TREND MICRO™
Client/Server/ Messaging Suite
for Small and Medium Businesses

Comprehensive Virus Protection for Business Workstations, Servers, and Email

Administrator's Guide

TREND MICRO™

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

www.trendmicro.com/download/documentation/

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

Trend Micro, the Trend Micro t-ball logo, eManager, OfficeScan, and ScanMail for Microsoft Exchange are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2003 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. NAEM21620/31003

Release Date: November, 2003

Protected by U.S. Patent Nos. 5,951,698 and 5,889,943

The Administrator's Guide for Trend Micro Client/Server/Messaging Suite for SMB is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Chapter 1: Introducing the Client/Server/Messaging Suite for SMB

What is the Trend Micro Small and Medium Business Solution 1-2
What is included in the Client/Server/Messaging Suite for SMB 1-4
What's new in version 2.0 1-5
Overview of suite deployment 1-6
1. Installing the OfficeScan server 1-7
2. Installing the OfficeScan clients 1-8
3. Configuring and update OfficeScan 1-8
4. Installing ScanMail for Microsoft Exchange 1-9
5. Configuring ScanMail for Microsoft Exchange 1-10
6. Configuring ScanMail eManager for Exchange 1-10

Chapter 2: Introducing OfficeScan

What is OfficeScan? 2-2
OfficeScan technology 2-3
How viruses spread 2-3
How does OfficeScan work? 2-3
What you can do with OfficeScan 2-4
Analyze your network's protection against viruses 2-5
Enforce antivirus policies 2-5
Update your protection 2-5
Perform virus scans from one location 2-5
Quarantine infected files 2-6
Control outbreaks on the network 2-6
Manage OfficeScan domains and clients 2-6
Protect your PDAs from viruses 2-6
Benefits and Capabilities 2-7
Single-console operation 2-7
Virus Outbreak Monitor 2-7
Outbreak Prevention 2-7

Trend Micro IntelliScan 2-8
Trend Micro ActiveAction 2-8
Typical virus types 2-8
Trend Micro Damage Cleanup Services 2-9
Secure Web console communication 2-9
What's new in OfficeScan 2-10
Understanding the OfficeScan architecture 2-11
OfficeScan server 2-11
HTTP-based server 2-11
OfficeScan client 2-12
Normal clients 2-13
Roaming clients 2-14
About Damage Cleanup Services 2-15
Management (Web) console 2-16

Chapter 3: Planning for Deployment

Planning for deployment 3-2
Deployment architectures 3-2
Overview of installation and deployment 3-2
Deploying OfficeScan Server 3-4
Determining the number of clients 3-4
Planning for network traffic 3-4
Planning the placement of program files 3-5
Determining the number of domains 3-6
Deciding how to deploy the client 3-6
Conducting a pilot deployment 3-7
Choosing a pilot site 3-7
Creating a rollback plan 3-7
Deploying your pilot 3-7
Evaluating your pilot deployment 3-8

Chapter 4: Deploying and Installing OfficeScan

Installing OfficeScan Server 4-2
Minimum system requirements 4-2
Minimum system requirements for the Web console 4-2
Preparing for server installation 4-2
Running setup 4-3

Required protocols 4-3
Required rights 4-3
Required restarts 4-3
Required information 4-4
Shared directories 4-4
Windows licenses 4-5
TCP port for HTTP communication 4-5
Running master setup to install OfficeScan server 4-5
Verifying a successful installation 4-9
Registering OfficeScan 4-9
Viewing OfficeScan and component license information 4-10
Activating a component license 4-10
Setting a Product Registration proxy 4-10
Default OfficeScan Server Settings 4-11
Uninstalling the OfficeScan server 4-12
Installing OfficeScan clients 4-12
Minimum system requirements 4-12
Minimum system requirements for the Windows Me/98 client 4-13
Minimum system requirements for the Windows 2000/NT client 4-13
Minimum system requirements for the Windows XP/2003 client 4-13
Preparing for installation using Trend Micro Vulnerability Scanner 4-14
Installing OfficeScan clients 4-14
Installing from the internal Web page 4-15
Installing with Login Script Setup 4-16
Installing with Client Packager 4-19
Sending the package via email 4-22
Installing with Windows Remote Install 4-22
Installing from a client disk image 4-23
Installing with Vulnerability Scanner 4-24
Installing the client using Microsoft SMS 4-25
Verifying a successful installation 4-28
Using Vulnerability Scanner to verify the client installation 4-28

Testing the client installation 4-29
Removing the client 4-31
Removing the client from the OfficeScan Web console 4-31
Removing the client using its uninstallation program 4-32
Migrating to and Upgrading OfficeScan 4-32
Migrating from third-party antivirus applications 4-32
Plan your migration 4-33
Pilot your migration 4-33
Install the OfficeScan server 4-33
Manual client migration 4-34
Automatic client migration 4-34
Verify the migration 4-36
Upgrading from a previous version 4-36

Chapter 5: Getting Started with OfficeScan

Exploring the Web console 5-2
Getting around the Web console 5-2
Other links on the console 5-10
Understanding the domain tree 5-11
Creating domains 5-12
Selecting domains and clients from the domain tree 5-12
Searching for clients 5-12
Refreshing the tree 5-13
Understanding the domain tree icons 5-14
Working with OfficeScan domains 5-14
Updating OfficeScan 5-16
Updating the server 5-16
Configuring scheduled updates for the server 5-17
Updating the server manually 5-18
Configuring Internet Proxy Settings 5-18
Updating clients 5-20
Updating clients using Automatic Deployment 5-20
Updating clients using Manual Deployment 5-21
Updating clients using Update Now 5-22
Verifying a successful update 5-23
Verifying client-server connection 5-23
Setting up standard notifications 5-24

Configuring standard alerts 5-25
Configuring outbreak alerts 5-26
Configuring the scan settings 5-29
About IntelliScan 5-29
About ActiveAction 5-29
Configuring Manual Scan 5-30
Configuring Real-time Scan 5-32
Configuring Scheduled Scan 5-35
Excluding files and folders from scanning 5-37
Running Scan Now 5-38
Granting privileges to clients 5-41

Chapter 6: Configuring Outbreak Prevention

Blocking shared folders 6-2
Blocking ports 6-3
Modifying Port Blocking Settings 6-5
Denying write access to files and folders 6-5
Configuring client notification for outbreaks 6-7
Restoring network settings to normal 6-7

Chapter 7: Configuring Virus Outbreak Monitor

Configuring Virus Outbreak Monitor 7-2

Chapter 8: Viewing and Interpreting Logs

Viewing and Interpreting Logs 8-2
Viewing Virus Logs 8-2
Deleting Virus Logs 8-3
Viewing Server Update Logs 8-3
Viewing Client Update Logs 8-4
Viewing System Event Logs 8-5
Viewing GateLock Intrusion Detection and Prevention (IDP) Logs 8-5
Viewing Verify Connection Logs 8-6
Managing Logs 8-6

Chapter 9: Installing and Launching ScanMail for Microsoft Exchange

System requirements for ScanMail for Microsoft Exchange 2000 and 2003 9-1
Target servers 9-1
System Requirements for ScanMail for Microsoft Exchange 5.5 9-2
Target Servers 9-2
Determining Your Version of MDAC and Microsoft Jet 9-3
System Requirements for ScanMail eManager Windows-based Console 9-4
ScanMail eManager for Microsoft Exchange 2000 and 2003 9-4
ScanMail eManager for Microsoft Exchange 9-4
Installing and Launching ScanMail for Exchange from the OfficeScan Console 9-6
Installing the eManager Windows-based console 9-6
Verifying a successful installation 9-7
Removing ScanMail 9-8
Removing ScanMail Using the Windows Control Panel 9-8
Removing ScanMail using the Trend Micro Small and Medium Business Solution CD or the Uninstall.exe program 9-8

Chapter 10: The eManager and ScanMail consoles

Managing the eManager Web-based console 10-3
Anti-spam 10-3
Content Filter 10-4
Default Separators 10-5
Update Screen 10-5
Log Files 10-6
Settings 10-6
Understanding differences between the eManager Windows-based and Web-based consoles 10-7

Chapter 11: Introducing Trend Micro ScanMail for Microsoft Exchange

ScanMail for Microsoft Exchange Versions 11-2
ESE Version for ScanMail 5.5 users 11-2
ScanMail for Microsoft Exchange 2000 and 2003 Technology 11-2
How viruses spread in a Microsoft Exchange environment 11-3
How ScanMail works 11-5
Benefits and capabilities 11-5
Web console trusted IP zones 11-7
Trend Micro IntelliScan 11-7
Trend Micro ActiveAction 11-7
Typical virus types 11-7
Attachment blocking and Active Message filtering 11-8
Information Store database selection 11-9
Quarantine Manager 11-9
ScanMail eManager 11-9

Chapter 12: Configuring Real-time Scanning

About real-time scanning 12-2
Enabling/disabling real-time scanning 12-3
Enabling/Disabling ScanMail eManager 12-4
Information Store database selection 12-4
Configuring virus (real-time) scan options for ScanMail for Exchange 2000 and 2003 12-4
Configuring the Real-time Scan Options for ScanMail for Exchange 5.5 12-6
Configuring the virus scan actions 12-8
Configuring attachment blocking 12-8
Warning on “Red Alert” attachment blocking feature usage 12-8
Advanced options 12-10
Selecting the file attachments to scan 12-11
Using Trend Micro IntelliScan 12-11
Specifying the file types to scan 12-12
Configuring the Active Message Filter for ScanMail for Exchange 2000 and 2003 12-12

Using the Active Message Filter for ScanMail for Exchange 5.5 12-13
Changing the default embedded message deletion layer 12-14
Configuring the virus detection actions 12-15
Using Trend Micro ActiveAction 12-16
Specifying the scan actions 12-16
Configuring the attachment replacement settings 12-17
Specifying the quarantine directory 12-17
Configuring virus scan options through the Web console 12-18
Monitoring real-time scanning 12-20
Displaying the virus scan status for ScanMail for Microsoft Exchange 2000 and 2003 12-20
Displaying the Real-time Scan Status for ScanMail for Microsoft Exchange 5.5 12-21
Displaying the Real-time Scan Monitor for ScanMail for Exchange 2000 and 2003 12-21
Displaying the Real-time Scan Monitor for ScanMail for Exchange 5.5 12-23
Displaying the ScanMail Performance Monitor 12-24

Chapter 13: Configuring Manual and Scheduled Scans

About manual and scheduled scans 13-2
Warning on enabling ScanMail eManager while performing manual or scheduled scans 13-2
Configuring and running manual scans for ScanMail for Exchange 2000 and 2003 13-3
Running a manual "Scan Now" 13-3
Configuring and Running Manual Scans for ScanMail for Exchange 5.5 13-4
Displaying Manual Scan Results 13-5
Configuring scheduled scans for ScanMail for Exchange 2000 and 2003 13-6
Configuring scheduled scan options 13-6
Configuring the Information Store databases to scan 13-6
Configuring scheduled scans from the Windows console 13-6
Configuring scheduled scans from the Web console 13-8
Configuring Scheduled Scans for ScanMail for Exchange 5.5 13-9

Configuring Scheduled Scans from the Windows Console 13-9
Configuring Scheduled Scans from the Web Console 13-11
Displaying manual and scheduled scan results 13-12

Chapter 14: Configuring Notification Messages and ActiveUpdate

Configuring notification messages 14-2
Configuring virus notification messages for ScanMail for Exchange 2000 and 2003 14-2
Configuring Virus Notification Messages for ScanMail for Exchange 5.5 14-4
Configuring Outbreak Alert notification messages for ScanMail for Exchange 2000 and 2003 14-6
Configuring Outbreak Alert Notification Messages for ScanMail for Exchange 5.5 14-8
Configuring attachment blocking notification messages for ScanMail for Exchange 2000 and 2003 14-10
Configuring Attachment Blocking Notification Messages for ScanMail for Exchange 5.5 14-11
Changing subject line notifications through the registry 14-12
About ActiveUpdate technology 14-13
Virus pattern file 14-14
Scan Engine 14-14
Configuring pattern file and Scan Engine updates 14-14
Configuring “Update Now” 14-14
Configuring scheduled updates 14-16

Chapter 15: Using Quarantine Manager and ScanMail’s Log Files

Quarantine Manager 15-2
Quarantined email and attachments 15-2
Viewing quarantined email and attachment information 15-4
Resending quarantined email 15-4
Quarantine Maintenance 15-6
Automatic quarantine file deletion 15-7
Manual quarantine file deletion 15-8
ScanMail log files 15-8
Viewing log file entries 15-8
Log screen details 15-10

Maintaining the log files 15-12
Automatically deleting log files 15-13
Manually deleting log files 15-14

Chapter 16: Content Management with Trend Micro ScanMail eManager Windows-based Console

Content Management 16-2
Spam Filtering 16-2
Content Filtering 16-3
What is Spam Mail? 16-3
Why is Spam Mail Bad? 16-3
Tracking Spammers 16-4
Anti-spam Rules 16-4
Anti-spam Rules Strategy 16-5
Content Filter Policies 16-5
Example "Free offer" Policy 16-6
Boolean Expressions Implied in the Content Filter 16-6
ScanMail for Microsoft Exchange and ScanMail eManager Processing Order 16-7
Control Manager Agent for ScanMail eManager 16-8
Summary of New Features 16-9

Chapter 17: Introducing Trend Micro ScanMail eManager

Starting and stopping eManager 17-1
Restarting ScanMail for Microsoft Exchange and eManager 17-2
Stopping ScanMail for Microsoft Exchange and eManager 17-3
Starting the ScanMail eManager Console 17-4
Selecting the Server to Administer 17-4
Viewing the ScanMail eManager Processes 17-6
Removing ScanMail eManager 17-6
Removing ScanMail eManager Using the Windows Start Menu 17-6
ScanMail eManager Files 17-7

Chapter 18: Spam Filtering

Viewing Email Headers 18-2
Example Message Header 18-2
Configuration Files 18-3
Using the Spam Filter 18-4
Creating Anti-spam Rules 18-4
Current Rules Strategy 18-6
Rules Strategy Example 18-6
User-defined Current Rules 18-7
Add-Edit Rule Options Screen 18-7
Rule Name 18-8
Action on Unwanted Mail 18-9
Rule Result 18-9
Address and Subject Fields 18-9
Message or Attachment Size 18-10
Attachment Blocking 18-11
Anti-spam Notifications 18-11
Current Rules Notifications 18-11

Chapter 19: Content Filtering

Understanding ScanMail eManager Content Filter 19-2
Creating Content filter policies 19-2
Creating Keyword Lists 19-3
Understanding ScanMail eManager's Content Filter Policies 19-4
Anti-spam 19-5
Profanity and Discrimination Lists 19-5
Hoaxes and Chain mail Lists 19-5
Blocking HTML Script Messages 19-6
Customizing the Trend Micro ScanMail eManager Content Filter Policies 19-6
Creating content filter policies 19-7
Step-by-Step Example 19-7
Using the Content Filter to block spam 19-9
Content Filter Options 19-9
Policies 19-10
Details 19-11

Keyword Lists 19-11
Add/Edit Policy Options 19-11
Policy Name 19-13
Action 19-13
Keyword List(s) 19-13
Using Synonym Checking 19-14
Keyword List Example 19-15
Creating exception keyword lists 19-16
Import File 19-16
Import File Format 19-17
Notifications 19-17
Using Global Policy Settings 19-18
Exact Matches 19-18
Case-Sensitive Comparisons 19-19
Enable Scanning the Content of Attached Files 19-19
Using the Quarantine Screen 19-19
Quarantine and Archive Directory Structure 19-19
Reporting spam messages to Trend Micro 19-20

Chapter 20: Troubleshooting

Client-server communication 20-2
Incorrect number of clients on the Web console 20-2
Incorrect client status on the Web console 20-3
Incorrect component versions 20-4
Unsuccessful installation from the Web page or with Remote Install 20-5
Client icon does not appear on the Web console after installation 20-5
Issues during migration from third-party antivirus software 20-6
Client migration 20-6
Modify the service for the third-party software 20-8
Unload the service or process for the third-party software 20-8
Contacting the Trend Micro Virus Information Center 20-9
Contacting Technical Support 20-9
Accessing Technical Support from the ScanMail for Microsoft Exchange Windows Console 20-10
Speeding Up Your Support Call 20-10

Contacting Trend Micro Knowledge Base 20-11
Contacting TrendLabs 20-11

Appendix A: Using OfficeScan Tools

Administrative Tools A-2
Database Backup A-2
Login Script Setup A-3
Vulnerability Scanner A-4
Other Settings A-7
Client Tools A-8
Client Packager A-9
Image Setup Utility A-9
Remote Agent A-9
What you can do with Remote Agent A-10
Restore Encrypted Files A-10

Appendix B: Configuring OfficeScan with Add-ons and Third-party Software

Configuring OfficeScan Wireless Protection Manager B-1
About Wireless Protection Manager B-2
PDA System Requirements B-3
Installing Wireless Protection Manager B-3
Opening Wireless Protection Manager B-4
Using Wireless Protection Manager B-5
Updating OfficeScan for Wireless B-5
Downloading Update Components B-5
Enabling and Configuring Proxy Settings B-6
Synchronizing with Your PDA B-7
Working with Logs B-7
Viewing logs B-7
Managing logs on your PDA B-8
Deleting logs B-8

Index

Chapter 1

Introducing the Client/Server/Messaging Suite for SMB

Designed to suit the needs of small- to medium-sized corporate IT networks, Trend Micro™ Client/Server/Messaging Suite for Small and Medium Businesses (SMB) combines spam filtering, secure email storage and delivery with the essentials of network-wide desktop and server protection.

Spam filtering increases productivity and conserves network resources by stopping unwanted email from reaching its destination. Fully customizable content filtering rules and exception lists helpscontrol what kinds of messages reach the desktop.

Secure email virus scanning and spam filtering helps prevent dangerous worms and trojans from entering the network, preventing these types of malware from infecting systems and consuming valuable network bandwidth.

Network-wide desktop and server protection helps shield every file server and computer on the network from virus threats. Computers on your network are kept up-to-date with the latest pattern files through centralized management and automatic updates of client installations.

Seamless integration with Microsoft™ Windows™ and Microsoft Exchange Server™ makes Trend Micro Client/Server/Messaging Suite for SMB a powerful,

multi-layered defense against viruses and other malicious code. Centralized management tools and intelligent malicious code scanning offers excellent antivirus and content security in a scalable high-performance software architecture.

The Client/Server/Messaging Suite for SMB is one component of the Trend Micro Small and Medium Business Solution.

What is the Trend Micro Small and Medium Business Solution

The Trend Micro Small and Medium Business Solution helps provide comprehensive virus protection and spam filtering from the gateway to the desktop. The solution offers flexibility to choose where to install Trend Micro solutions: from virus protection at gateways, servers, and desktops, to content filtering at the mail server.

The Trend Micro Small and Medium Business Solution consists of three easy-to-install software packages, including:

- Trend Micro Client/Server/Messaging Suite for SMB - integrated, centrally managed antivirus for desktops, file servers, and email servers
- Trend Micro Client/Server Suite for SMB- best-of-breed, centrally managed antivirus for desktops and file servers
- InterScan VirusWall - best-of-breed antivirus for the gateway
- Trend Micro PC-cillin Internet Security - standalone antivirus and firewall protection

All three components can be quickly and easily installed from the Trend Micro Small and Medium Business Solution CD. Figure 1-1 illustrates what is protected by the different components of the Trend Micro Small and Medium Business Solution.

