the pilot process. Identify potential "pitfalls" and plan accordingly for a successful installation.

Testing your installation

Trend Micro recommends verifying success of the installation by testing ScanMail features using the EICAR test script. EICAR, the European Institute for Computer Antivirus Research, developed the test script as a safe way for you to confirm that you have properly installed and configured your antivirus software.

Visit the EICAR Web site for more information:

`http://www.eicar.org`

The EICAR file is a text file with a *.com extension. It is inert. It is not a virus, it does not replicate, and it does not contain a payload. Never use real viruses to test your antivirus installation.

WARNING! *Depending on how you have configured your Exchange servers, you might need to disable antivirus products for the duration of the EICAR test (otherwise, the virus might be detected before it arrives at the Exchange server). This leaves your servers vulnerable to infection. For this reason, Trend Micro recommends that you only use the EICAR test in a test environment.*

To test Virus Scanning with EICAR:

1. Before testing, make sure you have a valid mail client connected to the Exchange 2000 or 2003 Server you are testing.
2. If necessary, disable antivirus products that might detect the EICAR test file before it arrives at your Exchange server.
3. Verify that Real-time Scan and Real-time Monitor services are running correctly.
   a. Click the Real-time monitor link at the top of your Web management console.
   b. On the Real-time Monitor screen you can read the message **Real-time scan has been running since**. If the Real-time scan is not working, you will see a blank screen with the message Real-time Scan has been stopped.
4. Test real-time Virus Scanning.
   a. Prepare the EICAR test script
      i. Open an ASCII text file and copy the following 68-character string to it.

      ```
      X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
      ```

      ii. Save the file as `eicar_test.com` to a temp directory and then close it.
   b. Send the email to the your test mailboxes.
5. Open the Real-time monitor again. You will see ScanMail scanning and detecting the test file as passes through the Real-time Monitor.
6. In addition to the Real-time monitor you can also review the virus detection result from the Virus Summary page or by making a log query.

Note: Trend Micro also recommends testing a zipped version of the EICAR file. Using compression software, zip the test script and perform the steps above.

To test notification

1. Configure Virus Scanning to detect the virus and notify the administrator.
   a. Click **Virus Scanning** > **Target**. Select IntelliScan if necessary.
   b. Click **Action**. Select **ActiveAction** and select **Notify** from the drop-down list.

c. Click **Notification**. Click **Notify administrator** and then click on the icon to expand the page. Select **To** and type the email address where you want to send the notification.

d. Click **Save**.

2. Send an email containing the EICAR test script and verify that the administrator received the email.

a. Create a test message called "Test ScanMail" and attach a copy of the EICAR test script to your email.

b. Send the email to the your test mailboxes.

c. Go to the test mailbox inbox and view the notification.

Deployment Strategy

The ScanMail installation program supports installation to single or multiple local or remote servers. ScanMail was designed to protect both front-end (bridgehead) and back-end servers and fully supports server clustering.

When deploying and configuring ScanMail on your LAN segments consider:

- The network traffic burden on your servers
- Whether your network uses multiple mail servers and/or a bridgehead server and back-end servers
- Whether your enterprise network contains more than one Local Area Network (LAN) segment

Planning for network traffic

When planning for deployment, consider the network traffic and CPU load that ScanMail will generate.

ScanMail generates network traffic when it does the following:

- Connects to the Trend Micro update server to check for and download updated components
- Sends alerts and notifications to administrators and other designated recipients

ScanMail increases the burden on the CPU when it scans email messages arriving at the Exchange server in real time or during scheduled and manual scans. Unlike some

other antivirus products, ScanMail uses multi-threaded scanning which reduces the CPU burden.

Deploying ScanMail to multiple servers

If your network has only one Exchange server, deploying ScanMail is a relatively simple task. Install ScanMail on the Exchange servers and configure it to optimize your messaging security.

If your company has multiple Exchange servers, deploying ScanMail can be more complex. A popular strategy deploys one server as a front-end server just behind the gateway and the rest of the mail servers as back-end servers. Back-end servers are often installed to clusters to gain the benefit of failover recovery. If your company uses this model, consider the points in Table 2-1 when you deploy ScanMail.

Another strategy is to deploy ScanMail to an Exchange server on the DMZ. This increases the risks to which the servers are exposed. When exposing Exchange servers to the Internet, SMTP traffic is a major concern. Trend Micro recommends enabling SMTP scanning when installing ScanMail on Exchange servers exposed to the Internet (this is the default value). ScanMail scans SMTP traffic during real-time scanning. Carefully consider your configurations and only depart from Trend Micro default configurations when you understand the consequences.

Server type	Trend Micro recommends
Front-end mail servers: • Are usually located directly behind a perimeter device and/or firewall • Frequently communicate with the Active Directory to locate mailbox addresses and routing information • Primarily forward all email messages to back-end mail servers for delivery to client mailboxes • Receive a lot of messages using SMTP protocol • Receive a lot of messages that are encrypted for safe passage across the Internet and resolve mail authentication • Have a heavy traffic load, especially when communicating with the Active Directory to resolve email addresses and read configuration data	• Setting the Trend Micro ActiveUpdate server as the source of component updates for the front-end server, and setting back-end servers to use the front-end server as the source for updates, this decreases overall network traffic and reduces exposure to the Internet • Configuring SMTP scanning on front-end mail servers. Note: Only ScanMail version 7.0 and 6.21 offer SMTP scanning • Configuring ScanMail to screen out email messages and attachments that contain spam or undesirable content at the front-end mail servers to reduce the burden for back-end servers that will no longer have to process these messages
Back-end mail servers: • Are located within the local network, behind the network perimeter and shielded from the Internet • Deliver and store email messages to client mailboxes on the Information Store • May receive local messages using the x.400 protocol, especially in mixed environments • Are often clustered, therefore, less likely to need restoring from backups	• Setting back-end mail servers to perform virus scanning with vigorous screening options • Regularly scheduled scans on Exchange mailboxes to prevent threats from creeping in from unexpected sources not covered in your configurations

TABLE 2-1. Deploying ScanMail to front-end and back-end servers

Deploying ScanMail to multiple Local Area Network (LAN) segments

Large enterprises might have multiple Exchange servers on different LAN segments separated by the Internet. In these cases, Trend Micro recommends installing ScanMail on each LAN segment separately. See *Deploying ScanMail to front-end and back-end servers* on page 2-8.

Note: ScanMail for Microsoft Exchange is designed to guard your Exchange mail servers. ScanMail does not provide protection to non-Exchange mail servers, file servers, desktops, or gateway devices. ScanMail protection is enhanced when used together with other Trend Micro products such as Trend Micro OfficeScan™ to protect your file servers and desktops, and Trend Micro InterScan VirusWall™ or InterScan™ Messaging Security Suite to protect your network perimeter.

Preparing to Install

To prepare for a smooth installation process, preview the information in this section and consult the pre-installation checklist.

For complete protection, Trend Micro recommends that you install one copy of Trend Micro ScanMail on each of your Microsoft Exchange servers. In ScanMail, you can perform local and remote installations from one installation program. The local machine is the one on which the installation program runs and the remote machines are all other machines to which it installs ScanMail. You can simultaneously install ScanMail on multiple servers. The only requirements are that you integrate these servers into your network and access them using a Windows Administrator account with Domain Admin privileges.

Pre-Installation Checklist

Consider the following items before installing to a server:

Item	Notes
Account privileges	To install the server, you must log on with an Administrator account with Domain Admin privilege. If you do not log on with Domain Administrator privileges, you must manually create an administrative group before proceeding with the installation. For more information about manually installing an administration group, see *Overview of the Installation Process* starting on page 2-11. During the installation, the Setup program prompts you to enter an account and password for the Web management console. Setup uses the account and password that you specify to log on to the Web management console and manage ScanMail servers.
Restart	You do not need to stop the Exchange services before installing or restart them after a successful installation except when installing on a cluster. When uninstalling or upgrading ScanMail, the IIS Admin service and all related services will be automatically stopped and restarted. **Warning**: If you are installing ScanMail on a server which is running lockdown tools (such as typically implemented for Windows 2000 server with IIS 5.0), remove the lockdown tool so that it does not disable IIS service and cause the installation to be unsuccessful.
Registration Key and Activation Code	During installation, the setup program prompts you to type an Activation Code. You can use the Registration Key that came with ScanMail to obtain an Activation Code online from the Trend Micro Web site. The setup program provides a link to the Trend Micro Web site. If you do not Activate your product during registration, you can do so at a later time from the Web management console. However, until you Activate, ScanMail will only provide a limited service.
Proxy server	During installation, the setup program prompts you to enter proxy information. If a proxy server handles Internet traffic on your network, you must type the proxy server information, your user name, and your password to receive virus pattern file and scan engine updates. If you leave the proxy information blank during installation, you can configure it at a later time from the Web management console.

Item	Notes
End User Quarantine configurations	The End User Quarantine is a tool that adds extra spam management features to ScanMail. The installation program gives you the option of installing EUQ to one or more servers in your installation. To upgrade to EUQ 1.1, you must log on using a Domain Administrator account. Trend Micro recommends that you use the same account to log on that you used when you installed EUQ 1.0. If this is unsuitable, we recommend that you first remove EUQ 1.0 before upgrading to EUQ 1.1. Decide if you want to install EUQ on one or more servers. If you decide to install EUQ, prepare a name for the spam folder for each server. You require a Domain administrator account and password for creating the EUQ report mail box.

TABLE 2-2. Pre-installation checklist

Overview of the Installation Process

The following is a quick overview of a typical installation process.

1. Log on with appropriate account privileges

Installing ScanMail involves logging on to Windows 2000 or 2003 Server with the appropriate account and privileges. Trend Micro recommends that you use an account that has Domain Administrator privileges. If you do not have Domain Administrator privileges, you must do the following:

a. Manually create an administrative group named "SMEX Admin group" on the Active Directory.

There are two types of groups in Active Directory - Distribution and Security. When creating the "SMEX Admin group", specify the Security group.

b. Assign a domain user account to this group for each person who will need to log on and manage ScanMail servers. The Setup program requests that you input this information during the installation.

Managing ScanMail servers includes using the Server management tool to replicate settings from one ScanMail server to another.

Note: Previous versions of ScanMail did not have this requirement.

2. Select a source for the Setup program
   - Trend Micro Web site.
     - Download ScanMail from the Trend Micro Web site.
     - Unzip the file to a temporary directory
     - Run setup.exe to install ScanMail
   - The Trend Micro Enterprise Solution CD
     - Insert the CD and follow the online instructions.
3. Run the Setup program. See *Running the Setup Program* on page 2-17 for the detailed instructions of this procedure.
   a. Choose the installation options.
   - Choose whether you want to install, upgrade, or uninstall ScanMail
   - Accept the license agreement

   b. Activate ScanMail.

   Register ScanMail and type your Activation Code in the Product Activation screen to activate ScanMail. You can register ScanMail online before you begin your installation from the Trend Micro Web site:

   c. Set up and log on to the target servers.

   Select the servers that will run ScanMail. You need to log on to these servers using an Administrator account with Domain Administrator privilege.

   d. Select components to install and to enable.

   Choose to enable or disable SMTP scanning and choose whether or not you want to install the optional EUQ component.

   e. Configure the Web server and Web management console.

   Configure the Web server, the log on account for the Web management console, and the proxy settings for the Web management console.

   f. Review and complete the installation.

   Review your selections and change them if necessary.

Performing a Fresh Install

If you do not have a previous version of ScanMail installed on your Exchange server, then you need to perform a fresh installation. Before beginning your installation, preview the section *Overview of the Installation Process* starting on page 2-11 and consult the pre-installation checklist, Table 2-2.

Installing on a cluster

You can install ScanMail on Windows 2000 or 2003 clusters. For cluster installation, ScanMail adds a resource for each virtual server and installs all nodes in the cluster simultaneously.

Note: For uniform protection, Trend Micro recommends that you install one copy of ScanMail on each of your Microsoft Exchange servers.

Upgrading to ScanMail 7.0

To upgrade ScanMail, run the Setup program. Before beginning your installation, consult the pre-installation checklist, Table 2-2.

ScanMail for Microsoft Exchange 7.0 supports upgrade for ScanMail version 6.0, 6.1, or 6.2. If you are currently using one of these versions, the Setup program automatically removes it and installs ScanMail 7.0.

Note: If you have a version of ScanMail that does not support upgrading, remove it using the same version of the uninstallation program that you used to install it. For example, if you are using ScanMail 5.1, uninstall using the ScanMail 5.1 uninstallation program.

Upgrade requires a new Activation Code, even when the previous code has not yet expired.

When upgrading, if ScanMail 7.0 has configuration settings similar to the previous version, then the upgraded version maintains these customized configurations. However, when ScanMail 7.0 has no equivalent configuration setting, it installs and uses the Trend Micro default configurations.

For detailed information about ScanMail default actions, refer to *Trend Micro default actions* starting on page 7-3.

Upgrade effect on logs and folders

Upgrading to ScanMail 7.0, has the following effects on logs and folders:

- Logs are retained and can be queried in the upgraded version.

  Tip: Before upgrading, check the size of your log files. If the log file is very large, Trend Micro recommends that you run maintenance using your current version before you upgrade. This will greatly reduce the amount of time required for upgrade.

- The quarantine and backup folders are retained during upgrading; however, you will no longer be able to query the quarantined log or resend the quarantined items from the previous version from the Web management console of the upgraded version.
- eManager anti-spam logs are retained.

Upgrade effect on configurations

Upgrading to ScanMail 7.0, has the following effects on old ScanMail configurations:

- End User Quarantine (EUQ).

  The approved sender lists are maintained in the upgraded version.
- Control Manager agent for ScanMail or eManager. Trend Micro recommends manually removing it before performing upgrade.
- ScanMail with eManager.

  Previous versions of ScanMail with eManager used anti-spam rules to block email messages that matched specified keywords. In ScanMail 7.0, this function is provided by Content Filtering rules. The anti-spam rule name from the previous version is imported to ScanMail 7.0. For detailed information about how ScanMail upgrades anti-spam rules from eManager see Table 2-3.

The old anti-spam rule used ...	ScanMail imports the rule as a Content Filtering rule
Exactly matching keywords	By default, ScanMail 7.0 uses exact matches on all keywords to filter content.
Partially matching keywords	ScanMail uses *regular expressions* with the specified keywords. See *Using Regular Expressions* on page 7-55
Global exception	ScanMail sets the rule to trigger a *Pass* action so that ScanMail takes no action against messages configured with global exceptions rules. ScanMail assigns this imported rule the lowest rule order number so that it is always filtered first.
Notifications	ScanMail retains the notification settings.

TABLE 2-3. Effect of upgrading eManager anti-spam rules

ScanMail supports all eManager message blocking actions described in the following table:

Old anti-spam action	Upgraded Content Filtering action
Quarantine Archive	Quarantine Archive
Delete	Quarantine

TABLE 2-4. Effect of upgrading eManager anti-spam actions

See *Viewing Content Filtering Rules* on page 7-37 for more information.

Upgrade effect on ScanMail actions

Upgrading from ScanMail 6.x affects ScanMail actions. Consult the following table for each action.

Before Upgrade Action	After Upgrade Action
Clean	Clean
Quarantine ScanMail 6.x used Quarantine to move infected messages to a quarantine directory, replace the infected files, and deliver the remaining message to the original recipient.	Quarantine entire message In ScanMail 7.0 Quarantine entire message copies the original infected message into a quarantine folder and does not deliver the message to the original recipient. After upgrading, the old *Quarantine* action is replaced with the new *Quarantine entire message* action.
Delete ScanMail 6.x used Delete to remove the contents of a message and replace it with a warning text.	Replace with text/file The behavior of the Replace with text/file action is the same as the behavior of *delete* in ScanMail 6.x. ScanMail 7.0 converts this action to *replace with tex/file*.
Pass	Pass

TABLE 2-5. Effect of upgrading on actions

Upgrading on clusters

The upgrade process for clusters is the same as the normal server.

When you upgrade to a cluster environment, logs cannot be queried in the upgraded version. This is because ScanMail 7.0 in a cluster environment is virtual server-based.

WARNING! *Never upgrade a cluster during failover.*

When upgrading on clusters:

- Use the Cluster Administrator to take the Exchange System Attendant service off-line
- Use Windows to stop IIS Admin service. If you do not stop the IIS Admin service, you will receive a pop-up message advising you to stop the service from the Checking Target System Requirements screen.

Running the Setup Program

The following section describes the process for a typical installation. Preview the process to help ensure a smooth installation.

Note: If, at any time, you click **Cancel** from the Setup program, the program will display an "Exit Setup" dialog box. When you click **Yes** from this dialog box, the installation aborts. Aborting the installation removes all files and registry changes from your operating system (except the files in the temp directory).

Step 1 Choose installation options

1. The **Welcome to Trend Micro ScanMail Setup** screen appears. Click **Next** to continue the installation.

FIGURE 2-1. Welcome screen

2. The **Select an Action** screen appears.

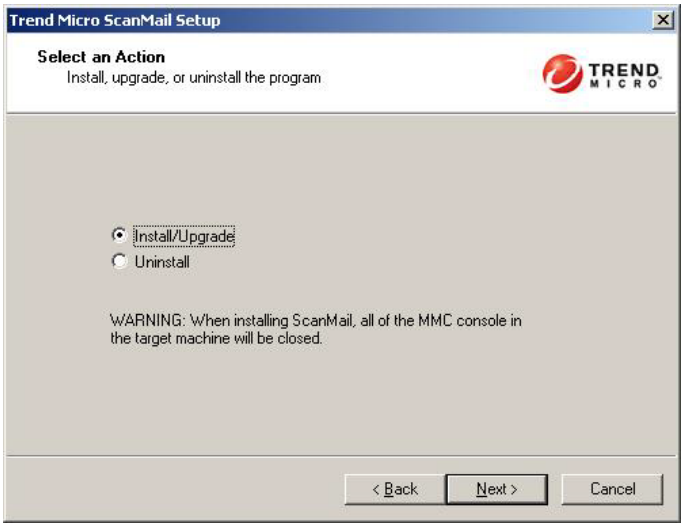

FIGURE 2-2. Select an installation action

- Select Install/Upgrade if you want to:
  - Perform a fresh install
  - Upgrade ScanMail 6.x to ScanMail 7.0. For more information about upgrading, see *Upgrading to ScanMail 7.0* starting on page 2-13.
- Select Uninstall if you want to remove ScanMail from your server. For more information about uninstalling, see *Removing ScanMail* starting on page 2-36.
- Click **Next** to continue with the installation or uninstallation.

3. The **License Agreement** screen appears.

   You must agree to the terms of the agreement to continue with the installation.

   - To agree, click **I Accept the terms in the license agreement**
   - If you do not accept the terms, click **I do not accept the terms in the license agreement.** This terminates the Setup without modifying your operating system

- Click **Next** to continue with the installation

Step 2 Activate ScanMail

The **Product Activation** screen appears.

FIGURE 2-3. Product Activation

You must enter an Activation Code to get full ScanMail protection. You must register ScanMail to receive an Activation Code. If you have not done so already, click **Register Online** to register and obtain an Activation Code. For more information about registration and activation, see *Registering and Activating ScanMail* on page 3-2.

To activate ScanMail and continue the installation:

1. Type the Activation Code in the space provided.
2. Click **Next**.

Tip: You can copy an Activation Code and paste it in the first input field of the Activation Code on this screen. The Setup program parses the entire string and populates the remaining fields for the Activation Code.

Step 3 Set up and log on to the target servers

1. The **Select Target Server(s)** screen appears.

   The Setup program can install ScanMail to a number of single servers or to all the computers in a domain. You must be using an account with the appropriate privileges to access every target server.

   Installing to clusters

   ScanMail also supports installing to all virtual servers in a cluster environment. When installing to a cluster, input a virtual server name or a node name, the install program will install all virtual servers and nodes at the same time.

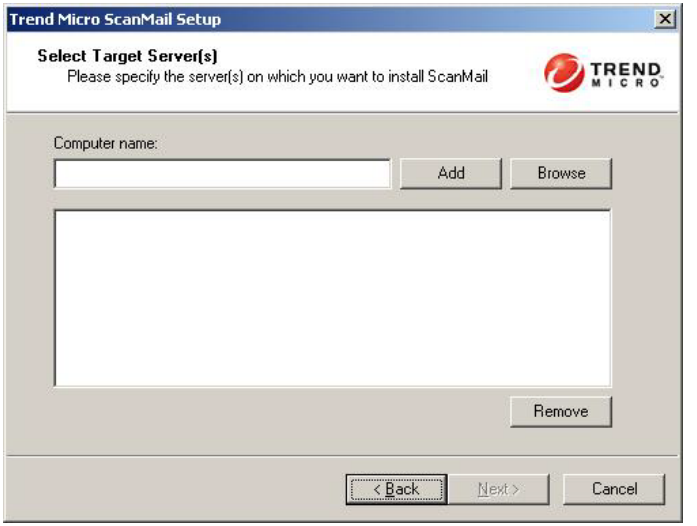

FIGURE 2-4. Add your target servers

To select a server for installation:

a. Select the computers to which you want to install ScanMail.

- Type the name of the server to which you want to install in the **Computer name** field.
- Click **Browse** and browse the computers that are available on your network, double-click on the computers you want to add to the list.

b. Click **Add** to add the computers to the list of servers to which you want to install ScanMail, or click **Remove** to remove a server from the list.

c. Click **Next** to save your list of target servers and continue the installation.

2. The **Log On** screen appears. Log on to target servers where you want to install ScanMail.

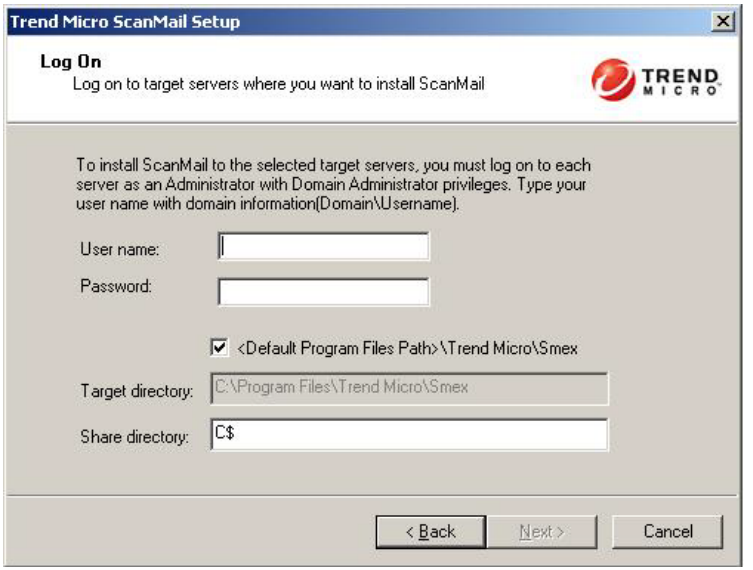

FIGURE 2-5. Log on to the servers to install ScanMail

Note: You must log on using an account with Domain Administrator privileges unless you have manually created the "SMEX Admin group" and user account for the Web management console administrator account in your domain.

- Type the user name and password to log on to the target server to install ScanMail.
- Type the directory path to where you will install ScanMail on the target server.

- Type the directory share name for which the specified user has access rights or keep the default temporary share directory, C$. The Setup program uses the share directory to copy temporary files during installation and is only accessible to the administrator.

Step 4 Select components to install and to enable

1. The **Component Selection** screen appears.

   Choose to enable or disable SMTP scanning and choose whether or not you want to install the optional EUQ component.

FIGURE 2-6. Select your component(s)

Enabling/Disabling SMTP scanning

Check the **Enable SMTP scanning** check box to enable SMTP scanning or clear the box to disable SMTP scanning. If you choose to disable SMTP scanning, you also disable all anti-spam features and prevent ScanMail from executing some actions. If you disable SMTP scanning during the installation, you can still enable it later from the Web management console.

For more information about enabling and disabling SMTP scanning, see *About Notifications* on page 7-10.

Installing/Skipping EUQ

ScanMail has two major parts: the regular ScanMail services and the optional End User Quarantine (EUQ) tool. The End User Quarantine is a tool that adds extra spam management features to ScanMail. You must install ScanMail to install EUQ, but you do not need to install EUQ when installing the core ScanMail component.

Note: To upgrade to EUQ 1.1, you must log on using a Domain Administrator account. Trend Micro recommends that you use the same account to log on that you used when you installed EUQ 1.0. If this is unsuitable, we recommend that you first remove EUQ 1.0 before upgrading to EUQ 1.1.

For more information, refer to *Managing the End User Quarantine Tool* starting on page 7-68.

Step 5 Configure the Web server and the Web management console

1. The **Select Web Server Type** screen appears. Select the IIS or Apache Web server.

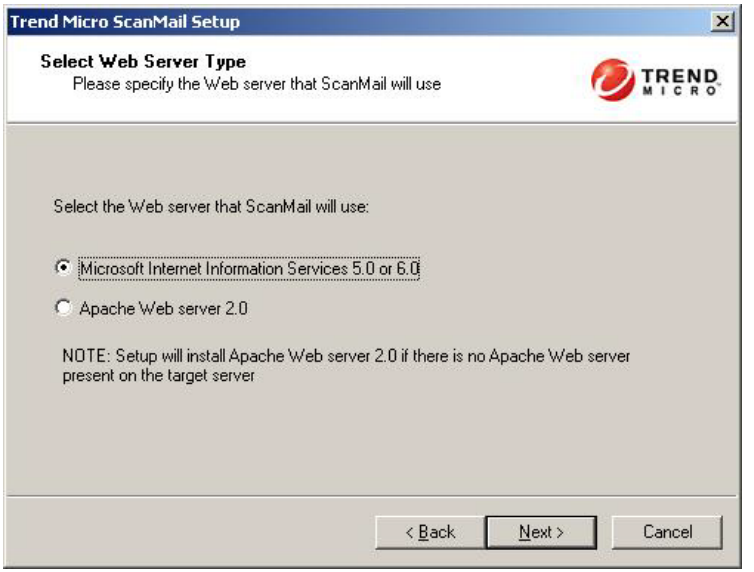

FIGURE 2-7. Select a Web server - IIS

Select one of following for ScanMail to use as a Web server, then click **Next** to proceed with the installation.

- Microsoft Internet Information Services (IIS)

  If you are using Windows 2003 Server, you require IIS 6.0. If you are using Windows 2000 Server, you require IIS 5.0.

- Apache Web server 2.0.

  If an Apache Web server version 2.0 or later is not found, the Setup program will automatically install Apache 2.0.

2. Configure your IIS or Apache Web server.

WARNING! *Trend Micro recommends that you do not use SSL in a cluster environment. If you use SSL in a cluster environment, it will cause SMTP services to be pending for a long time and finally cause SMTP resource to fail. If it is necessary to use SSL on your clusters, please extend the pending timeout of SMTP resource in each Exchange virtual server group.*

A. If you selected to install ScanMail on an IIS server:

i. Select your IIS Web:

- IIS Default Web Site – click to install as an IIS default Web site

  The default value is 80 or 443 for the SSL port.

- IIS Virtual Web Site – click to install as an IIS virtual Web site

  For virtual Web site, the default value ports are: 16372 for default listening port and 16373 for the SSL port. ScanMail uses the virtual Web site as the default for installing the Web server.

ii. You also have the option of enabling Secure Socket Layer (SSL) security. Disabled is the default value for SSL.

- Select **Enable SSL**
- Type the number of years to keep the SSL certificate valid
- Type the SSL port number

B. If you selected Apache as a Web server in the previous screen, then IIS Web options are grayed-out.

i. Type the port to use as a listening port for this server in the **Port** field. The default value ports are: 16372 for default listening port, and 16373 for the SSL port.

ii. You also have the option of enabling Secure Socket Layer (SSL) security. Disabled is the default value for SSL.

- Select **Enable SSL**
- Type the number of years to keep the SSL certificate valid (default is 3 years)
- Type the SSL port number

3. The **Web Management Console Administrator Account** screen appears. Use this screen to select whether you want to create a new administrator account or use an existing account from the Active Directory.

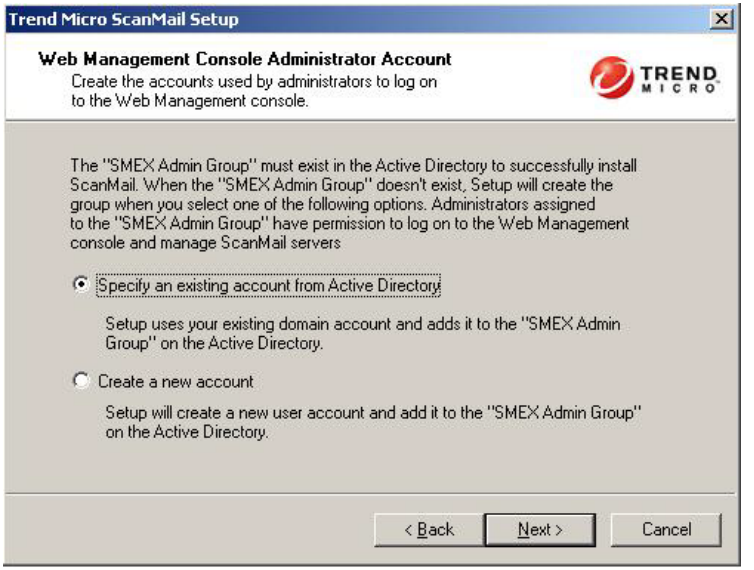

FIGURE 2-8. Web Management Console Administrator Account screen

This screen creates the log on accounts for ScanMail administrators. An administrator using an account created here can log on to the ScanMail Web management console and manage ScanMail servers. Administrators with these accounts can use the Server management tool to replicate settings from one ScanMail server to another.

You must use Windows Administrator account that has Domain Administrator privileges on the **Log On** screen to create the Web management console log on accounts. If you do not have Domain Administrator privileges, you must manually create the necessary administrative group and accounts. See *Overview of the Installation Process* on page 2-11.

- Select **Specify an existing account from Active Directory.** The Web Management Console Administration Account screen displays the username and password information.

  i. Type a username and password or accept the Trend Micro default.

  ii. Click **Next** to proceed with the installation.

  Setup creates the "SMEX Admin Group" on the Active Directory and adds your account to the group. This is the default setting for installation.