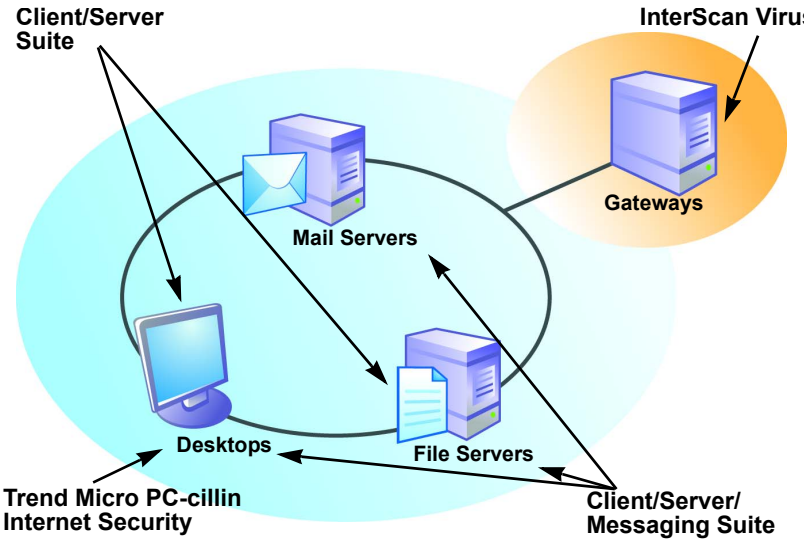

FIGURE 1-1. Different components of the Small and Medium Business Solution provide protection for the network

This manual describes how to install, configure, maintain, and troubleshoot the Client/Server/Messaging Suite for SMB. For information about InterScan VirusWall and Trend Micro PC-cillin Internet Security, refer to the *InterScan VirusWall Getting Started Guide* and the *Trend Micro PC-cillin Internet Security Quick Start Guide*. You can view electronic copies of product manuals in PDF form on the Trend Micro Small and Medium Business Solution CD. PDF files are located on the CD in the documents folder.

```
{CD-ROM drive}\Documentation
```

Replace {CD-ROM drive} with the drive letter of the CD-ROM drive on your computer.

What is included in the Client/Server/Messaging Suite for SMB

The Client/Server/Messaging Suite for SMB is an integrated package that combines OfficeScan, ScanMail for Microsoft Exchange, and ScanMail eManager. OfficeScan protects file servers and desktop computers. ScanMail for Microsoft Exchange helps prevent email-borne viruses by scanning email passing in and out of the Microsoft Exchange™ Mailbox Store as well as email that passes between the Exchange Server and external destinations. ScanMail eManager™ for Exchange helps stop spam before it arrives at its destination.

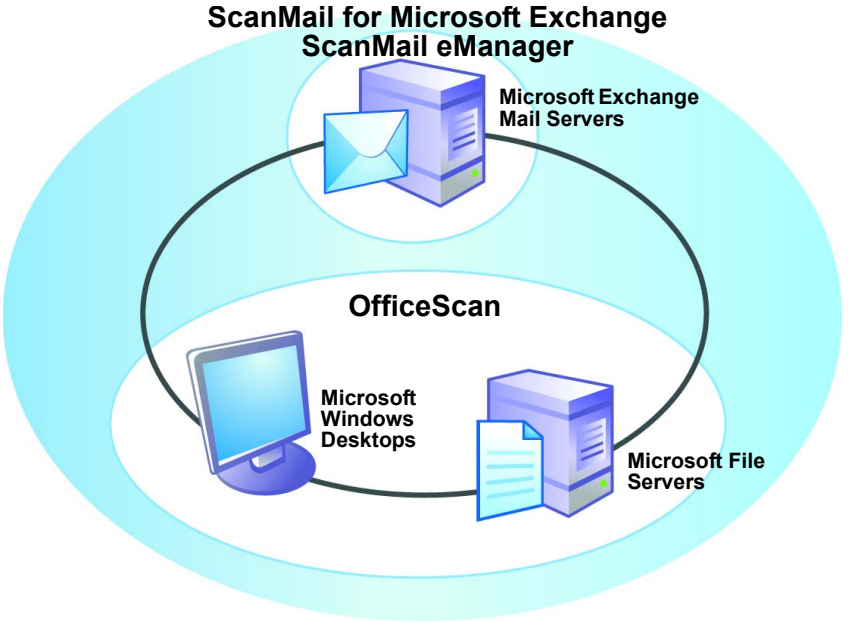

FIGURE 1-2. The Client/Server/Messaging Suite for SMB consists of OfficeScan and ScanMail for Microsoft Exchange

All three components have been integrated to provide an easy-to-use package that provides complete protection inside for Microsoft Windows™ networks.

What's new in version 2.0

Version 2.0 of the Client/Server/Messaging Suite for SMB brings a host of benefits to small and medium businesses that lack dedicated resources for antivirus management, including:

- Simplified installation from the Trend Micro Solutions CD for small and medium businesses
- Virus protection for file servers with the OfficeScan client
- Spam prevention and content filtering with ScanMail eManager for Microsoft Exchange
- Integrated virus protection for Exchange servers and spam filtering
- A simplified interface that allows ScanMail for Microsoft Exchange to be installed and launched from the OfficeScan Web console

Overview of suite deployment

You can deploy the entire Client/Server/Messaging Suite for SMB from a single workstation on your network if you have the permissions to install applications on the target servers and workstations.

Suite deployment consists of installing, configuring, and updating each of the components, and follows these basic steps:

1. Install the OfficeScan Server
2. Install the OfficeScan clients
3. Configure OfficeScan
4. Install ScanMail for Microsoft Exchange
5. Configure ScanMail for Microsoft Exchange
6. Configure ScanMail eManager for Exchange

This section provides a conceptual overview of the steps involved in installing, configurating, and updating OfficeScan and its components. For detailed step-by-step instructions, see the relevant chapters in this guide.

1. Install the OfficeScan server

To install the OfficeScan server, use the Trend Micro Solutions CD for small and medium businesses on a computer attached to the network. The computer will become your OfficeScan server, and should meet or exceed the requirements specified in *Minimum system requirements* on page 4-2.

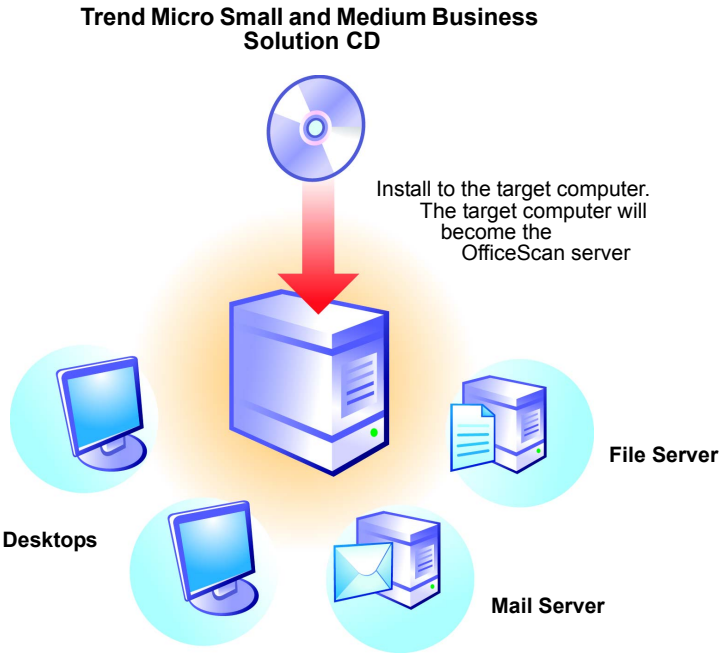

FIGURE 1-3. Install the OfficeScan Server from the Trend Micro Small and Medium Business CD

How you install the OfficeScan server depends on your network and the number of clients you plan to install. Refer to the introductory information in *Introducing OfficeScan* on page 2-1, and deployment scenarios in *Planning for Deployment* on page 3-1 before installing the OfficeScan server. For instructions on how to install the OfficeScan server, refer to *Installing OfficeScan Server* on page 4-2.

2. Install the OfficeScan clients

After you have installed the OfficeScan server, you are ready to install the clients. The new OfficeScan client package allows for greater flexibility and can protect Windows desktops and servers. Install the OfficeScan client to desktop or file server computers to protect, including the OfficeScan server.

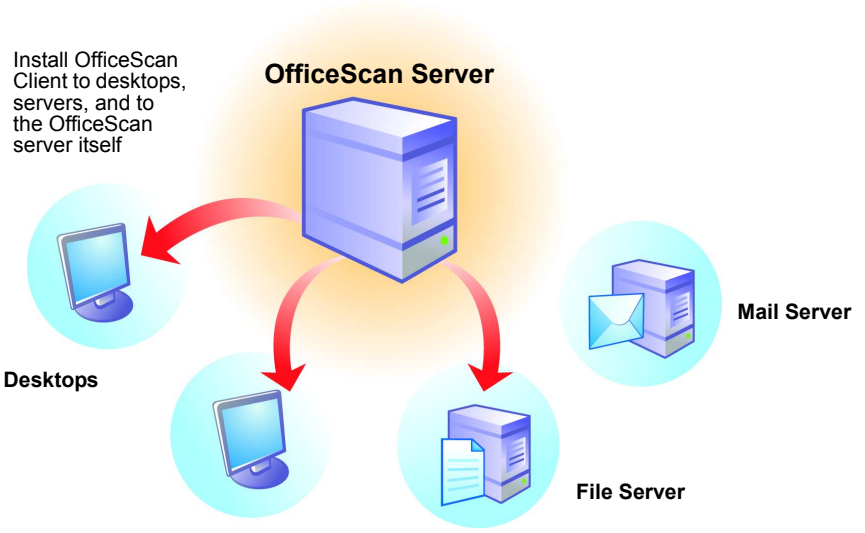

FIGURE 1-4. Install the OfficeScan clients to computers that require virus protection

For instructions on how to install OfficeScan clients, refer to *Installing OfficeScan clients* on page 4-12

3. Configure and update OfficeScan

Configure OfficeScan installaion of the server and clients. OfficeScan configurations include:

- Updating the scan engine, virus pattern file, and other components
- Setting up notifications and alerts

- Configuring the scan schedule, scan actions, and types of files to scan
- Configuring client privileges

For instructions on how to configure OfficeScan, refer to *Deploying and Installing OfficeScan* on page 4-1.

4. Install ScanMail for Microsoft Exchange

After you have installed OfficeScan and rolled out the OfficeScan clients, you are ready to install ScanMail for Microsoft Exchange and eManager.

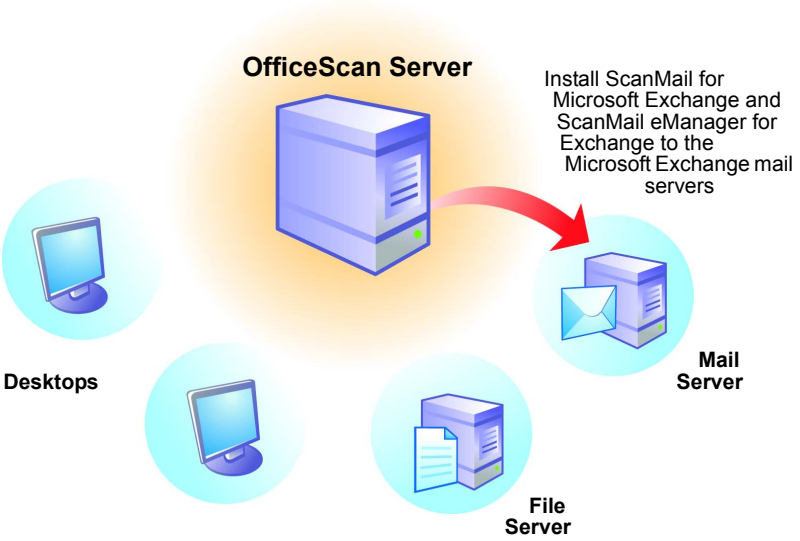

FIGURE 1-5. Install ScanMail for Microsoft Exchange and eManager to the Microsoft Exchange mail servers

The ScanMail for Microsoft Exchange installer on the OfficeScan Web console automatically installs spam prevention and content management with ScanMail eManager for Exchange. There is no need to separately install eManager. For instructions on how to install ScanMail for Microsoft Exchange, refer to *Installing and Launching ScanMail™ for Microsoft™ Exchange* on page 9-1.

5. Configure ScanMail for Microsoft Exchange

After installing ScanMail for Microsoft Exchange and ScanMail eManager for Exchange to the mail servers, you are ready to configure ScanMail for Microsoft Exchange. ScanMail for Microsoft Exchange configurations include:

- Updating the scan engine, virus pattern file, and other components
- Setting up notifications and alerts
- Configuring the Real-time Scan settings, scan actions, and types of attachments to scan

For instructions on how to configure ScanMail for Microsoft Exchange, refer to *Configuring Real-time Scanning* on page 12-1, *Configuring Manual and Scheduled Scans* on page 13-1, and *Configuring Notification Messages and ActiveUpdate* on page 14-1.

6. Configure ScanMail eManager for Exchange

After configuring ScanMail for Microsoft Exchange, configure ScanMail eManager for Exchange. ScanMail eManager for Exchange configurations include:

- Configuring the spam filter
- Setting up lists of approved senders and blocked senders
- Setting up notifications and alerts
- Configuring the content filter

For instructions on how to configure ScanMail eManager for Exchange, refer to *Spam Filtering* on page 18-1.

Chapter 2

Introducing OfficeScan

This chapter introduces OfficeScan, providing an overview of its benefits, features, and architecture.

The topics discussed in this chapter include:

- *What is OfficeScan?* on page 2-2
- *OfficeScan technology* on page 2-3
- *What's new in OfficeScan* on page 2-10
- *Understanding the OfficeScan architecture* on page 2-11

What is OfficeScan?

Trend Micro OfficeScan is a centrally managed antivirus solution for desktops, notebook computers, and servers. OfficeScan helps protect your organization's Windows 2000/NT/XP/Server 2003 and Windows Me/98 computers from viruses and malicious code, including file viruses, macro viruses, and malicious Java™ applets and ActiveX™ controls.

The antivirus function of OfficeScan is provided through the client, which reports to and gets updates from the server. Configure, monitor, and update these clients via the server's management (Web) console.

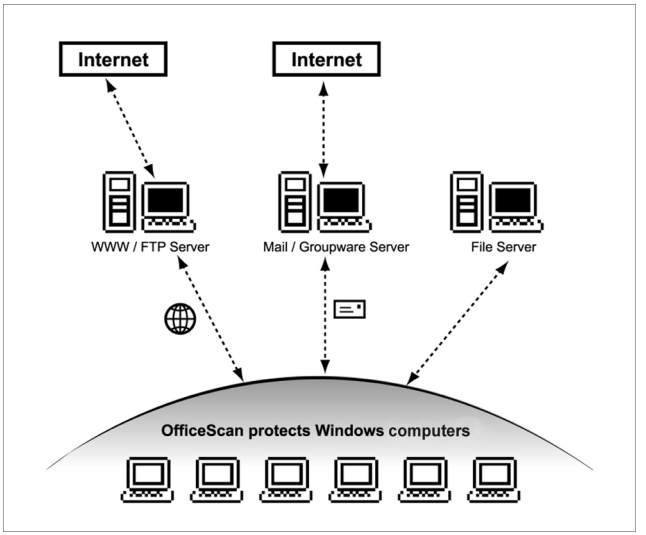

FIGURE 2-1. OfficeScan protects desktops, notebook computers, and file servers

OfficeScan includes the following components:

- OfficeScan server, which hosts the management console, downloads updates from the Trend Micro ActiveUpdate server, collects and stores logs, helps you control virus outbreaks, and manage both GateLock devices and ScanMail for Exchange servers
- OfficeScan client, which protects your Windows 2000/NT/XP/Server 2003 and Windows Me/98 computers from viruses, Trojans, and other malicious programs
- OfficeScan management console, also referred to as the Web console, which you use to manage your clients from one location

OfficeScan technology

OfficeScan is a reliable virus scanning and virus removal technology with the capabilities to protect your network environment from malicious code.

How viruses spread

In today's increasingly interconnected work place (email, the Internet, intranets, shared drives, FTP sites, removable drives, etc.) virus outbreaks can now occur in a flash. Whereas historically, viruses typically spread by sharing files or trading floppy disks, now there are many ways for a virus to infect a computer and even bring down the entire mail system, Web server, or LAN:

- Email, and email attachments
- Web traffic and sites
- FTP traffic from the Internet (file downloads)
- Shared network files and network traffic in general

How does OfficeScan work?

The server-based, centralized deployment and management features of OfficeScan give you tools to manage and enforce antivirus policies for an entire organization and to react quickly to virus emergencies from nearly anywhere using its Web console.

The OfficeScan client program is installed on Windows 2000/NT/XP/Server 2003 and Windows Me/98 computers. It scans for viruses and performs real-time reporting

of all virus incidents to the server, allowing you to view virus activities on each client from the Web console.

With the Web console, you can accomplish the following tasks:

- Configure antivirus settings
- Initiate an enterprise-wide update of components
- Scan desktop and notebook computers for viruses

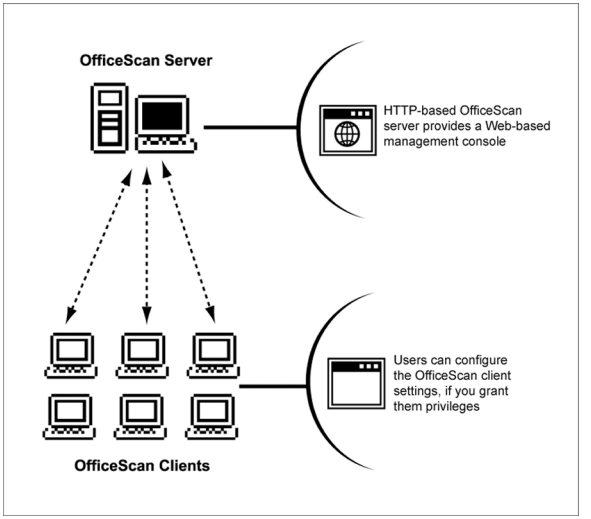

FIGURE 2-2. How OfficeScan works

What you can do with OfficeScan

Perform key administrative tasks using the OfficeScan management console:

- Analyze your network's protection against viruses
- Enforce antivirus policies
- Update your protection
- Perform virus scans from one location
- Quarantine infected files
- Control outbreaks on the network

- Manage OfficeScan domains and clients
- Protect your PDAs from viruses

Analyze your network's protection against viruses

OfficeScan can generate various types of logs, including virus logs, system event logs, update logs, and verify connection logs. Use these logs to verify update deployment, check client-server communication, and determine which computers are vulnerable to infection.

Also use these as a basis for designing and redesigning network protection, identifying computers that are at a higher risk of infection, and changing the antivirus settings accordingly for these computers.

Enforce antivirus policies

OfficeScan provides three types of scans: Real-time Scan, Scheduled Scan, and Manual Scan. Enforce your organization's antivirus policies throughout the network by configuring the three types of scans based on these policies. Specify the types of files to scan and the action to take when a virus is found.

To ensure that uniform scan settings are applied to all clients, choose not to grant privileges to clients and lock the client program with a password to prevent users from removing or turning it off.

Update your protection

New viruses are written and released via different media everyday, especially the Internet. To ensure that you stay protected against the latest threats, you must periodically update the OfficeScan components, including the pattern file, scan engine, and program. Trend Micro usually releases new virus patterns files on a weekly basis.

Perform virus scans from one location

The Web console provides the option of performing Scan Now (Manual Scan) and configuring scheduled scans on clients to run during off-peak hours when network traffic is low.

Quarantine infected files

Control live viruses and infected files by specifying a quarantine folder for all viruses detected on the network and configuring OfficeScan to automatically forward infected files to the quarantine folder. If you encounter files infected with new viruses that OfficeScan cannot clean, contact Trend Micro technical support.

Control outbreaks on the network

Defining the criteria for an outbreak and setting up outbreak notifications allows you to quickly respond to outbreaks that may be developing on the network. When you receive an outbreak notification, enable Outbreak Prevention to prevent viruses from spreading.

By blocking shared folders and vulnerable ports and denying write access to files on clients, Outbreak Prevention helps prevent the outbreak from overwhelming your network. Download the latest pattern file (if any), and then perform Scan Now on all clients to remove any existing virus.

Manage OfficeScan domains and clients

A domain in OfficeScan is a group of clients that share the same configuration and run the same tasks. An OfficeScan domain is different from a Windows domain. There can be several OfficeScan domains in one Windows domain.

Group clients into domains to simultaneously apply the same configuration to all domain members, making clients easier to manage.

Protect your PDAs from viruses

Viruses and other malicious code can infect your personal digital assistant (PDA) devices during beaming, synchronization, or Internet access. Protect your Palm™, Pocket PC™, or EPOC™ devices from these threats by installing OfficeScan for Wireless.

To install OfficeScan for Wireless on your Palm, Pocket PC, or EPOC device, open the client console and download Wireless Protection Manager.

For detailed instructions on how to install OfficeScan for Wireless, refer to the help topic *Protecting your PDA* on the OfficeScan client.

For more information on OfficeScan for Wireless, refer to the *Windows Protection Manager Manual*. In Windows Explorer, you can also open the Quick Start Guide by double-clicking `Wireless Protection Manager Manual.pdf` in the `Trend Micro\Wireless Protection Manager` folder.

Note: To open `Wireless Protection Manager Manual.pdf`, you must have Adobe™ Reader™ installed. You can download Acrobat Reader for free from `www.adobe.com`.

Benefits and Capabilities

OfficeScan brings many benefits to your organization by providing a comprehensive yet user-friendly method of managing your antivirus initiatives. The following is a summary of the advantages you can obtain with OfficeScan.

Single-console operation

OfficeScan server allows you to manage your entire anti-virus system through a single Web console. The Web console is installed when you install the HTTP-based version of the OfficeScan server and uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Virus Outbreak Monitor

Virus Outbreak Monitor gets OfficeScan clients involved in virus-detection. Clients can notify the OfficeScan server when they detect suspicious activity occurring on the network. OfficeScan can then send an automatic notification message to the administrator to take proper action.

Outbreak Prevention

With Outbreak Prevention, you can take preemptive steps to secure your network:

- Block shared folders to help prevent viruses from infecting files in shared folders
- Block ports to help prevent viruses from using vulnerable ports to infect files on the network
- Deny write access to files and folders to help prevent viruses from modifying files

- Create an alert message to display on OfficeScan clients when an outbreak prevention policy is created

Trend Micro IntelliScan

IntelliScan is a new method of identifying files to scan. For executable files (for example, .zip and .exe), the true file type is determined based on the file content. For non-executable files (for example, .txt), the true file type is determined based on the file header. Using IntelliScan provides the following benefits:

- Performance optimization — IntelliScan does not affect crucial applications on the client because it uses minimal system resources
- Shorter scanning period — Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than when you scan all files.

Trend Micro ActiveAction

Different types of viruses require different scan actions. Customizing scan actions for different types of viruses requires knowledge about viruses and can be a tedious task. ActiveAction is a set of pre-configured scan actions for viruses and other types of malware. The recommended action for viruses is Clean, and the alternative action is Quarantine. The recommended action for Trojans and joke programs is Quarantine. 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 that are 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 help 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.

Typical virus types

Tens of thousands of viruses are known to exist, with more being created each day. Although once most common in DOS or Windows, computer viruses today can often wreak instantaneous havoc by exploiting vulnerabilities in corporate email systems

and Web sites. Associated virus prefixes help identify virus types in logs and reports. A list of common virus categories and their prefixes are as follows:

- ActiveX malicious code – ATVX
- Boot sector viruses – no prefix
- COM and EXE file infectors – PE, NE, or no prefix
- Executable and Link format – ELF
- Joke programs – JOKE
- Java malicious code – JAVA
- Macro viruses – W2KM, W97M, X97M, P97M, A97M, WM, XM, V5M
- Trojan horses – TROJ
- VBScript, JavaScript or HTML viruses – VBS, JS, HTML
- Worms – 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.

Trend Micro Damage Cleanup Services

If OfficeScan detects a virus on your system, it can scan and clean infected files and folders. However, dangerous virus remnants that can re-attack your network may remain. You can run Trend Micro Damage Cleanup Services (DCS) to clean system registries and terminate any active Trojan and worm processes. OfficeScan can then rescan and clean any remaining infected files and directories.

Through OfficeScan server, notify clients to run DCS using the latest damage cleanup template that OfficeScan can download from TrendLabs.

Secure Web console communication

OfficeScan provides secure communications between the OfficeScan server and the Web console browser through two new security features:

Secure Socket Layer (SSL): OfficeScan server can generate a certificate for each Web console session, allowing the Web Console browser to encrypt data based on Public Key Infrastructure (PKI) cryptography standards. The default time period for the certificate is three years.

Note: SSL is available only when you use Microsoft IIS server as your OfficeScan Web server.

What's new in OfficeScan

This version of OfficeScan inherits all the features of previous versions and provides the following enhancements tailored for small and medium-sized businesses:

- **Virus Outbreak Monitor**– Use Virus Outbreak Monitor to get clients involved in monitoring the network for suspicious activity that may indicate malware infections
- **Outbreak Prevention** – Activate Outbreak Prevention during a virus outbreak to block specified folders and ports, and deny write access to specified files and folders
- **Policy Manager** – Use Policy Manager to import and export client policies, which include scan settings, and privileges
- **Advanced Search** – When you want to modify client settings, such as scan settings and privileges, you can search for specific clients and GateLock devices based on a wide range of criteria, such as IP address, online status, and virus pattern file version
- **Damage Cleanup Services** – Run Cleanup Now to detect Trojans and other malware. Damage Cleanup Services can also delete Trojan processes and the files they produce, as well as recover modified system files and restore your system settings to their original pre-infection state
- **Manage GateLock devices** – Configure GateLock virus scan settings, network zones, and interfaces, manage VPN tunnels and policies, and check GateLock device status
- **Manage ScanMail for Exchange** – Install and manage ScanMail for Exchange on clients through remote consoles that can be accessed through the OfficeScan Web console
- **HTTP Server Selection** – Install OfficeScan server on the included Apache HTTP server (Windows 2000 computers only) or on your own pre-installed Microsoft IIS server

- **Protection from spyware** – OfficeScan protects clients from software that installs components on a computer for the purpose of recording Web surfing habits
- **Windows server protection** – OfficeScan protects Windows servers without requiring you to install any additional components

Understanding the OfficeScan architecture

OfficeScan is a three-tier application consisting of the following parts:

- The server, which hosts the management console and downloads updates from the Trend Micro update server
- The client, which protects Windows 2000/NT/XP/Server 2003 and Windows Me/98 computers from viruses, Trojans, and other malicious programs
- The management console (Web console), which you use to configure and manage the clients from one location

OfficeScan server

The OfficeScan server is the central repository for all client configurations, virus logs, and client software and updates.

The server performs these important functions:

- It installs, monitors, and manages clients on the network
- It downloads pattern, scan engine, and program updates from the Trend Micro update server, and then distributes them to clients

Note: This version of OfficeScan only supports the HTTP-based server.

HTTP-based server

The HTTP-based server is installed on a Windows NT, Windows 2000, Windows XP, or Windows Server 2003 with Internet Information Server™ (IIS) 4.0 or later. You may also install Apache web server 2.0 or later on Windows 2000 machines. The HTTP-based server is capable of providing real-time, bidirectional communication between the server and clients.

If you install an HTTP-based server, you manage the clients from a Web browser-based management console, which you can access from virtually anywhere on the network.

As the name indicates, an HTTP-based server communicates with the client (and vice versa) via HyperText Transfer Protocol (HTTP). An HTTP-based server can only install HTTP-based clients. You cannot install an HTTP-based client if the client computer does not support TCP/IP (see Figure 2-3).

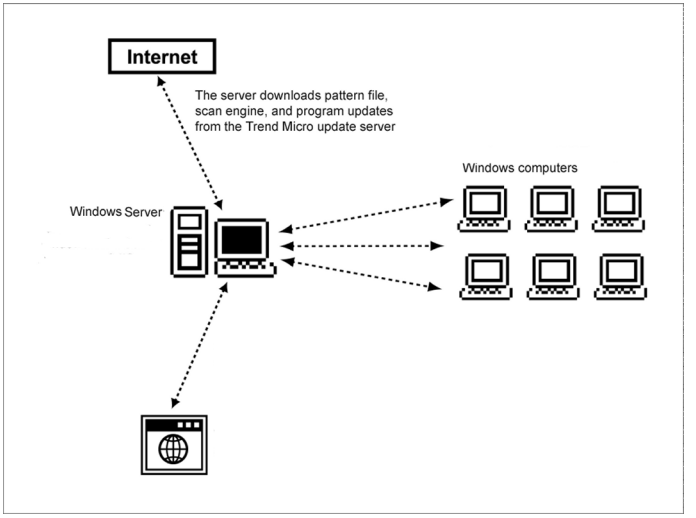

FIGURE 2-3. How the HTTP-based server works

OfficeScan client

Protect Windows computers from viruses by installing the OfficeScan client on each computer. The client provides three methods of scanning – Real-time Scan, Scheduled Scan, and Manual Scan.

The client reports to the parent server from which it was installed. It sends events and status information to the server in real time to provide you with updated client information. Examples of events are virus detection, client startup, client shutdown, start of a scan, and completion of an update.

Scan settings on clients can be configured from the client console (if you grant users this privilege) and the management console. To enforce uniform desktop protection across the network, choose not to grant the clients privileges to modify the scan settings or to remove the client program.

Tip: If you have clients in low-bandwidth remote offices reporting to the server in the main office, Trend Micro recommends installing Remote Agent on these clients. Remote Agent minimizes bandwidth usage by allowing a single client to download updates from the Trend Micro ActiveUpdate server and share these updates with other clients. For more information on Remote Agent, refer to the *Remote Agent Configuration Guide*.

OfficeScan clients are classified into two categories:

- Normal clients
- Roaming clients

Normal clients

Normal clients are computers with the OfficeScan client installed that are stationary and that maintain a continuous network connection with the server.

Icons that appear in a client's system tray indicate the status of the normal client. See Table 2-1 for a list of icons that appear on the normal client.

Icon	Description	Real-time scan	Manual and scheduled scans
	Normal client	Enabled	Enabled
	Pattern file is outdated	Enabled	Enabled
	Scan Now, manual scan, or scheduled scan is running	Enabled	Enabled
	Real-time scan is disabled	Disabled	Enabled
	Real-time scan is disabled and the pattern file is outdated	Disabled	Enabled
	Real-time Scan Service is not running	Disabled	Disabled

Icon	Description	Real-time scan	Manual and scheduled scans
	Real-time Scan Service is not running and the pattern file is outdated	Disabled	Disabled
	Disconnected from the server	Enabled	Enabled
	Disconnected from the server and the pattern file is outdated	Enabled	Enabled
	Disconnected from the server and real-time scan is disabled	Disabled	Enabled

TABLE 2-1. Icons that appear on a normal client

Roaming clients

Roaming clients are computers with the OfficeScan client installed that do not always maintain a constant network connection with the server, such as notebook computers. These clients continue to provide antivirus protection, but have delays in sending their status to the server.

Assign roaming privileges to clients that are disconnected from the OfficeScan server for an extended period of time. Roaming clients do not accept commands/requests from the server, except when you select the **Including roaming client(s)** check box on the client update screens (**Manual Deployment** and **Automatic Deployment**).

Roaming clients get updated only on these occasions:

- When the client performs an Update Now
- When you configure automatic update deployment and select **Include roaming clients** on the **Automatic Deployment** screen

For more information on how to update clients, see *Updating clients* on page 5-20.

The status of a roaming client is indicated by icons that appear in its system tray. See Table 2-2 for a list of icons that appear on roaming clients.

Icon	Description	Real-time scan	Manual and scheduled scans
	Roaming client	Enabled	Enabled
	Real-time scan is disabled	Disabled	Enabled
	Pattern file is outdated	Enabled	Enabled
	Real-time scan is disabled and the pattern file is outdated	Disabled	Enabled
	Real-time Scan Service is not running	Disabled	Disabled
	Real-time Scan Service is not running and the pattern file is outdated	Disabled	Disabled

TABLE 2-2. Icons that appear on the roaming client

About Damage Cleanup Services

OfficeScan also protects Windows computers against Trojans (or Trojan horse programs) using a built-in Trojan cleaner called Damage Cleanup Services (DCS).

A Trojan is a malicious program that masquerades as a harmless application. Trojans do not replicate like viruses but can just be as destructive. Traditional antivirus solutions can detect and remove most viruses but are often unable to do the detect Trojans, especially those that are already running on the system.

DCS detects and removes live Trojans and repairs system files that were modified by Trojans. It kills Trojan processes and deletes files that they have dropped.

The OfficeScan server executes DCS on the client when you do the following:

- Run Cleanup Now from the Web console
- Run Scan Now from the Web console and OfficeScan finds a Trojan
- Enable a manual, scheduled, or real-time scan and OfficeScan finds a Trojan
- Enable a scheduled clean
- Run DCS from OfficeScan client on a client computer

Because DCS is automatically executed, you do not need to configure it to help ensure that clients are protected against Trojans. Users are not even aware when it is executed because it runs in the background (when the client is running). However, DCS may sometimes require the user to restart the computer to complete the process of removing a Trojan from the computer.

Management (Web) console

The management console is the central point for monitoring OfficeScan across the entire network, as well as for configuring server and client settings.

It gives you complete control over desktop and notebook computers' antivirus settings. Use to the management console to do the following:

- Deploy the client to desktop and notebook computers
- Group desktop and notebook computers into logical domains for simultaneous configuration and management
- Set scan configurations and start manual scan on a single computer or on multiple computers
- Receive notifications and view log reports for virus activities
- Receive notifications when viruses are detected on clients and send virus outbreak alerts via email, pager, SNMP Trap, or Windows Event Log
- Control outbreaks by configuring and enabling Outbreak Prevention

The Web browser-based management console, or Web console, is installed when you install the HTTP-based version of the OfficeScan server. The Web console uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

Open the Web console from any computer on the network that has the required Web browser and communication protocols.

Chapter 3

Planning for Deployment

This chapter explains how to plan your network environment for the deployment of OfficeScan Server and OfficeScan for clients.

The topic discussed in this chapter is:

- *Planning for deployment* on page 3-2

Planning for deployment

To take advantage of the benefits OfficeScan can bring your organization, you will need an understanding of the possible ways to deploy OfficeScan Server and OfficeScan clients. This section provides an overview of deployment architectures and strategies, network traffic planning, and an approach to pilot deployment.

Deployment architectures

Deploying enterprise-wide, client-server software like OfficeScan to a homogenous or heterogeneous environment requires careful planning and assessment.

Note: This version of OfficeScan does not support multiple-site server installation.

Overview of installation and deployment

This guide groups installation and deployment tasks into three phases. Each phase has corresponding sections that discuss in detail the tasks that you need to perform.

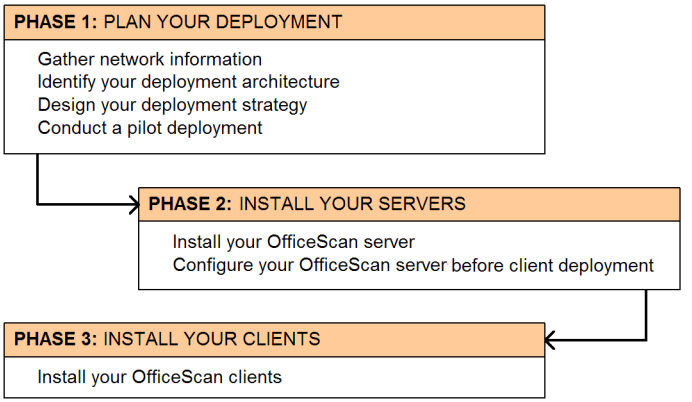

FIGURE 3-1. Installation and deployment tasks

Phase 1 summary

During phase 1, plan how best to deploy OfficeScan by completing these tasks:

- Determine the number of clients
- Plan the placement of the program files
- Determine the number of domains
- Decide how to deploy the client

Trend Micro highly recommends conducting a pilot deployment before doing a full-scale deployment.

If you are deploying OfficeScan to multiple sites, you need to perform these additional tasks:

- Determine the number of sites
- Plan for network traffic
- Determine where you need to install the servers
- Decide how to deploy the server
- Decide how to deploy the clients

Refer to the succeeding sections for details.

Phase 2 summary

During phase 2, start implementing the plan you have created in phase 1 for server installation. You complete this phase by performing the following tasks:

- Verify that your server meets the minimum system requirements
- Prepare for server installation
- Install your OfficeScan server
- Verify that the installation was successful
- Check if you need to modify the default settings (for example, scan settings and privileges) before deploying the clients

Refer to *Installing OfficeScan Server* starting on page 4-2 for details.

Phase 3 summary

During phase 3, complete your installation and deployment by rolling out the client to your desktop and notebook computers. You complete this phase by performing the following tasks:

- Verify that the target computers meet the minimum system requirements
- Prepare for client installation
- Roll out your clients using Trend Micro tools or third-party tools

Refer to *Installing OfficeScan clients* starting on page 4-12 for details.

Deploying OfficeScan Server

This section provides information on deploying the OfficeScan server.

Determining the number of clients

A client is a computer that has the OfficeScan client software installed on it. This includes desktop and notebook computers, including those that belong to users who telecommute or connect to the corporate network from their homes.

If you have a heterogeneous client base (that is, if your network has different Windows operating systems, such as Windows 2003, XP, 2000, NT, Me, and 98), identify how many clients are using a specific Windows version. Use this information to decide which client deployment method will work best in your environment.

Planning for network traffic

When planning for deployment, consider the network traffic that OfficeScan will generate. OfficeScan generates network traffic when the server and client communicate with each other.

The server generates traffic when it does the following:

- Connects to the Trend Micro update server to check for and download updated components
- Notifies clients to download updated components
- Notifies clients about configuration changes

The client generates traffic when it does the following:

- Starts up
- Performs scheduled update
- Switches between roaming mode to normal modes
- Performs Update Now

Network traffic during pattern file updates

Significant network traffic is only generated when there is an updated version of the virus pattern file, scan engine, program, spyware pattern file, and Damage Cleanup Services. To reduce network traffic generated during pattern file updates, OfficeScan uses a method called incremental update. Instead of downloading the full pattern file every time it is updated, only the new patterns that have been added since the last release are downloaded. These new patterns are merged with the old pattern file.

If clients are regularly updated, they only have to download the incremental pattern, which is around 500KB to 900KB. If clients are not regularly updated, they may have to download the full pattern, which is around 2.5MB to 3MB when compressed and 5MB when uncompressed.

Trend Micro releases new pattern files every week. However, if a particularly damaging virus is actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available.

Determining to install a dedicated server

When selecting a server that will host OfficeScan, consider the following:

- How much CPU load is the server carrying?
- What other functions does the server perform?

If you are installing OfficeScan on a server that has other uses (for example, application server), Trend Micro recommends that you install on a server that is not running mission-critical or resource-intensive applications.

Planning the placement of program files

During the OfficeScan server installation, specify where to install the program files on the clients. Either accept the default client installation path or modify it. Trend

Micro recommends that you use the default settings, unless you have a compelling reason (such as insufficient disk space) to change them.

The default client installation path is:

```
C:\Program Files\Trend Micro\OfficeScan Client
```

Determining the number of domains

A domain in OfficeScan is a group of clients that share the same configuration and run the same tasks. By grouping your clients into domains, you can simultaneously configure, manage, and apply the same configuration to all domain members.

An OfficeScan domain is different from a Windows domain. There can be several OfficeScan domains in one Windows domain.

For ease of management, plan how many OfficeScan domains to create. Group clients based on the departments they belong to or the functions they perform. or group together clients that are at a greater risk of infection, to simultaneously apply a more secure configuration to all of them.

Deciding how to deploy the client

OfficeScan provides several client deployment methods. Determine which ones are most suitable for your environment. For a complete list of available client deployment methods, see *Installing OfficeScan clients* on page 4-12.

For single site deployment, IT administrators can choose to deploy using Login Script Setup, wherein a program called `autopcc.exe` is added to the login script. When an unprotected client logs on to the domain, the server detects it and automatically deploys the client setup program. The OfficeScan client is deployed in the background and the client user does not notice the installation process.

In organizations where IT policies are strictly enforced, client installation via the internal Web page is recommended. The administrator sends out an instruction to users to visit an internal Web page where they can install the OfficeScan client with just a click of the button.

Conducting a pilot deployment

Before performing a full-scale deployment, Trend Micro recommends that you first conduct a pilot deployment in a controlled environment. A pilot deployment provides an opportunity for feedback to determine how features work and the level of support you will likely need after full deployment.