FIGURE 2-9. Specify information about an existing account

- Select **Create a new account**. The Web Management Console Administration Account screen displays the username and password information for a new account.

  i. Type a username and password or accept the Trend Micro default.

  ii. Click **Next** to proceed with the installation.

  Setup creates the "SMEX Admin Group" on the Active Directory and then creates a new domain user account and adds it to the group.

Note: Setup will not create a new "SMEX Admin Group" if one already exists on the Active Directory.

FIGURE 2-10. Create the new account

4. The **Connection Settings** screen appears.

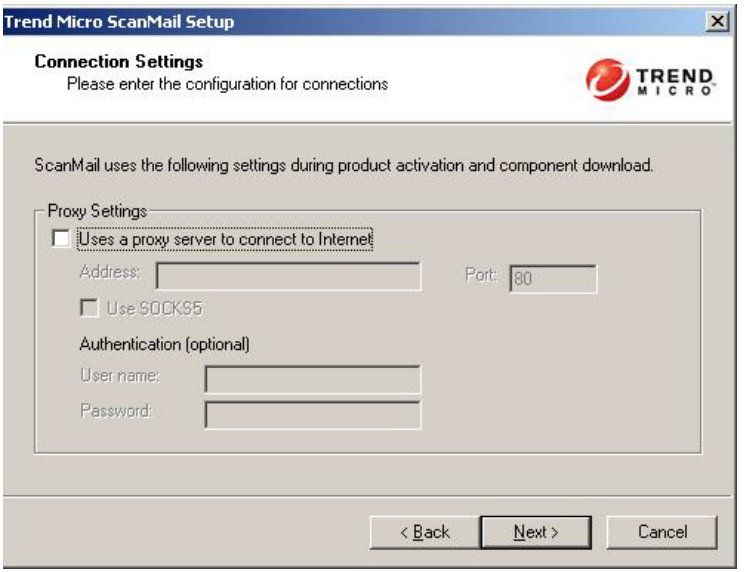

FIGURE 2-11. Connection settings screen

If a proxy server handles Internet traffic on your network, you must enter the proxy server information from this screen. By default, the proxy server is disabled.

To configure your proxy server:

a. Select **Use a proxy server to connect to Internet**

b. Type the URL address and Port number that your proxy uses

c. If you want to use SOCKS5 for secure communication behind the proxy, select **Use SOCKS5**.

d. If your proxy requires authentication, type the user name and password used for authentication.

e. Click **Next**.

Step 6 Review and complete the installation

1. The **World Virus Tracking Program** screen appears. Read the statement and click **Yes** to enroll. If you decline to participate, you can still proceed with the installation.
2. The **Checking Target System Requirements** screen appears.

   Clear the check boxes to remove installation options that you do not want to use.

   - When the settings are correct, click **Next** to proceed with the installation.
   - If the settings are not correct, you can click **Back** to go back to a previous screen in the installation.

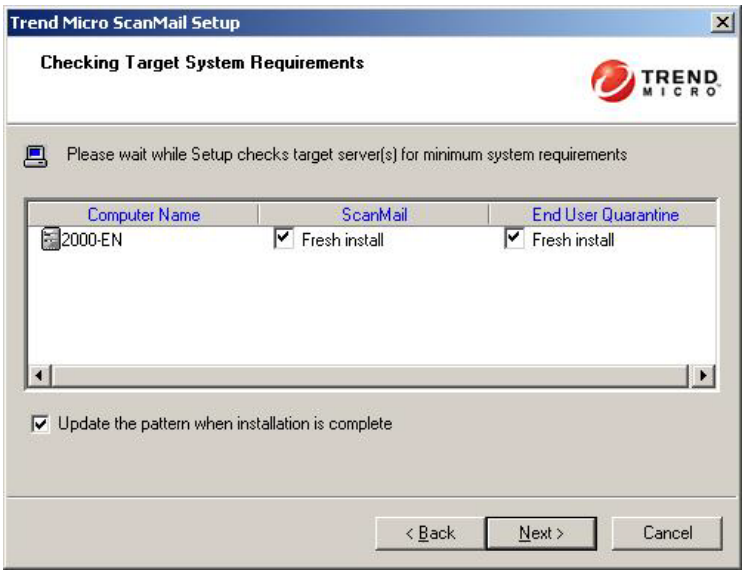

FIGURE 2-12. Checking Target System Requirements screen

Note: For cluster installation, virtual servers appear as shown in Figure 2-13.. You can double-click on the virtual server to select the share disk on which to install ScanMail data files.

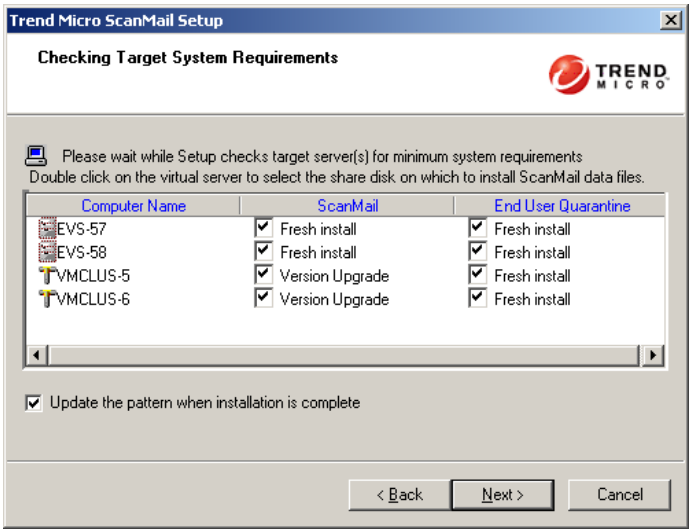

FIGURE 2-13. Checking Target System Requirements screen for Cluster Installation

3. The **Installation Progress** screen appears showing you the progress of the installation.
   - Click **View details** to display a list of each computer to which you are installing ScanMail and the status of each computer.
   - Click **Next** when the installation completes.

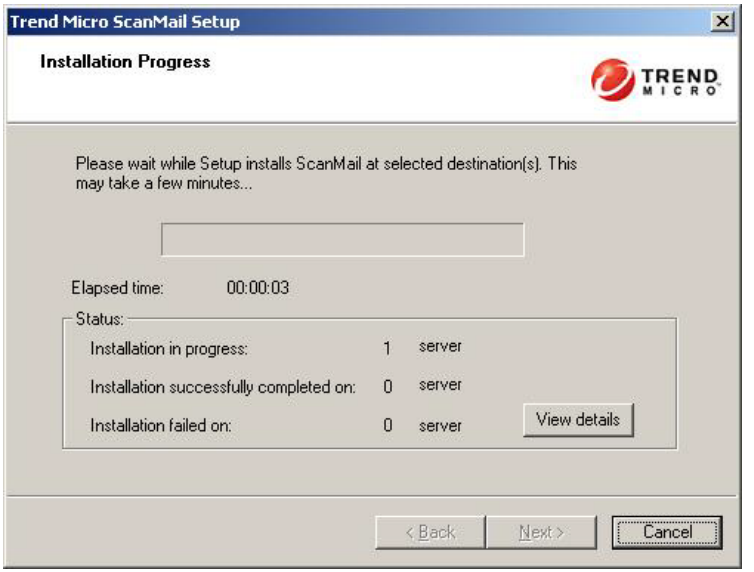

FIGURE 2-14. Installation progress screen

4. The **Installation Complete** screen appears.

   This screen informs you that the installation was successful.

   - Click the **View the Readme file** check box to open the readme file when the installation completes.
   - Click **Finish** to exit the Setup program.

Cluster installation

You can use the regular ScanMail Setup program to install ScanMail on all virtual servers on Windows 2000 or 2003 clusters. For cluster installation, you can select virtual servers just like you usually select target servers. The Setup program will install ScanMail on each node belonging to the cluster simultaneously, and add a ScanMail resource to each virtual server group.

Log on using a Windows Administrator account with Domain Admin privileges. The instructions to install ScanMail from a cluster server are nearly identical to the non-cluster installation instructions. See *Running the Setup Program* starting on page 2-17 for instructions for installing ScanMail to a cluster server environment.

If the Exchange virtual server is off-line or is not installed when installing ScanMail, the installation to the cluster will not be successful. In this case, manually create a resource on the virtual server group after the server is on-line.

For more information about manually installing a cluster server, see *Manually Creating a ScanMail Resource for Virtual Servers* on page 4-10.

Post-Installation

Set Up Spam Prevention

Trend Micro Spam Folder

If you chose to install the End User Quarantine tool during installation, then ScanMail creates a spam folder on all mailboxes on the Exchange server where you installed ScanMail. During the installation, the Setup program prompted you to name this folder and it will have the name that you entered.

After installation, you can rename the spam folder using Microsoft Outlook. Trend Micro identifies the folder by ID, not by folder name.

Spam detection levels

ScanMail also sets the spam detection level defaults. The spam detection level filters out spam messages arriving at the Exchange server. You can view the spam threshold to see ScanMail spam configuration from the **Summary > Spam** screen.

Verifying a Successful Installation

ScanMail is installed to the following directory:

```
C:\Program Files\Trend Micro\SMEX\
```

ScanMail adds the following services:

```
ScanMail for Microsoft Exchange Master Service
ScanMail for Microsoft Exchange Remote Configuration Server
ScanMail for Microsoft Exchange System Watcher
```

ScanMail adds the following keys to the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TRENDMICRO\SMEX

HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<
Server-Name>\Private-<MDB-GUID>\VirusScanEnabled

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<
Server-Name>\Private-<MDB-GUID>\VirusScanBackgroundScanningEnabled

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<
Server-Name>\Private-<MDB-GUID>\VirusScanProactiveScanningEnabled

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<
Server-Name>\Public-<MDB-GUID>\VirusScanEnabled

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<
Server-Name>\Public-<MDB-GUID>\VirusScanBackgroundScanningEnabled

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<
Server-Name>\Public-<MDB-GUID>\VirusScanProactiveScanningEnabled
```

If you installed EUQ, ScanMail adds the following key to the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TRENDMICRO\EUQ
```

Removing ScanMail

Uninstallation removes the following components:

- ScanMail Web console
- All program files
- EUQ, including end-user approved senders list
- Program folders
- Items
- Directories
- Entries made to the registry.

WARNING! *Uninstall ScanMail from the Windows Control Panel or the Uninstall program. The Setup program automatically removes many registry entries. Do not manually uninstall ScanMail.*

Removing ScanMail using the Trend Micro™ Enterprise Solution CD

1. To remove ScanMail, run setup.exe from the Trend Micro Enterprise Solution CD. Select uninstall when prompted.

Note: If, at any time, you click **Cancel** from the Setup program, the program will display an "Exit Setup" dialog box. When you click **Yes** from this dialog box, the uninstallation aborts.

2. The **Welcome to Trend Micro ScanMail Setup** screen appears. Click **Next** to continue with the uninstallation.
3. The **Select an Action** screen appears. Select **Uninstall** to remove ScanMail from your server(s).
4. The **Select Target Server(s)** screen appears.

   To uninstall ScanMail from a server:

   a. Select the computers from which you want to uninstall ScanMail:

- Type the name of the server from which you want to uninstall ScanMail in the **Computer name** field
- Click browse and browse the computers that are available on your network, double-click on the computers you want to add to the list

b. Click **Add** to add the computers to the list of servers from which you want to uninstall ScanMail or click **Remove** to remove a server from the list.

c. Click **Next** to save your list of target servers and continue the uninstallation.

5. The **Log On** screen appears. Use this screen to type the log on information for the target servers from where you will uninstall ScanMail.
6. The **Component Selection** screen appears. Select ScanMail and\or End User Quarantine to uninstall. You cannot uninstall ScanMail without uninstalling End User Quarantine.
7. The **Checking Target System Requirements** screen appears:

   View the screen and ensure the settings for the uninstallation are correct.

   - Click **Back** to change a setting,
   - Click **Next** to uninstall ScanMail from these servers.
8. The **Uninstallation Progress** screen appears. When the uninstallation is complete, click **Next** to proceed.

   Click **View details** to display the uninstallation for each individual computer.
9. The Uninstallation Complete screen appears to inform you that the servers were successfully uninstalled. Click **Finish** to exit the Setup program. The Setup program removes ScanMail from the selected servers.

Removing ScanMail Using the Windows Control Panel

You can remove ScanMail using the Windows Control Panel, but you must remove EUQ and Apache separately. Using the Setup program to uninstall ScanMail, removes all related components and programs; therefore, Trend Micro recommends using the Setup.exe program to uninstall ScanMail.

1. Go to **Start > Settings > Control Panel > Add/Remove Programs**.
2. Click **Trend Micro ScanMail for Microsoft Exchange** and then click **Remove**.
3. At the prompt, select **Yes** to remove ScanMail.
4. After uninstallation finishes, click **Close**.

Removing ScanMail from Clusters

The instructions to uninstall ScanMail from clusters is similar to the non-cluster uninstallation instructions.

See *Removing ScanMail using the Trend Micro™ Enterprise Solution CD* on page 2-36.

WARNING! *Clusters do not support uninstallation using the Add/Remove program.*

To remove ScanMail from clusters

1. If necessary, first remove End User Quarantine (EUQ).
   a. Run `setup.exe` from the Trend Micro Enterprise Solution CD and select uninstall.
   b. Follow the instructions that Setup provides. When The **Component Selection** screen appears. Choose **Uninstall EUQ** only.
   c. After the uninstalling successfully, take the Exchange System Attendant resource in each virtual server off-line and stop IIS Admin service.
2. Run `setup.exe` again and uninstall ScanMail.

   Remove ScanMail together from each cluster node belonging to the same cluster and remove the resources on each online virtual server. Remove all the changes from each Exchange virtual server accordingly.

   When uninstalling clusters you must take the Exchange System Attendant service off-line and stop IIS Admin service. If you do not stop the service, you will receive a pop-up message advising you to stop the service from the Checking Target System Requirements screen. Use the Cluster Administrator to take the System Attendant off-line and use Windows to manually stop IIS service.

Note: If users choose to uninstall EUQ and ScanMail at the same time, the uninstallation will still succeed. The only difference is that the Approved Senders list folder and client rule will be retained in the users' mailboxes. Users can delete the approve sender list manually.

Chapter 3

Activating and Updating ScanMail

This chapter explains how to register and activate ScanMail and describes the update process.

In this chapter, you will find information about:

- *Registering and Activating ScanMail* starting on page 3-2
- *Activating ScanMail* starting on page 3-4
- *Updating ScanMail* starting on page 3-5
- *Manually updating your components* starting on page 3-7
- *Setting a scheduled update* starting on page 3-8

Registering and Activating ScanMail

When you purchase ScanMail you receive a Registration Key with your product package or from your Trend Micro reseller. Registering ScanMail entitles you to standard support that consists of pattern file updates, product version upgrades, and telephone and online technical support. The length of the maintenance agreement depends on the contract you arrange with your Trend Micro representative, but is usually 12 months.

When you register, you receive an Activation Code (AC) that you can use to activate ScanMail. See *Activating ScanMail* on page 3-4.

To register your product:

Use one of the following methods to register:

- During installation

  The installation program will prompt you to use your Registration Key to register online. Follow the link to the Trend Micro Web site, register your product, and then return to the installation program to complete your installation.

- Online

  Visit the following Trend Micro Web site to register online. You receive an Activation Code to activate your product.

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

- Contact Trend Micro directly

  Provide a Trend Micro representative with your Registration Key and he or she will give you an Activation Code. Trend Micro maintains a list of contacts at:

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

For more information, see *Contacting Trend Micro* starting on page 11-2

Activation Codes

ScanMail has two types of Activation Code (AC): Standard and Suite. Both of these have two types of maintenance agreement: evaluation and full. When you register ScanMail, you receive one AC depending on whether you chose Standard or Suite and the evaluation or fully licensed version.

For example: You choose ScanMail Suite and decide to install the evaluation version. You download ScanMail Suite, register, and receive a Suite evaluation AC. When you enter the AC, ScanMail Suite evaluation service begins.

Tip: Run a pilot installation in a test environment using an Evaluation version of ScanMail. When you decide to install the fully licensed version, use the experience gained from this cost-free evaluation.

Standard AC

Using the Standard AC activates ScanMail Virus scanning and Attachment Blocking. You will receive scan engine and virus pattern file updates and be able to run scans in real time, manually, and according to schedules. ScanMail detects infected attachments and takes actions against them.

Maintenance agreement	Features
Evaluation	Using the evaluation AC allows you to implement all ScanMail functions for a limited duration. During the evaluation period, ScanMail performs Virus scanning and Attachment blocking as well as scan engine and virus pattern file updates.
Fully licensed	A fully licensed AC entitles you to standard maintenance agreement and allows you to implement all ScanMail functions except anti-spam, content filtering, and the End User Quarantine tool. ScanMail warns you when your license agreement is close to expiration.

Suite AC

Using the Suite AC activates all the functions of the ScanMail Standard AC plus activates Content Filtering, Anti-spam, and End User Quarantine functions. In addition to scan engine and virus pattern file updates, you also receive spam engine and spam pattern file updates. Content filtering screens out undesirable content from email messages arriving at the Exchange server. The spam engine and spam pattern file work to prevent the delivery of spam messages to Exchange client mailboxes.

Maintenance agreement	Features
Evaluation	Using the evaluation AC allows you to use ScanMail functions for a limited duration. During the evaluation period, ScanMail performs Virus scanning, Attachment blocking, Content Filtering, Anti-Spam, and End User Quarantine functions, as well as scan engine and virus pattern file updates.
Fully licensed	A fully licensed AC entitles you to standard maintenance agreement and allows you to implement the full functions of ScanMail. ScanMail warns you when your license agreement is close to expiration.

Activating ScanMail

The following conditions require Activation.

- Installing ScanMail for the first time

  For example, when you purchase the standard or suite version from a Trend Micro reseller and use the registration key to obtain an AC.

- Changing from an evaluation version to a full version, or changing to a Suite version from a Standard version.

  For example, when you obtain a new AC from a Trend Micro representative and want to use the Web management console to activate your new version.

Note: The evaluation version is fully functional for 30 days, after which ScanMail tasks will continue to run, but no virus scanning, message filtering, nor component update will occur.

You can activate ScanMail by one of the following methods:

To Activate ScanMail During the Installation:

1. Run the Setup program.
2. Type the AC in the Product Activation screen.
3. Complete the installation to activate ScanMail.

To Activate ScanMail After Installing Using the Web management console:

1. Click **Administration > Product License**.

2. If you have not registered ScanMail, click **view detailed info**. This opens the Trend Micro Web site which allows you to register online. Register online to get an AC.
3. From the Product License screen, click **Reactivate**.
4. Type your Activation Code in the space provided.
5. Click **Activate**.

Updating ScanMail

ScanMail installation	Activation required
Installing ScanMail for the first time.	You have purchased the standard or suite version from a Trend Micro reseller; the Registration Key is included in the product package • Register online and obtain an Activation Code to activate the product • Enter the AC during installation or when installation is complete from **Administration > Product License**.
Changing from an evaluation version to a full version, or changing to a Suite version from a Standard version.	• Contact a Trend Micro representative to receive a new AC. • Type the new AC in the Product License screen available from **Administration > Product License** screen.

Antivirus software can only be effective if it is using the latest technology. Since new viruses and other malicious code are constantly being released, it is crucial that you regularly update your ScanMail components to protect against new security threats. ScanMail components available for updating are:

- Scan engine
- Virus pattern file
- Spam engine
- Spam pattern file
- Additional threat pattern file

To find out if you have the latest components, view the ScanMail Summary screen from the Web management console. It shows your current version and lists the latest version available for download.

Before you can update ScanMail, you must complete the following tasks:

- Register your software. See *Registering and Activating ScanMail* on page 3-2.
- If a proxy server handles Internet traffic on your network, you must set the proxy server information.
- Configure your update method and source. Methods include **Manual Update** and **Scheduled Update**. Sources include the ActiveUpdate server, the Internet, and the Intranet UNC path.

Updating Components on Clusters

You must install and configure ScanMail separately for each node of a cluster. All virtual servers on a node share the same components and update source. When a virtual server from one node has a failover to another node, then ScanMail will compare the components' versions and retain the most recent one. For this reason, when you check the Summary screen for the component version after a failover, it may show a more recent update then before the failover happened.

Setting your proxy server

Most enterprises use proxy servers for added security and more efficient use of bandwidth. If your system uses a proxy server, configure the proxy settings to connect to the Internet and download updated components necessary to keep ScanMail updated and check the license status online.

The following feature use Proxy servers:

- ActiveUpdate
- Product Registration
- World Virus Tracking

To set the Internet proxy:

1. Open the ScanMail Web console.
2. On the sidebar, click **Administration** > **Proxy**. The **Proxy Settings** screen appears.
3. Select **Use a proxy server for update and product license notification**.

4. Select the proxy type.
5. Type the server name or IP address of the proxy server and its port number.
6. If your proxy server requires a password, type your user name and password in the fields provided.
7. Click **Save** to save your settings.

Manually updating your components

Trend Micro recommends manually updating your scan engine, virus pattern file, spam engine, spam pattern file, and additional threat pattern immediately after installing ScanMail or whenever there is a virus outbreak. This establishes a security baseline for your Exchange environment.

Manual updating components is a two-step process. First, select the source from where your updates download; next, select the components that you want to update. When you click **Update**, ScanMail downloads the current components from the specified source.

To manually install your components:

1. Select the component that you wish to update.
2. Click **Update**. ScanMail begins downloading the components and displays a progress bar that shows you the elapsed time and the percentage of the download remaining.

Setting a scheduled update

Configure ScanMail to regularly check the update server and automatically download any available components. During a scheduled update, ScanMail checks the user specified download source for the latest components.

Tip: During times of virus outbreaks, Trend Micro responds quickly to update virus pattern files (updates can be issued more than once each week). Trend Micro also regularly updates the scan engine and other components. Trend Micro recommends updating components daily - or even more frequently in times of virus outbreaks - to help ensure ScanMail has the most up-to-date components.

To configure Scheduled Update:

1. Click **Enable scheduled updates** to have ScanMail begin to update according to your schedule.
2. Set your schedule.
   a. Select an update frequency: by minute, hour, day, or week.
   b. Set the **Start time** for the schedule by selecting the hour and minute. Each time the update occurs, the download begins at this time.
3. Select the components that you want ScanMail to download during the scheduled update.
   a. Click the **Component** tab. All the components available for downloading appear on this page.
   b. Select the components that ScanMail downloads during each scheduled update.

   Note: When you select the check box at the top of the table, all components are selected.

4. Click **Save**. ScanMail will begin downloading the selected components according to your schedule.

Download Source

To keep ScanMail updated, you need to download the latest components. Use this page to set the source from where ScanMail receives the latest components. The default location is the Trend Micro ActiveUpdate server. During manual or scheduled downloads, ScanMail checks the location you specify here, and downloads the latest components from that source.

To set the update source, select one of the following locations:

- Trend Micro ActiveUpdate Server

  Trend Micro uploads new components to the ActiveUpdate server as soon as they are available. Select the ActiveUpdate server as a source if you require frequent and timely updates.

  For more information, see *About ActiveUpdate* starting on page 1-10

- Intranet location containing a copy of the current file

  Download components from an Intranet source that receives updated components.

  Type the Universal Naming Convention (UNC) path of another server on your network.

  Note: Setting one or more centralized Intranet locations can greatly reduce network traffic and speed update time. This option is also useful when you do not want to connect an email server directly to the Internet. Instead, you can connect a front-end server to the Trend Micro ActiveUpdate server on the Internet and then set your back-end servers to receive updates from the front-end server.

- Other update source

  Download components from an Internet or other source.

  You might choose to receive updates from a special server during testing. For example, when customers participate in Trend Micro beta testing, they type the name of the designated test server.

Duplicating the update package

Click **Duplicate the update package onto this server** to set ScanMail to create a duplicate copy of the update package on the current server. Normally, ScanMail only downloads components that the user has set it to download or the increments of the components that it needs. See *Incremental updates of the virus pattern file* on page 1-10. When you set ScanMail to duplicate the update package, it will download all the components that are available for downloading.

For example: There are two Exchange servers (a and b) and each one has ScanMail installed. ScanMail is set up to update server "a" daily and download all components. ScanMail is set to update server "b" every week and download only the spam pattern component. Both servers receive updates from the Trend Micro ActiveUpdate server as required. Therefore, the components on these servers are not always identical and they require different incremental updates when they poll the ActiveUpdate server. Another, more efficient, way to configure your servers would be to set up server "a" to duplicate the update package. Then, you could set server "a" as the source for downloads for server "b", and server "b" could receive incremental updates from server "a" just as if server "a" was the ActiveUpdate server.

Note: You must duplicate the update package to clusters. That is, this option is enabled and grayed-out so that you must reproduce the components from one virtual server across all virtual servers on that node by default.

Rolling Back a Component Update

If ScanMail has downloaded the current components, but you want to use a previous component, you can manually roll back the component update.

To manually roll back to a previous component:

1. Stop the following ScanMail services:
   - `ScanMail for Microsoft Exchange Remote Configuration Server (scanmail_RemoteConfig)`
   - `ScanMail for Microsoft Exchange Master Service (scanmail_Master)`
2. Delete all the files in:
   - `"<Install folder>\AU_Cache\"`
   - `"<Install folder>\AU_Temp\"`
   - `"<Install folder>\web\activeupdate\"`
3. Roll back the Virus pattern file and the Additional Threats pattern file.
   a. Remove the most recently downloaded pattern files from this location:
      `"<Install folder>\engine\vsapi\"`
   b. Remove the following files. Verify that ScanMail has already downloaded an older version of these files to which you can roll back.
      - The Virus pattern file:
        `ex:lpt$vpn.xxx`
      - The Additional Threats pattern file:
        `tmaptn.xxx`

      Where "xxx" refers to the latest pattern file download.

      For example: If you have recently downloaded Virus pattern file `ex:lpt$vpn.345` and you want to roll back to a previous download pattern, `ex:lpt$vpn.344`, then delete `ex:lpt$vpn.345` and ScanMail will begin to use `ex:lpt$vpn.344`.
   c. Delete all files in:
      - `"<Install folder\engine\vsapi\primary\pattern\"`
      - `"<Install folder\engine\vsapi\secondary\pattern\"`

4. To roll back Anti-spam pattern file:
   a. Remove the latest pattern in:
      - `"<Install folder>\engine\TMASE\latest\rule"`
      - `ex:tmxxxxxx.*`

      "xxxxxx" means the latest version.
   b. Delete all files in:
      - `"<Install folder>\engine\TMASE\primary\rule\"`
      - `"<Install folder>\engine\TMASE\secondary\rule\"`
5. Start the following ScanMail services again:
   - `ScanMail for Microsoft Exchange Remote Configuration Server (scanmail_RemoteConfig)`
   - `ScanMail for Microsoft Exchange Master Service (scanmail_Master)`

Chapter 4

Managing ScanMail Servers

This chapter describes how to open and use the Web management console, and how to manage your ScanMail servers.

In this chapter, you will find information about:

- *Using the Web Management Console* starting on page 4-2
- *Getting Help While Using the ScanMail Web Management Console* starting on page 4-5
- *Understanding the Real-time Monitor* starting on page 4-7
- *Understanding the Server Management Console* starting on page 4-8

Using the Web Management Console

Access and control ScanMail through the intuitive Web management console. Use the Web management console to manage multiple Exchange servers and remote servers from any computer on your network. The ScanMail Web management console is password protected, ensuring only authorized administrators can modify ScanMail settings.

Note: To access and manage the Web management console, your computer must be running a Java-enabled Web browser that supports frames, such as Internet Explorer 5.5 with SP3.

Management console main view

The ScanMail management console has an intuitive user interface that provides easy access to all the functions you need to configure and manage ScanMail.

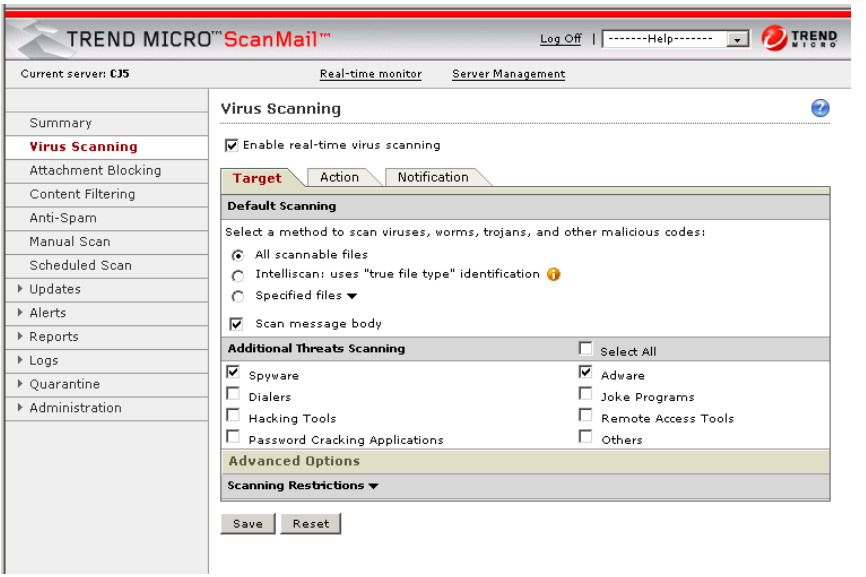

FIGURE 4-1. The Web management console

The Web management console elements

Banner

The banner identifies and describes the product and provides access to Trend Micro support

FIGURE 4-2. Web management console banner

The banner displays the following:

- **Current server**—the server you manage from this console
- **Real-time monitor**—click to access the real-time monitor

  For more information, see *Understanding the Real-time Monitor* on page 4-7.
- **Server Management** console—click to access the Server Management console.