It also gives the installation team a chance to rehearse and refine the deployment process and test if your deployment plan meets your organization's business requirements.

Perform the following tasks to conduct a pilot deployment:

- Choose a pilot site
- Create a rollback plan
- Deploy your pilot
- Evaluate your pilot deployment

Choosing a pilot site

Choose a pilot site that matches your production environment. Try to simulate the type of topology that would serve as an adequate representation of your production environment.

Creating a rollback plan

Trend Micro recommends creating a disaster recovery or rollback 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.

Deploying your pilot

Evaluate the different deployment architectures (see *Deployment architectures* on page 3-2) to see which ones are suitable for your particular environment.

Evaluating your pilot deployment

Create a list of successes and failures encountered throughout the pilot process. Identify potential "pitfalls" and plan accordingly for a successful deployment. This pilot evaluation plan can be rolled into the overall production deployment plan.

Chapter 4

Deploying and Installing OfficeScan

This chapter explains installation of OfficeScan Server and OfficeScan for clients. It also illustrates how to migrate and upgrade to this current version.

The topics discussed in this chapter include:

- *Installing OfficeScan Server* on page 4-2
- *Registering OfficeScan* on page 4-9
- *Installing OfficeScan clients* on page 4-12
- *Migrating to and Upgrading OfficeScan* on page 4-32

Installing OfficeScan Server

This section provides information on installing OfficeScan server.

Minimum system requirements

The following are minimum requirements to install the OfficeScan server:

- 300MHz Intel Pentium™ II processor or equivalent
- Microsoft™ Windows™ NT series, Windows 2000 series, Windows XP, Windows Server 2003, or Small Business Server 2000
- 128MB of RAM
- 300MB of disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft™ Internet Explorer 5.5 or later
- Microsoft™ Internet Information Server (IIS) 4.0 or later or Apache Web server 2.0 or later (for Windows 2000 machines only)

Minimum system requirements for the Web console

HTTP-based server installation also includes Web console installation. However, if you plan to open the Web console using other computers on the network, these computers must have the following:

- 133MHz Intel Pentium processor or equivalent
- 64MB of free RAM
- 30MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher
- Microsoft Internet Explorer 5.5 or later

Preparing for server installation

To help you deploy OfficeScan to your network smoothly, check the following items before installing the server:

- Where to run the setup program
- Required protocols

- Required rights
- Required restarts
- Required information
- Shared directories
- Windows licenses
- TCP port for HTTP communication

Running setup

Run the setup program on any computer running:

- Windows XP
- Windows 2000 Server/Advanced Server/Professional
- Windows NT series
- Windows Server 2003
- Small Business Server 2003

Required protocols

Before starting the installation, ensure that the server and clients have Transmission Control Protocol/Internet Protocol (TCP/IP) installed.

Required rights

To install the server, you must have administrator or domain administrator rights to the target computer.

Required restarts

Installing the OfficeScan server does not require you to restart the computer. After completing the installation, immediately configure the server, and then proceed to rolling out clients.

While installing the Web server, the setup program automatically stops and restarts the IIS service.

WARNING! *Make sure that you do not install the server on a computer that is running applications that might lock IIS, which will cause the installation to be unsuccessful.*

Required information

Have the following information ready before starting the installation:

- **Registration Key/Activation Code**. Your version of OfficeScan comes with a Registration Key. During installation, OfficeScan prompts you to enter the Activation Code and can redirect you to the Trend Micro Web site. Register your version of OfficeScan with the Registration Key and Trend Micro will provide you the Activation Code.
- **Proxy information**. If a proxy server handles Internet traffic on your network, you must type the proxy server information and your user name and password to be able to download the latest virus pattern, scan engine and program from the Trend Micro update server. If you leave the proxy information blank during installation, you can still configure it on the OfficeScan console.
- **Console password**. To prevent unauthorized access to the OfficeScan Web console, specify a password that will be required of anyone who tries to open the console.
- **Custom client virus alert message (optional)**. When the OfficeScan client detects a virus on a computer during real-time scan, a virus alert message appears. Customize the message that is displayed on the clients.
- **Client software installation path (optional)**. Configure the client installation path where OfficeScan files will be copied to during client setup.

Shared directories

Before installing the server, you must share a directory on the server (with write privileges) where you want the program files to be installed. The setup program will prompt for this shared folder during master setup.

If you plan to use Login Script Setup to install the clients, you must share the target directory as `admin$`.

Windows licenses

Make sure your organization has sufficient licenses for all clients to simultaneously connect to the server.

TCP port for HTTP communication

Most hacker and virus attacks these days are delivered over HTTP. A large number of these attacks are directed at port 80, which is used in most organizations as the default Transmission Control Protocol (TCP) port for HTTP communication.

If your organization is currently using port 80 as its HTTP port, Trend Micro recommends using another port number that is less susceptible to hacker and virus attacks.

OfficeScan uses the same port number as your HTTP server's TCP port. Setup automatically retrieves this information when you install the OfficeScan server. If you are currently using port 80 as your HTTP port and want to change to another port number, do this before installing the OfficeScan server. Otherwise, reinstall the OfficeScan server to ensure successful client-server communication.

Running master setup to install OfficeScan server

Before running the OfficeScan setup program, try testing the server's fully-qualified domain name using the "ping" command in Windows to ensure that communication with it can be established. Also test the port number, IIS anonymous user logon, and the network's proxy settings.

Note: You need to remove the server program of your existing third-party antivirus software before installing the OfficeScan server.

WARNING! *Close any running applications before installing the server. If you install while other applications running, the installation process may take longer to complete.*

To install OfficeScan server:

1. Open the folder that contains the setup files and double-click **Setup** (`SETUP.EXE`). The **Welcome** screen appears.

2. Click **Next**. The **Software License Agreement** screen appears.
3. Read the agreement carefully, then click **Yes** to agree to all terms. The **Web Server** screen appears.
4. Select one of the following options:
   - **Install OfficeScan on the IIS server** – click to install OfficeScan server on an already-installed version of IIS server (version 4.0 or later)
   - **Install OfficeScan server on Apache web server 2.0**– click to install OfficeScan on an Apache Web server (version 2.0.47 or later). OfficeScan will install Apache 2.0.47 on the server if no previous Apache installations exist.

Note: Select the Apache server for machines running Windows 2000 only.

---

5. Click **Next**. the **Server Information** screen appears.
6. Specify how clients will identify the server by clicking either **Domain name** or **IP address**.
   - If you click **Domain name**, verify that the server's domain name is correct. Use the server's fully qualified domain name (FQDN) if necessary to ensure successful client-server communication.
   - If you click **IP address**, verify that the server's IP address is correct.

Note: Do not select **IP address** if the server's IP address is subject to change (as in a DHCP environment).

Tip: If the server has multiple network interface cards (NICs), Trend Micro recommends using one of the IP addresses, instead of the domain name or FQDN, to ensure successful client-server communication.

---

7. If you selected to install OfficeScan on an IIS server, select one of the following in the **IIS web site** section. The difference between these two selections is where IIS locates the web site on its domain tree.
   - **IIS default web site** – click to install OfficeScan server under IIS's default Web site list

- **IIS virtual web site** – click to install OfficeScan server as an independent Web site

8. Type a port to server as the server listening port. The OfficeScan server's address will be as follows:
   - http://{OfficeScan_Server_Name}:{port number}
9. If you selected to install OfficeScan on an IIS server, you also have the option of enabling Secured Socket Layer (SSL) security. Select the **Enable SSL** check box. Type the number of years to keep the SSL certificate valid (the default is 3 years) and type an SSL port number. If you enable SSL, this port number will serve as the server's listening port. The OfficeScan server's address will be as follows:
   - https://{OfficeScan_Server_Name}:{port number}

Note: Trend Micro recommends enabling SSL to enhance security between the Web console and the server. See *OfficeScan secure communication* on page 2-9 for more information on SSL.

If you want to change the target directory location to install OfficeScan server, click **Browse** and select or create a new folder.

10. Click **Next**. A confirmation window appears. Verify that the port number is correct. OfficeScan uses the same TCP port number that your HTTP server is using. Setup automatically retrieves this port number and displays it on this screen.

    Make sure your HTTP port number and the port number are the same. This will be the port number on the server through which the administrator connects to the Web console.
11. Click **Yes**. The **Proxy Server** screen appears. If your organization uses a proxy server, type the required information such as the proxy address, port, and your user name and password for proxy server authentication. If your organization uses SOCKS 4, select the **Use SOCKS 4** check box.

    Verify that the information you provided on-screen is correct. The server uses this information to connect to the Trend Micro update server and download updated components, such as pattern files and scan engines.
12. Click **Next** to continue. The **Administrator Account Password** screen appears. Type your password and confirm that password in the text boxes. This helps

prevent unauthorized users from accessing the management console and modifying the settings or removing the clients.

13. Click **Next**. The **Server Settings Finished** screen appears. This screen indicates that OfficeScan will continue with the configuration of client settings.
14. Click **Next**. The **Components Selection** screen appears.
15. Select the components to install by selecting their corresponding check boxes. Select the **Install client protections to target OfficeScan server** check box to install OfficeScan client on the server machine.

Tip: Trend Micro recommends installing the OfficeScan client to the server machine to help protect the server and take advantage of OfficeScan client's virus protection capabilities.

---

16. If you do not have the OfficeScan Activation Code, click **Register Online**. The browser will redirect to the Trend Micro Web site, where you can enter the Registration Key that came with your product. Use that to register your version of OfficeScan and Trend Micro will send you an Activation Code. When you have the Activation Code, click **Next**. The **Product Activation Code** screen appears.
17. Type the Activation Code for OfficeScan Standard Antivirus. If you want to install Damage Cleanup Services, also type the Damage Cleanup component Activation Code.
18. Click **Next**. The **Client Installation Path** screen appears. The client installation path is where the client setup program will place program files during client installation. The default client installation path is `$Program Files\Trend Micro\OfficeScan Client`. Type a port number to serve as the client listening port (trusted port). Click **Next**. A confirmation screen appears.
19. Click **OK**. The **Select Program Folder** window appears.
20. Setup will add program icons to the folder listed under **Program Folders**. Type a new folder name, or select an existing folder from the list. Click Next to continue. The **Client Alert Message** screen appears.
21. Accept the default client virus alert message or customize it. The clients see the virus alert message whenever OfficeScan detects a virus. Click **Next**. The **Client Settings Finished** screen appears.

22. Click **Next** to begin installation. The OfficeScan server installation progress screen appears, followed by the **Shared Folder** screen, indicating the creation of the shared directory.
23. Click **Next**. The OfficeScan client installation progress screen appears, followed by the **Setup Complete** screen.

    OfficeScan server installation is complete. Open the Web console or view the readme file by selecting the corresponding check box.
24. Click **Finish** to close the setup program.

Verifying a successful installation

After completing the installation, verify that the OfficeScan server properly installed.

To verify the installation, do the following:

- Look for the OfficeScan program shortcuts on the Windows **Start** menu of OfficeScan server
- Check if OfficeScan is in the **Add/Remove Programs** list of the OfficeScan server's Control Panel
- Log on to the Web console with the server's URL:

  http://{OfficeScan_server_Name}:{port number}

  If using SSL:

  https://{OfficeScan_server_Name}:{port number}

Registering OfficeScan

Before registering OfficeScan, please read the Trend Micro license agreement:

License Agreement: The Corporate License Agreement gives the Customers a perpetual right to our software under the terms and conditions of the License Agreement in the sense that the Customer has the right to use the last version of the software they installed before letting Maintenance lapse. Our software will not be as useful without the updates, but the customer is not required to remove it.

The License Agreement can be viewed from the Registration screen of the product console and in the Registration Web.

To get the Activation Code:

- Before installing OfficeScan, find the included Registration Key
- Fill out the Online Registration form at www.trendmicro.com/support/registration.asp
- Trend Micro will give you an Activation Code to enter when you install OfficeScan

Viewing OfficeScan and component license information

View detailed information about your licenses online, including the current license status.

To view current license information and status:

1. Open the OfficeScan Web console.
2. On the sidebar, click **Administration** > **Product License** on the sidebar. The **Product License** screen appears.
3. Click **View detailed license online** to see your license and click the **Check Status Online** button to see the status of your license.

Activating a component license

You must register a component before using it. You will need the component Activation Code or Registration Key for activation.

To activate a new license:

1. Click **Administration** > **Product License** on the sidebar, then click **Enter a new code for the component you want to register**. The **Enter a New Code** screen appears.
2. Enter the Activation Code and click **Activate**. If you do not have the Activation Code, click the register online link at the top of the screen and use the Registration Key that came with your product.

Setting a Product Registration proxy

If your network uses a proxy server to connect to the Internet, configure proxy settings to connect to the Product Registration server.

To set the Internet proxy:

1. Open the OfficeScan Web console.
2. On the sidebar, click **Administration** > **Product License** > **Product Registration Proxy**. The **Product Registration Proxy** screen appears.
3. Select the **Use a proxy server** check box.
4. Type the address of the proxy server and its port number.
5. If your proxy server uses version 4 of the SOCKS protocol to handle Transmission Control Protocol (TCP), select the **Use SOCKS 4** check box.
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.

Default OfficeScan Server Settings

When you install OfficeScan server, the following default settings will apply. You may change the default settings to customize your installation.

- **Web Server** – IIS Server

  A version of IIS server must already be installed on your computer if you keep the default selection.

  If you select the Apache web server and it is not already installed on your computer, OfficeScan installation automatically installs Apache Web server 2.0.47 (for Windows 2000 only).

- **Components** – Standard Antivirus, Damage Cleanup

  Standard antivirus protection installs the Trend Micro antivirus scan engine on client computers so client users can perform manual scans and have the maximum level of protection with real-time scan. Damage Cleanup installs the Trend Micro Damage Cleanup Services to remove remnants of Trojans that may exist on the system if an infection occurs.

- **Default Server Port** – 8080
- **SSL Port** – 4343
- **Target Directory** – C:\Program Files\Trend Micro\OfficeScan
- **Shared Folder Directory** – C:\Program Files\Trend Micro\OfficeScan\PCCSRV

- **Client-Server Port (Trusted Port)** – OfficeScan generates a random port number

  OfficeScan server uses this port to communicate with OfficeScan clients. Ensure that this port does not conflict with your network environment.
- **Client Alert Message** – OfficeScan displays an alert message on an infected client whenever a virus is detected. A general message is provided during installation. If you do not want an message to appear, delete it. Create a new message at any time through the Web console.

Uninstalling the OfficeScan server

OfficeScan uses an uninstal program to safely remove OfficeScan server from your computer. Remove all clients before removing the server.

To remove the OfficeScan server:

1. On the computer you used to install the server, click **Start** > **Programs** > **{OfficeScan program group}** > **Uninstall OfficeScan**.

   A confirmation screen appears.
2. Click **Yes**. Master Uninstaller, the server uninstallation program, prompts you for the administrator password.
3. Type the administrator password in the text box and click **OK**. Master Uninstaller then starts removing the server files. A confirmation message appears.
4. Click **OK** to close the uninstallation program.

Installing OfficeScan clients

This section provides information on installing OfficeScan clients.

Minimum system requirements

The OfficeScan client has a slightly different set of requirements for Windows Me/98, Windows 2000/NT and Windows XP/2003.

Minimum system requirements for the Windows Me/98 client

To install the client to Windows Me/98 computers, they must have the following:

- 133MHz Intel™ Pentium™ processor or equivalent
- Microsoft Windows 98/98 SE/Me
- 64MB of RAM
- 80MB of disk space
- Monitor that supports 640 x 480 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.01 or later

Minimum system requirements for the Windows 2000/NT client

To install the client to Windows 2000/NT computers, they must have the following:

- 150MHz Intel Pentium processor or equivalent
- Microsoft Windows NT 4.0 Workstation/Server with SP5 or above, Windows 2000 Server/Advanced Server/Professional with SP2 or above
- 64MB of RAM
- 80MB of disk space
- Monitor that supports 640 x 480 resolution at 256 colors or higher
- Microsoft Internet Explorer 4.01 or later

Minimum system requirements for the Windows XP/2003 client

To install the client to Windows XP/2003 computers, they must have the following:

- 300MHz Intel Pentium processor or equivalent
- Microsoft Windows XP with SP1 or above or Windows 2003
- 128MB of RAM
- 80MB of disk space
- Monitor that supports 800 x 600 resolution at 256 colors

Preparing for installation using Trend Micro Vulnerability Scanner

Use Trend Micro Vulnerability Scanner to identify the desktop and notebook computers on your network that are not protected against viruses. This tool checks computers on your network for installed antivirus software based on an IP address range you specify.

Get Vulnerability Scanner from the `\PCCSRV\Admin\Utility\TMVS` folder of the OfficeScan server.

For more information on Vulnerability Scanner, see*Vulnerability Scanner* on page A-4 in Appendix A.

Installing OfficeScan clients

OfficeScan provides several methods to deploy the client. This section discusses the various deployment methods to help you decide which will work best in your environment.

Install OfficeScan client with any of the following methods:

- **Internal Web page** – instruct the users in your organization to go to the internal Web page and download the client setup files
- **Login Script Setup** – automate the installation of the OfficeScan client to unprotected computers when they log on to the network
- **Client Packager** – deploy the client setup or update files to client via email. This is especially useful for low-bandwidth remote offices
- **Windows Remote Install** – install the client program on all Windows XP/2000/NT/2003 clients from your Web console
- **From a client disk image** – create an image of an OfficeScan client and make clones of it to other computers on your network
- **Vulnerability Scanner (TMVS)** – install the client program on all Windows 2003/XP (Professional Edition Only) /NT/2000 clients with the Trend Micro Vulnerability Scanner
- **Microsoft System Management Server (SMS)** – use Microsoft System Management Server (SMS) to distribute the client program

Table 4-1 summarizes the benefits of each client deployment method.

	Web page	Login scripts	Client packager	Windows Remote Install	Client image setup	TMVS	Microsoft SMS
Suitable for deployment across the WAN	No	No	Yes	No	Yes	Yes	Yes
Suitable for centralized administration and management	No	Yes	No	Yes	Yes	Yes	Yes
Requires client user intervention	Yes	No	Yes	No	No	Yes	Yes
Requires IT resource	No	Yes	Yes	Yes	Yes	Yes	Yes
Suitable for mass deployment	No	Yes	Yes	No	Yes	Yes	Yes
Bandwidth consumption	Low, if scheduled	High, if clients are started at the same time	Low, if scheduled	Low, if scheduled	Low, if scheduled	Low, if scheduled	Low, if scheduled

TABLE 4-1. OfficeScan client deployment tools

To use any of these client deployment methods, you must have local admin rights to the target computers.

If you use any of these client deployment methods, your clients will inherit the default settings of OfficeScan, unless you modify them after installing the server.

Installing from the internal Web page

If you installed OfficeScan server to a computer running Windows NT, Windows 2000, Windows XP, or Windows Server 2003 with Internet Information Server (IIS) 4.0 or later or Apache 2.0.47 (only on Windows 2000 machines), users can install the client from the internal Web server created during master setup.

This is a convenient way to deploy the OfficeScan client. You only have to instruct users to go to the internal Web page and download the client setup files. However, there is no way to ensure that all your client users will follow your instructions.

Users must have Microsoft Internet Explorer 4.01 or later to successfully download the client setup files. Email your users the following instructions to install the OfficeScan client from the internal Web server.

To install from the internal Web page

1. Open an Internet Explorer window and type one of the following:
   - **OSCE server with IIS server and SSL:**

     https://{OfficeScan_server_name}:{port}/officescan/console/clientinstall
   - **OSCE server with IIS server, without SSL:**

     http://{OfficeScan_server_name}:{port}/officescan/console/clientinstall
   - **OSCE server with Apache:**

     http://{OfficeScan_server_name}:{port}/officescan/console/ClientInstall/

   Alternatively, click the **Click here** link under **Install OfficeScan Client** on the main page of the OfficeScan server Web console.
2. Click **Install Now** to start installing the OfficeScan client.

   The client installation starts. Once installation is completed, the screen displays the message, "Client installation is complete". To verify a successful installation, check if the OfficeScan client icon appears in the Windows system tray.

Installing with Login Script Setup

Use Login Script Setup to automate the installation of the OfficeScan client on unprotected computers when they log on to the network. Login Script Setup adds a program called `autopcc.exe` to the server login script. `Autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected computer and installs the appropriate version of the OfficeScan client
- Updates the scan engine, virus pattern file, Damage Cleanup Services components, spyware pattern file, and program files

To add autopcc.exe to the login script using Login Script Setup

1. On the computer you used to run the server installation, click **Programs** > **Trend Micro Client Server Messaging Suite** > **Login Script Setup** from the Windows **Start** menu.

   The Login Script Setup utility loads. The console displays a tree showing all domains on your network.

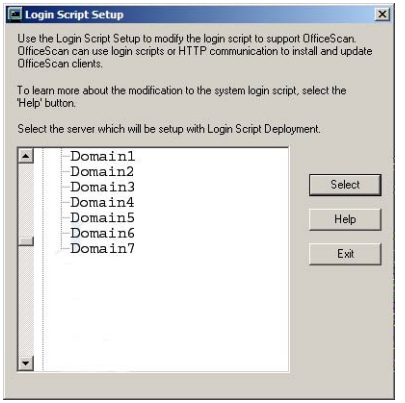

FIGURE 4-1. Browse for the OfficeScan server

2. Browse for the Windows NT/2000/2003 Server whose login script you want to modify, select it, and then click **Select**. The server must be a primary domain controller and you must have administrator access.

   Login Script Setup prompts you for a user name and password.

FIGURE 4-2. Type your user name and password

3. Type your user name and password. Click **OK** to continue.

The **User Selection** screen appears. The **Users** list shows the computers that log on to the server. The **Selected users** list shows the users whose computer login script you want to modify.

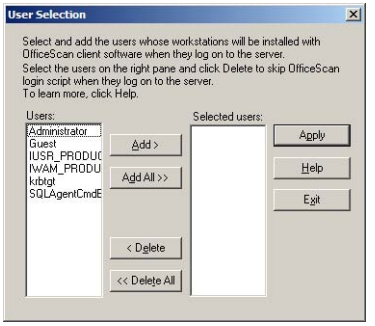

FIGURE 4-3. Select the computers whose login scripts you want to modify

- To modify the login script of a single or multiple users, select them from the **Users** and then click **Add**
- To modify the login script of all users, click **Add All**
- To exclude a user whose computer you previously modified, select the name in the **Selected users** and click **Delete**
- To reset your choices, click **Delete All**

4. Click **Apply** when all the target users are in the **Selected users** list.

   A message appears, informing you that you have modified the server login scripts successfully.

5. Click **OK**. The Login Script Setup utility will return to its initial screen.
   - To modify the login scripts of other servers, repeat steps 2 to 4
   - To close Login Script Setup, click **Exit**

When an unprotected computer logs on to the servers whose login scripts you modified, `autopcc.exe` will automatically install the client to it.

Installing with Windows 2000/NT/2003 scripts

If you already have an existing login script, Login Script Setup will append a command that executes `autopcc.exe`; otherwise, it will create a batch file called `ofcscan.bat` (which contains the command to run `autopcc.exe`).

Login Script Setup appends the following at the end of the script:

```
\\{Server_name}\ofcscan\installation_path
```

where:

- `{Server_name}` is the computer name or IP address of the computer where the OfficeScan server is installed
- `ofcscan` is the OfficeScan directory on the server
- `installation_path` is the directory where you installed the server files (by default, the `PCCSRV` folder)

The Windows 2000 login script is on the Windows 2000 server (through a net logon shared directory), under:

```
\\Windows 2000 server\system
drive\WINNT\SYSVOL\domain\scripts\ofcscan.bat
```

The Windows NT login script is on the Windows NT server (through a net logon shared directory), under:

```
\\Windows NT server\system
drive\windir\system32\repl\export\scripts\ofcscan.bat
```

```
\\Windows NT server\system
drive\windir\system32\repl\import\scripts\ofcscan.bat
```

The Windows 2003 login script is on the Windows 2003 server (through a net logon shared directory), under:

```
\\Windows 2003 server\system
drive\windir\sysvol\domain\scripts\ofcscan.bat
```

Installing with Client Packager

Client Packager is a tool that can compress setup and update files into a self-extracting file to simplify delivery via email, CD-ROM, or similar media. It also includes an email function that can open your Microsoft™ Outlook address book and allow you to send the package from within the Client Packager console.

When users receive the package, all they have to do is double-click the file to run the setup program. OfficeScan clients you install using Client Packager report to the server where Client Packager created the setup package. This tool is especially useful when deploying the client setup or update files to clients in low-bandwidth remote offices.

Client Packager can create two types of self-extracting files:

- **Executable** – this common file type has an .exe extension
- **Microsoft Installer Package Format (MSI)** – this file type has an .msi extension and conforms to Microsoft's installer package specifications. For more information on MSI, see the Microsoft Web site (www.microsoft.com).

Note: To run Client Packager on the server, you need to install two items: **Microsoft Outlook** to run the Client Packager send mail option and **InstallShield Developer Version 8.0 Service Pack 2/ Windows Installer 2.0** to create an MSI package.

To create a package with Client Packager

1. On the OfficeScan server, open Windows Explorer.
2. Browse to `\PCCSRV\Admin\Utility\ClientPackager`.
3. Double-click `ClnPack.exe` to run the tool. The Client Packager console opens.

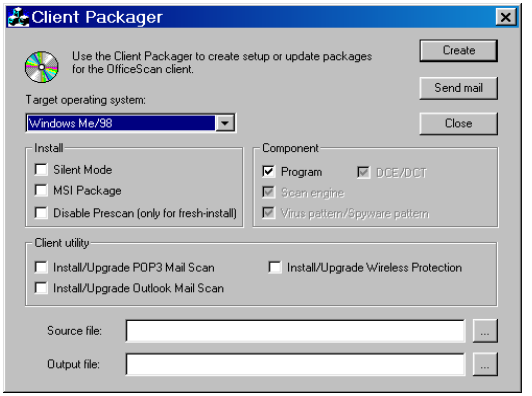

FIGURE 4-4. The Client Packager console

4. Under **Target operating system**, select the operating system for which you want to create the package.

   The options are **Windows Me/98** and **Windows XP/2000/NT/2003**.

5. Select from among the following installation options under **Install**:
   - **Silent Mode** – creates a package that installs on the client machine in the background, unnoticeable to the client without showing an installation status window
   - **MSI Package** – creates a package that conforms to the Microsoft Installer Package Format
   - **Disable Prescan (only for fresh-install)** – disables the normal file scanning that OfficeScan performs before starting setup

   Note: If you select MSI Package, the package file has an .msi extention; otherwise, it has an .exe extension.

6. Under Component, select the components you want to include in the installation package:
   - **Program** – all components (if you select Program, Client Packager automatically selects the other components)
   - **Scan engine** – the latest scan engine on the OfficeScan server
   - **Virus pattern/Spyware pattern**– the latest virus pattern file and spyware pattern file on the OfficeScan server
   - **DCE/DCT** – the latest Damage Cleanup Service engine and template on the OfficeScan server
7. Select the OfficeScan client utilities you want to include in the package:
   - **POP3 Mail Scan** – performs a virus scan on the client's Post Office Protocol 3 (POP3) mail messages and attachments as they are downloaded from the mail server
   - **Outlook Mail Scan** – performs a virus scan on the client's Microsoft Outlook folders
   - **Wireless Protection** – an antivirus module to protect your Personal Digital Assistants (PDA). This is not available with Silent Mode or MSI packages.

8. In **Source file**, click ... to browse for the `ofcscan.ini` file. By default, this file is located in the `\PCCSRV` folder of the OfficeScan server.

   In **Output file**, click ... to specify the file name (for example, ClientSetup.exe) and the location you want to create the client package.

9. Click **Create** to build the client package. When Client Packager finishes creating the package, the message "Package created successfully." appears. To verify that the package has been created successfully, check the output directory you specified.

10. Send the package to your users via email, or copy it to a CD or similar media and distribute among your users.

Sending the package via email

You need to have Microsoft Outlook installed to use Client Packager email function.

To send the package from the console:

1. Click **Send mail**. The **Choose Profile** window appears.
2. Choose a profile name from the list and click **OK**.
3. Enter the user name and password required to access Outlook on your computer.
4. The **Send mail** screen opens with the default subject and message. Click **To** and specify the recipients of the package. Client Packager opens your Microsoft Outlook address book. Click **Cc** or **Bcc** to send copies to other recipients in your organization.
5. Edit the default subject and message (optional) and click **Send**.

Note: If the Client Packager is unable to find your Microsoft Outlook address book, an error message is displayed when you click **Send mail**, **To**, **Cc**, or **Bcc**.

Installing with Windows Remote Install

Remotely install the OfficeScan client to Windows 2003/XP (Professional Edition Only) /NT/2000 computers connected to the network, and install to multiple computers at the same time. To use Windows Remote Install, you need administrator rights for the target computers.

Note: You cannot use Windows Remote Install to install OfficeScan client on machines running Windows XP Home Edition.

To install with Windows Remote Install

1. From the OfficeScan Web console sidebar, click **Clients** > **Remote Install** on the OfficeScan server sidebar.

   The **Remote Install** screen appears. The domains and computers list displays all the Windows domains on your network.
2. From the list of computers, select a client, and then click **Add >>**. OfficeScan prompts you for a user name and password to the target computer. You need administrator rights to the target computer.
3. Type your user name and password, and then click **Login**. The target computer appears in the selected computers list.
4. Repeat these steps until the list displays all the Windows computers to install OfficeScan client.
5. Click **Install** to install the client to your target computers. A confirmation box appears.
6. Click **Yes** to confirm that you want to install the client to the target computers. A progress screen appears as OfficeScan copies the program files to each target computer.
7. When OfficeScan completes the installation to a target computer, the installation status will appear in the **Result** field of the selected computers list, and the computer name appears with a green check mark.

Note: Windows Remote Install will not install OfficeScan client on a machine already running OfficeScan server.

Installing from a client disk image

Disk imaging technology allows you to create an image of an OfficeScan client and make clones of it to other computers on your network.

Each client installation needs a Globally Unique Identifier (GUID), so that the server can identify your clients individually. Use an OfficeScan program called `imgsetup.exe` to create a different GUID for each of the clones.

Note: The computers you are installing to must have the same Windows platform type as the source computer. There are two types of Windows platforms: Windows 98/Me and Windows NT/2000/XP/2003.For example, if the source OfficeScan client machine is running Windows XP, you can only create clones for computers running Windows NT, 2000, XP, or 2003, not Windows 98 or Me.

To create a disk image of an OfficeScan client

1. Obtain disk imaging software.
2. Install the OfficeScan client to a computer. You will use this client as the source of the disk image.
3. Copy `ImgSetup.exe` to this computer from the OfficeScan server's `\PCCSRV\Admin\Utility\ImgSetup` folder.
4. Run `imgsetup.exe` on this computer. A RUN registry key will be created under `HKEY_LOCAL_MACHINE`.
5. Create a disk image of the OfficeScan client using your disk imaging software.
6. Restart the clone. ImgSetup.exe will automatically start and create one new GUID value. The client will report this new GUID to the server and the server will create a new record for the new client.

WARNING! *To avoid having two computers with the same name in the OfficeScan database, remember to manually change the computer name or domain name of the cloned OfficeScan client.*

Installing with Vulnerability Scanner

The Trend Micro Vulnerability Scanner (TMVS) can search for unprotected computers on your network and install OfficeScan client on them.

To install OfficeScan client with Vulnerability Scanner:

1. In the drive where you installed OfficeScan server, open the following directories: **OfficeScan** > **Admin** > **Utility** > **TMVS**. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **OfficeScan server Setting (for Install and Log Report)**, type the OfficeScan server name and port number.
4. Select the **Auto-Install OfficeScan Client for unprotected computer** check box.
5. Click **Start** to begin checking the computers on your network and begin OfficeScan client installation.

Note: Refer to the Vulnerability Scanner help for complete information on how to use and configure this tool.

Installing the client using Microsoft SMS

You can also install the client using Microsoft System Management Server (SMS). However, you must have Microsoft BackOffice SMS installed on the server.

Installing the client using Microsoft SMS is a two-step process:

- Create the setup package
- Distribute or "advertise" the package to the target computers

Note: The following instructions are applicable if you are using Microsoft SMS 2.0.

To create the setup package:

1. Open the SMS Administrator console.
2. On the **Tree** tab, click **Packages**.
3. On the **Action** menu, click **New** > **Package From Definition**. The **Welcome** screen of the **Create Package From Definition Wizard** appears.
4. Click **Next**. The **Package Definition** screen appears.

5. Click **Browse**. The **Open** screen appears.
6. Browse for the package description file (PDF) on the server. The location of the PDF depends on the operating system of the target clients. The PDF for the Windows XP/2000/NT/ 2003 client is in `\PCCSRV\PCCNT\Disk1\setup.pdf`. The PDF for the Windows 98/ME client is in `\PCCSRV\PCC95\Disk1\setup.pdf`.
7. Select the PDF for the target clients, and then click **OK**.

   The package name for the PDF you have selected appears on the **Package Definition screen**. If you selected the PDF for the Windows XP/2000/NT/2003 Server client, it will show "OfficeScan Client NT/2K/XP/2003 setup 6.0". If you selected the PDF for the Windows 98/ME client, it will show "OfficeScan Client 98/ME setup 6.0".
8. Click **Next**. The **Source Files** screen appears.
9. Click **Always obtain files from a directory source**, and then click **Next**.

   The **Source Directory** screen appears, displaying the name of the package you are creating and the source directory.
10. Click **Next**. The wizard creates the package. When it completes the process, the name of the package appears on the SMS Administrator console.

To distribute the package to target computers:

1. On the **Tree** tab, click **Advertisements**.
2. On the **Action** menu, click **All Tasks** > **Distribute Software**. The **Welcome** screen of the Distribute Software Wizard appears.
3. Click **Next**. The **Package** screen appears.
4. Click **Distribute an existing package**, and then click the name of the setup package you created.
5. Click **Next**. The **Distribution Points** screen appears.
6. Select a distribution point to which you want to copy the package, and then click **Next**. The **Advertise a Program** screen appears.
7. Click **Yes** to advertise the client setup package, and then click **Next**. The **Advertisement Target** screen appears.
8. Click **Browse** to select the target computers. The **Browse Collection** screen appears.
9. Click the collection to which you want to distribute the setup package.

- If you created a client setup package for Windows XP/2000/NT/Server 2003, click **All Windows NT Systems**.
- If you created a client setup package for Windows 98, click **All Windows 98 Systems**.

Note: To distribute the client setup package to Windows Me computers, you must create a new collection. For instructions on how to create a new collection, refer to the Microsoft SMS documentation.

---

10. Click **OK**. The **Advertisement Target** screen appears again.
11. Click **Next**. The **Advertisement Name** screen appears.
12. In the text boxes, type a name and comments for the advertisement, and then click **Next**. The **Advertise to Subcollections** screen appears.
13. Choose whether to advertise the package to subcollections. You can choose to **Advertise the program only to members of the specified collection** or **Advertise the program to members of subcollections as well**.
14. Click **Next**. The **Advertisement Schedule** screen appears.
15. Specify when to advertise the client setup package by typing or selecting the date and time in the list boxes.

    If you want Microsoft SMS to stop advertising the package on a specific date, click **Yes**. **This advertisement should expire**, and then specify the date and time in the **Expiration date and time** list boxes.
16. Click **Next**. The **Assign Program** screen appears.
17. Click **No. Do not assign the program**, and then click **Next**.

    Microsoft SMS creates the advertisement and displays it on the SMS Administrator console.

When Microsoft SMS distributes the advertised program (that is, the OfficeScan client program) to target computers, a screen will pop up on each target computer. Instruct users to click **Yes** and follow the instructions provided by the wizard to install the OfficeScan client to their computers.

Verifying a successful installation

Use Vulnerability Scanner to detect installed antivirus solutions, search for unprotected computers on your network, and install OfficeScan client. To determine if computers need protection, Vulnerability Scanner pings ports that antivirus solutions normally use.

Using Vulnerability Scanner to verify the client installation

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the OfficeScan online help.

You can run Vulnerability Scanner on the server or on any Windows 2000 computer on the network. To run Vulnerability Scanner on a computer other than the server, copy the TMVS folder from the `\PCCSRV\Admin\Utility` folder of the server to the computer.

WARNING! *You cannot run Vulnerability Scanner on computers running Windows 2003/XP/NT/Me/98.*

To verify client installation using Vulnerability Scanner

1. In the drive where you installed OfficeScan server, open the following directories: **OfficeScan** > **Admin** > **Utility** > **TMVS**. Double-click `TMVS.exe`. The **Trend Micro Vulnerability Scanner** console appears.
2. Click **Settings**. The **Settings** screen appears.
3. Under **Product Query**, select the **OfficeScan** check box and specify the port that the server uses to communicate with clients.
4. Under **Description Retrieval Settings**, click the retrieval method to use. Normal retrieval is more accurate, but it takes longer to complete.

   If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.
5. If you want to automatically send the results to yourself or to other administrators in your organization, select the **Email results to the system administrator** check box under **Alert Settings**. Then, click **Configure** to specify your email settings.

- In **To**, type the email address of the recipient
- In **From**, type your email address. If you are sending it to other administrators in your organization, this will let the recipients know who sent the message
- In **SMTP server**, type the address of your SMTP server. For example, type `smtp.company.com`. The SMTP server information is required
- In **Subject**, type a new subject for the message or accept the default subject

Click **OK** to save your settings.

6. If you want to display an alert on unprotected computers, click the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears.
7. Type a new alert message in the text box or accept the default message, and then click **OK**.
8. To save the results as a comma-separated value (CSV) data files, select the **Automatically save the results to a CSV file** check box. By default, Vulnerability Scanner saves CSV data files in the TMVS folder. If you want to change the default CSV folder, click **Browse**, select a target folder on your computer or on the network, then click **OK**.
9. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout** fields.
10. And if you want to send log to server, select the **Report log to OfficeScan server** check box.
11. Click **OK**. The **Vulnerability Scanner** console appears.
12. In **IP Range to Check**, type the IP address range to check for installed antivirus solutions and unprotected computers.
13. Click **Start** to begin checking the computers on the network.

Testing the client installation

After installing the client, Trend Micro recommends testing it to verify that the antivirus function is working properly and to see how virus detection and notifications actually work.

The European Institute for Computer Antivirus Research (EICAR) has developed a test script that can be used to test antivirus software. This script is an inert text file whose binary pattern is included in the virus pattern file of most antivirus vendors.

The EICAR test script is not a virus and does not contain any program code. Trend Micro recommends only using harmless scripts to test your antivirus installation.

To test the client installation using the EICAR test script

1. Make sure that real-time scan is enabled on the client.
2. Copy the following string and paste it into Notepad or any plain text editor:

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

3. On the **File** menu, click **Save As**. The **Save As** dialog box appears.
4. In **File name**, type `eicar.com`, and then click **Save**. Real-time scan detects the test script and displays the screen shown in Figure 4-5.

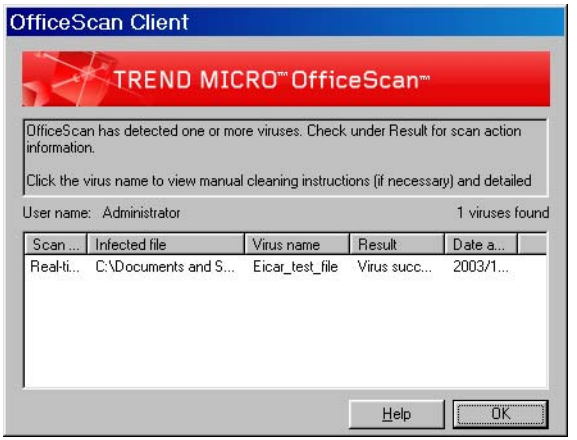

FIGURE 4-5. Real-time scan detects the EICAR test script

Also download the EICAR test script from the following URLs:

`www.trendmicro.com/vinfo/testfiles/`

`www.eicar.org/anti_virus_test_file.htm`

If you are downloading the EICAR test script, disable any antivirus software running on the computer before downloading. Otherwise, it will detect the EICAR test script as a virus and stop the download.