  For more information, see *Understanding the Server Management Console* on page 4-8.
- **Log Off**—click this to end your session and close the Web management console. Logging off the Web console prevents unauthorized users from modifying the settings.
- **Help**—get support by selecting an option from the drop-down list

  Help options include:

  - **Contents and Index**—open the online help table of contents and index
  - **Knowledge base**—access Knowledge base to get the most up-to-date information about product troubleshooting and frequently asked questions
  - **Security Info**—visit the Trend Micro Security Information page to read about the latest virus threats
  - **Sales**—view the Trend Micro Web page to find resellers and service providers in your area
  - **Support**—access technical support
  - **About**—view ScanMail and component version numbers and ScanMail system information

Sidebar — provides access to the main menu items for ScanMail

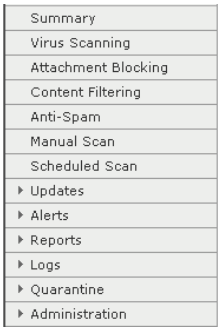

FIGURE 4-3. Web management console sidebar

Configuration area — this is the working area where you set and modify all ScanMail configurations and options

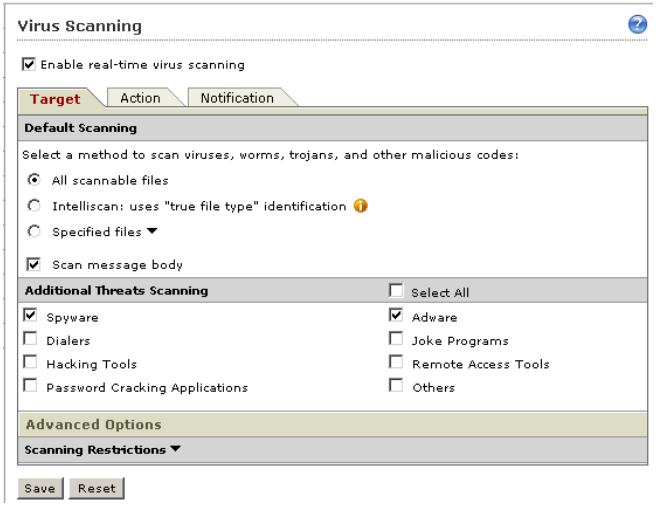

FIGURE 4-4. Web management console configuration area

Getting Help While Using the ScanMail Web Management Console

ScanMail offers the following types of help:

- To get help on using ScanMail features, read the context-sensitive help. Access context-sensitive help by clicking on help icon ( ) or open the Table of Contents by selecting **Contents and Index** from the **Help** drop list in the banner area.
- To access troubleshooting and FAQ information, select **Knowledge Base** from the drop list in the banner area.
- To Access general information about computer security threats and virus alerts, select **Security Info** from the drop list in the banner area.
- To get information about how to contact Trend Micro sales representatives or service providers, select **Sales** from the drop list in the banner area.

Viewing Servers from the Web Management Console

You can administer one server at a time using the ScanMail Web management console.

To view the Web management console for a local server

1. Click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **ScanMail Management Console**.
2. Enter your **User name** and **Password** and click **Enter**.

Note: Use a Windows Administrator account or an account under "SMEX Admin Group" to log on.

To view the Web management console from a remote server:

Use Internet Explorer and access one of the following:

```
http://<servername>:<portnumber>/smex
```

```
https://<servername>:<portnumber>/smex
```

Where "servername" is the name of the server on which you installed ScanMail and "port number" is the port number you use to access that computer.

Note: By default HTTP uses port 16372 and HTTPS uses port 16373.

Viewing Virtual Servers on a Cluster

Each Exchange virtual server is an independent management unit and must have its own configuration and log storage, no matter how many virtual servers are on one single cluster node. The Web management console should use the network name/IP address associated with the specified Exchange virtual server to control ScanMail operations on that server.

Note: At times components might appear out of date when viewing servers through the Server Management console. This is caused by a synchronization delay between the Web management console and the Server Management console. Wait a few moments and the component version will refresh.

Understanding the Real-time Monitor

The Real-time Monitor displays information about one Exchange server in real time. It shows ScanMail scanning incoming and outgoing messages as they arrive. It also gives the current count of detected viruses and spam on the server.

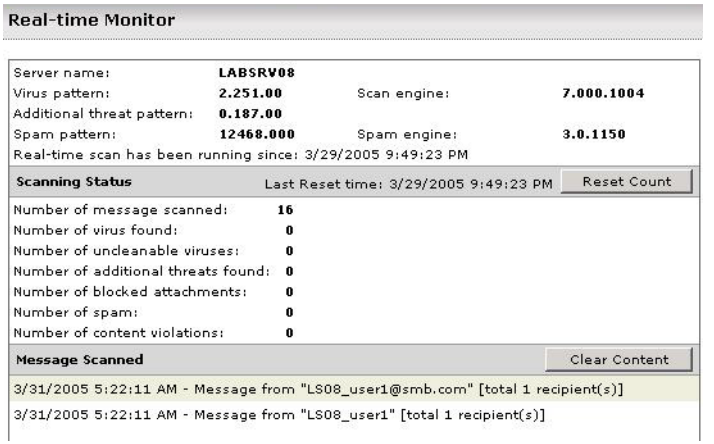

FIGURE 4-5. The Real-time monitor

You can use the Real-time monitor to monitor your local server, or any server connected to your network. This is a useful method of managing your ScanMail servers from a centralized location.

To view the Real-time monitor for a remote server:

1. Access the remote server using the Web management console.
2. Click **Real-time monitor**. The Real-time monitor screen opens displaying information about the remote servers.

Understanding the Server Management Console

The ScanMail Server Management console enables you to view all of the ScanMail servers on a network.

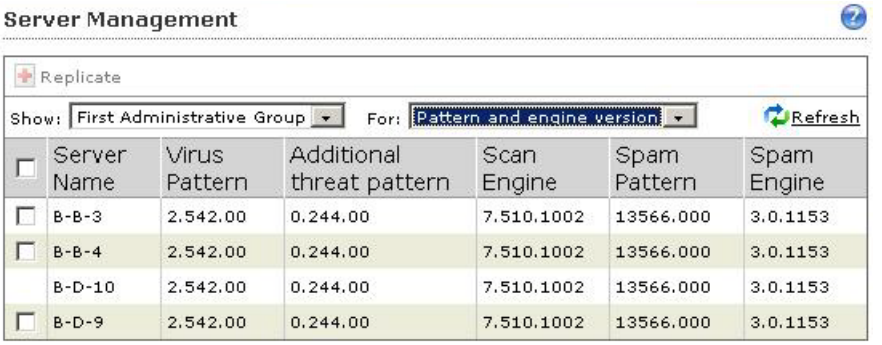

FIGURE 4-6. The Server Management console

You can use the following features from the Server Management console:

Feature	Description
Pattern and engine version	View information about the current scan engine, virus pattern file, spam engine, and spam pattern file.
Scanning result	View information about the total messages scanned and the scan results. Scanning results also shows the number of blocked attachments, spam, and content violations.
Scanning status	View whether or not ScanMail features are enabled. Check Virus scanning, Attachment Blocking, Anti-Spam, and Content Filtering.
Last replication	View the status of the last replication and the duration of the last replication.

TABLE 4-1. Server Management console features

Using Server Management to Replicate Configurations

You can use Server Management to replicate any or all of your configurations from one ScanMail server to another. Replicating servers in this way is much faster and easier than configuring each server separately. In addition, it ensures that all ScanMail servers - or group of servers - that provide the same kind of protection share the same configuration.

To replicate the settings from a server to one or more target server(s):

1. Click **Server Management** to open the Server Management screen.
2. Select target servers.
3. Click **Replicate**. The Replication settings screen appears.
4. Select the settings that you want to replicate:
   - Click **All settings** to replicate all the configurations to the target server(s)
   - Click **Specified settings** to set each configuration that you want to replicate individually

   Note: The server on which you are currently logged on is the source for the replication.

5. Select the check box to overwrite server-dependent settings. When this check box is selected, ScanMail can copy directory paths that you have set for such folders as the quarantine, backup, and archive folders.
6. Click **Deploy**. A screen appears showing a progress bar and the ongoing status of the replication.

Manually Creating a ScanMail Resource for Virtual Servers

During installation you can install ScanMail to virtual servers on clusters. However, once the installation is complete, you cannot run the setup program again to install ScanMail on more servers. This is because ScanMail does not support the same build upgrade in a cluster environment. If you want to add virtual servers to a cluster after installation and have ScanMail protect that server, then you must first manually create a ScanMail resource for the new virtual servers to use.

To create a ScanMail resource for a virtual server:

1. Create a ScanMail resource on the server group for the target's virtual server. The new resource will have a dependency on the following resource types: **Disk**, **Network Name**, and **Information Store**. ScanMail puts data on the disk created for your **Disk** resource. Do not move or modify the data on the disk.
2. Uncheck **Affect the group** in the SMEX resource properties. Right click the **SMEX resource > properties > Advanced > Uncheck** and clear the **Affect the group** checkbox.
3. Create a virtual directory for viewing reports about the target server on each node where a virtual server is installed. Before doing this step, ensure that the target virtual server is on the current node. Depending on your installation options, you can create the virtual directory using Internet Information Services (IIS) or Apache.
   - Using IIS Web server to create the virtual directory:
     i. To open IIS click the following path:

        `<computername> > SMEX Web Site > SMEX > virtual directory`

        Where <computername> is the name of the local computer.

     ii. Create the virtual directory. Type the directory path as follows:

        `<ShareDisk on the target server>:\SMEX\data\report`

        For example: G:\SMEX\data\report
   - Using Apache Web server to create the virtual directory:
     i. To open `Httpd.conf`, click the following path from the **Start** menu:

        `Programs > Apache HTTP Server 2.0.52 > Configure Apache Server > Edit the Apache Httpd.conf Configuration File.`

     ii. Find the following text string:

        `# SMEX Virtual Path -- Start`

iii. Type the following:

```
Alias /smex/<report directory name>/ "<ShareDisk
Label>:/SMEX/data/report/"
<DirectoryMatch "^[<ShareDisk Label>]:/SMEX/data/report">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</DirectoryMatch>
```

For example:

```
Alias /smex/report-ZERO1/ "F:/SMEX/data/report/"
<DirectoryMatch "^[F]:/SMEX/data/report">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
</DirectoryMatch>
```

iv. When using SSL, find the following text string:

```
# SMEX SSL -- Start
```

Type the following in the area provided for virtual servers:

```
Alias /smex/<report directory name>/ "<ShareDisk
Label>:/Smex_1300/data/report/"
        <Directory "<ShareDisk Label>:/Smex/data/report">
                Options None
                AllowOverride None
                Order allow,deny
                Allow from all
        </Directory>
```

v. Restart the Apache server from the **Start** menu.

4. Create an account and mailbox for End User Quarantine functions as follows:

```
EUQ_<Virtual Server Name>
```

For example:

```
EUQ_VirtualServer1
```

Chapter 5

Understanding Threats to an Exchange Environment

ScanMail stops the spread and acquisition of viruses, Trojans, worms, spyware and other grayware in an Exchange environment.

In this chapter, you will find information about:

- *What do the terms mean?* starting on page 5-2
- *How Can these Things Affect the Exchange Environment?* on page 5-9
- *How ScanMail Protects the Exchange Environment* starting on page 5-10

What do the terms mean?

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a discussion of these terms and their meanings as used in this document.

Some of these terms refer to real security risks and some refer to relatively harmless, but annoying or unsolicited incidents. Trojans, viruses, and worms are examples of terms used to describe real security risks. Joke programs, Spyware and other grayware are terms used to describe incidents that might be harmful, but are sometimes simply annoying and unsolicited. ScanMail can protect Exchange servers against all of the incidents described in this chapter.

Viruses

A computer virus is a segment of code that has the ability to replicate. Viruses usually replicate by infecting files. When a virus infects a file, it attaches a copy of itself to the file in such a way that when the former executes, the virus also runs. When this happens, the infected file also becomes capable of infecting other files. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

Generally, there are three kinds of viruses:

- File

  File viruses may come in different types– there are DOS viruses, Windows viruses, macro viruses, and script viruses. All of these share the same characteristics of viruses except that they infect different types of host files or programs.

- Boot

  Boot viruses infect the partition table of hard disks and boot sector of hard disks and floppy disks.

- Script

  Script viruses are viruses written in script programming languages, such as Visual Basic Script and JavaScript and are usually embedded in HTML documents.

  VBScript (Visual Basic Script) and Jscript (JavaScript) viruses make use of Microsoft's Windows Scripting Host to activate themselves and infect other files. Since Windows Scripting Host is available on Windows 98, Windows 2000 and other Windows operating systems, the viruses can be activated simply by double-clicking a `*.vbs` or `*.js` file from Windows Explorer.

  What is so special about script viruses? Unlike programming binary viruses, which require assembly-type programming knowledge, virus authors programs script viruses as text. A script virus can achieve functionality without low-level programming and with code as compact as possible. It can also use predefined objects in Windows to make accessing many parts of the infected system easier (for example, for file infection, for mass-mailing). Furthermore, since the code is text, it is easy for others to read and imitate the coding paradigm. Because of this, many script viruses have several modified variants.

  For example, shortly after the “I love you” virus appeared, antivirus vendors found modified copies of the original code, which spread themselves with different subject lines, or message bodies.

Whatever their type is, the basic mechanism remains the same. A virus contains code that explicitly copies itself. In the case of file viruses, this usually entails making modifications to gain control when a user accidentally executes the infected program. After the virus code has finished execution, in most cases, it passes back the control to the original host program to give the user an impression that nothing is wrong with the infected file.

Take note that there are also cross-platform viruses. These types of viruses can infect files belonging to different platforms (for example, Windows and Linux). However, such viruses are very rare and seldom achieve 100% functionality.

Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. Unlike viruses, worms do not need to attach themselves to host programs. Worms often use email and applications, such as Microsoft™ Outlook™, to propagate. They may also drop copies of themselves into shared folders or utilize file-sharing systems, such as Kazaa, under the assumption that users will likely download them, thus letting the worm propagate. In some cases, worms use chat applications such as ICQ, AIM, mIRC, or other Peer-to-Peer (P2P) programs to spread copies of themselves.

Trojan horse programs

A Trojan horse programs, or Trojans, are programs that come concealed in software that appears harmless. Trojans are non-replicating – unlike viruses they do not replicate by themselves – and they rely on the user to send out copies of the Trojan to others. They sometimes achieve this by hiding inside desirable software (that is, computer games or graphics software), which novice users often forward to other users. There may be instances when a Trojan does not have a destructive payload. However, it may contain routines that can compromise the security of your system or the entire network.

Joke Programs

A Joke program is an ordinary executable program with normally no malicious intent. Virus authors create joke programs for making fun of computer users. They do not intend to destroy data but some inexperienced users may inadvertently perform actions that can lead to data loss (such as restoring files from an older backup, formatting the drive, or deleting files).

Since joke programs are ordinary executable programs, they will not infect other programs, nor will they do any damage to the computer system or its data. Sometimes, joke programs may temporarily reconfigure the mouse, keyboard, or other devices. However, after a joke program finishes its execution or the user reboots the machine, the computer returns to its original state. Joke programs, while normally harmless, can be costly to an organization.

About Mass-Mailing Attacks

Email-aware viruses, like the infamous Melissa, Loveletter, AnnaKournikova and others, have the ability to spread via email by automating the infected computer's email client. Mass-mailing behavior describes a situation when an infection spreads rapidly between clients and servers in an Exchange environment. Mass-mailing attacks can be expensive to clean up and cause panic among users. Trend Micro designed the scan engine to detect behaviors that mass-mailing attacks usually demonstrate. The behaviors are recorded in the Virus Pattern file that is updated using the Trend Labs™ ActiveUpdate Servers.

You can enable ScanMail to take a special action against mass-mailing attacks whenever it detects a mass-mailing behavior. The action set for mass-mailing behavior takes precedence over all other actions. The default action against mass-mailing attacks is *delete*.

For example: You configure ScanMail to quarantine messages when it detects a worm or a Trojan in an email message. You also enable mass-mailing behavior and set ScanMail to delete all messages that demonstrate mass-mailing behavior. ScanMail receives a message containing a worm such as a variant of MyDoom. This worm uses its own SMTP engine to send itself to email addresses that it collects from the infected computer. When ScanMail detects the MyDoom worm and recognizes its mass-mailing behavior, it will delete the email message containing the worm - as opposed to the quarantine action for worms that do not show mass-mailing behavior.

About Compressed Files

Compression and archiving are among the most common methods of file storage, especially for file transfers - such as email attachments, FTP, and HTTP. Before any virus detection can occur on a compressed file, however, you must first decompress it. Recognizing the fundamental importance of decompression in the detection of viruses, Trend Micro is committed to supporting all major decompression routines, present and future. For other compression file types, ScanMail performs scan actions on the whole compressed file, rather than individual files within the compressed file.

ScanMail currently supports the following compression types:

- Extraction–used when multiple files have been compressed or archived into a single file: PKZIP, LHA, LZH, ARJ, MIME, MSCF, TAR, GZIP, BZIP2, RAR, and ACE.

- Expansion–used when only a single file has been compressed or archived into a single file: PKLITE, PKLITE32, LZEXE, DIET, ASPACK, UPX, MSCOMP, LZW, MACBIN, and Petite.
- Decoding–used when a file has been converted from binary to ASCII, a method that is widely employed by email systems: UUCODE and BINHEX.

Note: When ScanMail does not support the compression type, then it cannot detect viruses in compression layers beyond the first compression layer. For more information about compression layers, see Figure 7-2.

When ScanMail encounters a compressed file it does the following:

1. ScanMail extracts the compressed files and scans them.

   ScanMail begins by extracting the first compression layer. After extracting the first layer, ScanMail proceeds to the second layer and so on until it has scanned all of the compression layers that the user configured it to scan up to a maximum of 20.

2. ScanMail performs a user-configured action on infected files.

   ScanMail performs the same action against infected files detected in compressed formats as for other infected files. For example, if you configure the action for infected files to be *quarantine*, then ScanMail quarantines messages in which it detects infected files.

   ScanMail can clean files from two types of compression routines: PKZIP and LHA. However, ScanMail can only clean the first layer of files compressed using these compression routines.

About Macro viruses

Macro viruses are application-specific. They infect macro utilities that accompany such applications as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications such as .doc, .xls, and .ppt. Macro viruses travel between data files in the application and can eventually infect hundreds of files if undeterred.

As these file types are often attached to email messages, macro viruses spread readily by means of the Internet in email attachments.

How ScanMail prevents macro viruses from infecting your Exchange server:

- Detects malicious macro code using heuristic scanning

  Heuristic scanning is an evaluative method of detecting viruses. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature
- Blocks attachment files commonly attacked by macro viruses and *quarantines*, *blocks*, or *deletes*

Spyware and other Grayware

Your clients are at risk from potential threats other than viruses. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization.

Types of grayware

ScanMail can detect several types of grayware, including the following:

Spyware: gathers data, such as account user names and passwords, and transmits them to third parties.

Adware: displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser.

Dialers: changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem.

Joke Programs: causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.

Hacking Tools: helps hackers enter computers.

Remote Access Tools: help hackers remotely access and control computers.

Password Cracking Applications: helps hackers decipher account user names and passwords.

Potential risks and threats

The existence of spyware and other types of grayware on your network have the potential to introduce the following:

- **Reduced computer performance:** to perform their tasks, spyware/grayware applications often require significant CPU and system memory resources
- **Increased Web browser-related crashes:** certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.
- **Reduced user efficiency:** by needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users can be unnecessarily distracted from their main tasks
- **Degradation of network bandwidth:** spyware/grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network
- **Loss of personal and corporate information:** not all data that spyware/grayware applications collect is as innocuous as a list of Web sites users visit. Spyware/grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network.
- **Higher risk of legal liability:** if hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties.

How Can these Things Affect the Exchange Environment?

Microsoft Exchange's architecture makes it possible to share information among users regardless of their physical location. However, this architecture also provides an environment where viruses, Trojans, worms, spyware and other grayware thrive and persist. With the capabilities of Microsoft Exchange 2003, there is a greater opportunity for virus infections and other malicious code to enter the Information Store.

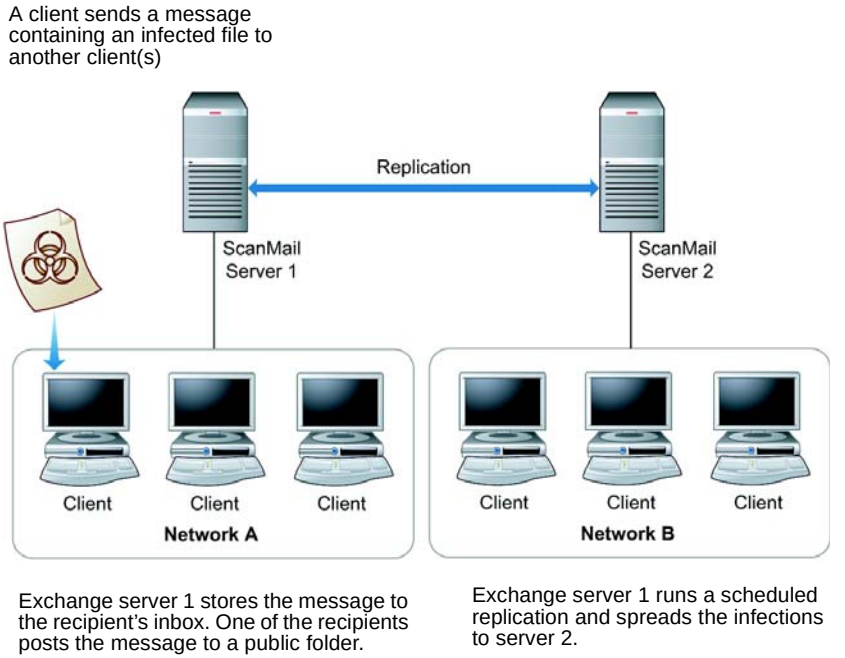

FIGURE 5-1. Infection spreading in an Exchange environment

How ScanMail Protects the Exchange Environment

Trend Micro recognizes the unique dangers posed by viruses and other malware to Microsoft Exchange servers. It designed ScanMail to protect Exchange from these numerous and diverse security threats.

ScanMail uses the Trend Micro scan engine and spam engine to detect viruses and other security threats and to screen out spam messages. These two engines rely on the most up-to-date pattern files supplied by TrendLabs and delivered through ActiveUpdate servers or a user-configured update source.

ScanMail uses filtering strategy to protect Exchange. When messages arrive at the Exchange server, ScanMail subjects each email message to a number of filters. Each filter checks the email messages for security threats and unwanted content. ScanMail filters screen out email messages that contain viruses, Trojans, worms, spyware and other grayware.

- Anti-spam

  ScanMail screens each email message for spam before delivering them to the Information Store.

- Content filtering

  ScanMail filters incoming and outgoing email messages and screens out unwanted content.

- Attachment blocking

  ScanMail can block attachments according to user-defined attachment types or by specific names.

- Virus scanning

  Virus scanning detects viruses, worms, Trojans, and other additional threats. ScanMail can also detect and take action against spyware and other grayware.

For a more detailed explanation, see *ScanMail filtering strategy* on page 7-5.

Chapter 6

Establishing and Maintaining Security for your Exchange Servers

ScanMail was designed to provide comprehensive security for your complete Exchange environment. The following information gives an overview of the major features of ScanMail and describes how to quickly establish and maintain a security baseline.

In this chapter you will find information about:

- *Establishing a Security Baseline* starting on page 6-2
- *Maintaining Security* starting on page 6-3
- *Managing Outbreak Situations* starting on page 6-5
- *Updating ScanMail* starting on page 6-4

Establishing a Security Baseline

When you have registered and activated ScanMail, you are ready to configure ScanMail features. Trend Micro recommends the following steps to establish a security baseline for your Exchange servers.

1. Update ScanMail.

   Trend Micro released ScanMail for Microsoft Exchange in July, 2005. When ScanMail is released it contains a scan engine, virus pattern file, spam engine, and spam pattern file that was available at the time. However, Trend Micro continuously updates their pattern files and engines. Update these components immediately following installation to gain optimal protection for ScanMail.

   Refer to *Updating ScanMail* starting on page 6-4.

2. Verify that ScanMail is running and functioning correctly.

   From the Web management console, click **Real-time monitor**. The Real-time monitor page opens and shows ScanMail activities in real time. When you can read **Real-time scan has been running since**, then you know ScanMail is running.

3. Perform a manual scan of your entire Information Store.

   Trend Micro recommends you perform a manual scan of your entire Information Store following installation. When ScanMail detects viruses or other malicious code it takes action against them according to Trend Micro defaults. The Trend Micro default action for viruses is *clean*, or *quarantine* when it is unable to *clean*.

   See *Running Manual Scans* on page 7-29

When the manual scan is complete, you have established a security baseline for your Exchange environment and you can start to focus on maintaining a secure environment.

Note: As soon as you have finished installing and activating ScanMail, it begins to protect your Exchange servers. ScanMail uses Trend Micro default values to filter undesirable content, block potentially harmful attachments and scan for viruses and other security threats in real time. When you are ready, customize ScanMail configurations to gain the optimal protection and efficiency.

Maintaining Security

To maintain security on your Exchange servers, Trend Micro recommends the following:

1. To ensure that ScanMail is always up-to-date, regularly update your scan engine, virus pattern file, spam engine, spam pattern file, and additional threat pattern file. To facilitate this, ScanMail allows you to configure scheduled updates. Scheduled updates check the Trend Micro update server according to the schedule you set and automatically download any available components.

   Refer to *Setting a scheduled update* starting on page 3-8.

2. Viruses and other security threats can attack your Exchange servers from unexpected sources such as local unprotected computers and servers or by bypassing too lenient configurations. Run regular scheduled scans to significantly reduce this risk.

   See *Managing Scheduled Scans* on page 7-30.

3. Select **Enable action on Mass-mailing behavior** from the Virus Scanning page to provide early warning of virus outbreaks.

   See *About Mass-Mailing Attacks* on page 5-5 for more information.

4. When an attack occurs, it is vital that administrators receive early warning to prevent the attack from spreading. Trend Micro recommends setting ScanMail to send alerts to key network security professionals when outbreak conditions threaten your network. You can use Outbreak Alert to set ScanMail to automatically notify designated individuals.

   See *Configuring Outbreak Alerts* on page 8-6.

5. Consider your overall network security. ScanMail for Microsoft Exchange is designed to guard your Exchange mail servers. ScanMail does not provide protection to non-Exchange mail servers, file servers, desktops, or gateway devices. ScanMail protection is enhanced when used together with other Trend Micro products such as Trend Micro OfficeScan™ to protect your file servers and desktops, and Trend Micro InterScan VirusWall™ or InterScan™ Messaging Security Suite to protect your network perimeter.

   Visit the Trend Micro Web site for a more comprehensive list of solutions for all your network security needs.

   `http://www.trendmicro.com/en/products/global/enterprise.htm`

6. File-based antivirus software usually allows you to set up folders to exclude from scanning. Trend Micro recommends setting up the following folders to exclude from scanning when using ScanMail with other antivirus software:
   - SMEX/storage/quarantine
   - SMEX/storage/backup folder
   - SMEX/storage/archive
   - SMEX/temp
   - SMEX/debug

   Note: These directory names are the names that ScanMail uses by default when it installs.

Updating ScanMail

Antivirus software can only be effective if it is using the latest technology. Since new viruses and other malicious code are constantly being released, it is crucial that you regularly update your ScanMail components to protect against new security threats. ScanMail components available for updating are: scan engine, virus pattern file, spam engine, spam pattern file, and additional threat pattern file.

Before you can update ScanMail, you must complete the following tasks:

- Register your software. See *Registering and Activating ScanMail* on page 3-2.
- If a proxy server handles Internet traffic on your network, you must set the proxy server information. See *Setting your proxy server* on page 3-6
- Configure your update method and source. Methods include **Manual Update** and **Scheduled Update**. Sources include the ActiveUpdate server, the Internet, and the Intranet UNC path. See *Manually updating your components* on page 3-7 and *Setting a scheduled update* on page 3-8.

Managing Outbreak Situations

Virus outbreaks happen when viruses, Trojans, worms, or other spyware/grayware suddenly attack many Exchange servers or personal computers on your network. There are many reasons why an attack might occur such as out-of-date components, poor configuration of anti-virus software, or a new malware arising for which there is not yet a pattern file. Outbreaks are a critical time when administrators must endure a chaotic, time-consuming process of communication—often to global and decentralized groups within their organizations.

The actions that administrators take when outbreaks happen, can be broken down into four general stages:

1. Confirming the security incidence is a legitimate problem and not a false alarm
2. Responding to the security incidence
3. Analyzing the security incidence
4. Recovering the Exchange servers and mailboxes

ScanMail has some very useful features that can assist administrators in every stage of an outbreak. Consider the following features when an outbreak threatens:

1. To confirm that the security incident is truly a malware outbreak:
   - Check the Trend Micro Web site for virus alerts and the latest security advisory information.

     `http://www.trendmicro.com/vinfo/`
   - Check ScanMail notifications. ScanMail can be set to automatically send alerts when outbreak conditions exist. In addition, ScanMail can be set to notify administrators or other designated individuals when ScanMail takes actions against detected threats.

     See *Setting Notifications* on page 8-2 for more information about ScanMail notifications.
   - For a quick analysis of the security incident, view the ScanMail Summary screen or create a one-time report. For more detailed information about the security incident, query the logs.

     See *Generating, Viewing, and Sending Reports* on page 9-4 for more information about reports.

2. Responding
   - Use the manual update to immediately download the latest ScanMail components.

     Refer to *Updating ScanMail* starting on page 6-4.
   - Follow-up the update with a manual scan of the entire information store. Use the Trend Micro recommended defaults such as IntelliScan and ActiveAction or set even more aggressive scanning filters. If you know exactly what you are scanning for, select **Specified files** from the Virus Scanning screen and type the name of the file for ScanMail to detect.

     See *Running Manual Scans* on page 7-29
3. Analyzing
   - Perform a Log Query to discover information about the attack. The log contains such useful information as the time and date, sender and receiver, and infected attachment names. See *Setting up and running log queries* on page 9-6.
   - If you need some assistance to help analyze the security problem, send your virus case to the Trend Micro Virus Response Service.

     `https://premium.trendmicro.com/virusresponse/en/us/VRS/logon/logon.asp`
   - If you need more assistance, contact Trend Micro support. See *Contacting Technical Support* on page 11-2.
4. Recovering
   - When you have restored your Exchange environment, consider changing your configurations and security policies. Consider the following points:
     - Set ScanMail to backup files before taking action and then set very aggressive configurations. This allows ScanMail to detect and eliminate many threats without taking irreversible actions.
     - Monitor the results using the real-time monitor or by generating logs and reports.
     - Use the Server Management tool to quickly and easily replicate configurations from one secure and tested ScanMail server to another.

Chapter 7

Configuring and Performing ScanMail Tasks

This chapter explains how to configure ScanMail to protect your Exchange environment.

This chapter contains the following topics:

- *About ScanMail Configurations* starting on page 7-2
- *About Virus Scanning* starting on page 7-5
- *Running Manual Scans* starting on page 7-29
- *Managing Scheduled Scans* starting on page 7-30
- *About Blocking Attachments* starting on page 7-33
- *Filtering Undesirable Content* starting on page 7-37
- *Screening Out Spam* starting on page 7-62
- *Setting Up and Managing the Quarantine Folder* starting on page 7-69

About ScanMail Configurations

Configuring ScanMail for optimal performance can be a challenging task. There are many factors to consider. Fortunately, Trend Micro designed default values to assist you with configuration. For a simple and secure configuration, install ScanMail and accept all default values, then monitor the results and adjust as needed.

Optimizing your ScanMail configurations

Trend Micro recommends the following guidelines to help you optimize your ScanMail configurations:

- Test your configurations

  Set up and test your configurations in a test environment before deploying to a live environment. When you are confident that your settings are suitable to your environment, replicate your configurations using Server Management.

- Set more aggressive scans at first

  After running aggressive scans for a while, check your log information to give you insights into which files are being filtered and for what reasons. Based on this information, customize your scans and scan actions to only filter those attacks that are a problem for your environment.

- Backup or quarantine suspect files before taking irreversible action

  After running ScanMail with these configurations, examine the quarantine and backup folders to see what types of files it is detecting. You can resend unnecessarily quarantined messages. Fine-tune your configurations appropriately.

Trend Micro default actions

Consider the actions listed in Table 7-1 to help you optimize your ScanMail actions. The default value appears in bold. In some cases, when the first action is unsuccessful, ScanMail automatically performs a secondary action.

TABLE 7-1. Trend Micro default actions for ScanMail

Scan option	Real-time scan	Manual scan	Scheduled scan
Anti-spam			
Action	• **Tag and deliver** • Quarantine to user's spam folder (default, if EUQ installed) • Delete entire message	Not supported	Not supported
Content filtering			
Filter message that match any condition defined	• **Quarantine entire message** • Replace with text/file • Delete • Archive	Replace	Replace
Filter message that match all conditions defined	• **Quarantine entire message** • Delete entire message • Archive • Pass	Not available	Not available
Monitor the message content of particular email account(s)	• **Quarantine entire message** • Delete entire message • Archive	Replace	Replace
Create exemption for particular email account(s)	• Pass	Pass	Pass
Attachment blocking			
Action	• **Replace attachment with text/file** • Delete entire message • Quarantine	Replace attachment with text/file	Replace attachment with text/file

Scan option	Real-time scan	Manual scan	Scheduled scan
Virus Scanning			
Scanning for email message body and attachment	Primary action: • **Clean** • Delete entire message • Quarantine entire message • Replace with text/file • Pass Secondary Action (when clean is unsuccessful): • **Quarantine entire message** • Delete entire message • Replace with text/file • Pass	• Primary action: • **Clean** • Replace with text/file • Pass • • Secondary Action (when clean is unsuccessful): • **Replace with text/file** • Pass	Primary action: • **Clean** • Replace with text/file • Pass Secondary Action (when clean is unsuccessful): • **Replace with text/file** • Pass
Other			
Password protected or encrypted	• **Pass** • Delete entire message • Quarantine entire message • Replace with text/file	• **Pass** • Replace with text/file	• **Pass** • Replace with text/file
Compressed file over scanning restrictions	• **Replace with text/file** • Delete entire message • Quarantine entire message • Pass	• **Replace with text/file** • Pass	• **Replace with text/file** • Pass

About Virus Scanning

ScanMail protects your Exchange environment by performing scans on all incoming and outgoing email messages. You can simply accept the Trend Micro default values set by the installation program or you can customize scanning by setting a number of configurations described in this chapter. You can set ScanMail to run scans on-demand (manual scanning), according to a schedule (scheduled scanning), or in an ongoing and persistent manner (real-time scanning). You configure scans using the Virus Scanning screen, accessible from the sidebar, or from the Manual Scan and Scheduled Scan screens.

The following describes the key characteristics of virus scanning:

Real-time scanning

ScanMail scans the following in real time:

- All incoming and outgoing email messages
- SMTP messages arriving at Exchange from the Internet
- Public-folder postings
- All server-to-server replications

Manual and scheduled scanning

During manual and scheduled scans, ScanMail scans messages stored in the mailbox and public folder stores.

ScanMail filtering strategy

ScanMail uses a filtering strategy to protect Exchange. When messages arrive at the Exchange server, ScanMail subjects each email message to a number of filters. Each filter checks the email messages for security threats and unwanted content. ScanMail screens email messages through the filters described below in the following order: anti-spam, content filtering, attachment blocking, and virus scanning.

- Anti-spam

  ScanMail uses the Trend Micro spam engine and spam pattern file to screen each email message for spam before delivering them to the Information Store. The Exchange server will not process rejected spam mail and the messages do not end up in your clients' mailboxes. Administrators can create approved and blocked

senders lists for the Exchange servers and end users can create their own lists of approved senders.

ScanMail performs one of the following actions on detected spam:

- Quarantines spam messages to an end user spam folder
- Deletes the spam message
- Tags and delivers messages as spam

- Content filtering

  ScanMail filters incoming and outgoing email messages and screens out unwanted content. ScanMail can filter content in a message header, subject, body, and/or attachment based on policies set by the administrator. ScanMail can perform one of the following actions on email messages that contain undesirable content in the message body or attachments:

  - Replace with text/file
  - Quarantine
  - Delete entire message
  - Archive

- Attachment blocking

  ScanMail can block attachments according to user-defined attachment types or by specific names. During manual or scheduled scanning, ScanMail can replace the detected file with a text message and then deliver the message to the intended recipient. During real-time scanning, ScanMail can perform one of three actions against blocked attachments:

  - Replace with text/file
  - Quarantine
  - Delete entire message

- Virus scanning

  Virus scanning employs the latest version of the Trend Micro scan engine to detect viruses, worms, Trojans, and spyware and other grayware. The Trend Micro scan engine uses pattern recognition and rule-based technologies to scan all incoming and outgoing messages for viruses and other security threats in real time or on-demand.

  This is an overview of how virus scanning with ScanMail works:

i. ScanMail uses SMTP scanning to check all mail messages arriving from outside the Exchange environment for viruses.

ii. ScanMail scans all outgoing messages and attachments that originate from an Exchange mailbox. For each message, the Microsoft virus scanning API checks ScanMail records to determine if the message or attachment has been scanned. If the message has not been scanned, it passes the message to ScanMail for scanning.

iii. ScanMail filters each email message for spam, content rule violations, specified attachments, and viruses and other malicious code. ScanMail takes user-configured actions against detected security threats.

iv. After the scanning is complete, ScanMail passes the message and attachments back to the Information Store and updates the scanning records ("stamps" the messages and attachments as previously scanned).

v. The Information Store database combines the original uninfected (or cleaned) attachments with the original uninfected (or cleaned) message and sends it to the intended recipients.

- Real-time scanning

  ScanMail guards all possible virus entry points with real-time scanning of all incoming messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. During real time scanning, ScanMail takes actions against security threats according to the administrator's configurations.

  See *About Notifications* on page 7-10 for more information about the specific actions an administrator can set for ScanMail.

- Manual and scheduled scanning

  ScanMail performs manual and scheduled scanning on demand according to a manual prompt or schedule. On demand scanning eliminates viruses from inside the Information Store databases, eradicates old virus infections, and minimizes the possibility of reinfection. When performing a manual or scheduled scan, ScanMail takes actions against security threats depending on the administrator's configurations.

  ScanMail allows the selection of individual Stores for scanning. For example, you can use this option to provide virus scanning and content security for a particular storage groups' databases, rather than for all storage groups.

See *About Notifications* on page 7-10 for more information about the specific actions an administrator can set for ScanMail.

- Alerts and notifications

  ScanMail can send alerts about virus outbreaks and significant system events. Outbreak alerts notify administrators when the number of detected viruses, uncleanable files, or blocked attachments exceed a set number. This enables administrators to react quickly to security breaches in their Exchange environment.

- Reports and logs

  ScanMail provides logs and reports to keep administrators informed about the latest security threats and system status. ScanMail logs significant events such as component updates and scan actions. Administrators can query these events to create log reports providing current and detailed information about the security of the Exchange environment. ScanMail can generate reports for system analysis that can be printed.

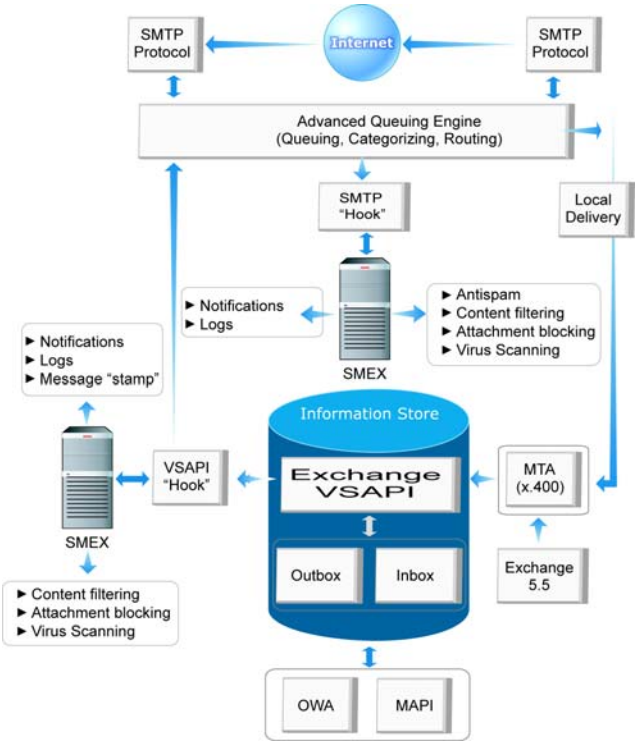

FIGURE 7-1. ScanMail filtering strategy

About Notifications

You can configure ScanMail to send notifications when it takes action against detected threats. You can send notifications by email and SNMP. You can also automatically record Notifications in the Windows Event Log.

Notifications serve a number of purposes as follows:

- Warn the original recipients that their email message was altered
- Notify an administrator or other network security professional of a security risk
- Display information to the recipient about threats and the actions taken, such as:
  - The name of the threat
  - The delivery or posting time
  - Sender, recipient
  - Subject, mailbox
  - The action taken by ScanMail.

  ScanMail gives you the option to append additional ScanMail fields to the default message or to create customized messages.

Tip: For correct resolution of ScanMail notification with SNMP, you can import the Management Information Base (MIB) file to your network management tools from the following path in ScanMail Package: `tool\admin\trend.mib`.

Setting up Notifications

You can configure ScanMail to send a notification when it detects and takes action during the following scans:

- Virus scanning
- Attachment Blocking
- Content Filtering

To set up a notification:

1. Click the **Notification** tab from the Virus Scanning, Attachment Blocking, or Content Filtering screen.
2. Click on the check boxes corresponding to the people ScanMail will notify.
3. Click (▼) to customize the notification for that recipient.

4. Set **Advanced Notification**:
   - Click **SNMP** to send notification by SNMP. Click (▼) to customize the SNMP message.
   - Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
5. Click **Finish**.

Note: For more detailed instructions, refer to the online help for the appropriate scanning filter.

Windows Event Logs

Event identifications for notifications written into Windows event logs have changed a lot from previous versions of ScanMail. This change might impact your monitoring efforts. Consult *Windows Event Log Codes* starting on page i-1 to understand the Windows event logs for ScanMail 7.0.

Enabling and Disabling Scans

You can enable or disable virus scanning for real-time or scheduled scans. You can also disable SMTP scanning.

Real-time scanning is persistent and ongoing. When you enable real-time scanning, ScanMail starts to scan all incoming and outgoing messages immediately. Real-time scanning consists of four filters: virus scanning, content filtering, attachment blocking, and anti-spam. You can enable and disable each filter separately. When all of the filters are disabled, no real-time scanning can occur. Disabling a real-time scanning filter does not disable or change your scan configurations.

WARNING! If you disable real-time scanning, you are vulnerable to infected files entering the Exchange environment while the scan is disabled.

Disabling SMTP scanning

By default, ScanMail provides scanning at both the SMTP and Mailstore (VSAPI) levels. As a result, some files are scanned more than once, which can slow down the scanning process. Disable SMTP scanning to speed up the scanning process. However, turning off SMTP scanning also disables all anti-spam features and prevents ScanMail from executing the *delete entire message* and *quarantine entire message* actions.

To disable SMTP scanning

1. Open the ScanMail Summary screen.
2. Click the green icon ( ) to turn off scanning. ScanMail replaces the green icon with a red icon ( ).
3. To enable the SMTP scan, simply click on the icon again. This toggles the icon back to green and enables SMTP scanning.

Tip: To optimize performance and maintain ScanMail protection, consider disabling SMTP scanning only for a back-end server and enabling it on front-end server(s).

Manual scans

You cannot disable Manual scans, but you can abort them by clicking **Cancel** when the scan is in progress. Canceling a manual scan was not possible in previous versions.

Scheduled scans

Scheduled scans occur according to the schedule you have configured. You can disable individual schedules for scans or you can disable all scheduled scanning. Scheduled scans occur according to the schedule you have configured. You can disable individual schedules for scans. When you disable a schedule for a scan, only the scan for that schedule will stop. Other scans run according to schedule. When you disable all scheduled scanning, then all scheduled scans stop. Disabling scheduled scanning is only temporary and does not disable or change your scan configurations.

Configuring Virus Scanning

The following are the basic steps for configuring virus scanning. ScanMail provides identical options to configure real-time, manual, and scheduled virus scans.

Refer to *Running Manual Scans* starting on page 7-29 and *Managing Scheduled Scans* starting on page 7-30 for more information about configuring these scans.

Step 1: Select the **Target** tab and set the files to include in your scan.

The target for a scan is the files or content contained in email messages. ScanMail usually scans the files according to the true file type unless you configure ScanMail to scan specific file types.

See *Selecting files to scan* on page 7-14.

Step 2: Select the **Actions** tab to set the actions that ScanMail takes when it detects a virus or other threat in the files you specified.

You can select ActiveAction to use the Trend Micro recommended actions or customize your actions according to the type of threat detected. You can also set ScanMail to notify a designated person when it takes a specified action against a detected threat.

Step 3: Select the **Notifications** tab to set who is notified when virus events occur and how they receive notification.

Selecting files to scan

File types eligible for scanning

By default, ScanMail scans all scannable outgoing, incoming and stored messages in your Exchange environment. Scanning all files provides the maximum security possible. However, scanning every message requires a lot of time and resources and might be redundant in some situations. Therefore, you might want to limit the amount of files ScanMail includes in the scan. Table 7-2 describes the methods that ScanMail can use to determine which files to scan.

Target type	Description
All scannable files	ScanMail scans for viruses, worms, Trojans, and other malicious code in all file attachments - except unscannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions. See *About Scannable Files* on page 7-15 for more information about files that ScanMail does not scan.
IntelliScan	IntelliScan uses Trend Micro recommended settings to perform an efficient scan See *True file type* on page 7-16 for more information about how ScanMail identifies true file types.
Specific file type	Click the link to expand the list and select the files you want ScanMail to scan. Add files to the list by typing them in the box.
Additional Threats, Spyware and other Grayware	By default, ScanMail scans the target files for viruses, worms, Trojans, and other malicious threats; however, you can select from this list of additional threats to customize the types of threats that ScanMail will scan for.

TABLE 7-2. Types of target files

For some files, such as very large attachments and compressed files, you can set restrictions on how ScanMail scans. See *Scan restrictions for large attachments and compressed files* on page 7-18.

To select targets for scanning

1. Open the Virus Scanning screen.
   - To configure a real-time scan, click Virus Scanning
   - To configure a manual scan, click **Manual Scan > Virus Scanning**
   - To configure a scheduled scan, click **Scheduled Scan > Virus scanning**
2. Click the **Target** tab.
3. Select a method that ScanMail will use to decide what files to scan for viruses, worms, and Trojans.

   See Table 7-2, “Types of target files,” on page 7-14 for more information.
4. Click on the **Additional Threats** that you want ScanMail to detect.

   For more information on these threats, refer to *What do the terms mean?* starting on page 5-2.
5. Click **Scan message body** when you want ScanMail to scan the body of the email message in addition to the attached files.
6. If necessary, set **Scanning restrictions** to prevent ScanMail from scanning very large attachments and compressed files.

   Click the expanding link (▼) to expand the screen and add your scanning restrictions.

   See *Scan restrictions for large attachments and compressed files* on page 7-18 for more details on how to set scanning restrictions.
7. Click **Save**.

About Scannable Files

When you select **All scannable files**, ScanMail scans all files except those it judges to be unscannable. ScanMail does not scan files that are unscannable. To protect yourself from threats contained in unscannable files, configure ScanMail to execute a special action against unscannable files. See *About ScanMail actions* on page 7-20.

A file is unscannable if:

- The file is encrypted or password-protected
- The file is outside the configured scanning scope. For example, you select not to scan image files (such as files with `.gif` extensions)

Files That Are Not Scanned

The scan engine does not scan some files that are unlikely to harbor viruses, for example, `.gif` files. The scan engine determines whether it is necessary to scan a file by examining the file header—if the scan engine determines that the file content matches a type that does not harbor viruses, then it does not examine the content of the file body.

About IntelliScan

Most antivirus solutions today offer you two options in determining which files to scan for potential threats. ScanMail either scans all scannable files (the safest approach), or it scans only those files with certain file name extensions (considered the most vulnerable to infection). But recent developments involving files being "disguised" through having their extensions changed has made this latter option less effective.

IntelliScan™ is a Trend Micro technology that identifies a file's "true file type", regardless of the file name extension. IntelliScan uses a method of identifying which files to scan that is more efficient, especially for SMTP traffic, than the standard **All scannable files** option.

Note: IntelliScan examines the header information of every file. Based on certain indicators, ScanMail selects only files that it determines are susceptible for virus scanning.

Because IntelliScan scans only files that are vulnerable to infection, using IntelliScan brings you the following benefits:

- Performance optimization. IntelliScan uses fewer system resources than scanning all files.
- Shorter scanning period. The scan time is shorter than when you **All scannable files**.

True file type

When set to scan true file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named "family.gif," it does not

assume the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that someone named to avoid detection.

True file type scanning works in conjunction with IntelliScan to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but with this reduction comes a potentially higher risk.

Note: There is one key difference between using IntelliScan and performing other scans using ScanMail true file type recognition. ScanMail true file type recognition allows users to define their own selection of files to scan, while IntelliScan always uses the Trend Micro recommended selection of files to scan.

For example, .gif files make up a large volume of all Web traffic, but they are unlikely to harbor viruses, launch executable code, or carry out any known or theoretical exploits. Therefore, does this mean they are safe? Not entirely. It is possible for a malicious hacker to give a harmful file a “safe” file name to smuggle it past the scan engine and onto the network. This file could cause damage if someone renamed it and ran it.

Tip: For the highest level of security, Trend Micro recommends scanning all files.

Scan restrictions for large attachments and compressed files

You can configure how ScanMail scans email messages that are very large or contain very large attachments and/or compressed files. You use the options from **Virus Scanning > Scanning restrictions** to set limits for ScanMail. ScanMail will not scan files that exceed your limits.

Note: A compression layer is added each time a file is compressed. That is, if a file is compressed and then compressed again, it has 2 layers of compression.

Tip: Trend Micro recommends using scanning restrictions to protect against Denial of Service attacks. Denial of Service attacks cause a loss of 'service', namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload computer resources such as memory.

See *Spam engine and spam pattern files* on page 1-12 for more information about how ScanMail processes compressed files.

To configure scanning for email messages that are very large or contain very large attachments:

1. Click **Virus Scanning > Target > Scanning restrictions**
   - Click **Message body size exceeds:** and type a number. ScanMail only scans email messages when the size of the body of the message is smaller or equal to the specified amount.
   - Click **Attachment size exceeds:** and type a number. ScanMail only scans email messages when the size of the attachment file is smaller than or equal to the specified amount.
2. Click **Save** to save your restrictions.

To configure compressed files for scanning:

1. Click **Virus Scanning > Target > Scanning restrictions**
   - Click **Decompressed file count exceeds:** and type a number to set a restriction for the amount of decompressed files that ScanMail will scan.

     When the amount of decompressed files within the compressed file exceeds this number, then ScanMail only scans files up to the limit set by this option.

For example, if you set the decompressed file limit to 4, and the Exchange server receives an email message with 7 compressed files, then ScanMail will only scan the first 4 decompressed files and will skip the remaining 3 files. Configure ScanMail to take action against the 3 unscannable files.

- Click **The size of decompressed files exceeds:** and type a number that represents the size limit in MB. ScanMail only scans compressed files that are smaller or equal to this size after decompression.
- Click **The number of layers of compression exceed:** and type a number from 1-20. ScanMail only scans compressed files that have less than or equal to the specified layers of compression.

  For example, if you set the limit to 5 layers of compression, then ScanMail will scan the first 5 layers of compressed files, but not scan files compressed to 6 or more layers.
- Click **Size of decompressed file is "x" times the size of compressed file:** and type a number. ScanMail only scans compressed files when the ratio of the size of the decompressed file compared to the size of the compressed file is less than or equal to this number.

  This function prevents ScanMail from scanning a compressed file that might cause a Denial of Service (DoS) attack. A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing ScanMail from scanning files that decompress into very large files helps prevent this problem from happening.

  Example: For the table below, the value typed for the "x" value is 100.

File size (not compressed)	File size (compressed)	Result
500 KB	10 KB (ratio is 50:1)	Scanned
1000 KB	10 KB (ratio is 100:1)	Scanned
1001 KB	10 KB (ratio exceeds 100:1)	Not scanned *
2000 KB	10 KB (ratio is 200:1)	Not scanned *

  * ScanMail takes the action you configure for unscannable files.

2. Click **Save** to save your restrictions.

Setting Scan Actions

About ScanMail actions

When ScanMail detects a file that matches your scanning configurations, it executes an action to protect your Exchange environment. The type of action it executes depends on the type of scan it is performing (real-time, manual, or scheduled) and the type of actions you have configured for ScanMail to take against the detected threat.

You can configure ScanMail to execute one of the following basic types of action:

- ActiveAction

  Select ActiveAction to have ScanMail execute actions recommended by Trend Micro. See *Using ActiveAction* on page 7-22.

- Customized Action

  You can configure ScanMail to take customized actions according to the type of threat presented by viruses, Trojans, worms, and other additional threats. See *Using customized actions* on page 7-22.

- Advanced Option

  Use the **Advanced Options** to set how ScanMail handles macros and unscannable files. You can also set up the backup and quarantine folders and customize the replacement file/text used when ScanMail replaces an infected attachment.

Types of Security Threats

The types of computer security threats are constantly changing. ScanMail is designed to counter all prevalent attacks. Table 7-3 introduces some common types of security threats that ScanMail can protect your Exchange environment against. For a more detailed explanation, refer to Chapter 5, Understanding Threats to an Exchange Environment.

Attack type	Description
Viruses	A virus is a malicious code that infects files so that it can replicate and cause damage to your computer. In messaging environments, infected files are often spread through email attachments. When infected files are executed, viruses replicate and may damage your computer's files or operations.
Trojans	A Trojan horse program is a program that performs some unexpected or unauthorized - usually malicious – actions. Trojans, like regular programs, must be run to be effective. Frequently Trojan horse programs are installed and/or run when users launch a seemingly harmless application by clicking on an email attachment.
Worms	A computer worm is a self-contained program (or set of programs) that can spread functional copies of itself or its segments to other computer systems. Worms often use email and applications to propagate.
Other malicious codes	ScanMail detects some malicious code that is difficult to categorize, but pose a significant threat to Exchange. This category is useful when you want ScanMail to perform an action against a previously unknown threat type.
Spyware and other grayware	Spyware and other grayware include such potential security problems as Dialers, Hacking tools, Adware, and Joke programs. Spyware, like Trojan horse programs, must be installed to function. Frequently, these programs install when an email client launches an attached executable file received in an email attachment.

TABLE 7-3. Types of security threats

Using ActiveAction

ActiveAction performs scan actions recommended by Trend Micro. These actions are preconfigured by ScanMail and based on how each type of attack invades a computer.

- When ActiveAction detects a file infected by a malicious code such as a virus, Trojan, or worm, it executes the Trend Micro recommended action against that file. By default, ScanMail attempts to clean files infected by malicious code. However, when ScanMail is unable to perform the clean action, it performs a secondary action instead.
- When ActiveAction detects spyware and other grayware, it takes an action appropriate to the security threat it detects.

If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:

- Time saving and easy to maintain — ActiveAction uses scan actions recommended by Trend Micro. You do not have to spend time configuring the scan actions.
- Updateable scan actions — Virus writers constantly change the way viruses attack computers. To ensure that clients are protected against the latest threats and the latest methods of virus attacks, new ActiveAction settings are updated in virus pattern files.

Using customized actions

You can configure ScanMail to take actions according to the type of threat presented by viruses, Trojans, worms, and spyware/grayware. If you use customized actions, you can set an action for each type of threat. ScanMail executes the action you set when it detects a threat of the matching type. Refer to Chapter 5, *Understanding Threats to an Exchange Environment* for more information about the types of security threats.

Mass-mailing behavior

Enable ScanMail to take action against these attacks whenever it detects a mass-mailing behavior. The action set for mass-mailing behavior takes precedence over all other actions. The real-time scanning default action is *delete entire message*.

See *About Mass-Mailing Attacks* on page 5-5 for more information about how ScanMail protects against mass-mailing attacks.

Action	Description
Clean	Removes malicious code from infected message bodies and attachments. The remaining email message text, any uninfected files, and the cleaned files are delivered to the intended recipient(s). Trend Micro recommends you use the default scan action *clean* for viruses. Under some conditions, ScanMail cannot clean a file. See *About Uncleanable Files* on page 7-24. During a manual or scheduled scan, ScanMail updates the Information Store and replaces the file with the cleaned one.
Replace with text/file	ScanMail deletes the infected content and replaces it with a text or file. The email message is delivered to the intended recipient, but the text replacement informs them that the original content was infected and was replaced.
Quarantine entire message	Move the email message to a restricted access folder, removing it as a security risk to the Exchange environment. The original recipient will not receive the message. This option is not available in manual and scheduled scanning. See *Setting Up and Managing the Quarantine Folder* on page 7-69 for more information about the quarantine folder.
Delete entire message	During real-time scanning, ScanMail deletes the entire email message. The original recipient will not receive the message. This option is not available in manual and scheduled scanning. The *delete* action in ScanMail 7.0 differs from that of ScanMail 6.x. ScanMail 6.x used the action *delete* to remove the contents of a message and replace it with a warning text. The *delete entire message* in ScanMail 7.0 will completely delete messages and will not send the message on to the original recipient.
Pass	Record virus infection of malicious files in the Virus logs, but take no action.

TABLE 7-4. ScanMail customized actions

To configure your scan actions:

1. Configure the action ScanMail executes when it detects a threat.

   Select one of the following methods:

   a. ActiveAction

      ActiveAction performs the Trend Micro recommended action based on threat type.

      See *Using ActiveAction* on page 7-22

   b. Customized action

      Set an action based on the specific type of security threat ScanMail detects.

      See *Using customized actions* on page 7-22

2. Click **Backup infected file before action is taken** to have ScanMail move a copy of the original infected file to a backup folder before it takes an action against the infected file. The cleaning process sometimes corrupts files and makes them unusable; backing up files before ScanMail takes action protects files against this.

   See *Back up files before taking action* on page 7-26.

3. Click **Do not clean infected compressed files to improve performance** to have ScanMail ignore compressed files when cleaning email messages for viruses.
4. If necessary, set **Advanced options** to set special actions for ScanMail to take against malicious macro code and unscannable email messages.

About Uncleanable Files

When ScanMail cannot successfully clean a file, it labels the file "uncleanable" and performs the user-configured action for uncleanable files. The default action is *Quarantine entire message*. ScanMail records all virus events and associated courses of action in the log file.

Some common reasons why ScanMail cannot perform the clean action are as follows:

- The file contains a Trojan, worm, or other executable program. To stop an executable from executing, ScanMail must completely remove it.

- ScanMail does not support the compression format used to compress the file. The scan engine only cleans files compressed using `pkzip` and only when the infection is in the first layer of compression.

  For example, consider a compressed file titled “EuropeanBusinessTrip.zip” which contains the following:

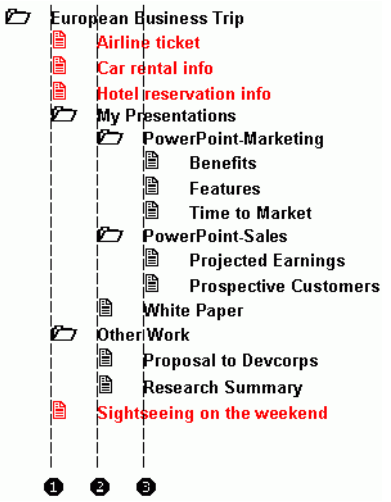

FIGURE 7-2. Compression layers explained

- An unexpected problem prevents ScanMail from cleaning, such as:
  - The temp directory that acts as a repository for files requiring cleaning is full
  - The file is locked or is currently executing
  - The file is corrupted
  - The file is password protected
  - The file is located in the Windows Recycle Bin, Windows Temp folder, or Internet Explorer temporary folder

Back up files before taking action

You can set ScanMail to backup a file to the Backup folder before taking action on it. This is a safety precaution designed to protect the original file from damage.

Tip: Trend Micro recommends quickly deleting backed up files once you have determined that the original file was not damaged and that it is usable. If the file becomes damaged or unusable, send it to Trend Micro for further analysis. (Even if ScanMail has completely cleaned and removed the virus itself, some viruses damage the original file code beyond repair.)

To specify the location of the Backup folder:

1. From the Virus scanning screen, click **Backup and quarantine directories**.
2. Type the path to the backup directory.
3. Click **Save**.