Removing the client

There are two ways to remove the OfficeScan program from the clients:

- Remove the client from the OfficeScan Web console
- Remove the client using its uninstallation program

Removing the client from the OfficeScan Web console

You can remove the client program from computers on the network using the Web console. Note that removing the client program will also remove virus protection on clients.

WARNING! *Removing the OfficeScan client may expose your computer to virus threats.*

To remove the client using Uninstall Now

1. On the OfficeScan Web console sidebar, click **Clients**. The domain tree for **Clients** screen appears.
2. Click the domains or clients on which you want to run Uninstall Now by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Uninstall Clients**. The **Uninstall Clients** screen appears.
4. Under **Computer**, select the clients to remove, and then click **Start Notification**. The server sends a request to the client to run the client uninstallation program.

To stop notifications

To stop notifications to clients that have not yet started the client uninstallation program, do the following:

- Select the clients that you no longer want to remove
- Click **Stop Notification**. Clients that have not yet started the client uninstallation program will skip the request. However, clients that are already running the uninstallation program do not stop the uninstallation procedure

Removing the client using its uninstallation program

If you granted users the privilege to remove the client program, instruct them to run the client uninstallation program from their computers. For more information, see *Granting privileges to clients* on page 5-41.

To run the client uninstallation program

1. On the Windows **Start** menu, click **Programs** > **Trend Micro OfficeScan Client** > **Uninstall OfficeScan Client**. The **OfficeScan Client Uninstallation** screen appears and prompts for the uninstall password.
2. Type the uninstall password, and then click **OK**. The **OfficeScan Client Uninstallation** screen shows the progress of the uninstallation.

You may need to restart your computer to complete the uninstallation.

Migrating to and Upgrading OfficeScan

If you are using third-party antivirus software or an older version of OfficeScan, you can easily migrate or upgrade to this version OfficeScan. This section helps you perform migration and upgrade by enumerating the tasks that you need to perform and provides detailed instructions on how to do them.

In this section, you will learn about the following topics:

- Migrating from third-party antivirus applications
- Upgrading from a previous version

Migrating from third-party antivirus applications

Migrating from third-party antivirus software to OfficeScan is a two-step process: the installation of the OfficeScan server, followed by the migration of the clients.

However, there may be other procedures that you need to complete, depending on your environment.

To help you migrate to OfficeScan, follow these guidelines:

1. Plan the migration
2. Pilot the migration
3. Install the OfficeScan server

4. Migrate the clients

Plan your migration

As with deployment, you need to plan how you will migrate existing antivirus software to OfficeScan. Trend Micro recommends planning the following for migration:

- Set a migration schedule
- Form a team that will handle the migration
- Identify which segments of your network will be migrated and when
- Decide on the best method to migrate the clients
- Create a rollback plan in case you encounter difficulties

Trend Micro recommends planning the migration on a non-working day or during off-peak hours to ensure that the process will not interfere with your organization's normal operations. If migrating a large client base, you may also want to stage the migration into segments to facilitate the process. Migrating 500 clients simultaneously is easier than migrating 20,000 clients.

Pilot your migration

Perform a small scale migration before doing a full-scale rollout. Choose a pilot site that matches your production environment, install the server, and then use different methods to migrate the clients.

Evaluate the results of the pilot migration, identify potential difficulties, and decide which client migration methods work best in your environment.

Install the OfficeScan server

The next step is to install the OfficeScan server. Before installing, verify that the server meets the minimum system requirements. You need to remove the server program of your existing third-party antivirus software before installing the OfficeScan server.

For instructions on how to install the OfficeScan server, refer to *Installing OfficeScan Server* on page 4-2.

OfficeScan cannot remove the server program of your existing third-party, client/server antivirus application.

Manual client migration

To remove third-party antivirus applications and install the OfficeScan client automatically, perform any of the following:

- Install from the internal Web page
- Install with Login Script Setup (`autopcc.exe`)
- Install with Windows NT Remote Install

For instructions on how to use these methods, refer to *Installing OfficeScan clients* on page 4-12. The procedures for deploying and migrating clients are similar, except for the fact that when migrating the clients, third-party antivirus applications are removed from your computers before the OfficeScan client installation.

Automatic client migration

Automatic client migration refers to replacing existing third-party antivirus software with the OfficeScan client. The client setup program automatically removes the third-party software on your client computers and replaces it with the OfficeScan client.

Refer to Table 4-2 for a list of third-party applications that OfficeScan can automatically remove.

Vendor	Product Name	Version	Platform
Ahnlab™	V3 Pro™	2000 Deluxe	Windows NT
Ahnlab	V3 Pro	98 Deluxe	Windows 98
Ahnlab	V3 Pro	98	Windows 9x
Computer Associates™	eTrust InoculateIT™	6.0	Windows NT and 9x
Computer Associates	InocuLAN™	5, 4.53	Windows NT and 9x
Computer Associates	Cheyenne AntiVirus™	9x	Windows 9x
Computer Associates	Cheyenne AntiVirus	NT	Windows NT
F-Secure™	Anti-Virus™	4.04, 4.08, 4.3, 5.3	Windows NT and 9x
F-Secure	Anti-Virus	BackWeb	Windows NT

Vendor	Product Name	Version	Platform
F-Secure	Anti-Virus	Management Agent	Windows NT
Hauri™	ViRobot™	2000 Professional	Windows NT and 9x
Intel™	LANDesk Virus Protect™	5.0	Windows NT and 9x
McAfee™	Dr. Solomon™	4.0.3	Windows 98
McAfee	Dr. Solomon	4.0.3 NT	Windows NT
McAfee	Dr. Solomon	7.77, 7.95 NT	Windows NT and 9x
McAfee	ePolicy Orchestrator™	Agent 1000, Agent 2000	Windows NT and 9x
McAffe	VirusScan	Enterprise 7.0	NT, 2000, XP
McAfee	VirusScan	ASaP	9x, Me, NT, 2000, XP
McAfee	VirusScan	6.01, 6.02	Windows NT
McAfee	VirusScan	NT	Windows NT
McAfee	VirusScan™	MSPlus98	Windows 9x
McAfee	VirusScan	TC	Windows NT and 9x
McAfee	VirusScan	4.5, 4.51, 5.15, 5.16, 5.21, 6.01	Windows NT and 9x
McAfee	NetShield™	NT 4.03a, 4.5	Windows NT
Panda Software™	Antivirus ™	Local Networks	Windows NT and 9x
Panda Software	Antivirus	6.0	Windows NT and 9x
Panda Software	Antivirus	Windows NT WS	Windows NT
Sophos™	Anti-Virus	3.37, 3.47, 3.5x	Windows NT and 9x
Symantec	Norton AntiVirus	2003, 2002, 2001, 2000	Windows NT and 9x
Symantec	Norton AntiVirus	2003 Cht	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition™	8.0 (2002)	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	7.5, 7.51, 7.6,	Windows NT and 9x

Vendor	Product Name	Version	Platform
Symantec	Norton AntiVirus Corporate Edition	2001	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	2000	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	7.0	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	6.524	Windows 9x
Symantec	Norton AntiVirus Corporate Edition	5.0, 5.31, 5.32	Windows NT and 9x
Symantec	Norton AntiVirus Corporate Edition	2.0	Windows NT
Tegam™	ViGUARD™	9.25e	Windows NT

TABLE 4-2. Third-party applications that OfficeScan can automatically remove

Verify the migration

After migrating to OfficeScan, Trend Micro recommends the Trend Micro Vulnerability Scanner (TMVS) to check if you still have clients using the previous antivirus application. This tool checks your computers for installed antivirus software and the versions they are using based on an IP address range you specify.

You can get Vulnerability Scanner from the `\PCCSRV\Admin\Utility\TMVS` folder of the OfficeScan server.

Upgrading from a previous version

The version of OfficeScan included in the Client/Server/Messaging Suite does not support automatic upgrades. To upgrade from a previous version of OfficeScan, perform the following:

- Develop a list of clients to upgrade
- Uninstall the previous version of OfficeScan (Refer to the Getting Started Guide of the OfficeScan version you are uninstalling)
- Install the OfficeScan server

- Deploy the OfficeScan client to all computers on the client list

Chapter 5

Getting Started with OfficeScan

This chapter explains how to use the OfficeScan web console and how to configure basic settings.

The topics discussed in this chapter include:

- *Exploring the Web console* on page 5-2
- *Updating OfficeScan* on page 5-16
- *Verifying client-server connection* on page 5-23
- *Setting up standard notifications* on page 5-24
- *Configuring the scan settings* on page 5-29
- *Running Scan Now* on page 5-38
- *Granting privileges to clients* on page 5-41

Exploring the Web console

When you install OfficeScan server, you also install the Web console, which uses standard Internet technologies such as Java, CGI, HTML, and HTTP.

To open the Web console:

1. On any computer on the network, open a Web browser and type `http://{OfficeScan_Server_Name}:{port number}/officescan` in the address bar.

   If using SSL, type `https://{OfficeScan_Server_Name}:{port number}/officescan` in the address bar.

2. The browser displays the OfficeScan login screen.

FIGURE 5-1. The browser displays the Welcome screen of the Web console.

3. Type your password in the **Password** text box, and then click **Enter**. The browser displays the Web console.

Getting around the Web console

There are two main parts to the Web console: the sidebar and the main frame. The sidebar groups tasks that you perform into sections. **Cleanup Now** and **Scan Now**, for example, are tasks to run under the section **Clients**.

When you click a task on the sidebar, the main frame displays the information that you need to perform the task or opens another screen that you use to perform the task.

The sidebar contains shortcuts to **Scan Now**, **Update Now**, and **Cleanup Now**. Click **Scan Now** to perform a manual scan on computers that you suspect to be infected. Click **Update Now** to check the Trend Micro update server for the latest updated components, including virus pattern files, scan engine and program, Damage Cleanup scan engine and template, and spyware pattern files. Click **Cleanup Now** to run Damage Cleanup Services on selected clients to check for Trojans.

The following table summarizes the tasks to perform for each category on the sidebar:

Summary	
Summary	**View a summary of the outbreak status, recent virus incidents, and the update and connection status of clients.**

Outbreak Prevention	
Deploy Now	**Apply Outbreak Prevention to control an outbreak that may be developing on your network.**
Restore	**Deactivate Outbreak Prevention to restore your network settings to normal after an outbreak is contained.**

Virus Outbreak Monitor	
Virus Outbreak Monitor	**Enable Virus Outbreak Monitor if you want OfficeScan to send you a message in the event that clients detect excessive network traffic.**

Clients	
Scan Options	**Configure Real-time Scan, Manual Scan, and Scheduled Scan options.**
Client Privileges	**Grant users privileges to modify individual scan settings, update components, and remove or unload the client.**
Policy Manager	**Import and export scan settings and Outbreak Prevention settings.**
Scan Now	**Perform a manual scan for viruses on selected clients from the Web console. Configure the action that OfficeScan takes on infected files under Manual Scan in the Scan Options section.**
Cleanup Now	**Search specifically for Trojans on selected clients using Damage Cleanup Services.**
Uninstall Client	**Remove the client program from client computers.**

View Status	**View client information, including its privileges and the versions of its components, such as virus pattern file, scan engine and program, DCS engine and template, and spyware pattern file.**
Notify Install	**Notify users via email to install OfficeScan client.**
Remote Install	**Install the client software to Windows 2000/NT/XP/2003 computers remotely using the Web console. Install to multiple computers at the same time without having to physically go to each computer.**
Verify Connection	**Check the connection status of clients manually or automatically.**
Global Client Settings	**Configure optional and advanced settings for clients, including scan settings, alert settings, reserved disk space and watchdog settings, Scheduled Update settings, and connection settings.**

GateLock	
Scan Options	**Configure SMTP, POP3, and HTTP settings to detect and prevent known viruses from passing through GateLock.**

Network	**Define zones, configure the interface between them, and configure Intrusion Detection System (IDS) rules for data passing in and out of zones. Also configure static and dynamic routing.**
Policies	**Use policies to define the rules for traffic passing across interfaces.**
VPNs	**Create Virtual Private Network instances and configure existing VPN tunnels. Define the type of key exchange, authentication, and encryption to use for VPN tunnels.**
Objects	**Create and manage addresses and services.**
Verify Connection	**Check the connection with GateLock Remote Appliances and synchronize configuration information.**
Check Status	**Check error logs and pending commands.**
Open Client Console	**Open the client management console for supporting GateLock devices (not all models support this feature).**

ScanMail for Exchange	
ScanMail for Exchange	**Install and manage ScanMail for Exchange servers from your OfficeScan Web console.**

Administration	
Set Password	**Change the password to the Web console periodically to prevent unauthorized users from modifying your settings or removing the clients.**
Standard Alert	**Send alerts to administrators in your organization whenever OfficeScan detects a virus on any client.**
Outbreak Alert	**Send alerts to administrators in your organization when OfficeScan determines that conditions on your network have met specified outbreak criteria.**
Client Alert Message	**Modify the message that is displayed on the clients whenever a virus is detected.**
Web Server	**Update OfficeScan server's name, IP address and HTTP port number.**
Inactive Clients	**Automatically remove inactive clients to ensure that the domain tree displays only active clients.**
Quarantine Manager	**Set both the capacity of the quarantine folder and the maximum allowable size of quarantined files.**
Product License	**Activate and check the status of component product licenses.**

Updates	
Server Update	**Manually or automatically update the components on the server as well as configure your proxy settings to download updates from the Trend Micro update server.**
Client Deployment	**Update the clients manually or automate the deployment of updates.**
Rollback	**Revert the pattern file or scan engine to the previous version if you encounter problems after deploying it.**

Logs	
Virus Logs	**View a list of viruses that have infected clients on the network, with details about each infection.**
Update Logs	**View the time and date that the server and clients received updates and a list of what components they updated. Use these logs to keep track of the server's update history and to verify that updates were successfully deployed to clients.**

System Event Logs	**View system events that have occurred on the server, such as shutdown and startup. Use these logs to verify that the server is running smoothly and that the services necessary for OfficeScan to work on the network are running.**
GateLock Clients Logs	**View the GateLock Intrusion Detection and Prevention (IDP) logs to see events that GateLock detects based on the IDP rules you configure.**
Verify Connection Logs	**View verify connection logs to determine the connection status between the server and clients.**
Log Maintenance	**To conserve disk space on the server, set a schedule to delete logs.**

Tools	
Administrative Tools	**View tools that can help you manage the server and clients.**
Client Tools	**View tools that can enhance the performance of the clients.**

Other links on the console

The Web console also has other links that you use to log off the console, open the online help, and view virus information. These are located at the upper right corner and below the main frame.

Links at the upper right corner	
Log Off	**Click to end your session. Logging off the Web console prevents unauthorized users from modifying the settings or removing clients.**
Help	**Select one of the following from the menu**
• Contents and index	**Select to open the online help system.**
• Knowledge Base	**Select to open the Trend Micro online knowledge base to view FAQs and updated product information, access customer support and register your version of OfficeScan.**
• Security Info	**Select to display the Trend Micro Security Information page to read about the latest virus threats.**
• Sales	**Select to display the Trend Micro sales Web page to contact your regional sales representative.**

• Support	**Select to display the Trend Micro support Web page to submit questions and find answers to common questions about Trend Micro products.**
• About	**Select to display the About page, which contains an overview of the product and tells you how to check the version of your components.**

Links below the main frame	
	Click this icon to open the online help system (not available on every screen).

Understanding the domain tree

The domain tree is a Java-based tree that displays OfficeScan domains and clients on the network. It appears in the main frame when you click **Outbreak Prevention**, **Clients**, or **Logs**.

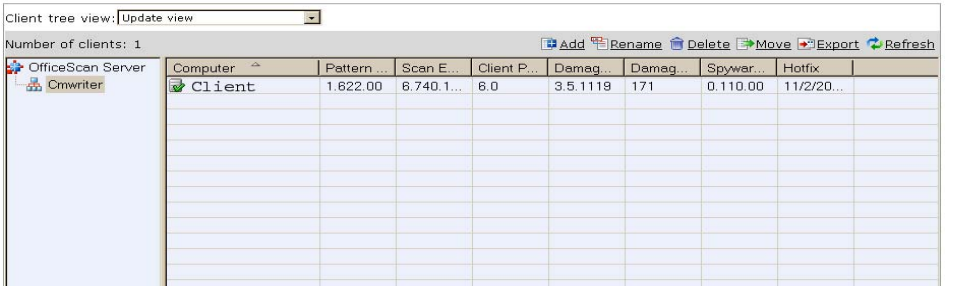

FIGURE 5-2. The clients domain tree

Creating domains

OfficeScan uses existing Windows domains on the network when assigning clients to domains.

For example, a network currently has a domain called 'YourCompany' with three computers named 'A', 'B', and 'C'. When you install OfficeScan on these three computers, it will automatically create a domain called 'YourCompany' and populate this domain with these three computers.

Also create new domains, modify the structure of the domain tree, or change the domain names so that they suit your organization's virus management policy.

Selecting domains and clients from the domain tree

Select domains or clients to simultaneously apply settings.

- To select a single domain or client, click the domain or client name.
- To select multiple, adjacent domains or clients, click the first domain or client in the range, hold down the SHIFT key, and then click the last domain or client in the range. OfficeScan will select all the domains or clients between the two mouse clicks.
- To select a range of non-adjacent domains or clients, click the first domain or client in the range. Hold down the CTRL key and then click the domains or clients that you want to select. All domains or clients that you click will be selected.
- To select all clients that report to the server, click the root icon .

Searching for clients

To search for clients, use either of the following two methods:

To do a simple search:

1. Type a client name in the **Simple Search** text field.
2. Click **Search**. A list of matching clients will appear highlighted in the domain tree.

To do an advanced search:

1. Click A**dvanced Search**. The Advanced Search screen appears.

2. Search for clients based on three types of criteria:
   a. Basic
      - **IP range** – click and type a range of client IP addresses
      - **IP Segment** – click and type a portion of an IP address starting with the first octet. The search will return all computers with IP addresses containing that entry. For example, typing 10.5 will return all computers in the IP address range 10.5.0.0 to 10.5.255.255.
      - **Platforms** – click and select the client platforms
      - **Domain** – click and select a client domain from the list
      - **MAC Address** – type a MAC address range (in hexadecimal notation)
   b. Version

      For the following, select either **Earlier than** or **Earlier than and including** from the list and type a version number in the text box:
      - **Scan Engine version**
      - **Virus Pattern File version**
      - **Client Program version**
      - **Damage Cleanup template version**
      - **Damage Cleanup engine version**
      - **Spyware pattern version**
   c. Status
      - **Connected** – select a connection status: **Online**, **Offline**, or **Roaming**
      - **Outbreak Prevention**– select either **Activated** or **Normal** Outbreak Prevention
      - **Infected client** – select and type the number of infected clients
3. Click **OK**. A list of matching clients will appear in the domain tree.

Refreshing the tree

To refresh the domain tree, click the refresh button .

Understanding the domain tree icons

The following icons indicate the status of clients in OfficeScan domains.

Windows 98/Me clients	Description	Windows 2000/ NT/ XP/ 2003 clients and servers
	OfficeScan domains, double-click to display clients that belong to this domain	
	Normal client/server	
	Offline client/server	
	Infected client/server	
	Roaming client/server	
	Normal client/server in Outbreak Prevention mode	
	Infected client/server in Outbreak Prevention mode	

Working with OfficeScan domains

An OfficeScan domain is a group of OfficeScan clients that share the same configuration and run the same tasks. By grouping clients into domains, simultaneously configure, manage, and apply the same configuration to all domain members.

For ease of management, group clients based on the departments to which they belong or the functions they perform. Also group clients that are at a greater risk of

infection, so you can apply a more secure configuration to all of them in just one setting.

An OfficeScan domain is different from a Windows domain. There can be several OfficeScan domains in one Windows domain.

By default, OfficeScan creates domains based on existing Windows domains and refers to each client according to its computer name. Delete or rename the domains that OfficeScan has created for you, or create a new domain. You can even transfer clients from one domain to another.