Do not clean infected compressed files to improve performance

Select this option to improve ScanMail performance. When ScanMail detects a security threat in a compressed file, it will not clean the file. Instead, it processes the files as if it were uncleanable.

Using Advanced Scanning Options

Use the **Advanced Options** to set how ScanMail handles macros and unscannable files. You can also set up the backup and quarantine folders and customize the replacement file/text used when ScanMail replaces an infected attachment.

Using advanced macro scanning

ScanMail uses the virus pattern file to identify known malicious macro codes during regular virus scanning. ScanMail takes action against malicious macro code depending on the action that you configure from the Virus Scanning page. Use Advanced macro scanning to gain additional protection against malicious macro code.

Advanced macro scanning supplements regular virus scanning. It uses heuristic scanning to detect macro viruses or simply strips all detected macro codes. Heuristic scanning is an evaluative method of detecting viruses that uses pattern recognition and rules-based technologies to search for malicious macro code. This method excels at detecting undiscovered viruses and threats that do not have a known virus signature. When a malicious macro code is detected using heuristic scanning, ScanMail takes action against the malicious code based on the action that you configured from the Virus Scanning page. When you select **Delete all macros detected by advanced macro scanning**, then ScanMail strips all macro code from the scanned files.

To set ScanMail to scan unknown macro viruses:

1. Click **Virus Scanning** > **Action**.
2. Click (▼) from **Advanced Options** > **Macros**.
3. Select **Enable advanced macro scanning**.
4. Select a detection type:
   - Select **Heuristic level** and set a level for the heuristic rules.
     - Level 1 uses the most specific criteria, but detects the least macro codes.
     - Level 4 detects the most macro codes, but uses the least specific criteria and may falsely identify safe macro code as harboring malicious macro code.

   Note: Trend Micro recommends a heuristic scan level of 2. This level provides a high detection level for unknown macro viruses, fast scanning speed, and it uses only the necessary rules to check for macro virus strings. Level 2 also has a low level of incorrectly identifying malicious code in safe macro code.

   - Select **Delete all macros detected by advanced macro scanning** to have ScanMail strip all of the macro code that it detects.
5. Click **Save**.

Running Manual Scans

Manual and scheduled scanning on the Microsoft Exchange server is similar to traditional hard drive antivirus scanning. However, ScanMail, unlike traditional antivirus scanners, can support the Microsoft Exchange database format, and can scan files and documents stored on Exchange servers.

You can run a manual scan to ensure that ScanMail scans all messages in the Information Store once. Completely scanning the Information Store in this way minimizes the chance of infections from unexpected sources such as unprotected mail servers or improper configurations. Manual scanning scans the entire Information Store by default; however, you can configure ScanMail to scan any of the Mailbox Stores and Public Folder Stores.

Tip: If you have more than one storage group, you may want to disable scanning the replicated databases. Go to **Manual Scan > Database Selection** and change the databases selected for scanning.

If you begin a manual scan when a scheduled scan is running, the scheduled scan is interrupted. The scheduled scan aborts, but runs again according to its schedule.

You can perform virus scanning, attachment blocking, and content filtering through manual scanning. These filters are similar to those used during real-time scanning, except some actions are not available during manual or scheduled scanning.

To run a manual scan:

Step 1: Select the database for ScanMail to scan:

1. Click **Manual Scan** to open the Manual Scan screen.
2. Click the check boxes that represent the Mailbox and Public Folder Stores that you want to include in your scan.

Step 2: Configure your scan:

1. Set the target to scan.

   See *Selecting files to scan* on page 7-14 for more detailed information.
2. Set the actions that ScanMail takes against security threats.

   See *Setting Scan Actions* on page 7-20 for more detailed information.
3. Set ScanMail to notify designated individuals when it takes an action.

4. Click **Save** to save your configurations and close the Virus Scanning screen.

Step 3: Run the scan:

Click **Scan Now**. A screen opens displaying a progress bar and displaying information about the progress of your scan.

Note: The progress bar will display on this screen until the scan is complete. This is true even if you open a different screen and then return to this one.

To view detailed scan status

1. Perform a manual scan.
2. When the scan is complete, click **view details.** The Manual Scan Results screen opens displaying detailed information about the scan. This screen includes information about the number of stores scanned, the spent time, and the number of viruses detected.

Managing Scheduled Scans

A scheduled scan is a manual scan that runs according to a schedule set by an administrator. Scheduled scans can run on a daily, weekly, or monthly schedule. You can set the time when to begin the scheduled scan. This allows you to run your scheduled scan at times when network traffic is low.

Tip: Trend Micro recommends that you do not schedule a scan to run at the same time as you set for a scheduled update. This may cause the scheduled scan to stop unexpectedly. Similarly, if you begin a manual scan when a scheduled scan is running, the scheduled scan is interrupted. The scheduled scan aborts, but runs again according to its schedule.

You can set up any number of scheduled scans, each configured differently. You can enable or disable scheduled scans.

Completely scanning the Information Store in regularly scheduled scans minimizes the chance of infections from unexpected sources such as unprotected mail servers or improper configurations. Scheduled scanning scans the entire Information Store by default; however, you can configure ScanMail to scan any of the Mailbox Stores and

Public Folder Stores. For clusters, ScanMail can only scan the one virtual server to which it is installed.

Tip: Trend Micro recommends that you set ScanMail to run scheduled scans at regular intervals for optimal protection of your Exchange Information Store.

To add a scheduled scan:

Step 1: Set the scan schedule:

1. Click **Scheduled Scan** > **Add** a scan task.
2. Select the time period for the scan.
   - Select **Daily** to have ScanMail run the scheduled scan every day. The scan begins in the next 24 hour period.
   - Select **Weekly** to have ScanMail run the scheduled scan once every week. Select the day of the week on which you want the scan to run.
   - Select **Monthly** to have ScanMail run the scheduled scan once every month. Select the day on which you want the scan to run.
3. Set a time when you want the scheduled scan to run during the specified period.

Step 2: Select the database for ScanMail to scan:

Click the check boxes that represent the Mailbox and Public Folder Stores that you want to include in your scan.

ScanMail scans the entire Information Store by default; however, you can configure ScanMail to scan any of the Mailbox Stores and Public Folder Stores.

Step 3: Configure your scan:

1. Set the target to scan.

   See *Selecting files to scan* on page 7-14 for more detailed information.
2. Set the actions that ScanMail takes against security threats.

   See *Setting Scan Actions* on page 7-20 for more detailed information.
3. Set ScanMail to notify designated individuals when it takes an action.

To view a scheduled scan:

On the Schedule Scan page, you can view each scan status type:

- **Success** — click to view scanning results
- **In progress** — scan is running, click to check status of scan
- **Queuing** — the scan had a schedule time conflict

Virus Scanning on Clusters

Node-based scanning

The Manual and Scheduled Scans are node based. This means, only one manual or scheduled scan can be run on one node at the same time.

For example: Virtual server A, B are on node1; if one scanning task is running on A, then B can't run a background scan at the same time.

Virus scanning during failover or following real-time scan change

During a failover period on clusters, the database of the Information Store will be unmounted and mounted by another node. After failover, manual or scheduled scan tasks stop. This is also true when the real-time scan status changes on the same node (as a result of enabling or disabling Virus scanning, attachment blocking, or content filtering).

For example: Virtual servers A and B are on node1. If server A has a failover to node 2, the scan task running on server B will stop.

Example2: Virtual servers A and B are on node1. If server A turns off real-time scanning (that is, disables all filters), the scan task running on server B will stop.

Manual scan on clusters

You can specify the store database that belongs to a current virtual server. Before you submit a manual scan, ScanMail needs to check if a running manual scan is already in progress. If there is a task in progress, ScanMail rejects the submitted task and prompts the user with a warning.

Scheduled scan on clusters

Each virtual server has a scan task list. You can specify the store database that belongs to the current virtual server. When there is a running scheduled scan task,

new tasks are queued. When another tasks is triggered at the same time, then the task will be queued and finished eventually.

About Blocking Attachments

Attachment blocking prevents email messages containing suspect attachments from being delivered to the Exchange Information Store. You can configure ScanMail to block attachments according to the attachment type or attachment name and then *replace*, *quarantine*, or *delete* all the messages that have attachments that match your configuration. Blocking can occur during real-time, manual, and scheduled scanning, but the *delete* and *quarantine* actions are not available for manual and scheduled scans. You can enable or disable attachment blocking.

Note: Selecting Attachment Blocking in real time on an Exchange 2003 mailbox server causes ScanMail to scan email twice: once at the SMTP transport level, and a second time - by default - at the mailbox level. Scanning emails twice can seriously degrade mailbox server performance.

The extension of an attachment identifies the file type, for example .txt, .exe, or .dll. However, ScanMail examines the file header rather than the file name to ascertain the actual file type. Many viruses are closely associated with certain types of files. By configuring ScanMail to block according to file type, you can decrease the security risk to your Exchange servers from those types of files. Similarly, specific attacks are often associated with a specific file name.

Tip: Using blocking is an effective way to control virus outbreaks. You can temporarily quarantine all high-risk file types or those with a specific name associated with a known virus. Later, when you have more time, you can examine the quarantine folder and take action against infected files.

Selecting blocking targets

Block attachments with two general strategies: either block all attachments and then exclude specified attachments or specify all the attachments to block.

- All attachments

  ScanMail can block all email messages that contain attachments. However, this type of scan requires a lot of processing and might be slow. Refine this type of scan by selecting attachment type or names to exclude.

- Specified attachments

  When you select this type of scan, ScanMail only scans for email messages containing attachments that you identify. This type of scan can be very exclusive and is ideal for detecting email message containing attachments that you suspect contain threats. This scan runs very quickly when you specify a relatively small amount of attachment names or types.

You can block attachments according to:

- Specific name

  By default, ScanMail examines the file header rather than the file name to ascertain the actual file type. When you set Attachment Blocking to scan for specific names, ScanMail will detect attachment types according to the name they were given.

- Attachment type.

  ScanMail examines the file header rather than the file name to ascertain the actual file type.

Attachment Blocking actions

You can configure ScanMail to take action against email messages containing detected threats. The following table lists the actions ScanMail can perform.

Action	Description
Replace with text/file	ScanMail deletes the attachment and replaces it with a text file. The email message is delivered to the intended recipient, but the text replacement informs them that the original content was infected and was replaced.
Quarantine	Move the email message that contains the attachment to a restricted access folder, removing it as a security risk to the Exchange environment. This action is not available for manual and scheduled scans.
Delete entire message	During real-time scanning, ScanMail deletes the entire email message. This option is not available in manual and scheduled scanning.

TABLE 7-5. Attachment Blocking Actions

To Configure Attachment blocking:

1. Select the attachment targets to block

Click **Target** to select the attachments for ScanMail to block.

2. Set the action

Click **Action** to set the action ScanMail takes when it blocks an attachment.

ScanMail performs an action whenever it detects an attachment that requires blocking. You set the action ScanMail performs.

Set one of the following actions:

- Replace attachment with text/file:
- Quarantine:
- Delete entire message:

3. Set the notification

- Click **Notification** to set up the notifications ScanMail sends when it takes an action against an attachment.
- Click on the check boxes corresponding to the people ScanMail will notify
  - Click (▼) to customize the notification for the administrator
  - Click (▼) to customize the notification for the sender
  - Click (▼) to customize the notification for the recipient
  - Click in the appropriate check box to set notification by SNMP or Windows event log

---

Note: For detailed instructions on setting the Attachment Blocking options, refer to the ScanMail online help.

Filtering Undesirable Content

The content filter evaluates inbound and outbound messages on the basis of user-defined rules. Each rule contains a list of keywords and phrases. Content filtering evaluates the header and/or content of messages by comparing the messages with the list of keywords. When ScanMail finds a word that matches a keyword it can take action to prevent the undesirable content from being delivered to Exchange clients. ScanMail can send notifications whenever it takes an action against undesirable content.

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. The content filter also provides a synonym checking feature which allows you to extend the reach of your policies.

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

- Sexually harassing language
- Racist language
- Spam embedded in the body of an email message

Viewing Content Filtering Rules

ScanMail displays all the content filter rules in the Content Filtering screen. This screen shows summary information about the rules including:

- **Action**: ScanMail takes this action when it detects undesirable content
- **Order**: ScanMail applies each filter in succession according to the order shown on this page.

- **Enabled**: During real-time scan, manual scan, or schedule scan, you can enable or disable all content filtering or each individual content filter rule. The icons on the Content Filtering screen show the status of the content filtering rule. Click on the icon to toggle between enabled and disabled.
  - Green check mark ( )—indicates that you have enabled the rule
  - The red circle "x"( )—indicates that you have disabled the rule

Note: By default, content filtering is not enabled.

When you click on an individual rule, the Edit rule page opens displaying details about the rule.

Enabling Content Filtering Rules

When content filtering is enabled, you can enable and disable individual content filter rules. The green check icon indicates the rule is enabled, the red "x" indicates the rule is disabled. Click on the icon to toggle between enabled and disabled.

To enable content filtering rules:

1. Click **Content Filtering**.
2. Click **Enable real-time content filtering**. Clear the check box to disable content filtering.
3. Click **Save**.

To enable an individual content filter:

1. Click **Content Filtering**.
2. If necessary, click **Enable real-time content filtering**.
3. Click to enable rules that are disabled. The icon toggles to a green check mark to indicate the rule is enabled.
4. Click **Save**.

Adding Content Filtering rules

To create a content filtering rule you move through a series of steps. At each step you add to your rule until it is complete. After you have created your rule, ScanMail begins to filter all incoming and outgoing messages according to your rule.

You can create the rules that do the following:

- Filter messages that match any condition defined

  This type of rule is capable of filtering content from any message in real-time or during a manual or scheduled scan.

- Filter message that match all conditions defined

  This type of rule is capable of filtering content from any message during real-time scanning. For customers who are migrating from previous versions of ScanMail with eManager, ScanMail upgrades the old anti-spam content filtering rules to this type of rule.

- Monitor the message content of particular email account(s)

  This type of rule monitors the message content of particular email account(s). Monitoring rules are similar to a general content filter rules, except that they only filter content from specified email account(s).

- Create exemption for particular email account(s)

  This type of rule creates an exemption for particular email account(s)

  When you exempt a particular email account, this account will not be filtered for content rule violations.

To create a rule that filters messages that match any condition defined:

Step 1: Select the type of content rule

1. From the Content Filtering page, click **Add**.
2. Select **Filter messages that match any condition defined**.
3. Click **Next**.

Step 2: Name your rule and select the message part to filter

1. Type the name of your rule in the **Rule name** space.
2. Click the message part that you want to filter for undesirable content. ScanMail can filter email messages by **Header** (**From**, **To**, and **CC**), **Subject**, **Body**, or **Attachment**.

Note: ScanMail only supports filtering of header and subject content during real-time scans. It does not support filtering of header and subject content during manual and scheduled scans.

---

3. Click **Next**.

Step 3: Set the keywords for which ScanMail searches

1. Select whether ScanMail filters content for "any" or for "all" of the keywords.
   - "Any" keyword tells ScanMail to take action against content that contains any of the keywords in the list.
   - "All" tells ScanMail to take action against content only when the content contains all of the keywords in the list.
2. Type or import keywords.
   - Type a keyword in the space provided.
     - Click **Add** to add it to the list of keywords that ScanMail checks when filtering content. ScanMail can support content filtering for Microsoft Office, PDF, and text files.
     - Click **Delete** to remove keywords from the list.

   By default, ScanMail searches for exact matches of the keywords that you add.

   See *About Filtering Keywords* on page 7-51 for more information.

   - Click **Import** to import keyword lists.

     When you import a keyword file, the imported keywords appear in the keyword list. The imported file must be a text (`.txt`) file. The imported keywords use the same format as they had in the text file. You can import keyword lists from previous versions of ScanMail. ScanMail imports the keywords and applies the same syntax as used in ScanMail 7.0. See Table 7-6 below.

The imported text file contains:	The keyword list displays:
win cash prize	win cash prize
win cash prize	win cash prize

TABLE 7-6. Importing keyword lists

3. Click **Match case-sensitive** to have ScanMail disregard words that do not match the keyword's case when filtering content.
4. Set up your list of synonyms.
   - Click **Match synonym** to have ScanMail consider all the synonyms of the keyword when filtering content.
   - Click (▼) next to **Match synonym** to display the list of synonyms. When you select a keyword, all of the keyword's synonyms display in the **Synonyms to exclude** list. Use the arrow keys to add and delete synonyms for each corresponding keyword.
5. Click **Next**.

Step 4: Set the action ScanMail takes against content that matches the keyword

1. Select an action for ScanMail to take when it detects undesirable content. ScanMail can perform the following actions when it detects content that matches the rule conditions:
   - **Replace with text/file** — replaces the filtered content with a text file.

     You cannot replace text from the **From**, **To**, **CC**, or **Subject** fields.
   - **Quarantine** — moves the message to the quarantine directory
   - **Delete entire message** — deletes the entire email message
   - **Archive** — moves the message to the archive directory and delivers the message to the original recipient

   See *Content Filtering Actions* on page 7-61 for an explanation of these actions.
2. Select whether or not ScanMail notifies designated individuals when it takes action against undesirable content.

Note: The actions *delete entire message* and *quarantine* are unavailable during manual or scheduled scans.

3. Click **Next**.

Step 5: Set the notifications ScanMail sends when it takes an action

1. Click on the check boxes corresponding to the people ScanMail will notify.
2. Click (▼) to customize the notification for that recipient.
3. To set **Advanced Notification**:
   - Click **SNMP** to send notification by SNMP. Click (▼) to customize the SNMP message.
   - Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
4. Click **Finish**.

Note: For detailed instructions on setting the Content Filtering notification options, refer to the ScanMail online help.

Step 6: Save your configuration

Click **Save**.

To create a rule that filters messages that match all conditions defined:

Step 1: Select the type of content rule

1. From the Content Filtering page, click **Add**.
2. Select **Filter message that match all conditions defined**.
3. Click **Next**.

Step 2: Name your rule and select the message part to filter for keywords

1. Type the name of your rule in the **Rule name** space.
2. Set the part of the message that ScanMail filters. ScanMail can filter messages according to:
   - Message header

     Type a keyword in the **From**, **To**, **CC**, and/or **Subject** field to have ScanMail take action against email messages that contain matching keywords in the corresponding fields. Separate multiple keywords with a semi-colon (**;**).
   - Attached files

     Type a name in the **Attachment file name** field. ScanMail takes action against messages that have attachments with the name you specify. Separate multiple keywords with a semi-colon (**;**).

     Tip: ScanMail performs Content Filtering before Attachment Blocking.

   - Size

     Select an option from the **Size** drop list and type a number to indicate a size in bytes. The maximum amount of digits for this field is 10. ScanMail cannot filter messages that exceed 2GB.

     Note: ScanMail only supports filtering of header and subject content during real-time scans. It does not support filtering of header and subject content during manual and scheduled scans.

3. Click **Next**.

Step 3: Set the action ScanMail takes against content that matches the keyword

1. Select an action for ScanMail to take when it detects undesirable content during a real-time scan. ScanMail can perform the following actions when it detects content that matches the rule conditions:
   - **Quarantine** — moves the message to the quarantine directory.
   - **Delete entire message** — deletes the entire email message
   - **Archive** — moves the message to the archive directory and delivers the message to the original recipient
   - **Pass** — delivers the message without triggering any action.

   See *Content Filtering Actions* on page 7-61 for an explanation of these actions.
2. Select whether or not ScanMail notifies designated individuals when it takes action against undesirable content.
3. Click **Next**.

Step 4: Set the notifications ScanMail sends when it takes an action

1. Click on the check boxes corresponding to the people ScanMail will notify.
2. Click (▼) to customize the notification for that recipient.
3. To set **Advanced Notification**:
   - Click **SNMP** to send notification by SNMP. Click (▼) to customize the SNMP message.
   - Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
4. Click **Finish**.

Note: For detailed instructions on setting the Content Filtering notification options, refer to the ScanMail online help.

Step 5: Save your configuration

Click **Save**.

To create a rule that monitors message content for a particular email account(s):

Step 1: Select the type of content rule

1. From the Content Filtering page, click **Add**.
2. Select **Monitor the message content of particular email account(s)**.
3. Click **Next**.

Step 2: Name your rule and enter the email account(s) you want to monitor

1. Type a name for your rule in the space provided.
2. Type the mailbox address for the email account that you want to monitor. You can monitor an email account located in the **From**, **To**, and **CC** part of the header.
3. Click **Next**.

Step 3: Select the message part to filter and add keywords

1. Click the message part that you want to filter for undesirable content. ScanMail can filter email messages by **Subject**, **Body**, or **Attachment**. ScanMail can support content filtering for Microsoft Office, PDF, and text files.

   Note: ScanMail only supports filtering of header and subject content during real-time scans. It does not support filtering of header and subject content during manual and scheduled scans.

2. Type a keyword in the space provided.
   - Click **Add** to add it to the list of keywords that ScanMail checks when filtering content.
   - Click **Delete** to remove keywords from the list.

   By default, ScanMail searches for exact matches of the keywords that you add.

   See *About Filtering Keywords* on page 7-51 for more information.
3. Click **Match case-sensitive** to have ScanMail disregard words that do not match the keyword's case when filtering content.

4. Set up your list of synonyms.
   - Click **Match synonym** to have ScanMail consider all the synonyms of the keyword when filtering content.
   - Click (▼) next to **Match synonym** to display the list of synonyms. When you select a keyword, all of the keyword's synonyms display in the **Synonyms to exclude** list. Use the arrow keys to add and delete synonyms for each corresponding keyword.
5. Click **Next**.

Step 4: Set the action ScanMail takes against content that matches the keyword

1. Select an action for ScanMail to take when it detects undesirable content. ScanMail can perform the following actions when it detects content that matches the rule conditions:
   - **Replace with text/file** — replaces the filtered content with a text file.

     You cannot replace text from the **From**, **To**, **CC**, or **Subject** fields.
   - **Quarantine** — moves the message to the quarantine directory.
   - **Delete entire message** — deletes the entire email message
   - **Archive** — moves the message to the archive directory and delivers the message to the original recipient

   See *Content Filtering Actions* on page 7-61 for an explanation of these actions.

   Note: The actions *delete entire message* and *quarantine* are unavailable during manual or scheduled scans.
2. Select whether or not ScanMail notifies designated individuals when it takes action against undesirable content.
3. Click **Next**.

Step 5: Set the notifications ScanMail sends when it takes an action

1. Click on the check boxes corresponding to the people ScanMail will notify.
2. Click (▼) to customize the notification for that recipient.
3. To set **Advanced Notification**:
   - Click **SNMP** to send notification by SNMP. Click (▼) to customize the SNMP message.

- Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.

4. Click **Finish**.

Note: For detailed instructions on setting the Content Filtering options, refer to the ScanMail online help.

Step 6: Save your configuration

Click **Save**.

To create an exemption rule:

Step 1: Select the type of content rule

1. From the Content Filtering page, click **Add**.
2. Select **Create exemption for particular email account(s)**.
3. Click **Next**.

Step 2: Name your rule and enter the email account(s) you want to exempt

1. Type the name of your rule in the **Rule name** space.
2. Type the email address that you want to exempt from content filtering in the space provided and click **Add** to add it to the list.
3. When you are satisfied with your list, click **Finish**.

Step 3: Save your configuration

Click **Save**.

Specifying global directories

You can configure ScanMail to quarantine or archive email messages when it detects content filtering violations. You can set the quarantine or archive folder for each content filtering rule individually from the **Select an action screen**, or you can specify a global directory. When you specify a global quarantine or archive directory, ScanMail moves all files that it quarantines or archives as a result of content rule violations to the directory that you specify.

To specify a global directory

1. Click **Content Filtering**.
2. Click **Specify global directories**. The **Content Filtering > Directories** screen opens.
3. Type the directory path that you want ScanMail to use as the global directory.
4. Click **Apply to All**. ScanMail will move all files that violate content filtering rules to the directory you specify.

Note: You must click **Apply to All** to set the new directory. If you click **Save**, then ScanMail will only save the directory paths that you typed, but it will not be applied.

Modifying Content Filter rules

You can modify a rule by clicking on the rule name from the Content Filtering screen. When you click on a rule name, the Content Filtering > Edit Rule screen opens displaying information that corresponds to that rule.

You can modify the following parts of a rule:

- Enable or disable the rule
- Modify the rule name
- Modify the keywords for which ScanMail searches
- Modify the part of the email message that ScanMail filters
- Set the action ScanMail takes against content that matches the keyword
- Set the notifications ScanMail sends when it takes an action

To enable or disable the rule

- Select the **Enable this rule** check box to enable the rule.
- Clear the check box to disable the rule.

To modify the rule name

1. Click on a rule name. The Content Filtering > Edit Rule screen opens.
2. Type a new name in the **Rule name** field
3. Click **Save**.

To modify the keywords for which ScanMail searches

1. Click on a rule name. The Content Filtering > Edit Rule screen opens.
2. Select a keyword from the **Keyword list**.
3. Click **Delete** to remove it from the list.
4. Click **Import** to import keyword lists.

   When you import a keyword file, the imported keywords appear in the keyword list. The imported file must be a text (`.txt`) file. The imported keywords use the same format as they had in the text file. You can import keyword lists from previous versions of ScanMail. ScanMail imports the keywords and applies the same syntax as used in ScanMail 7.0. See Table 7-6.
5. Click (▼) next to **Match synonym** to display the list of synonyms. When you select a keyword, all of the keyword's synonyms display in the **Synonyms to exclude** list. Use the arrow keys to add and delete synonyms for each corresponding keyword.
6. Click **Save**.

To modify the part of the email message that ScanMail filters

1. Click on a rule name. The Content Filtering > Edit Rule screen opens.
2. If necessary, click the **Target** tab.
3. Choose the parts of the email that you want to modify. Different rules are able to filter different parts of the email message. Refer to the procedure for creating the type of rule for detailed information about the parts of the message that it can filter.
4. Modify the keywords for the part that you want to filter for undesirable content.
5. Click **Save**.

To modify the action that ScanMail takes when it detects a Content Rule violation

1. Click on a rule name. The Content Filtering > Edit Rule screen opens.
2. If necessary, click the **Action** tab.
3. Select an action for ScanMail to take when it detects undesirable content.
4. Set the action for ScanMail to take against messages that match the keyword.
5. Click **Save**.

To modify the notifications ScanMail sends when it takes an action

1. Click on a rule name. The Content Filtering > Edit Rule screen opens.
2. If necessary, click the **Notification** tab.
3. Click on the check boxes corresponding to the people ScanMail will notify.
4. Click (▼) to customize the notification for that recipient.
5. To set **Advanced Notification**:
   - Click **SNMP** to send notification by SNMP. Click (▼) to customize the SNMP message.
   - Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
6. Click **Save**.

Note: For detailed instructions on modifying the Content Filtering options, refer to the ScanMail online help.

Changing the Rule Order

ScanMail applies the content filtering rules to email messages according to the order shown in the Content Filtering screen. You configure the order in which the rules are applied. ScanMail filters all email messages according to each rule until a content violation triggers an action that prevents further scanning (such as *delete* or *quarantine*). You can change the order of these rules to optimize content filtering.

To change the order of the content filtering rules:

1. Select a checkbox that corresponds to the rule for which you want to change the order.
2. Click **Reorder**. A box appears around the order number for the rule.
3. Type a new order number in the box. The rule order number will change to the number that you type and all the other rule order numbers will change accordingly.

   For example: If you select rule number 5 and change it to rule number 3, then rule numbers 1 and 2 will remain the same, and rule numbers 3 and higher will increase by one number.

About Filtering Keywords

Keywords are not strictly words. They can be any of the following:

- Numbers
- Typographical characters
- Short phrases
- Words or phrases connected by logical operators
- Words or phrases that use *regular expressions*

Using keywords effectively

ScanMail offers simple and powerful features to create highly specific filters. Consider the following, when creating your Content Filtering rules:

- By default, ScanMail searches for exact matches of keywords. Use *regular expressions* to set ScanMail to search for partial matches of keywords. See *Using Regular Expressions* on page 7-55.
- ScanMail analyzes multiple keywords on one line differently than multiple keywords when each word occupies a single line. See Table 7-7 for more information about using keywords on multiple lines.

- You can also set ScanMail to search for synonyms of the actual keywords.

Situation	Example	Match / non-match
Two words on same line	bare sexy	Matches: "Click here to see bare sexy beauties." Does not match: Click here to see bare naked sexy hotties.
Two words separated by a comma	bare, sexy	Matches: "Click here to see hot, bare, sexy beauties." Does not match: "Click here to see hot, bare, and sexy beauties."
Multiple words on multiple lines	nude sexy bare naked	When you choose **Any specified keywords** Matches: "This is a nude picture" Also matches: "See young, hot, and sexy beauties" When you choose **All specified keywords** Matches: "This is a nude picture of sexy buff and bare naked" Does not match: "This is a nude picture of sexy buff bare and naked" Also does not match: "See nude, sexy, and bare naked beauties"
Many keywords on same line	sex bare nude naked buff	Matches: Click here for sex bare nude naked buff Does not match: "Click here to see sex that s bare and buff"

TABLE 7-7. Using exact matching and keywords on multiple lines

Formatting keywords that use operators

When typing a keyword or phrase that includes an operator, follow the format in the example below:

Example: `.WILD. valu*`

Note: The operator has a dot immediately preceding and following. There is a space between the final dot and the keyword.

Supported keyword	How it works	How to format the keyword
any keyword	ScanMail searches content that matches the word	Type the word and add it to the keyword list
OR	ScanMail searches for any of the keywords separated by OR For example: apple OR orange. ScanMail searches for either apple or orange. If content contains either, then there is a match.	Type ".OR." between all the words you want to include For example: "apple .OR. orange"
AND	ScanMail searches for all of the keywords separated by AND For example: apple AND orange. ScanMail searches for both apple and orange. If content does not contain both, then there is no match.	Type ".AND." between all the words you want to include For example: "apple .AND. orange"
NOT	ScanMail excludes keywords following NOT from search. For example: .NOT. juice. ScanMail searches for content that does not contain juice. If the message has "orange soda", there is a match, but if it contains "orange juice", there is no match.	Type ".NOT." before a word you want to exclude For example: ".NOT. juice"

Supported keyword	How it works	How to format the keyword
WILD	WILD means wildcard. The wildcard symbol replaces a missing part of the word. Any words that are spelled using the remaining part of the wildcard are matched. For example, if you want to match all words containing "valu", type "**.**`WILD`**.**`valu`". The words Valumart, valucash, and valubucks all match. Note: ScanMail does not support using "?" in the wildcard command ".WILD.".	Type ".WILD." before the parts of the word you want to include
REG	To specify a *regular expression*, add a **.**REG**.** operator before that pattern (for example, .REG. a.*e).	Type ".REG." before the word pattern you want to detect. For example: ".REG. a.*e" matches: "ace", "ate", and "advance", but not "all", "any", nor "antivirus"

TABLE 7-8. How to use keywords

Using Regular Expressions

Regular expressions are used to perform string matching. See the following tables for some common examples of regular expressions. To specify a *regular expression*, add a ".REG." operator before that pattern.

There are a number of Web sites and tutorials available online. One such site is the PerlDoc site, which can be found at:

`http://www.perl.com/doc/manual/html/pod/perlre.html`

Note: *Regular expressions* are a powerful string matching tool. For this reason, Trend Micro recommends that administrators who choose to use *regular expressions* be familiar and comfortable with *regular expression* syntax. Poorly written *regular expressions* can have a dramatic negative performance impact. Trend Micro's recommendation is to start with simple *regular expressions* that do not use complex syntax. When introducing new rules, use the archive action and observe how ScanMail manages messages using your rule. When you are confident that the rule has no unexpected consequences, you can change your action.

TABLE 7-9. Counting and Grouping

Element	What it means	Example
.	The dot or period character represents any character except new line character.	do**.** matches doe, dog, don, dos, dot, etc.d**.**r matches deer, door, etc.
*	The asterisk character means zero or more instances of the preceding element.	do***** matches d, do, doo, dooo, doooo, etc.
+	The plus sign character means one or more instances of the preceding element.	do**+** matches do, doo, dooo, doooo, etc. but not d
?	The question mark character means zero or one instances of the preceding element.	do**?**g matches dg or dog but not doog, dooog, etc.

Element	What it means	Example
( )	Parenthesis characters group whatever is between them to be considered as a single entity.	d**(**eer**)+** matches deer or deereer or deereereer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping "eer."
[ ]	Square bracket characters indicate a set or a range of characters.	d**[**aeiouy**]+** matches da, de, di, do, du, dy, daa, dae, dai, etc. The + sign is applied to the set within brackets parentheses, so the regex looks for d followed by one or more of any of the characters in the set [aeioy]. d[A-Z] matches dA, dB, dC, and so on up to dZ. The set in square brackets represents the range of all upper-case letters between A and Z.
[^]	Carat characters within square brackets logically negate the set or range specified, meaning the regex will match any character that is not in the set or range.	d[^aeiouy] matches db, dc or dd, d9, d#--d followed by any single character except a vowel.
{ }	Curly brace characters set a specific number of occurrences of the preceding element. A single value inside the braces means that only that many occurrences will match. A pair of numbers separated by a comma represents a set of valid counts of the preceding character. A single digit followed by a comma means there is no upper bound.	da{3} matches daaa--d followed by 3 and only 3 occurrences of "a". da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa)--d followed by 2, 3, or 4 occurrences of "a". da{4,} matches daaaa, daaaaa, daaaaaa, etc.--d followed by 4 or more occurrences of "a".

TABLE 7-10. Character Classes (shorthand)

Element	What it means	Example
\d	Any digit character; functionally equivalent to [0-9] or [[:digit:]]	\d matches 1, 12, 123, etc., but not 1b7--one or more of any digit characters.
\D	Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]	**\D** matches a, ab, ab&, but not 1--one or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.
\w	Any "word" character--that is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [_[:alnum:]]	**\w** matches a, ab, a1, but not !&--one or more upper- or lower-case letters or digits, but not punctuation or other special characters.
\W	Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^_[:alnum:]]	**\W** matches *, &, but not ace or a1--one or more of any character but upper- or lower-case letters and digits.
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[:space]]	vegetable**s** matches "vegetable" followed by any white space character. So the phrase "I like a vegetable in my soup" would trigger the regex, but "I like vegetables in my soup" would not.
\S	Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [^[:space]]	vegetable**\S** matches "vegetable" followed by any non-white space character. So the phrase "I like vegetables in my soup" would trigger the regex, but "I like a vegetable in my soup" would not.

TABLE 7-11. Character Classes

Element	What it means	Example
[:alpha:]	Any alphabetic characters	.REG. [[:alpha:]] matches abc, def, xxx, but not 123 or @#$.
[:digit:]	Any digit character; functionally equivalent to \d	.REG. [[:digit:]] matches 1, 12, 123, etc.
[:alnum:]	Any "word" character--that is, any alphanumeric character; functionally equivalent to \w	.REG. [[:alnum:]] matches abc, 123, but not ~!@.
[:space:]	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to \s	.REG. (vegetable)[[:space:]] matches "vegetable" followed by any white space character. So the phrase "I like a vegetable in my soup" would trigger the regex, but "I like vegetables in my soup" would not.
[:graph:]	Any characters except space, control characters or the like	.REG. [[:graph:]] matches 123, abc, xxx, ><", but not space or control characters.
[:print:]	Any characters (similar with [:graph:]) but includes the space character	.REG. [[:print:]] matches 123, abc, xxx, ><", and space characters.
[:cntrl:]	Any control characters (e.g. CTRL + C, CTRL + X)	.REG. [[:cntrl:]] matches 0x03, 0x08, but not abc, 123, !@#.
[:blank:]	Space and tab characters	.REG. [[:blank:]] matches space and tab characters, but not 123, abc, !@#
[:punct:]	Punctuation characters	.REG. [[:punct:]] matches ; : ? ! ~ @ # $ % & * ' " , etc., but not 123, abc
[:lower:]	Any lowercase alphabetic characters (Note : 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])	.REG. [[:lower:]] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Any uppercase alphabetic characters (Note : 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])	.REG. [[:upper:]] matches ABC, DEF, STRESS, DO, etc., but not abc, Def, Stress, Do, 123, !@#.
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)	.REG. [[:xdigit:]] matches 0a, 7E, 0f, etc.

TABLE 7-12. Pattern Anchors

Element	What it means	Example
^	Indicates the beginning of a string.	**^**(notwithstanding) matches any block of text that began with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would not.
$	Indicates the end of a string	(notwithstanding)**$** matches any block of text that ended with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would not trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would.

TABLE 7-13. Escape Sequences and Literal Strings

Element	What it means	Example
\	In order to match some characters that have special meaning in regular expression (for example, "+").	(1) .REG. C****C\+\+ matches 'C\C++'. (2) .REG. * matches *. (3) .REG. \? matches ?.
\t	Indicates a tab character.	(stress)**\t** matches any block of text that contained the substring "stress" immediately followed by a tab (ASCII 0x09) character.
\n	Indicates a new line character. NOTE: Different platforms represent a new line character. On Windows, a new line is a pair of characters, a carriage return followed by a line feed. On Unix and Linux, a new line is just a line feed, and on Macintosh a new line is just a carriage return.	(stress)**\n**\n matches any block of text that contained the substring "stress" followed immediately by two new line (ASCII 0x0A) characters.

Element	What it means	Example
\r	Indicates a carriage return character.	(stress)**\r** matches any block of text that contained the sub-string "stress" followed immedi-ately by one carriage return (ASCII 0x0D) character.
\b	Indicates a backspace character.	(stress)**\b** matches any block of text that contained the sub-string “stress” followed immedi-ately by one backspace (ASCII 0x08) character.
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).	**\x**7E(\w){6} matches any block of text containing a "word" of exactly six alphanumeric char-acters preceded with a ~ (tilde) character. So, the words ‘~ab12cd’, ‘~Pa3499’ would be matched, but ‘~oops’ would not.

Content Filtering Actions

The following table lists the actions available to ScanMail for content filtering and describes what happens when the action is performed:

When the ScanMail action is ...	ScanMail performs the following action	... and the message is
Delete entire message	deletes the entire email message	not processed further
Replace with text/file	replaces the filtered content with a text file and informs the recipient that the original content violated the content rules set by the administrator Note: When the content comes from the subject of the email message, ScanMail cannot perform the replace action.	sent to the intended recipient.
Quarantine	moves the message to the quarantine directory.	not sent to the intended recipients
Archive	moves the message to the archive directory	delivered to the intended recipient
Pass	delivers the message without triggering any action	delivered to the intended recipient

TABLE 7-14. Content filtering actions

During manual and scheduled scans, ScanMail does not support taking any action against content in the **From**, **To**, **CC**, and **Subject** fields. However, ScanMail performs the *replace with text/file* action against content filtered in the **body** or **attachment** of a message during manual and scheduled scans.

Tip: Archive messages for the first few weeks after introducing a new rule, and monitor the logs closely to assess the efficacy of your rule(s). In this way, you will be able to act quickly in case there are unanticipated consequences from your original configurations.

Screening Out Spam

ScanMail uses the following basic features to screen messages for spam:

- Approved and Blocked sender lists

  Approved and Blocked sender lists. ScanMail does not classify addresses from the Approved senders list as spam (unless it detects a phishing incident), nor does it filter messages from this list as spam. ScanMail filters addresses from Blocked senders lists and always classifies them as spam with the action depending on the rule set by the administrator.

  Note: The Exchange administrator maintains a separate Approved and Blocked Senders list for the Exchange server. If an end-user creates an approved sender, but that sender is on the administrator's Blocked Senders list, then ScanMail detects messages from that blocked sender as spam and takes action against those messages.

- A spam filter

  Administrators set the **spam detection rate** to screen out spam. Administrators can set global detection levels for all messages, or set one detection level for each category.

  The detection level determines how tolerant ScanMail will be towards suspect email messages. A high detection level quarantines the most email as spam, but it might also falsely identify and quarantine legitimate email messages as spam, creating "false positive" spam mail. A low detection level does not rigorously screen email messages, but does not create many false positive spam messages.

  See *Setting the spam detection level* on page 7-66.

- Seven spam categories

  ScanMail screens spam according to seven categories and allows administrators to specify a detection level for each category:

  - Adult
  - Commercial
  - Financial
  - Spiritual
  - Health
  - Racial
  - Others

  Example: If an administrator's clients work in a banking field, the administrator might decide to set a high sensitivity level for the "sexual" category - messages in this category are very likely to be classified as spam. However, it might be more difficult to filter "commercial" type messages. Therefore, the administrator can set a low sensitivity level for email messages in the "commercial" category.

The following are the basic steps to setting up spam screening:

Step 1: Select the **Target** tab to select the method and spam detection rate that ScanMail uses to screen for spam.

1. Select screening method and detection level.
   - Select **low**, **medium**, or **high** from the **spam detection rate** list. ScanMail uses this rate to screen all messages.
   - Click the **Specified detection level by category**. The screen expands to display seven categories of spam. Select a spam detection level for each message category that you want ScanMail to use to screen messages for spam.
2. Add addresses to your list of **Approved Senders** and **Blocked Senders**.
3. Click **Detect Phishing incidents** to have ScanMail screen out Phishing incidents.

Step 2: Select the **Action** tab to set the actions that ScanMail takes when it detects a spam message or phishing incident.

Step 3: Enable Anti-Spam.

Step 4: **Save** your changes.

Note: For detailed instructions on setting the Anti-spam options, refer to the ScanMail online help.

Using Approved and Blocked Senders

An Approved Senders list is a list of trusted email addresses. ScanMail does not filter messages arriving from these addresses for spam - except when **Detect Phishing incidents** is enabled**.** When you have enabled **Detect Phishing incidents**, and ScanMail detects a phishing incident in an email, then that email message will not be delivered even when it belongs to an approved sender list. A Blocked Senders list is a list of suspect email addresses. ScanMail always categorizes email messages from blocked senders as spam and takes the appropriate action.

There are two Approved Senders lists: one for the Exchange administrator and one for the end-users.

- The Exchange administrator uses the **Anti-Spam** page to manage his or her lists. The Exchange administrator's Approved Senders list and Blocked Senders list control how ScanMail handles email messages bound for the Exchange server.
- The end-user manages the Spam Mail folder that is created for them during installation. The end-users' lists only affect the messages bound for the server-side mailbox store for each individual end-user.

For example: The sender "user@singles.com" is on the administrator's Blocked senders list, but the end-user has added that address to his Approved senders list. Messages from that sender arrive at Exchange and ScanMail detects them as spam and takes action against them. If ScanMail takes the *Quarantine message to user's spam folder* action, it will attempt to deliver the message to the end user's Spam folder, but the message will be redirected to the end user's inbox instead because the end user has approved that sender.

Note: When you are using Outlook, there is a rule size limit for the amount and size of addresses on the list. To prevent a system error, ScanMail limits the amount of addresses that an end user can include in his or her approved sender list (this limit is calculated according to the length and the number of email addresses)

ScanMail supports wildcard matching for Approved and Blocked Senders lists. It uses the asterisk (*) as the wildcard character.

Pattern	Matched samples	Unmatched samples
john@trend.com	john@trend.com john@trend.com.	Any address different from the pattern
@trend.com *@trend.com	john@trend.com mary@trend.com	john@ms1.trend.com john@trend.com.tw mary@trend.comon
trend.com	john@trend.com john@ms1.trend.com mary@ms1.rd.trend..com mary@trend.com.	john@trend.com.tw mary@mytrend.com.tw joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com	john@trrend.com john@trend.com.tw mary@ms1.trend.comon
trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw	john@trend.com john@trend.com.tw mary@ms1.trend.com john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com
..*.trend.com *****.trend.com	The same as "*.trend,com"	
trend.com trend.com trend.*.com @*.trend.com	All invalid.	

TABLE 7-15. Email address matches for wildcards

ScanMail does not support the wildcard match on the username part. However, if you type a pattern such as “*@trend.com”, ScanMail still treats it as “@trend.com”. This feature applies to user-defined Approved Senders and Blocked Senders.

To add an approved or blocked sender:

1. Click **Anti-Spam > Target**. The Anti-Spam screen opens.
2. Add addresses or domain names to a list of approved or blocked senders
   - Type the email address or domain name in the space provided and click **Add**,

     - or -
   - Click **Import**, to import a list of approved or blocked senders.
3. Click **Save**.

Setting the spam detection level

The spam engine makes use of spam signatures and heuristic rules to screen email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. ScanMail compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, ScanMail takes action against the spam.

For example: Many spammers use many exclamation marks, or more than one consecutive exclamation mark(!!!!) in their email messages. When ScanMail detects a message that uses exclamation marks in this way, it increases the spam score for that email message.

Select one of these options for your spam detection :

- **High**: Spam score 4 or more. This is the most rigorous level of spam detection. ScanMail monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those emails that ScanMail filters as spam when they are actually legitimate emails.
- **Medium**: Spam score 5 or more. ScanMail monitors at a high level of spam detection with a moderate chance of filtering false positives.
- **Low**: Spam score 7 or more. This is the default setting. This is most lenient level of spam detection. ScanMail will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.

Setting Anti-spam action

ScanMail takes one of the following actions depending on your configuration:

- **Quarantine message to user's spam folder**

  ScanMail moves the message to the Spam Mail folder located on the server-side of the Information Store.

  This action is only available if EUQ is installed.

- **Delete entire message**

  ScanMail deletes the entire message and Exchange does not deliver it.

- **Tag and deliver**

  ScanMail adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.

Detecting and Taking Action against Phish

A Phish is an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click on a link that will redirect their browsers to a fraudulent Web site where the user is asked to update personal information such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that will be used for identity theft.

When ScanMail detects a Phish message, it can take the following actions:

- **Delete entire message**

  ScanMail deletes the entire message and Exchange does not deliver it.

- **Tag and deliver**

  ScanMail adds a tag to the header information of the email message that identifies it as phish and then delivers it to the intended recipient.

Managing the End User Quarantine Tool

During installation, ScanMail adds a folder to the server-side mailbox of each end user. You name the spam folder and set the storage time limit during the installation process. Trend Micro recommends naming the spam folder "Spam Mail". When spam messages arrive, the system quarantines them in this folder according to spam filter rules predefined by ScanMail. End users can view this spam folder to open, read, or delete the suspect email messages.

See *Setting up the Spam Folder* on page 10-4

End users can open email messages quarantined in the spam folder. When they open one of these messages, two buttons appear on the actual email message: **Approved Sender** and **View Approved Sender List**. When they click **Approved Sender**, ScanMail moves the message from that sender to their local inbox, adds the address of the message to their personal Approved Sender List and logs an entry of the event (the administrator can view this log in a report at a later time). Clicking **View Approved Sender** opens another screen which allows the end user to view and modify their list of approved senders by name or domain. When the Exchange server receives messages from the addresses on the end user's approved sender list, it delivers them to the end user's inbox, regardless of the header or content of the message.

Note: ScanMail also provides administrators with an Approved Senders and Blocked Senders list. ScanMail applies the administrator's approved senders and blocked senders before considering the end user list.

End User Quarantine housekeeping feature

The ScanMail housekeeping feature performs programmed tasks every 24 hours at the default time of 2:30 AM. It performs such duties as auto-deleting expired spam messages, recreating the quarantine folder when it has been deleted, and maintaining email message rules. The housekeeping feature is an integral part of ScanMail and requires no configuration.

Setting Up and Managing the Quarantine Folder

ScanMail quarantines email messages according to your configured actions. You can create one quarantine folder for each action. ScanMail can quarantine email messages as the result of the following:

- Virus scanning

  ScanMail quarantines email messages containing viruses, worms, Trojans, and other malicious threats. Set the quarantine folder from **Virus Scanning > Action > Backup and quarantine directories**.

- Attachment blocking

  ScanMail quarantines email messages containing infected attachments. Set the quarantine folder from **Attachment Blocking > Action**.

- Content filtering

  ScanMail quarantines email messages containing undesirable content. Set the quarantine folder from **Content Filtering> Action**.

View the quarantine folder to determine whether or not messages are safe. When you think a message is safe, delete the entire message or resend the complete email messages to the original recipients.

WARNING! *The quarantine folder contains email messages that have a high-risk of being infected. Be cautious when handling email messages from the quarantine folder so that you do not accidentally infect your computer.*

Chapter 8

Configuring and Sending Alerts and Notifications

ScanMail can send alerts to specified recipients whenever significant system events or virus outbreak events occur. Notifications are customizable and ScanMail can send them through email, SNMP, Pager, and write them to Windows event logs.

In this chapter, you will find information about:

- *Setting Notifications* starting on page 8-2
- *Configuring System Event Notifications* starting on page 8-3
- *Configuring Outbreak Alerts* starting on page 8-6

Setting Notifications

You can set ScanMail to automatically send notifications when it does the following:

- Detects and takes action against a virus or other threat detected in an email message
- Blocks an infected attachment
- Filters out undesirable content from an email message
- Detects a significant system event
- Detects virus outbreak conditions

ScanMail can notify designated individuals during real-time, manual or scheduled scanning.

About Outbreak Alerts and System Events

When ScanMail is installed, a separate "system watching" program is installed with it. The System Watcher monitors ScanMail and logs when significant system events occur or when security outbreak conditions exist.

You can configure the System Watcher to send notifications to designated individuals when significant system events or security outbreaks occur. Notifications can be sent by email, Simple Network Management Protocol (SNMP), Pager, and written to a Windows event log.

Tip: Use outbreak alerts to improve and refine your protection strategy. For example, when you receive an alert that ScanMail is detecting an excessive amount of a particular virus, you might investigate the source of the virus. If you discover that most of the viruses are sent in an excel file attachment (.xls), you might set ScanMail to block all attachments of that file type (.xls). This would provide the optimal protection to your Exchange environment and decrease the workload of the scan engine - blocked attachments do not require scanning. You could follow-up with an email to your Exchange clients to warn them not to open attachments of that type. As a final precaution, you could perform a manual scan to detect and clean that virus from your Information Store.

Configuring System Event Notifications

ScanMail provides the system events for which you can set alerts. For some system events, you can customize the conditions that trigger an alert. Click on a system event to view information about the associated notification.

The following is a list of available system events.

ScanMail services:

- **ScanMail service process started unsuccessfully**

  Select to have System Watcher send an alert when ScanMail service starts unsuccessfully.

- **ScanMail process is unexpectedly unavailable**

  Select to have System Watcher send an alert when the ScanMail main process (`SMEX _Master.exe`) stops unexpectedly.

- **Update - update is unsuccessful**

  Select to have System Watcher send an alert when the update action is not successful. Updates can fail because of network interruptions or other unexpected errors.

  See *Setting a scheduled update* on page 3-8.

- **Update - every time update is finished**

  Select to have System Watcher send an alert when the update action is successfully completed.

- **Update - last update time is older than specified time**

  Select to have System Watcher send an alert when components do not update within the specified amount of time. Set the time amount by selecting hr(s) or day(s) and typing a number in the space provided.

  For example: You set the time to be 24 hours. When ScanMail fails to perform an update within 24 hours, System Watcher sends a notification.

  Network interruptions or errors can cause Updates to be unsuccessful.

- **Manual/Scheduled scan tasks were** (unsuccessful or successful):

  Select to have System Watcher send an alert when a scan task was successful or unsuccessful.

- **Manual/Scheduled Scan time exceeds**:

  Select to have System Watcher send an alert when the scanning time exceeds the specified time limit. Set the time limit by selecting minutes or hours and typing a number in the space provided.

- **The disk space on the local drive (volume) of the backup, quarantine, and archive directory is less than**:

  Select to have System Watcher send an alert when any of the directories (backup, quarantine or archive directory) becomes less than the specified size limit.

  To set the size limit, select **MB** or **GB** and type a number in the space provided.

  You can also set System Watcher to continue to send alerts until the problem is fixed. Select **hr(s)** or **min(s)** and type a number to set a time interval. System Watcher sends a message during each time interval, until enough space is made available on the local drive

- **The size of database to keep quarantine and logs exceeds**:

  Select to have System Watcher send an alert when the size of the database for storing quarantine and log information exceeds the specified size.

  To set the size limit, select **MB** or **GB** and type a number in the space provided.

  You can also set System Watcher to continue to send alerts until the problem is fixed. Select **hr(s)** or **min(s)** and type a number to set a time interval. ScanMail sends a message during each time interval, until the size of the database is reduced.

Exchange services:

- **The SMTP messages queued continuously exceed the following number within the specified time**

  Select to have System Watcher send an alert when the number of queued SMTP messages exceeds a specified amount within a set time interval.

  To set the amount queued messages, type a number in the space provided. Set the time interval by selecting min(s) or hr(s) and typing a number in the space provided.

- **The disk space on the local drive of the transaction log is less than**:

  Select MB or GB and type a number in the space provided to set a size limit.

  ScanMail sends an alert when the disk space for storing the transaction log is less than the specified size. You can also set System Watcher to continue to send

alerts until the problem is fixed. Select hr(s) or min(s) and type a number to set a time interval.

- **The mail store size exceeds**:

  Select MB or GB and type a number in the space provided to set a size limit.

  ScanMail sends an alert when the size of the mail store exceeds the specified size. The mail store includes both the Exchange database (EDB) and the streaming database (STM). You can also set System Watcher to continue to send alerts until the problem is fixed. Select hr(s) or min(s) and type a number to set a time interval.

To send an alert notification:

1. Click **Alerts > System Events** to open the System Events screen.
2. Select the conditions for which you want to send notifications and set the parameters for each condition.
3. Click on an underlined condition to open a screen to configure the notification for that condition.
4. Set up the notification to send to the administrator:
   a. Type the name of the administrator who will receive the alert.
   b. Type the subject of the email that the administrator will receive.
   c. Select the type of information to include in the email message, by selecting from a list of predefined elements. When the administrator receives the message, ScanMail completes the missing details inside the square brackets.
5. Set up a notification to send by SNMP trap, Pager, or by writing to Windows event log:
   a. Select **SNMP** to send notification by SNMP. Add the following details about the SNMP:
      - Type the **IP address**
      - Type the **community name**
      - Select the type of information to include in the email message, by selecting from a list of predefined elements. When ScanMail sends the message, it completes the missing details inside the square brackets.
   b. Select **Pager** to send a notification by pager to the recipient.
   c. Select **Write to Windows event log** to send a notification to the Windows event log.

Configuring Outbreak Alerts

ScanMail provides the outbreak events for which you can set alerts. For each outbreak event, you can customize the specific conditions that trigger the alert. Click on an outbreak alert to view information about the associated notification.

The following is a list of available outbreak events.

- **Viruses detected exceed the following number within the shown time**:

  Set the conditions for the outbreak by setting the number of detected viruses and a duration of time. ScanMail sends an alert when the number of detected viruses exceeds this limit.

  The default value is 25 viruses detected within 24 hours.

- **Uncleanable viruses exceed the following number within the shown time**:

  Set the conditions for the outbreak by setting the number of uncleanable viruses detected and a duration of time. ScanMail sends an alert when the number of detected uncleanable viruses exceeds this limit.

  The default value is 25 uncleanable viruses detected within 24 hours.

- **Blocked attachments exceed the following number within the shown time**:

  Set the conditions for the outbreak by setting the number of blocked attachments and a duration of time. ScanMail sends an alert when the number of blocked attachments exceeds this limit.

  The default value is 25 blocked attachments detected within 24 hours.

To configure a virus outbreak alert:

1. Click **Alerts > Outbreak Alert** to open the Outbreak Alert screen.
2. Select the conditions for which you want to send notifications and set the parameters for each condition.
3. Click on an underlined condition to open a screen to configure the notification for that condition.
4. Set up the notification to send to the administrator:
   a. Type the name of the administrator who will receive the alert.
   b. Type the subject of the email that the administrator will receive.

c. Select the type of information to include in the email message, by selecting from a list of predefined elements. When the administrator receives the message, ScanMail completes the missing details inside the square brackets.

5. Set up a notification to send by SNMP trap, Pager, or by writing to Windows event log:

a. Select **SNMP** to send notification by SNMP. Add the following details about the SNMP:

- Type the **IP address**
- Type the **community name**
- Select the type of information to include in the email message, by selecting from a list of predefined elements. When ScanMail sends the message, it completes the missing details inside the square brackets.

b. Select **Pager** to send a notification by pager to the recipient.

c. Select **Write to Windows event log** to send a notification to the Windows event log.

Chapter 9

Managing Reports, Logs, and the Quarantine Folder

In this chapter, you will find information about:

- *Managing Reports* starting on page 9-2
- *Managing Logs* starting on page 9-6
- *Managing the Quarantine Folder* starting on page 9-8

Managing Reports

You can generate reports to view ScanMail log events in an organized and graphically appealing format. Reports can be printed or sent by email to a specified address.

You set how many reports you want ScanMail to save from the Report Maintenance page. When the number of reports exceeds the number you set, the excess reports are deleted beginning with the report that has been retained for the longest time.

Example: If you have 15 reports and you set 10 for the maximum number of reports to save, then ScanMail deletes the five oldest reports, leaving the 10 most recently saved reports.

Types of reports

You can generate one-time reports or scheduled reports.

- One-time reports

  Generate a one-time report to get a quick summary of ScanMail information. The Web console displays the report as soon as it is generated. You can print or email the one-time report.

  ScanMail saves generated reports in a cache so that you can view them at a later time. ScanMail retains reports until you delete them manually or ScanMail deletes them by following the report maintenance settings.

- Scheduled reports

  ScanMail generates scheduled reports according to the schedule you set. Schedules are daily, weekly, or monthly. ScanMail generates the report at the time you specify. ScanMail can be set to deliver reports by email to an administrator or other recipient.

  Scheduled reports follow a template. To generate individual scheduled reports, first set up the template. ScanMail generates reports according to that template. Specify the schedule and the content to include in each individual report for the report template. Then, at the specified time in the template, ScanMail generates a report. Each template can have many individual reports that can be viewed by clicking **List Reports** from the Scheduled Reports page. View the content of the template by clicking the template name.

Contents of a report

Reports can display content in any of the following categories or combination of categories:

- Scanning status summary

  Scanning status summary shows you information about scanning such as the number of viruses detected and the amount of uncleanable viruses, attachments blocked, the number of spam detected, and content violations.

- Virus report

  Virus reports show detailed information about the numbers and types of viruses ScanMail has detected and the actions it has taken against them. You can click on underlined labels to display detailed information on those topics. It includes graphical features showing viruses detected versus time and proportions of viruses detected versus total messages scanned.

- Attachment blocking report

  Attachment blocking reports show detailed information about the number of attachments ScanMail has blocked. It shows the Top attachments blocked by type, file name, and extension name. It includes a graph showing attachments blocked versus time.

- Content filtering report

  Content filtering reports show information about the number of messages the ScanMail has filtered. It shows the Top senders and recipients of messages that ScanMail filtered out and shows how frequently your rules are filtering content. It includes a graph showing messages filtered versus time.

- Anti-spam report

  Anti-spam reports show information about number of spam and phish detected in the total amount of messages scanned. It includes a graph showing spam messages detected by ScanMail versus time, and the amount of false positive identifications during the same time. It lists the reported false positives according to sender and domain. It shows the spam detected according to the spam detection rate for each of the spam categories.

- Traffic report

  Traffic reports show the total message count for a given hour, day, or week.

Generating, Viewing, and Sending Reports

To generate a one-time report

1. Click **Reports** > **One-time reports** to open the One-time Reports page.
2. Click **Generate report**. The page expands to display report options.
3. Type a name for the report.
4. Set the time range by typing a date or clicking the calendar icon to select a date. ScanMail gathers data to include in your report for the time range you specify.
5. Click the type of information that you want ScanMail to gather for your report. Click ▼ next to the report type to view detailed options for that report, then select the details that you want to include.
   - Scanning status summary
   - Virus report
   - Attachment blocking report
   - Content filtering report
   - Anti-spam report
   - Traffic report
6. Click **Generate**.

To view one-time reports

1. Click **Reports** > **one-time reports**. The One-time Reports screen opens, displaying a list of reports.
2. Click the **View** link of the report that you want to view from the Report column.

To generate a scheduled report

1. Click **Reports** > **Scheduled Reports** to open the Scheduled Reports page.
2. Click **Add**. The **Schedule Reports** > **Add Report** screen opens to let you set up your report.
3. Type a name for your report template.
4. Set the schedule that the template uses to generate individual reports. It can generate reports on a daily, weekly, and monthly basis.
   - Set the **Generate report at** time when the template generates the individual report.