To add a domain:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click **Add** in the main frame. The **Add Domain** screen appears.
3. Type a name for the domain to add, and then click **OK**. The new domain appears in the domain tree.

To move a client:

1. On the sidebar, click **Clients**. The domain tree appears.
2. Select the client that you want to move, and then click **Move**. The **Move Clients** screen appears.
3. To move clients to another domain, select the domain to move the client under **Move selected client(s) to another Domain**. Click **OK**. The client appears under the domain you have selected. To move clients to another OfficeScan server, enter the server name, port number, and client communication port under **Move selected client(s) to another OfficeScan Server**. Click **OK**.

   Alternatively, drag and drop the client to another domain.

To delete a domain:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. In the domain tree, double-click the domain to delete. The clients that belong to the domain are displayed.
3. Move the clients to other domains. Do this by dragging and dropping the clients to other domains.
4. When the domain is empty, click **Delete**. OfficeScan deletes the domain.

To rename a domain:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domain to rename, and then click **Rename**. The **Rename Domain** screen appears.
3. Type a new name for the domain, and then click **OK**. The new domain appears in the domain tree.

Updating OfficeScan

To help ensure that clients stay protected against the latest virus threats, regularly update the OfficeScan components, including the virus pattern file, scan engine, program, sypware pattern file, and Damage Cleanup engine and template. Updating the components is one of the key administrative tasks that you should regularly perform after installation.

Trend Micro recommends updating the components at least once every week. The easiest way to help ensure that components are updated regularly is to configure scheduled updates to run every week.

Updating the server

Update components by configuring the server to download component updates from the Trend Micro update server. After the server downloads any available updates, it deploys these to the clients based on the deployment schedule you specified on the **Automatic Deployment** screen under **Updates** > **Client Deployment**.

Trend Micro periodically updates the scan engine and program . On the other hand, Trend Micro updates virus pattern files every week and more often during virus outbreaks to help ensure that clients are protected from new virus threats.

Tip: Trend Micro recommends updating the server daily to help ensure OfficeScan server has current component versions.

OfficeScan provides these methods of updating the server:

- Configure automatic scheduled updates for the server

- Update the server manually

Configuring scheduled updates for the server

Configure the server to regularly check the update server and automatically download any available updates. Because clients normally get updates from the server, automating server update is an easy and effective way of ensuring that your protection against viruses is always current.

To update the server based on a schedule:

1. On the sidebar, click **Updates** > **Server Update** > **Automatic Update**. The **Automatic Update** screen appears.
2. Select the **Enable scheduled update of the OfficeScan server** check box.
3. In the **Components** box, select the components to update.
4. Under **Update schedule**, specify a schedule when to perform scheduled update.
   - **Hourly** – click to perform scheduled update every hour
   - **Daily** – click to perform scheduled update every day
   - **Weekly** – click to perform scheduled update once a week. You must select a day from the list.
   - **Monthly** – click to perform scheduled update once a month. You must select a date from the list.

   Regardless of the selection, specify when to perform scheduled update in the **Time** lists.
5. Under **Update Source**, select the location from where to download the update. Select either the **Trend Micro ActiveUpdate server** or **Other update source** and type in the source's URL.
6. To have the server continue retrying if an update attempt fails, select the **Retry update if update attempt fails** check box under **Program Update Retry**.

   In the **Number of attempts** list, select the number of times that the server will attempt the update.

   In the **Interval** list, select the time interval, in minutes, before the server continues to retry the update attempt.
7. Click **Save** to save your settings.

Updating the server manually

Also update the components on the server manually. Trend Micro recommends updating the server manually immediately after deploying OfficeScan and whenever there is a virus outbreak.

To update the server manually:

1. On the sidebar, click **Updates** > **Server Update** > **Manual Update**. The **Manual Update** screen appears, showing your current components, their version numbers, and the most recent update dates.
2. Under **Update Source**, choose whether to receive updates from the update server or from another source and type the source URL.
3. Click **Update**. The server checks the Trend Micro update server for updated components. If there are available updates, they appear on the **Available Updates From Trend Micro** screen, with the component names and version numbers.
4. Select the check boxes for the components to update.
5. Click **Update**. The server downloads the updated components.

> **Note:** If you do not specify a deployment schedule on the **Automatic Deployment** screen under **Client Deployment**, the server will download the updates but will not deploy them to clients.

To check if you have specified a download schedule, click **Updates** > **Server Update** > **Automatic Update** on the sidebar.

> **Note:** If you use a proxy server to connect to the Internet, make sure your proxy settings are properly configured to download updates successfully. For information on how to configure Internet proxy settings, see the next section.

Configuring Internet Proxy Settings

This section provides information on configuring proxy settings to connect to the Internet.

To set the Internet proxy:

1. On the sidebar, click **Updates** > **Server** > **Internet Proxy**. The **Internet Proxy** screen appears.
2. Select the **Use a proxy server** check box.
3. Type the address of the proxy server and its port number.
   - If the proxy server uses versions 4 of the SOCKS protocol to handle Transmission Control Protocol (TCP), select the **Use SOCKS 4** check box.
4. If the proxy server requires a password, type your user name and password in the fields provided.
5. Click **Save** to save your settings.

Updating clients

To help ensure that clients stay protected from the latest virus threats, regularly update their components. The clients get updates from the server, which downloads updates from the Trend Micro ActiveUpdate server.

Before updating the clients, verify that the server has the latest components. For information on how to update the server, refer to *Updating the server* on page 5-16.

Trend Micro periodically updates the scan engine and program . On the other hand, Trend Micro updates virus pattern files every week and more often during virus outbreaks to help ensure that clients are protected from new virus threats.

Tip: Trend Micro recommends updating the server daily to help ensure OfficeScan server has current component versions.

OfficeScan provides these methods of updating clients:

- Automatic Deployment
- Manual Deployment
- Update Now on the client

Except for using Update Now on the client, these methods can update the following components on the client:

- Virus pattern file
- Client program
- Scan engine
- Spyware pattern
- Damage Cleanup engine and template
- Configuration settings, including privileges, scan settings, and Outbreak Prevention settings

Updating clients using Automatic Deployment

Automating client updates is an easy and effective way of ensuring that clients always get the latest components from the server. Trend Micro recommends automating client updates to help protect clients from the latest virus threats.

To update clients using Automatic Deployment:

1. On the sidebar, click **Updates** > **Client Deployment** > **Automatic Deployment**. The **Automatic Deployment** screen appears.
2. Under **Event-triggered Deployment**, select when to deploy the updates:
   - **Deploy to clients immediately after the OfficeScan server downloads a new component**

     Also decide whether or not to include roaming client(s).
   - **Deploy to clients (For OfficeScan clients only and excluding roaming clients) when they are restarted**

Tip: Trend Micro recommends specifying an update schedule. If you do not specify a schedule, the clients will only be updated if you perform manual deployment from the console.

---

3. Under **Schedule to Deploy**, select the **Enable scheduled deployment from OfficeScan server or customized update source** check box to specify an update schedule. Ensure that you grant clients the privilege to enable a schedule update under **Clients** > **Client Privileges**.
4. Select how often to perform scheduled deployment. Click one of the following:
   - **Hours** – to deploy every { } hours. Select a number of hours
   - **Daily** – to deploy daily. Select the start time and the length of deployment time
   - **Weekly** – to deploy weekly. Select a day
5. Click **Save** to save your settings.

Updating clients using Manual Deployment

Update clients manually by deploying updated components on the server to the clients using Manual Deployment.

To update clients using Manual Deployment:

1. On the sidebar, click **Updates** > **Client Deployment** > **Manual Deployment**. The **Manual Deployment** screen appears.
2. Under **Deployment Target**, choose to update all clients whose components are out of date or choose specific clients:

- To update all online clients, including roaming clients with functional connections to the server, click **Select clients with out-of-date components** and select the **Include roaming client(s)** check box
- To update specific clients, click **Manually select clients** and do the following:

  a. Click the **Select** button to choose specific clients. The **Manual Deployment** screen shows the client tree.

  b. Click the clients you want to update or click the root icon to update all clients.

3. After selecting all clients to update, click **Notify**. The server starts notifying each client to download the updates.

Updating clients using Update Now

Instruct users to update the client components by performing Update Now on the client. Performing Update Now downloads updated components from the OfficeScan server. Users can also download update components directly from the Trend Micro update server, if you grant users this privilege.

To allow users to download from the Trend Micro update server:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to which to grant Scheduled Update privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Client Privileges**. The **Client Privileges** screen appears.
4. Under **Update**, select the **Download from the Trend Micro update server** check box.
5. Click **Save** to grant the privilege to the selected domains or clients.
6. On the sidebar, click **Updates**, **Client Deployment**, and then **Update Source**. The **Update Source** screen appears.
7. Click **Customized Update Source**. Clients will update from the first update source on the **Customized update source** list. If the Trend Micro update server is not on the list, you must add it. The default address is:

   `http://officescan-p.activeupdate.trendmicro.com/activeupdate`

To perform Update Now on the client:

1. Right-click the OfficeScan icon in the system tray of the OfficeScan client machine. The OfficeScan shortcut menu appears.
2. Click **Update Now!**. The **Update Now Settings** screen appears.
3. If your network requires you to use a proxy server, click **Use a proxy server** check box and enter the proxy server settings.
4. Click the **Update Now** button. A status screen appears showing the progress of the component download.

Verifying a successful update

Check the client update logs to verify that an update has been successfully deployed.

To view the Client Update Logs:

1. On the sidebar of the Web console, click **Logs** > **Update Logs** > **Client Update**. The **Client Update Logs** screen appears.
2. Select the number of results to view on each page from the Display results per page list.
3. To Sort the table, click on the **Time/Date** or **Update Components** column headings.
4. To view the progress of a particular update, click **View** under the **Progress** column. The **Client Update Progress** screen appears, displaying the number of clients updated for every 15-minute interval and the total number clients updated.
5. To view the details of a particular update, click **View** under the **Detail** column. The **Client Update Detail** screen appears.

Verifying client-server connection

Verify OfficeScan client-server connection to help ensure that all your clients will have the correct configuration, including scan settings and privileges. Verify client-server connection manually or automatically from the Web console.

To verify the client-server connection:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.

2. Click the domains or clients to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Verify Connection**. The **Verify Connection** screen appears.
4. To verify client-server connection manually, click **Verify Now** under **Manual Verification**.
5. To verify client-server connection automatically, click the **Scheduled Verification** tab and select the **Enable scheduled verification** check box. Choose from these options:
   - **Once** – click to perform only one connection verification
   - **Hourly** – click to verify the client-server connection every hour
   - **Daily** – click to verify the client-server connection every day
   - **Weekly** – click to verify the client-server connection every week and select a day from the list

   If you clicked **Once**, **Daily**, or **Weekly**, select a time for the verification to begin under **Start time**.
6. Click **Save** to save the verification schedule.

Check the client tree again to verify that the client status changed. Also, view the verify connection log for a summary of your connection verification. See *Viewing Verify Connection Logs* on page 8-6 for more information.

Setting up standard notifications

The latest Internet-aware viruses, if left unchecked, can spread quickly throughout your organization and overwhelm network resources. Set up notifications for OfficeScan to inform you about viruses it detects or any outbreak that may be developing on the network.

Configure OfficeScan to send these types of alerts:

- Standard alerts
- Outbreak alerts

Configuring standard alerts

Send alerts to yourself or other administrators in your organization whenever OfficeScan detects a virus on any client. Standard alerts keep you informed about virus activities on the network.

To ensure that recipients get the alerts, OfficeScan provides multiple ways of sending alerts. Send standard alerts through the following:

- Email
- Pager
- SNMP trap
- Windows NT Event Log

OfficeScan includes the following information in all alert messages by default, except pager alerts:

- Computer name
- User name
- Domain name
- File path of the infected file
- Virus name
- Date and time of detection
- Scan action and result

To send alerts via email:

1. On the sidebar, click **Administration** > **Standard Alert** > **Email Notification**. The **Email Notification** screen appears.
2. Select the **Enable notification via email** check box and fill in these fields:
   - **SMTP** – type the domain name of the mail server
   - **Port number** – type the port number that the OfficeScan server uses to communicate with the mail server (default is 25)
   - **To** – type the destination email address
   - **From** – type the name of the sender
   - **Subject** – type the subject of the alert
   - **Message** – type the alert message

3. Click **Save** to save the settings.

To send alerts via pager:

1. On the sidebar, click **Administration** > **Standard Alert** > **Pager Notification**. The **Pager Notification** screen appears.
2. Select the **Enable notification via pager** check box.
3. Type both the pager number to which to send the alert message and the COM (communications) port to which your modem is connected.
4. Type a message in the **Message** text box.
5. Click **Save** to save the settings.

To send alerts via SNMP Trap:

1. On the sidebar, click **Administration** > **Standard Alert** > **SNMP Trap**. The **SNMP Trap** screen appears.
2. Select the **Enable notification via SNMP Trap** check box.
3. Type the IP address for SNMP trap notifications and the community name.
4. Type a message in the **Message** text box.
5. Click **Save** to save the settings.

To send alerts to the Windows NT Event Log:

1. On the sidebar, click **Administration** > **Standard Alert** > **NT Event Log**. The **NT Event Log** screen appears.
2. Select the **Enable notification via NT Event Log** check box.
3. Type a message in the **Message** text box.
4. Click **Save** to save the settings.

Configuring outbreak alerts

An outbreak refers to a sudden increase in the incidence of viruses on the network. In OfficeScan, you define the criteria for outbreaks; that is, how many virus incidents within a certain period of time will constitute an outbreak.

Responding to an outbreak is critical. Unless you take corrective action, an outbreak can spread quickly throughout and beyond the network.

To help you respond to outbreaks that may be developing on the network, send outbreak alerts to administrators whenever the outbreak criteria is met.

When OfficeScan sends an outbreak alert, use Outbreak Prevention to control the outbreak on the network. For more information on Outbreak Prevention, see *Configuring Outbreak Prevention* on page 6-1.

OfficeScan provides the following ways to send alerts:

- Email
- Pager
- SNMP trap
- Windows NT Event Log

To send alerts via email:

1. On the sidebar, click **Administration** > **Outbreak Alert** > **Email Notification**. The **Email Notification** screen appears.
2. Select the **Enable notification via email** check box.
3. Under **Outbreak Criteria**, define how many virus incidents within a certain period of time will constitute an outbreak.

Tip: Trend Micro recommends declaring an outbreak if OfficeScan detects 100 viruses in 24 hours (the default values).

---

4. Under **Alert Message Settings**, fill in these fields:
   - **SMTP** – type the domain name of the mail server
   - **Port number** – type the port number that the OfficeScan server uses to communicate with the mail server (default is 25)
   - **To** – type the destination email address
   - **From** – type the name of the sender
   - **Subject** – type the subject of the alert
   - **Message** – type the alert message
5. Select the information to include in the email body under **Alert Information to Include**.
6. Click **Save** to save the settings.

To send alerts via pager:

1. On the sidebar, click **Administration** > **Outbreak Alert** > **Pager Notification**. The **Pager Notification** screen appears.
2. Select the **Enable notification via pager** check box.
3. Under **Outbreak Criteria**, define how many virus incidents within a certain period of time will constitute an outbreak.

Tip: Trend Micro recommends declaring an outbreak if OfficeScan detects 100 viruses in 24 hours (the default values).

---

4. Type both the pager number to which to send the alert message and the COM (communications) port number to which the modem is connected.
5. Type a message in the **Message** text box.
6. Click **Save** to save the settings.

To send alerts via SNMP trap:

1. On the sidebar, click **Administration** > **Outbreak Alert** > **SNMP Trap**. The **SNMP Trap** screen appears.
2. Select the **Enable notification via SNMP Trap** check box.
3. Under **Outbreak Criteria**, define how many virus incidents within a certain period of time will constitute an outbreak.

Tip: Trend Micro recommends declaring an outbreak if OfficeScan detects 100 viruses in 24 hours (the default values).

---

4. Type the IP address to use for SNMP trap notifications and the community name.
5. Type a message in the **Message** text box.
6. Click **Save** to save the settings.

To send alerts to the Windows NT Event Log:

1. On the sidebar, click **Administration** > **Outbreak Alert** > **NT Event Log**. The **NT Event Log** screen appears.
2. Select the **Enable notification via NT Event Log** check box.
3. Type a message in the **Message** text box.

4. Click **Save** to save the settings.

Configuring the scan settings

OfficeScan provides three types of scans: real-time scan, scheduled scan, and manual scan. Enforce your organization's antivirus policies throughout the network by configuring the three types of scans based on these policies. Specify the types of files to scan and the action to take when a virus is found.

If you do not configure the scan settings, clients will scan files using the default settings of OfficeScan. The default scan settings provide adequate level of protection for most environments.

Exclude files and folders from scans to save time or to skip problem files that trigger false alarms. File and folder exclusion applies to all types of scans. For information on how to exclude files and folders, see *Excluding files and folders from scanning* on page 5-37.

About IntelliScan

IntelliScan is a new method of identifying files to scan that is more efficient than the standard **All scannable files** option. For executable files (for example, `.zip` and `.exe`), the true file type is determined based on the file content. For non-executable files (for example, `.txt`), the true file type is determined based on the file header.

IntelliScan provides the following benefits:

- Performance optimization — IntelliScan does not affect crucial applications on the client because it uses minimal system resources
- Shorter scanning period — Because IntelliScan uses true file type identification, it only scans files that are vulnerable to infection. The scan time is therefore significantly shorter than scanning all files.

About ActiveAction

Different types of viruses require different scan actions. Customizing scan actions for different types of viruses requires knowledge about viruses and can be a tedious task. For this reason, Trend Micro developed ActiveAction.

ActiveAction is a set of pre-configured scan actions for viruses and other types of malware.

Tip: 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.

ActiveAction provides the following benefits:

- Saves time and is easy to maintain — ActiveAction uses scan actions that are recommended by Trend Micro. You do not have to spend time customizing the scan actions.
- Updateable scan actions — Virus writers constantly change the way viruses attack computers. To help ensure that clients are protected against the latest threats and the latest methods of virus attacks, Trend Micro periodically updates ActiveAction settings.

Configuring Manual Scan

Also called Scan Now, manual scan occurs momentarily after being invoked and scans all files specified. The length of the scan depends on the number of files you are scanning and the computer's hardware resources.

To configure Manual Scan:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to which to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options** > **Manual Scan**. The **Manual Scan Settings** screen appears.
4. Under **Scan Target**, specify the files to scan:
   - **All scannable files** – click to scan all files that the client opens or saves
   - **Use IntelliScan – True file type identification** – click to use IntelliScan
   - **Scan files with the following extensions –** click to manually specify the files to scan based on their extensions:

.ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP

- **Scan compressed files –** select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan extensions include
- **Enable Exclusion list –** select to exclude certain directories, files (virus-proof system files) and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen to configure exclusion settings. See *Excluding files and folders from scanning* **on page 5-37**.
- **Scan memory (not applicable to Windows 2003/XP/2000/NT clients) –** select to scan the Random Access Memory (RAM) of the client.
- **Scan boot area –** select to scan the boot sector of the hard disk on the client
- **Scan hidden folders –** select to include hidden folders in any scan
- **Scan for spyware –** select to scan for software that installs components that record Web surfing habits
- **Scan mapped drives and shared folders on the network –** click to scan all mapped drives and shared folders on the network

5. Under **Scan Action**, specify how to handle viruses when OfficeScan detects them.
   - **Use ActiveAction – recommended actions by file type** – click to use ActiveAction
   - **Use Customized scan action** – click to manually specify how to handle different types viruses
   - **Use the same action for all malware types** – click to handle all virus types in the same manner.

     In the **Action1** and **Action2** lists, select the action to perform on infected files:
     - **Pass** – take no action on the file
     - **Delete** – delete the file

- **Rename** – rename the file to identify it as infected
- **Quarantine** – move the file to the quarantine directory
- **Clean** – clean the file of the virus

Tip: Trend Micro recommends selecting **Clean**. Save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

OfficeScan performs **Action 2** only if **Action 1** is not successful.

- In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files.