     Note: ScanMail uses a 24-hour clock for all time settings.

For example: If you set the schedule to be weekly every Sunday and set the time for report generation to be 02:00, then ScanMail uses the template to generate an individual report every Sunday at 02:00.

5. Select the type of report that ScanMail generates according to your schedule.
   - Scanning status summary
   - Virus report
   - Attachment blocking report
   - Content filtering report
   - Anti-spam report
   - Traffic report
6. Set a person to receive a report each time the template generates one.
   - Click **Send to email:**
   - Type the recipient's email address
7. Click **Save**. The browser returns to the Scheduled Reports page. The new template is added to the list of Report templates and begins generating reports.

Deleting Reports

You can use the Report Maintenance page to set the amount of reports that ScanMail saves. For one-time reports and report templates, simply type a number. When the number of reports exceeds your specified limit, excess reports are deleted, beginning with the report that has been retained the longest amount of time. For Scheduled reports saved in each template, the number that you type limits the amount of saved reports for each template.

For example: You have five saved report templates: Report-virus, Report-spam, Report-blocking, Report-content, and Report-traffic. You set the limit for Scheduled reports saved in templates to 4. This means that each template can generate four individual reports, for a total of 20 reports (5 templates x 4 reports each). If the Report-virus template generated another report, then ScanMail would delete the oldest generated report for that template, keeping the total number of reports at 20.

Managing Logs

ScanMail keeps detailed logs of virus scanning, content filtering, attachment blocking, updates, scan events, backup. and archive. These logs provide a valuable source of system information. You can use them when analyzing your system security and configuring ScanMail to provide optimal protection for your Exchange environment.

To view log information, you must perform a log query. You can use the Log Query page to set up and run your queries. Results can be exported in the CSV file format or printed.

Setting up and running log queries

To set up and run a log query:

1. Select date range.

   Set the time range by typing a date or clicking the calendar icon to select a date. You can also set a time range. ScanMail gathers data to include in your log query from the time range you specify

2. Select query type:
   - Virus Scanning

     Query information about the number of messages scanned and the viruses detected.
   - Attachment blocking

     Query information about the amount of attachments scanned and blocked.
   - Content filtering

     Query information about the messages ScanMail filtered for undesirable content.
   - Updates

     Query information about whether components were updated successfully or not. Components include the scan engine, virus pattern file, the spam engine, the spam pattern file, and the additional threat pattern file.
   - Scan events

     Query information about whether manual and scheduled scans have been successful or unsuccessful.

- Backup

  Query information about the files that ScanMail moved to the backup folder before taking action against them.

- Archive

  Query information about the files that ScanMail moved to the archive folder.

3. Specify whether you want to query information taken from the Sender, Recipient, Subject, or Attachment file name.
4. Sort by ascending or descending order.
5. Set the number of log queries to display per page.

Deleting Logs

ScanMail provides a Log Maintenance screen where you can configure how long to keep the log files and schedule regular log maintenance.

You can perform the following maintenance tasks:

- Delete logs individually
- Delete all logs
- Schedule regular log deletion

To manually delete a log:

1. Click **Logs > Maintenance > Manual.**
2. Select the logs you want to delete.

   Select **All logs** or select **Specified logs** and then select the specific types of logs you want to delete.
3. In **Delete logs older than:**, type the number of days you want to ScanMail to retain logs.

   For example: If it is the tenth day and you type 3 days, then ScanMail deletes all logs saved on the sixth day or before.

> **Note:** To delete all logs, type "0" from the number of days you want ScanMail to retain logs.

4. Click **Delete now**. ScanMail deletes all logs older than the number of days you specified in step 3.

To automatically delete a log:

1. Click **Logs > Maintenance > Automatic.**
2. Select the logs you want to delete.

   Select **All logs** or select **Specified logs** and then select the specific types of logs you want to delete.
3. In **Delete logs older than:**, type the number of days you want to ScanMail to retain logs.

   For example: If it is the tenth day and you type 3 days, then ScanMail deletes all logs saved on the sixth day or before.
4. Click **Enable automatic maintenance**. ScanMail checks logs and automatically delete logs according to your options. ScanMail continues to delete logs everyday at 2:30 AM.

Managing the Quarantine Folder

When ScanMail quarantines a message, ScanMail sends the message to a designated quarantine folder. You can set up a separate quarantine folders for messages quarantined as a result of virus scanning, attachment blocking, and content filtering.

When ScanMail quarantines an email message, it logs the event. You can query the quarantine database to gather information about quarantined messages. See *Making Quarantine queries* on page 9-9.

Note: Do not confuse the quarantine folder with the Spam Mail folder. An administrator sets up the quarantine folder after installing ScanMail. The quarantine folder is a file-based folder. ScanMail creates the Spam Mail folder during installation. The spam folder is located in the Information Store for each user's mailbox. Whenever ScanMail does a quarantine action on an email message it sends the message to the quarantine folder. The Spam Mail folder only receives email messages as a result of an anti-spam quarantine action.

Use Quarantine to:

- Reduce the chance of important messages being deleted, if they are erroneously detected by aggressive filters
- Review messages that trigger content filters to determine the severity of the policy infraction
- For disciplinary purposes, maintain evidence of an employee's continued misuse of your company's messaging system

WARNING! *The quarantine folder contains email messages that have a risk of being infected. Be cautious when handling email messages from the quarantine folder so that you do not accidentally infect your computer.*

Making Quarantine queries

To view information about quarantined messages, you must make a quarantine query. Use the **Quarantine > Query** to set up and run your queries. Results can be exported in the CSV file format or printed.

To set up and run a quarantine query:

1. Select date range.

   Set the time range by typing a date or clicking the calendar icon to select a date. You can also set a time range. ScanMail gathers data to include in your query from the time range you specify
2. Select query reasons
   - Select All reasons to query information about virus scanning, attachment blocking, and content filtering.
   - Select Specified types and then click virus scanning, attachment blocking, and/or content filtering to query only those reasons
3. Select the Resend Status of the messages you want to query.
4. Specify whether you want to query information taken from the Sender, Recipient, or Subject part of messages.
5. Sort by ascending or descending order.
6. Set the number of quarantine queries to display per page.

Resending quarantined messages

You can resend messages that you consider to be safe to the original recipient. When you resend messages, the entire email message is resent.

To resend quarantined messages:

1. Click **Quarantine** > **Query**.
2. Set up and run a query for the kind of message you want to resend. The query runs and displays a the results at the bottom of the screen.
3. Select the email messages that you want to resend from the results of your query.
4. Click **Resend**. The **Quarantine** > **Resend** screen opens displaying resending options.
5. Click **Add original recipients** to have ScanMail send the email message to the original recipient.
6. Type an email address in the **Fw** field. ScanMail will send the quarantined message to the person at this email address in addition to - or instead of - the original recipient.
7. To append the original email message:
   - Click **Append the original email subject**. This has ScanMail include the message that appears in the subject line when it resends the message.
   - Type a new subject for the resent email in the **Subject** field or do nothing to accept the default. The default subject line cautions the recipient about opening a resent message.
8. Type a message in the **Body** field for ScanMail to use as the body of your resent email message.
9. Click **Delete all related quarantined files after resend completes** to have ScanMail delete the original quarantined message after it is resent. By default email messages are not deleted when they are resent (the check-box is clear).
10. Click **Resend Now**. ScanMail sends the email message immediately. A progress bar appears to show you the progress of the Resend process.
11. When the Resend process is complete, click **OK** to return to the Quarantine Query screen.

Note: Automatically deleting messages after resending deletes the quarantine record in the database.

Deleting Quarantined Messages

ScanMail provides a Quarantine Maintenance screen where you can configure how long to keep the quarantined messages and schedule regular maintenance.

To manually delete quarantine files:

1. Click **Quarantine > Maintenance > Manual.**
2. Select the messages you want to delete:
   - **All quarantined files**
   - **Quarantined files that have never been resent**
   - **Quarantined files that have been resent at least once**
3. Type the amount of days you want ScanMail to retain files. Files that are older than this amount of days will be deleted.

   For example: If it is the tenth day and you type 7 days, then ScanMail deletes all files saved on the second day or before.

   The default is to keep the files 30 days before allowing deletion.
4. Click **Delete now**. ScanMail deletes all files older than the number of days you specified in step 3. ScanMail also deletes the related quarantine records in the database.

To automatically delete quarantine files:

1. Click **Quarantine > Maintenance > Automatic.**
2. Select the messages you want to delete:
   - **All quarantined files**
   - **Quarantined files that have never been resent**
   - **Quarantined files that have been resent at least once**
3. Type the amount of days you want ScanMail to retain files. Files that are older than this amount of days will be deleted.

   The default is to keep the files 30 days before allowing deletion.
4. Click **Enable automatic maintenance**. ScanMail begins to automatically delete all messages older than the number of days you specified in step 3. ScanMail also deletes the related quarantine records in the database. It continues to do this every day until automatic maintenance is disabled.

Chapter 10

Administrative Tasks

In this chapter, you will find information about:

- *Setting the Proxy Server* starting on page 10-2
- *Notification Settings* starting on page 10-2
- *Setting up the Spam Folder* starting on page 10-4
- *Understanding Product License Information* starting on page 10-6
- *Participating in World Virus Tracking* starting on page 10-8
- *Generating Debugger Reports* starting on page 10-10

Setting the Proxy Server

Most enterprises use proxy servers for added security and more efficient use of bandwidth. If your system uses a proxy server, configure the proxy settings to connect to the Internet and download updated components necessary to keep ScanMail updated and check the license status online.

The following features use Proxy servers:

- ActiveUpdate
- Product Registration
- World Virus Tracking

To set the Internet proxy:

1. Open the ScanMail Web console.
2. On the sidebar, click **Administration** > **Proxy**. The **Proxy** screen appears.
3. Select **Use a proxy server for update and product license notification**.
4. Type the server name or IP address of the proxy server and its port number.
5. If required, select Use **SOCKS 5 proxy protocol**.
6. If your proxy server requires a password, type your user name and password in the fields provided.
7. Click **Save** to save your settings.

Notification Settings

You can configure ScanMail to send notifications when it takes actions against various security threats. Usually, notifications are sent to the Exchange administrator. Use **Administration > Notification Settings** to set a global default for the administrator's email address.

Notifications can be set up for the person who is to receive the notification and the person who is listed as the sender for the notification. That is, when ScanMail sends notifications, it lists the address that you set up in this screen as the sender of the message. People receiving the message can contact the sender that you describe about the problem.

Setting a global default address for an administrator and applying the address, changes the address in the following locations:

- Virus Scanning
- Attachment Blocking
- Content Filtering
- System Alerts
- Outbreak Alerts

Note: You can customize the notification addresses for each of these locations after you apply a default address.

To set a global default address for the Administrator Notification:

1. Click **Administration > Notification Settings** to open the Notification Settings page.
2. Type the email address that ScanMail notifies for all notifications.
3. Click **Apply All**. The administrator's email address is updated. ScanMail sends all notifications to the address that you described.
4. Click **Save** to save the email address for the Administrator Notification, otherwise the field will retain the default value, even after you click **Apply All**.

ScanMail divides email traffic into two network categories: internal and external. ScanMail queries the Exchange server to learn how the internal and external addresses are defined. All internal addresses share a common domain and all external addresses do not belong to that domain. For example, if the internal domain address is "@trend_1.com", then ScanMail classifies addresses such as "abc@trend_1.com" and "xyz@trend_1.com" as internal addresses. ScanMail classifies all other addresses, such as "abc@trend_2.com" and "jondoe@123.com" as external.

You can also set up global SNMP notifications from this screen. ScanMail sends notifications for all events to the SNMP address you describe in this screen.

To set a global SNMP notification:

1. Click **Administration > Notification Settings** to open the Notification Settings page.
2. Type an IP address and Community name in the space provided under SNMP.
3. Click **Apply All**. ScanMail sends all notifications to the IP address and community that you described.
4. Click **Save** to save the SNMP information, otherwise the field will retain the default value, even after you click **Apply All**.

Setting up the Spam Folder

The Spam Maintenance page displays the name of the Spam Folder and the number of days that the End User Quarantine (EUQ) tool retains spam messages. End users can rename the spam folder using Microsoft Outlook. ScanMail identifies the folder by ID, not by folder name.

You can set the following features from this page:

- Disable the End User Quarantine tool

  Clear **Enable End User Quarantine** to disable the End User Quarantine tool for all mailboxes.
- Disable the End User Quarantine tool for one or more individual users

  This disables the End User Quarantine tool for each user you add to the **User List Settings**.
- Create a new Spam Folder

  Create a new spam folder for each new user that you add to the Exchange server where you have installed the End User Quarantine tool. Clicking **Create spam folder and delete spam messages** immediately creates the spam folder for the new user.
- Modify the amount of days that ScanMail will retain spam messages

See *Managing the End User Quarantine Tool* on page 7-68 for more information about the End User Quarantine tool.

To create the spam mail folder:

1. Click **Administration > Spam Maintenance**.
2. Select **Enable End User Quarantine tool**.

3. Do one of the following:
   - Click **Create spam folder and delete spam messages**.
   - Click **Save**.

To reset the storage time limit using:

1. Click **Administration > Spam Maintenance**.
2. Type the number of days you want ScanMail to retain the spam in the field next to **Delete spam messages older than:** (the default value is 14 days and the maximum time limit is 30 days).
3. Click **Save** to save your change and close the screen.

To disable an individual end-user's EUQ spam folder:

1. Click **Administration > Spam Maintenance**.
2. Under **User List Settings**, type the email address of the end-user for whom you want to disable EUQ.
3. Click **Add**. The end-user's email address is added to the list of addresses that have EUQ disabled. To remove an end-user from the list and restore EUQ service, select the end-user's email address from the list and click **Remove**.
4. Click **Save**.

Understanding Product License Information

To view information about the current license for ScanMail, click **Administration** > **Product License**. The Product License screen opens and displays details about your license. Depending on the options you chose during installation, you might have a fully licensed version of ScanMail or an evaluation version. In either case, your license will expire after a period of time as specified in your maintenance agreement. You can use the Product License screen to find out in advance when you license will expire.

See *Registering and Activating ScanMail* on page 3-2, for more information about activating or renewing your license.

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees.

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

Note: The Maintenance Agreement expires. Your License Agreement does not.

When your License Expires

When your license expires, ScanMail continues to protect your Exchange servers in a very limited manner. See Table 10-1 for a list of features available to ScanMail according to the license type and expiration. Trend Micro recommends that you keep your license activated at all times. If your license expires, obtain a new Activation Code or renew your expired license immediately.

TABLE 10-1. Available ScanMail features

	Suite - full version	Suite - trial version	Standard - full version	Standard - trial version
Management Console	Enabled	Enabled	Enabled	Enabled
Virus Scanning and Attachment Blocking	Enabled	Enabled *	Enabled	Enabled *
Anti-spam and Content Filtering	Enabled	Enabled *	N/a	N/a
ActiveUpdate	Enabled *	Enabled *	Enabled *	Enabled *

* These functions are disabled when the maintenance agreement expires.

Tip: You can view the expiry date from the Web management console Summary page (which is the first page that displays when you open the Web management console,). Click more info to see the details about your license. Click **Administration** > **Product License** to view and renew your current licenses. Trend Micro recommends that you keep your license agreement activated at all times.

Renew ScanMail Maintenance Agreement

When you purchase ScanMail you receive a product license. The license entitles you to standard support which consists of one year of virus pattern updates, product version upgrades, and telephone and online technical support. When your license expires, ScanMail can only protect your Exchange servers in a very limited way.

You cannot renew your license if you are changing from the Standard version of ScanMail to the Suite version of ScanMail. Instead, you must change your version by obtaining a new Activation Code.

To renew the product license:

1. Contact your Trend Micro sales representative or corporate reseller to renew your license agreement.
2. The representative will update your ScanMail registration information using Trend Micro Product Registration.
3. ScanMail polls the Product Registration and receives the new expiry date directly from the Product Registration server. You are not required to manually enter a new Activation Code when renewing your license.

Note: Click **Update License** to have ScanMail update the licensed information immediately based on it's latest poll of the Product Registration server.

Reactivating an Activation Code

You may need to reactivate ScanMail if you want to change your Standard version to a Suite version. Reactivating involves changing your Activation Code from one number to another. When you click **Reactivate**, you can type your new Activation Code and receive all the benefits of the ScanMail version that it matches.

Participating in World Virus Tracking

You can send virus scanning results from your ScanMail installation to the World Virus Tracking Program to better track trends in virus outbreaks. Your participation in this program can benefit the attempt to better understand the development and spread of virus infections. The ScanMail installer asks you whether or not you want

to participate in the World Virus Tracking Program; however, you can change this setting at any time.

To save Virus Tracking Program participation settings:

1. On the sidebar, click **Administration** > **World Virus Tracking**. The World Virus Tracking Program screen appears.
2. Read the disclaimer and click **Yes** to participate in the World Virus Tracking Program or click **No** to decline participation.
3. Click **Save**.

To view the current Trend Micro virus map, click Virus Map or enter the following address in your Web browser:

http://www.trendmicro.com/map

Generating Debugger Reports

ScanMail Debugger can assist you in debugging or just reporting the status of the ScanMail processes. When you are having unexpected difficulties you can use debugger to create debugger reports and send them to Trend Micro technical support for analysis.

How it works

Each ScanMail module inserts messages into the program, and then records the action into log files upon execution. You can forward the logs to Trend Micro Technical Support staff to help them debug the actual program flow in your environment. All of the modules produce text files you that you can view with any text editor.

You can use the debugger to generate logs on the following modules:

- ScanMail for Microsoft Exchange Master Service
- ScanMail for Microsoft Exchange Remote Configuration Server
- ScanMail for Microsoft Exchange System Watcher
- Virus Scan API (VSAPI)
- Simple Mail Transfer Protocol (SMTP)
- Common Gateway Interface (CGI)
- End User Quarantine (EUQ)

By default, ScanMail keeps the logs in the following directory:

```
c:\Program Files\Trend Micro\SMEX\Debug
```

To generate reports using the ScanMail Debugger:

1. Click **Administration > Trend Support/Debugger**.
2. Select the check boxes of the modules that you want to debug.
3. Click **Apply** to start collecting data for the module(s) that you have selected.

Note: ScanMail Debugger continues to collect debug data until you clear all items you were debugging and click **Apply**.

Chapter 11

Getting Support and Contacting Trend Micro

This chapter discusses how to perform miscellaneous administrator tasks as well as how to get technical support.

In this chapter, you will find information about:

- *Contacting Technical Support* starting on page 11-2
- *TrendLabsSM* starting on page 11-4
- *Known Issues* starting on page 11-5
- *Frequently Asked Questions (FAQ)* starting on page 11-11

Contacting Trend Micro

Trend Micro Incorporated has its world headquarters at:

Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku, Tokyo 151-0053 Japan.

In the United States, Trend Micro is located at:

10101 N. De Anza Blvd.
Cupertino, CA 95014-9985
Tel: +1-408-257-1500
Fax: +1-408-257-2003

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

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

Note: The information on this Web site is subject to change without notice.

The Trend Micro Web site has a wealth of sales and corporate information available.

- Corporate information includes our company profile, international business office contacts, and partnering and alliance information.
- Sales information includes product evaluation information and trial downloads, reseller contacts, and virus research information.

Contacting Technical Support

There is an abundance of security information and support available through the Web site. You can find the following:

- Downloadable product upgrades, component updates and hot fix patches
- Security advisories on the latest virus outbreaks
- Downloadable trial versions of Trend Micro products
- Expert advise on specific viruses in the wild and computer security in general
- An encyclopedia of computer security information, white papers, and virus statistics

- Free downloadable software for virus scanning, web feeds, and security testing

To contact Trend Micro technical support:

1. Visit the following URL:
   `http://kb.trendmicro.com/solutions/`
2. Click the link for the region you want to contact and follow the instructions for contacting support in that region.

You can find Trend Micro contacts in the following regions:

- Asia/Pacific
- Australia and New Zealand
- Latin America
- United States and Canada.

Before contacting Technical Support

While our basic technical support staff is always pleased to handle your inquiries, there are a couple things you can do to quickly find the answer you are seeking.

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

  The documentation set for this product includes the following:

  Administrator's Guide. The Administrator's guide introduces ScanMail and provides instructions for upgrading and installing. It explains the major features of ScanMail and guides you in configuring the product to provide optimal protection for your Exchange servers. The latest version of the Administrator's Guide is available in electronic form:

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

  Online help—The purpose of online help is to provide conceptual and procedural information. Online help is accessible from the ScanMail Web management console.

  Readme file—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and release history.

  Knowledge Base

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

This site contains the most up-to-date information about all Trend Micro products. Other inquiries that were already answered are also posted and a dynamic list of the most frequently asked questions is also displayed.

- To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:
  - Product serial number
  - ScanMail program, scan engine, pattern file, version number
  - OS name and version
  - Internet connection type
  - Exact text of any error message given
  - Steps to reproduce the problem

TrendLabs[SM]

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Irvine, CA, to mitigate virus outbreaks and provide urgent support.

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.

Known Issues

Known issues document unexpected ScanMail behavior that might require a temporary workaround.

The following are known issues for ScanMail 7.0:

- Apache service issue
- EUQ 1.0 upgrade to EUQ 1.1 issue
- Uninstallation issue
- Internal or external sender/recipient confusion
- Cluster - installation issue
- Cluster - Add new virtual server issue
- Cluster Failover issue
- All manual scan and scheduled scan tasks on the node stop due to real-time filter status change
- All virtual servers on a node write to the same debug log
- Resending a quarantine message fails
- Cannot view child domain servers from server management console
- Scanning conflict with ServerProtect
- Unexpected CGI error message appears when a manual scan is in progress
- ScanMail does not deliver pager notifications for System Event and Outbreak Alert
- Cannot log on to the console after updating with an Internet Explorer patch
- ScanMail delivers an email message containing unreadable information

Trend Micro recommends always checking the Readme file for information about system requirements and known issues that could affect installation or performance. Readme files also contain a description of what's new in a particular release, and other helpful information.

The latest known issues and possible workarounds can also be found in the Trend Micro Knowledge Base:

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

Apache service issue

If Apache Web Server 2.0 was installed previous to installing ScanMail 7.0, then ScanMail 7.0 cannot support SSL function on Apache Web Server 2.0, and you cannot change the listening port for the Web management console.

EUQ 1.0 upgrade to EUQ 1.1 issue

The log on privileges of EUQ 1.0 complicates upgrading to EUQ 1.1 from EUQ 1.0. To ensure a successful upgrade do the following:

1. Log on to your computer using the same log on account that you used when you installed EUQ 1.0.
2. When running the ScanMail installation program, you are prompted to type an account for installing EUQ. You must type the same account that you used when you installed EUQ 1.0. Otherwise, you will install two versions of EUQ on the same server, causing conflicts.

If you have already installed EUQ 1.0 and you want to remove it before doing a fresh install, you must use the same log on account that you used when you installed EUQ 1.0 for the first time. When you remove EUQ 1.0, the upgrade to EUQ 1.1 proceeds without complication.

Uninstallation issue

Uninstalling ScanMail 7.0 using the Windows Add/Remove Programs tool does not uninstall EUQ. You must uninstall EUQ manually using the Add/Remove Programs tool.

Internal or external sender/recipient confusion

You can only define one domain as the internal address for ScanMail. If you use Exchange System Manager to change your primary address on a server, ScanMail does not recognize the new address as an internal address because ScanMail cannot detect that the recipient policy has changed. If you restart ScanMail service, then the new policy will work.

For example:

You have two email addresses for a domain: @trend_1.com and @trend_2.com. You set @trend_1.com as the primary address. ScanMail considers email messages with the primary address to be internal (that is, abc@trend_1.com, or xyz@trend_1.com are internal). Later, you use Exchange System Manager to change the primary address to @trend_2.com. This means that Exchange now recognizes addresses such as abc@trend_2.com and xyz@trend_2.com to be internal addresses. However, ScanMail still considers these addresses to be external.

Cluster - installation issue

The Web console cannot be opened. This happens when you are running Windows Server 2003, using the IIS Web server, and you selected "Default Web Site" using port 80 instead of "Virtual Web Site" during installation. Trend Micro recommends selecting "Virtual Web Site" during installation when using IIS Web server.

Cluster - Add new virtual server issue

If you add a virtual server to a node on a cluster where ScanMail is already installed, you cannot install ScanMail on the newly added virtual server. ScanMail considers this to be the same as doing a same build upgrade and cannot support this. To install to the newly added virtual server, you must first create the ScanMail resource manually. See *Manually Creating a ScanMail Resource for Virtual Servers* on page 4-10.

Cluster Failover issue

Manual scan or Scheduled scan tasks being performed by one virtual server on a node will stop when another server on the same node is having a failover.

For example: virtual servers A, B, and C are all on node 1. If virtual server A is in failover, then the tasks being performed on virtual servers B and C will stop.

All manual scan and scheduled scan tasks on the node stop due to real-time filter status change

Enabling or disabling the Virus Scanning, Attachment Blocking, or Content Filtering filters affects the status of the virtual servers. All manual scan and scheduled scan tasks on the node stop when the following events happen:

- When Real-time scanning is enabled and you disable all of the scanning filters on one virtual server on a node
- When Real-time scanning is disabled and you enable any of the scanning filters (except the anti-spam filter) on one virtual server on a node

All virtual servers on a node see the same debug log setting

All virtual servers on a node see the same debug log setting because the debug log is node based. There is only one debug log generated for one node.

Resending a quarantine message fails

This can happen when the system mailbox on the Exchange server environment does not exist. The administrator should modify the following three values in the registry (you can modify the value by simply adding any data to it):

```
HKEY_LOCAL_MACHINE > software > ScanMail for Exchange >
CurrentVersion
```

- `ResendMailbox`

  (the mailbox name that exists in the Exchange domain, for example "administrator")
- `ResendMailboxDomain`

  (the Domain where ScanMail exists, for example "yourcompany.com")
- `ResendSender`

  (the account that exists in Exchange domain, for example "administrator@yourcompany.com")

Cannot view child domain servers from server management console

When using the server management console and viewing servers on a parent domain, the servers from the child domain do not display. This occurs because the parent domain does not have the required permissions to view the child domain. To resolve the problem, do the following:

For Windows 2003 operating system:

1. Execute `regedit`.
2. Go to:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winReg
   ```

3. Right click winReg > Permissions
4. Add 'Smex Admin Group' of target domain, and enable 'Allow Read'

For Windows 2000 operating system:

1. Execute `regedt32`
2. Go to

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winReg
   ```

3. Click winReg
4. Select winReg > Security > Permissions
5. Add 'Smex Admin Group' of target domain, and enable 'Allow Read"

Scanning conflict with ServerProtect

When ScanMail is installed on the same server as Trend Micro ServerProtect, a scanning conflict can occur. To resolve this issue, manually add the ScanMail folders to an exclusion list from the ServerProtect management console.

Unexpected CGI error message appears when a manual scan is in progress

An unexpected CGI error message may appear when a manual scan is in progress and the user clicks the manual scan link from console several times. To resolve this issue, open another screen in the management console and then return to the Manual Scan screen. The screen will refresh and the CGI error message will disappear. The false CGI error message does not disrupt the manual scan and it will progress normally.

ScanMail does not deliver pager notifications for System Event and Outbreak Alert

When more than one pager notification triggers at the same time, only one of them will succeed. This is because only one thread can access the `com` port at one time. When the `com` port is occupied by one alert, the other alerts cannot access the port. This condition persists until the port is free.

Cannot log on to the console after updating with an Internet Explorer patch

If there is an underscore (_) in the server name and a user adds an Internet Explorer patch for security (IE6 with SP1 or IE5.5 with patch), then you cannot log on the web console with the server name.

For example: `http://trend_micro:16372/smex/login.htm`

The Microsoft cookie doesn't work for the special name in this patch.

Refer to the document provided by Microsoft.

`http://support.microsoft.com/default.aspx?scid=kb;EN-US;q312461`

You can resolve this problem by using Internet Explorer and typing the IP address or by using Netscape to connect to the web console.

ScanMail delivers an email message containing unreadable information

This only happens in cluster environments. In a cluster environment, each virtual server has it own SMTP server instance. The Exchange server will choose one SMTP server instance to be the master SMTP server instance for a node. Normally, the SMTP server instance processes email messages containing detected threats and passes them to an event sink for ScanMail to delete or quarantine. However, in cluster environments the master SMTP server instance interferes with this process and prevents ScanMail from performing the delete or quarantine action on the email message. Consequently, the email message is delivered to the end user's inbox containing some unreadable information. The email will be unreadable, but not damaging.

As a side effect, ScanMail will record incorrect information in the log. It will report that the email message was deleted or quarantined, but it actually was passed to the original recipient. Another effect is the email messages that ScanMail falsely records as quarantined cannot be correctly resent.

Frequently Asked Questions (FAQ)

Logging on to the Web console

When I try to log on to the Web console, the log on fails. The screen displays a message explaining that the specified virtual server is currently off-line, but the Cluster management console shows that the virtual server is on-line. What can I do to log on?

Please use the Cluster management console to take the ScanMail For Exchange Cluster Agent Resource off-line then bring it on-line again. The web console can be used again.

Virtual server does not display

After manually creating a resource, I access the ScanMail Web management console from the Start menu, but the virtual server that I created the resource in was not displayed on the server list. What can I do to see the new virtual server on the list?

The server list in ScanMail 7.0 is static. You must modify the server list by editing the source file directly.

To edit the source file:

1. Go to : `<SMEX directory>\web\VirtualServerList.htm`
2. Open VirtualServerList.htm by NotePad or other text editor.
3. Add the following string in the server list.

```
<tr><td height="18"><li><a
href="http://WAP5:16372/smex/login.htm">WAP5</a></li></td></tr>
```

4. Save the file.

In the above string, “Wap5” is the virtual server Network name.

After I installed ScanMail 7.0 with End User Quarantine (EUQ), the older version End User Quarantine 1.0 wasn't removed successfully. Now, there are two versions of End User Quarantine on my server, how can I solve this problem?

To remove the older version of EUQ:

1. Open the **Administrative Tools > Services**.
2. Select **EUQ_Setup** service. From Properties, change its startup type to **Disabled**.
3. Log on the computer using the user the same account you used to log on when you installed EUQ1.0.
4. Open **Control Panel > Add or Remove Programs**. You will see two identical items named Trend Micro End User Quarantine. To find out the version for each one, click the **support information** link.
5. Click **Remove** to remove End User Quarantine 1.0.
6. After removing EUQ, manually remove the shortcuts that were associated with it from file system. By default, shortcuts are found in the following directory path:

   ```
   C:\Documents and Settings\LogonUserAccount\Start
   Menu\Programs\Trend Micro End User Quarantine
   ```

7. Change the startup type of **EUQ_Setup** service to Manual.

This procedure removes the older version or EUQ. The newer version of EUQ will now function normally and you will be able to configure it through Web management console successfully.

When I try to uninstall ScanMail7.0 with End User Quarantine (EUQ) an error message displays. The message says, "This action is only valid for products that are currently installed". How can I uninstall ScanMail?

Run the uninstallation again. You must log on to your computer using the same account that you used when you installed EUQ. You must also use the same log on account when the Setup program prompts you to enter the log on for the target servers.

When I connect to a ScanMail server using a terminal server connection I cannot find "SMEX Real Time Count" object in the performance counter. How can I open the object on a terminal server connection?

There are two ways to do that.

- Use console mode from a terminal server connection. (Add `"/console"` argument to run remote desktop connection).
- Input IP address in "Select counters from computer" to open performance counter monitor.

I opened my Approved Sender List, but it looks just like a normal email message, not an Approved Sender List form. How can I recover my Approved Sender List?

This problem is probably caused when Outlook caches old forms.

To recover your Approved Sender List, do the following:

1. Close Outlook and delete the cache files which are cached by Outlook.

   The default path is:

   ```
   C:\Documents and Settings\UserName\Local Settings\Application Data\Microsoft\FORMS
   ```

2. Open the Approved Sender List.
3. Open a spam message and click **View Approved Sender** List, or
4. Double-click the **Approved Sender List** folder underneath the Spam Folder

---

Note: If you execute step 1 and 2 and you still cannot recover your Approved Sender List, delete the Approved Sender List manually. EUQ housekeeping will recover your spam folder. After EUQ has recovered your spam folder, open the Approved Sender List using the instructions in step 2, above.

I cannot see the Approve Sender and the Approved Sender List buttons when I open my spam mail.

This problem is probably caused when Outlook caches old forms.

To recover your buttons:

1. Close Outlook and delete the cache files which are cached by Outlook.

   The default path is:

   ```
   C:\Documents and Settings\UserName\Local Settings\Application Data\Microsoft\FORMS
   ```

   This path is for reference only. Each user will have a different path depending on your unique environment.
2. Open the spam mail folder and double-click on a spam mail.

Note: Note: If you execute step 1 and 2 and you still cannot recover your buttons, delete the spam folder manually. EUQ housekeeping will recover your spam folder. After EUQ has recovered your spam folder, open a spam mail by following the instructions in step 2, above.

I cannot open the Web management console after I installed ScanMail 7.0. How can I connect to the Web management console?

1. Check that your Web server is functioning normally.
   - For IIS Web Server, open the **Administrative Tools > Internet Services Manager** to check if your web sites are started.
   - For Apache Web Server, open the **Administrative Tools > Services > Apache2** to check if the Apache service is started.
2. Check if ScanMail 7.0 was configured successfully on the Web server. See *If you selected to install ScanMail on an IIS server:* on page 2-25.
   - If you installed ScanMail on a IIS Web server
     - For a virtual web site, verify that you have correctly configured the TCP port number and SSL port number. The default value ports are: 16372 for default listening port, and 16373 for the SSL port.

- For default web site, verify that you have correctly configured the TCP port number and SSL port number. The default value ports are 80 for the web site and 443 for SSL.

  If the value for these ports changed, please add the port info in the URL for Web management console manually when you need to connect to the Web management console. (Such as http://ServerName:8080/smex/).

- If you installed ScanMail on Apache

  Open "httpd.conf" in the configuration file to check if “# SMEX Virtual Path” section is installed and configured correctly. Verify that the listening port and SSL port are correct.

Note: If Apache Web Server 2.0 was installed previous to installing ScanMail 7.0, then ScanMail 7.0 cannot support SSL function on Apache Web Server 2.0, and you cannot change the listening port for the Web management console.

When I run the installation program, I have problems with the Web Management Console Administrator Account step. How can I prepare the Web Management Console Administrator Account so that I can successfully install ScanMail?

Verify that you are logged on with the correct account and that you have the appropriate privileges. You input your account on the “Log On” screen of the Setup program. You must log on with an Administrator account with Domain Admin privilege. This is necessary to be able to create the account and “SMEX Admin Group” group in the Active Directory.

If you do not have Domain Administrator privileges, you must do the following manually before you launch the Setup program:

1. Manually create an administrative group and account:
   a. Manually create an administrative security group named "SMEX Admin group" on the Active Directory.
   b. Assign a domain user account to this group for each person who will need to log on and manage ScanMail servers.

2. On the **Web Management Console Administrator Account** screen, select **Specify an existing account from Active Directory**.
3. After you select the account, Setup displays a screen on which you can type the domain user account that you prepared in advance.

How come EUQ does not work after I move my mailbox to another Exchange server?

After moving your mailbox from one Exchange server to another, housekeeping must be performed so that EUQ can work properly.

What's the filtering process for anti-spam?

ScanMail anti-spam applies the following filters in the order as shown below:

i. Phishing
ii. Approved senders
iii. Blocked senders
iv. Spam

After using Server Management to replicate a server, why does the replication page show the previous result, not the current result?

This is the timing issue. The Web page displays before the replication process completes. Most of time this situation will not happen. To get the correct result, refresh the page by switching to another page and then switching back, the result of last replication will become current.

How can I replicate quarantine module configurations to other servers? I can't find an options to select for the quarantine on the Server Management screen > Replication.

The replication for quarantine module is included in the module of logs. To replicate the quarantine module to other servers, select **Logs** for the server that you want to replicate.

I can't see servers in a child domain from the management console of servers in a parent domain and vice versa, why?

This occurs because the parent domain does not have the required permissions to view the child domain. To resolve the problem, do the following:

For Windows 2003 operating system:

1. Execute `regedit`.
2. Go to:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winReg
   ```

3. Right click winReg > Permissions
4. Add 'Smex Admin Group' of target domain, and enable 'Allow Read'

For Windows 2000 operating system:

1. Execute `regedt32`
2. Go to

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winReg
   ```

3. Click winReg
4. Select winReg > Secutiry > Permissions
5. Add 'Smex Admin Group' of target domain, and enable 'Allow Read"

How does ScanMail obtain server information about other servers in the same domain? Does this consume a lot of network bandwidth?

The server management module keeps an updated ScanMail Server list by querying the exchange servers info from the Active Directory. This method does not consume a lot of network bandwidth.

For Quarantine, I select some records and click Resend, but ScanMail returns a failure.

If there is no system mailbox in Exchange mail store, the resend mechanism will fail. This is because ScanMail uses a system mailbox to resend mail by default.

How can I check if system mailbox exists?

Use the Exchange System Manager (ESM) to check this as follows:

1. Select a target server to view the mailbox store of the ScanMail server.
2. View the mailbox.
3. Check to see if the system mailbox exists.

If the system mailbox doesn't exist, the mail administrator can assign another mailbox and then resend will succeed.

This can happen when the system mailbox on the Exchange server environment does not exist. The administrator should modify the following three values in the registry (you can modify the value by simply adding any data to it):

```
HKEY_LOCAL_MACHINE > software > ScanMail for Exchange >
CurrentVersion
```

- `ResendMailbox` (the mailbox that exists in the Exchange domain)
- `ResendMailboxDomain` (the Domain where ScanMail exists)
- `ResendSender` (the account that exists in Exchange domain)

Why does ScanMail use the wrong settings for internal and external senders/recipients?

Unless otherwise specified, ScanMail decides if an address is from an internal or external sender according to the recipient policies of the Exchange server. This is the **Internal Mail Definition Default** setting found at **Administration > Notification Settings**. ScanMail only uses the eMail Addresses which are set under **Primary** in the Recipient Policy for "internal" and all others as "external".

When an Exchange administrator changes the eMail Policy, ScanMail still uses the older settings. This happens because ScanMail will load the policy from Exchange System Manager when starting ScanMail service.

To avoid this problem, restart the ScanMail service whenever you change the Exchange recipient policy

Why does Server Management fail to return a list of servers on my domain?

Sometimes when you select an option from the Server Management screen, the Server Management does not display a list of servers that match those options. To correct this problem, restart "ScanMail for Microsoft Exchange Remote Configuration Server" service.

If restarting the service does not solve your problem, verify that there is no network problem. If the network is working and restarting the service fails, it is probably because the domain account password of the "ScanMail for Microsoft Exchange Remote Configuration Server" changed. To resolve the problem, try using Exchange System Manager to set the account and change the password so that the password never expires.

Why do my Manual scans and Schedule scans stop unexpectedly?

Scans can sometimes be interrupted by the following actions:

- A component such as the engine or pattern file downloads during the scan.
- You disable “Virus Scanning”, “Attachment Blocking”, and “Content filter” when ScanMail is scanning.
- You stop SMEX_Master service when the scan is running.

Why can’t I log on to the ScanMail Web management console? I receive a message that "RPC server is unavailable".

Open the Service Management console. Check if the service "ScanMail_Master" service is started. If the service is not started, please restart "ScanMail_Master" service.

For compressed files, how can I calculate the "x" value and use it effectively for the option "Size of decompressed file is "x" times the size of compressed file"?

This function prevents ScanMail from scanning a compressed file that might cause a Denial of Service (DoS) attack. A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing ScanMail from scanning files that decompress into very large files helps prevent this problem from happening.

Example: For the table below the ratio, or "x" value, is 100

File size (not compressed)	File size (compressed)	Result
500 KB	10 KB (ratio is 50:1)	Scanned
1000 KB	10 KB (ratio is 100:1)	Scanned
1001 KB	10 KB	Not scanned *
2000 KB	10 KB	Not Scanned *

* ScanMail takes the action you configure for unscannable files.

Are files under quarantine/backup/archive folders dangerous?

ScanMail renames all files in quarantine/backup/archive folders with specially formatted filenames that have the extension name removed. This stops Windows from directly launching the file and prevents any executable files from being launched accidentally (by double-clicking on the file or other attempts to open).

However, there is danger for users with applications such as Microsoft™ Office 2003 that can recognize a file with it's true file type. In this situation, a user could unintentionally launch even a backup file that has no extension name.

Does "Block Attachment types or filenames within zip files" feature support blocking files in RAR files?

In ScanMail 7.0, only zip(pkzip) format is supported.

Are unscannable files counted as uncleanable viruses in reports and logs?

Yes. With current design, files that exceed scanning restrictions and password-protected files are counted as uncleanable viruses. However, these two categories of viruses won't be calculated in virus outbreak count and thus outbreak notification won't be triggered by a large amount of unscannable files detection.

My Real-time monitor is not displaying my server information correctly. Some information is missing.

This is possible when there are two Real-time monitor pages opened at the same time and these two Real-time monitor sessions share the same information. Trend Micro recommends that you do not open two Real-time monitor pages at the same time to prevent this problem.

How do I roll back to a previous version of my ScanMail components?

You can manually delete the latest version of your ScanMail components and have ScanMail use an older version. See *Rolling Back a Component Update* on page 3-11 for instructions.

When I want to failover the virtual server , the following warning message shows up when I move group. Why does this happen and what can I do?

```
A cluster node is not available for this operation. Error ID:5005
```

They are many reasons that this problem can happen. View your ScanMail resource by double clicking on the resource. Verify that all nodes are added in the owner list. If all the nodes are added in the owner list and the problem still happens, then ScanMail might not be the cause of the problem.

Windows Event Log Codes

Event Identifications for notifications written into windows event logs have changed a lot from previous versions of ScanMail. This change might impact your monitoring efforts. Consult Table to understand the Windows event logs for ScanMail 7.0.

Event ID	Facility	Type/ Severity	Category	Description
1	Application	Information	None	ScanMail service started successfully.
2	Application	Information	None	ScanMail service stopped successfully.
3	Application	Error	None	ScanMail service started successfully.
4	Application	Error	None	ScanMail service stopped successfully.
5	Application	Warning	None	Virus scanning notification
6	Application	Warning	None	Attachment blocking notification
7	Application	Warning	None	Content filtering notification
16	Application	Warning	None	Alert. Update is unsuccessful
17	Application	Warning	None	Alert. Update is finished
18	Application	Warning	None	Alert. Last update time is older than specified time
19	Application	Information	None	Alert. Scan is successful
20	Application	Error	None	Alert. Scan is unsuccessful
21	Application	Warning	None	Alert. Scan time exceeds specified time
22	Application	Warning	None	Alert. The disk space on the local drive (volume) of the backup, quarantine, or archive directory is less than specified size
23	Application	Warning	None	Alert. The size of database to keep quarantine and logs exceeds specified size

Event ID	Facility	Type/ Severity	Category	Description
257	Application	Warning	None	Outbreak Alert, Virus
258	Application	Warning	None	Outbreak Alert, Uncleanable virus
259	Application	Warning	None	Outbreak Alert, Blocked attachment
513	Application	Error	None	Filter loading exception
514	Application	Error	None	Adapter loading exception
4097	Application	Warning	None	Alert, The disk space on the local drive of the MS Exchange transaction log is less than specified size
4098	Application	Warning	None	Alert, The MS Exchange mail store size exceeds specified size
4099	Application	Warning	None	Alert, The MS Exchange SMTP messages queued continuously exceeds the specified number
8193	Application	Information	None	EUQ. Processing manual End User Quarantine maintenance task started.
8194	Application	Information	None	EUQ. Processing of manual End User Quarantine maintenance task ended.
8195	Application	Information	None	EUQ. Processing of schedule End User Quarantine maintenance task started.
8196	Application	Information	None	EUQ, End of processing schedule End User Quarantine maintenance task
8197	Application	Information	None	EUQ, Start to process enable End User Quarantine task
8198	Application	Information	None	EUQ, End of processing enable End User Quarantine task
8199	Application	Information	None	EUQ, Start to process disable End User Quarantine task
8200	Application	Information	None	EUQ, End of processing disable End User Quarantine task

ScanMail 7.0 Windows event log codes

Glossary of Terms

The following is a list of terms in this document:

Term	Description
Activation code	A 37-character code, including hyphens, that is used to activate ScanMail. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 Also, see Registration Key.
ActiveUpdate	A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.
Adware	Similar to spyware, adware gathers user data, such as Web surfing preferences, that could be used for advertising purposes.
Anti-spam	Refers to a filtering mechanism, designed to identify and prevent delivery of unsolicited advertisements, pornography, and other “nuisance” mail.
Approved sender	A sender whose messages are not processed by spam filters.
Attachment	A file attached to (sent with) an email message.
Blocked sender	A sender whose messages are always deleted.
Body (email body)	The content of an email message.
Boot sector viruses	A type of virus that infects the boot sector of a partition or a disk.
Clean	To remove virus code from a file or message.

Term	Description
Compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
Configuration	Selecting options for how ScanMail will function, for example, selecting whether to quarantine or delete a virus-infected email message.
Content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
Default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
Denial of Service Attack (DoS Attack)	An attack on a computer or network that causes a loss of 'service', namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload computer resources such as memory.
Dialers	Software that changes client Internet settings and can force the client to dial pre-configured phone numbers through a modem.
Domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
Dynamic Host Control Protocol (DHCP)	A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.
Dynamic IP Address (DIP)	A Dynamic IP address is an IP address that is assigned by a DHCP server. The MAC address of a computer will remain the same, however, the computer may be assigned a new IP address by the DHCP server depending on availability.

Term	Description
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
Executable file	A binary file containing a program in machine language which is ready to be executed (run).
False positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
File Transfer Protocol (FTP)	FTP is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.
File type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
Gateway	A device that enables data to flow between different networks.
Grayware	Files and programs, other than viruses, that can negatively affect the performance of the computers on your network. These include spyware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and others. The ScanMail scan engine scans for grayware as well as viruses.
Hacker	See virus writer.
Hacking tools	Tools used to help hackers enter computers, often through empty ports.
Hostname	The unique name composed of ASCII characters, by which a computer is known on a network.
Hot Fixes and Patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the ScanMail server and/or client program.
HTTP (Hypertext Transfer Protocol)	The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTML, VBScript, or JavaScript viruses	Viruses that reside in Web pages and are downloaded through a browser.

Term	Description
HTTPS (Hypertext Transfer Protocol Secure)	A variant of HTTP used for handling secure transactions.
Incoming	Email messages routed into your network.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet Protocol (IP)	"The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)
Java malicious code	Operating system-independent virus code written or embedded in Java.
Joke program	Software that causes a computer to behave abnormally, such as forcing the screen to shake.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
License	Authorization by law to use ScanMail for Microsoft Exchange.
Macro viruses	Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
Mass-mailing behavior	A malicious program that has high damage potential, because it causes large amounts of network traffic.
Message size	The number of bytes occupied by a message and all its attachments.
Maintenance Agreement	A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees.

Term	Description
Notification	A message that is forwarded to one or more of the following: • System administrator • Sender of a message • Recipient of a message, • Other email address • SNMP and Windows event log The purpose of the notification is to communicate that an event has occurred, such as a virus being detected in a message
Offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
Outgoing	Email messages or other data leaving your network, routed out.
Password cracking applications	Software that can help hackers decipher user names and passwords.
Pattern file	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
Phish sites	A Web site that lures users into providing personal details, such as credit card information. Links to phish sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses.
Ping	A utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the machine with the specified IP address is online or not.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the machine.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.
Quarantine	To place email messages in an isolated directory (the Quarantine Directory) on the ScanMail scanner. Items placed in the quarantine directory are indexed in the ScanMail database.
Registration key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8. Also see Activation Code
Remote access tools	Tools used to help hackers remotely access and control a computer.

Term	Description
Scan	To examine items in a file in sequence to find those that meet a particular criteria.
Scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
Secure Socket Layer (SSL)	SSL is a scheme proposed by Netscape Communications Corporation to use RSA public-key cryptography to encrypt and authenticate content transferred on higher-level protocols such as HTTP, NNTP, and FTP.
SSL certificate	A digital certificate that establishes secure HTTPS communication between the Policy Server and the ACS server.
Simple Mail Transport Protocol (SMTP)	SMTP is a standard protocol used to transport email messages from server to server, and client to server, over the internet.
SOCKS 4	A TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.
Spam	Unsolicited email messages meant to promote a product or service.
Spyware	A type of grayware that installs components on a computer for the purpose of recording Web surfing habits (primarily for marketing purposes). Spyware sends this information to its author or to other interested parties when the computer is online. Spyware often downloads with items identified as 'free downloads' and does not notify the user of its existence or ask for permission to install the components. The information spyware components gather can include user keystrokes, which means that private information such as login names, passwords, and credit card numbers are vulnerable to theft.
Standard maintenance	See Maintenance Agreement
Subject (message subject)	The title or topic of an email message, such as "Third Quarter Results" or "Lunch on Friday." ScanMail uses the subject from the message header to determine the message subject.
Tag	To place an identifier, such as "Spam:" in the subject field of an email message.
Telnet	Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.
Test virus	An inert file that acts like a real virus and is detectable by virus-scanning software. Use test files, such as the EICAR test script, to verify that your antivirus installation is scanning properly.
Traffic	Data flowing between the Internet and your network, both incoming and outgoing.

Term	Description
Transmission Control Protocol (TCP)	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.
TrendLabs	TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.
Trojan horses	Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter.
True file type	A virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
Undesirable content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
Unsolicited email	See spam
User Datagram Protocol (UDP)	A connectionless communication protocol used with IP for application programs to send messages to other programs. Refer to DARPA Internet Program RFC 768 for information.
Virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
Virus writer	Another name for a computer hacker, someone who writes virus code.
Wildcard	For ScanMail, an asterisk (*) represents any character. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on.
Worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email. A worm can also be called a network virus.
Zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.

Index

A

account privileges, required to install 2-10
actions, see individual actions by name 5-5
Activation Code
  Standard AC 3-3
  Standard or Suite edition 3-2
  suite 3-3
ActiveAction
  benefits of selecting 7-22
  how it works 1-11
  using 7-22
ActiveUpdate
  how it works 1-10
  incremental pattern file updates 1-10
  setting as download source 3-9
Advanced Options
  handling unscannable files 7-27
advanced options
  macro viruses 7-27
Adware
  defined 5-7
Anti-spam
  actions, setting 7-66
  ScanMail filtering explained 7-5
approved senders lists
  about 7-64
attachment blocking
  ScanMail filtering explained 7-6
attachments restriction, file too large 7-18

B

back-end servers, deploying ScanMail to 2-8
backing up a file before taking action 7-26
backup folder
  specifying location 7-26
blocked senders lists
  about 7-64

C

clean, ScanMail action 7-23
cluster servers
  manual scan restrictions 7-32
  node-based scanning 7-32
  scheduled scan restrictions 7-32
  updating components on 3-6
  virus scanning on 7-32
common computer security threats 7-21
components 3-5
compressed files
  do not clean to improve performance 7-26
  scanning 7-18
  scanning restrictions 7-18
compression types
  supported 5-5
configure scan actions
  how to 7-24
configuring tasks
  Anti-spam 7-62
  attachment blocking 7-33
  content filtering 7-37
  virus scanning 7-13
contacting Technical Support 11-2
content filtering
  about 7-37
  ScanMail default actions 7-3
  ScanMail filtering explained 7-6
content filtering actions, effect on messages 7-61
content filtering rules
  changing order 7-51
  enabling 7-38
  enabling individual rules 7-38
  how to create an exemption rule 7-47
  how to create general rule 7-39, 7-43
  how to create monitoring rule 7-44
  viewing 7-37
customized actions
  using 7-22

D

debugger reports, generating 10-10
default 7-3
delete entire message
  differs from previous version 7-23
delete entire message, ScanMail action 7-23, 7-35
deleting logs 9-7
deleting quarantined messages 9-11
deleting reports 9-5

deleting spam messages from Spam folder 10-5
deploying ScanMail
  network traffic, ScanMail effect 2-6
  to back-end servers 2-8
  to front-end servers 2-8
detectable threats, scanning 7-14
Dialers, defined 5-7
disabling
  real-time scan 7-10
disabling content filtering rules 7-38
Disabling SMTP scanning 7-12
download source 3-9
  duplicating to local server 3-10
  selecting 3-9
duplicating download source 3-10

E

enabling
  content filtering rules 7-38
  real-time scan 7-10
encrypted files
  ScanMail default actions 7-4
End User Quarantine
  about 7-68
  disabling 10-4
  end user Approved Senders lists 7-68
  end user functions 7-68
  housekeeping 7-68
  housekeeping features 7-68
  managing 7-68
EUQ 1.0, removing 11-12
European Institute for Computer Antivirus Research-see EICAR, test script 2-4
evaluation Maintenance Agreement 3-3
excluding folders
  file-based antivirus file-based antivirus
    excluding folders from 6-4
external address
  defined 10-3
  format 10-3

F

failover
  effect on scanning for cluster servers 7-32
failover, effect on components 3-6
FAQ, frequently asked questions 11-11
file type
  scanning for true file type 7-17
frequently asked questions (FAQ) 11-11
front-end servers, deploying ScanMail to 2-8
full license 3-3

G

generating debugger reports, how to 10-10
global default administrator address
  how to set 10-3
global directories
  about 7-48
  how to specify 7-48

H

Hacking Tools
  defined 5-7
heuristic rules
  screening email messages 7-66
housekeeping
  End User Quarantine 7-68

I

installing ScanMail
  activation code, entering 2-10
  cluster server installation 2-33
  End User Quarantine, name required for spam folder 2-11
  pre-installation tasks 2-10
  registration key required 2-10
  setting proxy server 2-10
  stopping and restarting services unnecessary 2-10
  testing 2-4
  verifying success 2-34
IntelliScan 7-16
  about 7-16
  benefits of selecting 7-16
  how it works 1-11
  scanning true file types 7-17
internal address
  defined 10-3
  format 10-3
internal and external addresses 10-3
InterScan Messaging Security Suite, enhanced security with 6-3

InterScan VirusWall, enhanced security with 6-3
ISO 9002 Certification-see TrendLabs 11-4

J

Java
  malicious code
    definition ii-4
joke program
  defined 5-4

K

keywords
  about 7-51
  supported 7-53
Knowledge base
  url 11-5
known issues 11-5

L

License Agreement 10-6
license expiry
  renewing 10-7
  viewing 10-6
license information
  viewing 10-6
lock-down tool, remove before installing ScanMail 2-10
log query, how to set up and run 9-6
logs
  deleting 9-7
  how to manually delete 9-7
  how to set automatic delete 9-8
  managing 9-6
  part of ScanMail protection strategy 7-8

M

macro viruses
  explained 5-6
  scanning 7-27
Maintenance Agreement 10-6
  about 10-6
  evaluation 3-3
maintenance agreement
  fully licensed 3-3
manual scans
  attachment blocking actions unavailable 7-33
  general content filtering 7-39
  part of ScanMail protection strategy 7-7
manually rolling back components 3-11
mass-mailing attack
  defined 5-5
  enabling action against 7-22
  ScanMail action against 5-5
Microsoft Exchange
  how viruses spread 5-9
minimum system requirements 2-2
multiple servers, managing with the Web management console 4-2

N

network traffic, ScanMail generating 2-6
notifications
  about 7-10
  part of ScanMail protection strategy 7-8
  triggers for sending 8-2

O

OfficeScan, enhanced security with 6-3
one-time reports
  deleting 9-5
  how to generate 9-4
online help
  accessing 4-5
outbreak alerts
  about 8-2

P

pass, ScanMail action 7-23
Password Cracking Applications
  defined 5-7
password protected files
  ScanMail default actions 7-4
pattern file
  incremental updates 1-10
Phish
  detecting 7-67
  ScanMail actions against 7-67
pilot installation
  testing 2-4
pre-installation checklist 2-11
proxy server
  ScanMail features requiring 3-6

setting 3-6

Q

quarantine entire message, ScanMail action 7-23, 7-35
quarantine folder, managing 7-69
quarantine query, how to set up and run 9-9
quarantined messages
how to delete automatically 9-12
how to delete manually 9-11
how to resend 9-10

R

Real-time monitor
about 4-7
how to view remote server using 4-7
real-time scan
enabling 7-10
real-time scanning
part of ScanMail protection strategy 7-7
recommended system requirements 2-2
registering ScanMail, methods 3-2
Registration Key
use 3-2
regular expressions
using 7-55
Remote Access Tools
defined 5-7
remote server
viewing with real-time monitor 4-7
removing EUQ 1.0 11-12
removing ScanMail 2-36
components removed 2-36
from cluster server 2-38
renewing license 10-7
reorder content filtering rules 7-51
replace with text/file, ScanMail action 7-23, 7-35
replicating server configurations, how to 4-9
replicating servers using Server Management 4-9
report templates
deleting 9-5
reports
described 9-3
generating 9-4
part of ScanMail protection strategy 7-8
sending 9-4
viewing 9-4
resending quarantined messages 9-10
rolling back components 3-11

S

scan
compressed files 7-18
scan actions
ActiveAction 7-22
scan engine
events that trigger an update 1-7
technology described 1-7
updates 1-7
URL to find current version 1-8
ScanMail actions 7-20
ScanMail components 3-5
ScanMail default actions 7-3
ScanMail protection strategy, explained 7-5
scannable files
defined 7-15
files that are not scanned 7-16
scanning restrictions
compressed files 7-18
how to set for compressed files 7-18
how to set for large files 7-18
large attachments 7-18
scheduled reports
deleting 9-5
how to generate 9-4
scheduled scanning
part of ScanMail protection strategy 7-7
scheduled scans
attachment blocking actions unavailable 7-33
content filtering of header and subject unavailable 7-45
disabling 7-12
general content filtering 7-39
Server Management
how to replicate server configurations 4-9
Spam
screening messages for 7-62
spam detection levels
defined 7-66
setting 7-66

Spam Folder
creating 10-4
deleting spam messages 10-5
renaming 2-34, 10-4
setting the retention time limit 10-5
spam messages
deleting 10-4
spam score
calculating 7-66
example 7-66
Spyware
and other grayware, defined 5-7
ScanMail protection against 7-6
Standard Activation Code 3-3
Suite Activation Code 3-3
support
Knowledge Base 11-3
online help 11-3
readme file 11-3
system event alerts
part of ScanMail protection strategy 7-8
system events
about 8-2
system requirements 2-2
System Watcher
monitors ScanMail service 8-2

T

target files
eligible for scanning 7-14
how to select for virus scanning 7-15
Technical Support
contacting 11-2
URL 11-3
terms 5-2
testing your installation 2-4
threats to computer security, common types 7-21
Trend Micro
contact URL 11-2
contacting corporate offices 11-2
headquarters 11-2
TrendLabs 11-4
Trojans
attack type 7-21
defined 5-4
ScanMail protection against 7-6
true file type
how it works 7-16

U

uncleanable files, defined 7-24
uninstalling ScanMail 2-36
updating components 3-5
rolling back 3-11
updating ScanMail 3-5
before you update 6-4
manual update 3-7
scheduled updates 3-8
upgrading ScanMail
on cluster servers 2-16
supported versions 2-13
URLs
Knowledge base 11-5
scan engine version 1-8
Technical Support 11-3
Trend Micro 11-2

V

version comparison 1-5
ScanMail 3.53
ScanMail 3.82
ScanMail 6.21
virtual servers, viewing with the Web management console 4-6
virus doctors-see TrendLabs 11-4
virus outbreak alerts
part of ScanMail protection strategy 7-8
Virus Scan Application Programming Interface (VS API)
scan engine use of 1-7
Virus scanning
about 7-5
virus scanning
on cluster servers 7-32
ScanMail default actions 7-4
ScanMail filtering explained 7-6
three steps to configure 7-13
viruses
boot 5-3
defined 5-2

file 5-2
ScanMail protection against 7-6
script 5-3

W

Web management console
getting help 4-5
parts described 4-3
viewing local server from 4-5
viewing remote servers from 4-5
wildcards
formatting 7-65
World Virus Tracking, participating 10-8
worms
attack type 7-21
defined 5-4
ScanMail protection against 7-6