  For example: `HTTP://<OfficeScan_server_name>`

6. Click **Save** to save the manual scan settings.

Note: If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

Configuring Real-time Scan

Set OfficeScan to scan a file in real-time whenever it is opened or saved. If OfficeScan does not detect a virus, the user can proceed with opening or saving the file. If it does detect a virus, OfficeScan displays an alert message, showing the name of the infected file and the virus name.

The performance of real-time scanning depends on its settings. Optimize the performance of real-time scans by specifying certain file types that are vulnerable to viruses or by limiting the maximum number of compression layers to scan.

To configure Real-Time Scan:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options** > **Real time Scan**. The **Real-time Scan Settings** screen appears.

4. Select the **Enable Real-time Scan** check box.
5. Under **Scan Target**, specify incoming or outgoing files
   - **Scan incoming file –** select to scan only files the client is receiving
   - **Scan outgoing file –** select to scan only files the client is sending
   - **Scan incoming and outgoing file –** select to scan both incoming and outgoing files

   Select the types of files to scan:
   - **All scannable files** – click to scan all files that the client opens or saves
   - **Use IntelliScan – all essential file types** – click to use IntelliScan
   - **Scan files with the following extensions –** click to manually specify the files to scan based on their extensions:

     .ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP
   - **Scan compressed files –** select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan extensions include.
   - **Enable Exclusion list –** select to exclude certain directories, files (virus-proof system files) and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen, to configure exclusion settings. See *Excluding files and folders from scanning* **on page 5-37**.
   - **Scan boot area (not applicable to Windows 2003/XP/2000/NT clients) –** select to scan the boot sector of the hard disk on the client
   - **Scan during system shutdown –** select to run real-time scan every time the client is shut down
   - **Scan for spyware –** select to scan for software that installs components that record Web surfing habits
   - **Scan mapped drives and shared folders on the network –** click to scan all mapped drives and shared folders on the network

6. Under **Scan Action**, specify how to handle viruses when OfficeScan detects them.
   - **Display an alert message on the client when a virus is detected** – select to have an alert message pop up on the client
   - **Use ActiveAction – recommended actions by file type** – click to use ActiveAction
   - **Use Customized scan action** – click to manually specify how to handle different types viruses

     In the **Action1** and **Action2** lists, select the action to perform on infected files.
   - **Use the same action for all malware types** – click to handle all virus types in the same manner

     In the **Action1** and **Action2** lists, select the action to perform on infected files.
     - **Pass** – take no action on the file
     - **Delete** – delete the file
     - **Rename** – rename the file to identify it as infected
     - **Quarantine** – move the file to the quarantine directory
     - **Clean** – clean the file of the virus

     Tip: Trend Micro recommends selecting **Clean**. Save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

     OfficeScan performs **Action 2** only if **Action 1** is not successful.
   - In **Quarantine directory**, type a Uniform Resource Locator (URL) or Universal Naming Convention (UNC) path to store the infected files.

     For example: `HTTP://<OfficeScan_server_name>`
7. Click **Save** to save your manual scan settings.

Note: If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

Configuring Scheduled Scan

A scheduled scan completely scans specified files at the time and frequency configured. Use scheduled scan to automate routine scans on the clients and improve virus management efficiency.

To configure Scheduled Scan:

1. On the sidebar, click **Clients**. The domain tree for the **Client** screen appears.
2. Click the domains or clients to which to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options** > **Scheduled Scan**. The **Scheduled Scan Settings** screen appears.
4. Select the **Enable Scheduled Scan** check box.
5. Under **Schedule**, specify when to perform scheduled scan:
   - **Daily** - click to perform scheduled scan every day
   - **Weekly** - click to perform scheduled scan once a week. You must select a day from the list
   - **Monthly** - click to perform scheduled scan once a month. You must select a date from the list

   Regardless if you click **Daily**, **Weekly**, or **Monthly**, you must specify a time to perform schedule scan in the **Start time** list boxes.
6. Under **Scan Target**, specify the files to scan by selecting the check boxes and clicking the options.
   - **All scannable files** – click to scan all files that the client opens or saves
   - **Use IntelliScan – all essential file types** – click to use IntelliScan
   - **Scan files with the following extensions –** click to manually specify the files to scan based on their extensions:

.ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP

- **Scan compressed files –** select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan extensions include:
- **Enable Exclusion list –** Select to exclude certain directories, files (virus-proof system files) and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen to configure exclusion settings. See *Excluding files and folders from scanning* **on page 5-37**.
- **Scan memory (not applicable to Windows 2003/XP/2000/NT clients) –** select to scan the Random Access Memory (RAM) of the client
- **Scan boot area –** select to scan the boot sector of the hard disk on the client
- **Scan for spyware –** select to scan for software that installs components that record Web surfing habits

7. Under **Scan Action**, specify how to handle viruses when OfficeScan detects them.
   - **Display an alert message on the client when a virus is detected** – select to have an alert message pop up on the client
   - **Use Customized scan action** – click to manually specify how to handle different types viruses

     In the **Action1** and **Action2** lists, select the action to perform on infected files.
   - **Use the same action for all malware types** – click to handle all virus types in the same manner

     In the **Action1** and **Action2** lists, select the action to perform on infected files:
     - **Pass** – take no action on the file
     - **Delete** – delete the file
     - **Rename** – rename the file to identify it as infected

- **Quarantine** – move the file to the quarantine directory
- **Clean** – clean the file of the virus

Tip: Trend Micro recommends selecting **Clean**. Save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

OfficeScan performs **Action 2** only if **Action 1** is not successful.

8. Click **Save** to save your manual scan settings.

Note: If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

Excluding files and folders from scanning

To increase the performance of scanning or to skip files that are causing false alarms, you can exclude certain files and folders from scanning. The files and folders you add to the exclusion list will be skipped by manual scan, real-time scan, and scheduled scan.

Note: If Microsoft Exchange is running on your client machines, Trend Micro recommends excluding all Microsoft Exchange folders from scanning. Trend Micro also recommends installing ScanMail for Microsoft Exchange to protect these folders.

To exclude files and folders from scanning:

1. On the sidebar, click **Clients**. The domain tree for the **Clients** screen appears.
2. Select the domains or clients on which to configure the scan options by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Options**. Next, click the type of scan to perform (manual, real time, scheduled). The settings screen for that scan type appears.

4. In that settings screen, select the check box next to **Enable Exclusion list**. Click the **Enable Exclusion list** link. The **Execution List** screen appears.
5. To exclude all folders containing Trend Micro products and components, select the **Excluding from scanning the directories where Trend Micro products are installed** check box.
6. To exclude specific directories, type the directory names under **Enter the directory path (E.g. c:\temp\ExcludeDir)** and click **Add**.
7. To exclude specific files by file name, type the file names under **Enter the file name or file name with full path (E.g. ExcludeDoc.hlp; c:\temp\excldir\ExcludeDoc.hlp)** and click **Add**.

Note: All subdirectories in the directory path you specify will also be excluded.

8. Specify the files to exclude based on their extensions.

   To use specified extensions, select the extensions to protect and click .

   To specify an extension that is not in the list, type this in the text box, and then click **Add**.
9. To apply this setting to all future clients that will belong to the domain you selected, click **Save**.
   - To apply this setting to all existing and future clients that belong and will belong to the domain you selected, click **Apply to All**
   - If you only selected a client or clients in Step 1, only **Save** will appear

Note: If Microsoft Exchange is running on your client machines, Trend Micro recommends excluding all Microsoft Exchange folders from scanning.

Running Scan Now

Run Scan Now on clients remotely using the Web console. In addition to turning on Real-time Scan and configuring Scheduled Scan, Trend Micro recommends running Scan Now on computers you suspect to be infected.

To run Scan Now:

1. On the sidebar, click **Clients**. The domain tree for the **Client** screen appears.
2. Click the domains or clients on which to run Scan Now by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Scan Now**. The **Scan Now** screen appears, displaying the clients or domains you selected.
4. Under **Computer**, select the clients on which to run Scan Now, and then click **Start Notification**. The server sends a request to the client to run Scan Now using the pre-configured settings.

To change Scan Now settings

1. Click **Scan Now Settings**. The **Scan Now Settings** screen appears.
2. Under **Scan Target**, specify the files to scan:
   - **All scannable files** – click to scan all files that the client opens or saves
   - **Use IntelliScan – all essential file types** – click to use IntelliScan
   - **Scan files with the following extensions –** click to manually specify the files to scan based on their extensions:

     .ARJ, .ASP, .BAT, .BIN, .BOO, .CAB, .CHM, .CLA, .CLASS, .COM, .CSC, .DAT, .DLL, .DOC, .DOT, .DRV, .EML, .EXE, .GZ, .HLP, .HTA, .HTM, .HTML, .HTT, .INI, .JAR, .JS, .JSE, .LNK, .LZH, .MDB, .MPD, .MPP, .MPT, .MSG, .MSO, .NWS, .OCX, .OFT, .OVL, .PDF, .PHP, .PIF, .PL, .POT, .PPS, .PPT, .PRC, .RAR, .REG, .RTF, .SCR, .SHS, .SYS, .TAR, .VBE, .VBS, .VSD, .VSS, .VST, .VXD, .WML, .WSF, .XLA, .XLS, .XLT, .XML, .Z, and .ZIP
   - **Enable Exclusion list –** Select to exclude certain directories, files (virus-proof system files) and extensions from scanning. Click the **Enable Exclusion List** link to go to the Exclusion List screen to configure exclusion settings**.** See *Excluding files and folders from scanning* **on page 5-37**.
   - **Scan memory (not applicable to Windows 2003/XP/2000/NT clients) –** select to scan the Random Access Memory (RAM) of the client
   - **Scan boot area –** select to scan the boot sector of the hard disk on the client
   - **Scan for spyware –** select to scan for software that installs components that record Web surfing habits

- **Scan compressed files –** select to scan compressed files that are stored on the client. In the **Up to { } layers of compression** list, select the maximum number of compression layers to scan extensions include:

3. Under **Scan Action**, specify how to handle viruses whenOfficeScan detects them.
   - **Use ActiveAction – recommended actions by file type** – click to use ActiveAction
   - **Use customized scan action** – click to manually specify how to handle different types viruses

     In the **Action1** and **Action2** lists, select the action to perform on infected files.
   - **Use the same action for all malware types** – click to handle all virus types in the same manner.

     In the **Action1** and **Action2** lists, select the action to perform on infected files.
     - **Pass** – take no action on the file
     - **Delete** – delete the file
     - **Rename** – rename the file to identify it as infected
     - **Quarantine** – move the file to the quarantine directory
     - **Clean** – clean the file of the virus

   Tip: Trend Micro recommends selecting **Clean**. Save a copy of the files before cleaning, select the **Back up files before cleaning** check box.

   OfficeScan performs **Action 2** only if **Action 1** is not successful.
4. Click **Save** to save the Manual Scan settings.

Note: If you clicked the root icon before setting the manual scan settings, another button named **Apply to All** will appear beside **Save**. If you want all existing and future clients to have these manual scan settings, click **Apply to All**.

To stop Scan Now:

1. Select the clients on which to stop Scan Now.
2. Click **Stop Scan**.

To stop notifications

1. Select the clients you no longer want to run Scan Now.
2. Click **Stop Notification**. Clients that have not yet started Scan Now will skip the request. However, clients that are already running Scan Now will not be affected. To stop Scan Now on these clients, click **Stop Scan**.

Note: Scan Now and manual scan are the same type of scan. The only difference is that you run Scan Now remotely from the Web console, while users run manual scan locally on the clients.

Granting privileges to clients

You have the option of granting users privileges to modify individual scan settings, update components, and remove or unload the client. This is a way of sharing control over individual client settings.

However, to enforce uniform antivirus policy throughout the organization, Trend Micro recommends granting limited privileges to users. This will ensure that scan settings are not modified or clients are not removed or unloaded without your permission.

To grant privileges to clients:

1. On the sidebar, click **Clients**. The domain tree for the **Client** tree appears.
2. Click the domains or clients to which to grant privileges by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Client Privileges**. The **Set Client Privileges** screen appears.
4. Select the privileges to grant users. Configure the following areas:
   - **Antivirus** – select the check boxes for the scan privileges to grant users

- **Mail Scan** – select the check boxes for the mail scan privileges to grant users
- **Toolbox** – select the check boxes to display a toolbox tab and grant users privileges to different client tools
- **Proxy Setting** – select the check box to allow the user to use a proxy
- **Update** – select the check boxes for the update privileges to grant users.

Note: If you grant clients the privilege to **Enable scheduled update**, make sure to select the check box labeled **Enable scheduled deployment (client scheduled update) from OfficeScan server or customized update source** under **Updates** > **Client Deployment** > **Automatic Deployment**.

- **Uninstallation** – To allow users to remove the client without requiring a password, click **Allow the client user to uninstall OfficeScan client**. To allow only users with the uninstall password to be able to remove the client, click **Require a password for the client user to unload OfficeScan client**, and then type an uninstall password in the text box.
- **Unloading** – To allow users to unload (or turn off) the client without requiring a password, click **Allow the client user to unload OfficeScan**. To allow only users with the unload password to be able to turn off the client, click **Require a password for the client user to unload OfficeScan client**, and then type an unload password in the text box.

5. Click **Save** to grant the privileges to the selected domains or clients.

Note: If you clicked the root icon before setting privileges, another button named **Apply to All** will appear beside **Apply**. If you want all existing and future clients to have this set of privileges, click **Apply to All**.

Chapter 6

Configuring Outbreak Prevention

OfficeScan helps you control outbreaks on the network with Outbreak Prevention. This chapter explains how to use Outbreak Prevention to block shared folders, block ports, and deny write access to files and folders.

The topics discussed in this chapter include:

- *Blocking shared folders* on page 6-2
- *Blocking ports* on page 6-3
- *Denying write access to files and folders* on page 6-5
- *Configuring client notification for outbreaks* on page 6-7
- *Restoring network settings to normal* on page 6-7

Blocking shared folders

During virus outbreaks, Trend Micro recommends blocking shared folders on the network to prevent viruses from spreading through the shared folders. Many types of viruses gain access to computers through shared folders.

To block shared folders:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select **Block shared folders**.
5. To configure the shared folder blocking settings, click **Settings**. The **Shared Folder Blocking** screen appears.
6. Under **Shared Folder Blocking Settings**, specify the access privilege to shared folders when you enable Outbreak Prevention. Click one of the following:
   - Read access only
   - No read and write access
7. Click **Save** to save your settings.
8. Click **Back** to return to the **Outbreak Prevention Settings** screen.
9. Click **Activate Settings** to enable Outbreak Prevention on the selected domains or clients.
10. The **Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

To verify that Outbreak Prevention is enabled, check if the client icons in the domains you selected appear as .

WARNING! *Enable Outbreak Prevention only when there is a virus outbreak. Configure the Outbreak Prevention settings carefully. Incorrect configuration may cause unforeseen network issues.*

Blocking ports

During virus outbreaks, block vulnerable ports that viruses and Trojans might use to gain access to clients. You may block all ports or specific ports on your workstations.

To block ports:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select the **Block ports** check box.
5. To configure the port blocking settings, click **Settings**. The **Port Blocking** screen appears.
6. To block the trusted port, which the server and client use for communication, select the **Block trusted port** check box.
7. To add ports to block, click **Add ports**. The **Add Ports to Block** screen appears.
8. Specify which ports to block. Click one of the following:
   - **Block all ports (Including ICMP)** — click to block all ports, including the Internet Control Message Protocol (ICMP). ICMP is an extension of Internet Protocol (IP), and supports packets containing error, control, and informational messages.

Note: Clicking **Block all ports (including ICMP)** will block all ports except the trusted ports. To block the trusted ports, select the **Block trusted ports** check box on the **Port Blocking** screen.

   - **Block specified ports** – click to specify the ports to block. Click one of the following:
     - **Commonly used ports** – click to block port numbers that are normally used for popular Internet services; for example, port 80 for Web (HTTP), port 25 for Send Email (SMTP). If you click **Commonly used**

ports, select at least one port number to have OfficeScan save your port blocking settings.

- **All Trojan ports** – click to block all ports that are known to be vulnerable to Trojan attacks. To learn more about these Trojan ports, see the topic *What are Trojan ports?* in the OfficeScan online help.
- **Specify a port number or port range between 1 and 65535** – click to specify the direction of traffic to block and the port range or port numbers

  To block incoming traffic, select **Incoming traffic**.

  To block outgoing traffic, select **Outgoing traffic**

  Click either **Port range** or **Port number(s)**. If you click **Port range**, type a range of port numbers between 1 and 65535 in the text boxes. If you click **Port number(s)**, type the port numbers to block in the text box. Separate entries with commas.

  From the **Protocol** list, select the communication method to block from the drop-down list. Select Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or both.

  In **Comments**, type optional information, such as reasons for blocking the ports you specified
- **Ping protocol (Reject ICMP)** – click to block ICMP packets, such as ping

9. Click **OK**. A confirmation screen appears.
10. Click **OK**. The **Port Blocking** screen appears, showing a summary of the port blocking settings, including the blocked ports, protocol, comments, and traffic direction.
11. Click **Back** to return to the **Outbreak Prevention** screen.
12. Click **Activate Settings** to enable Outbreak Prevention on the selected domains or clients. The **Outbreak Prevention** screen appears, showing your current outbreak prevention settings.

    To modify existing port blocking settings, see the next section *Modifying Port Blocking Settings* on page 6-5.

    To verify that Outbreak Prevention is enabled, check if the client icons in the domains you selected appear as .

WARNING! *Enable Outbreak Prevention only when there is a virus outbreak. Configure the Outbreak Prevention settings carefully. Incorrect configuration may cause unforeseen network issues.*

Modifying Port Blocking Settings

Modify port blocking settings on the **Port Blocking** screen.

To modify the existing settings of an individual port from the Port Blocking screen:

1. Click **Edit**. The **Port Blocking Setting** screen appears.
2. Select whether or not to block incoming/outgoing traffic.
3. Click **Port range** and type the port numbers to block all ports within a range or click **Port number(s)** and type one or more individual port numbers to block a set of ports.
4. Modify the protocol used by the port(s) by selecting **TCP**, **UDP**, or **TCP/UDP** from the **Protocol** menu.
5. Type a description in the port(s) **Comments** field, which typically provides a descriptive name for the port(s).
6. Click **OK**. A confirmation screen appears.
7. Click **OK** again to return to the **Port Blocking** screen.

Denying write access to files and folders

Some viruses modify or delete files and folders on host computers. Configure OfficeScan to prevent viruses from modifying or deleting files and folders on clients during a virus outbreak by denying write access to files and folders.

To deny write access to files and folder

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.

3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Under **Outbreak prevention settings**, select **Deny write files and folders**.
5. To configure the shared folder blocking settings, click **Settings**. The **Deny Write Settings** screen appears.
6. To deny write access to specific directories and file name extensions, type the path of the directory to protect in **Directory path**. For example, type `C:\temp`. Type the absolute path for the directory. If typing multiple paths, separate entries with semicolons (;).

   Next, click **Add**. The path appears under **Protected directories**. Before continuing, make sure all the directories to protect appear under **Protected directories**.

   Note: All subdirectories in the directory path you specify will also be protected.

7. Specify the files in the **Protected directories** list to deny write access based on their extensions. Click one of the following:
   - **All files in the protected directories**
   - **Files in the protected directories with the following extensions**

   To use specified extensions, select the extensions to protect from **Extensions list** and click .

   To specify an extension that is not in the list, type it in the text box, and then click **Add**. If typing multiple extensions, separate entries with semicolons (;).

   To protect specific files, type the full file names under **Files to Protect**.
8. Click **Save** to save the settings. A confirmation screen appears.
9. Click **OK**. The directory path to protect is visible under **Protected Directories** in the **Deny Write Settings** screen.
10. Click **Back** to return to the **Outbreak Prevention Settings** screen.
11. Click **Activate Settings** to enable Outbreak Prevention on the selected domains or clients. The **Outbreak Prevention** screen appears, showing the current outbreak prevention settings.

To verify that Outbreak Prevention is enabled, check if the client icons in the domains you selected appear as .

WARNING! *Enable Outbreak Prevention only when there is a virus outbreak. Configure the Outbreak Prevention settings carefully. Incorrect configuration may cause unforeseen network issues.*

Configuring client notification for outbreaks

Enabling Outbreak Prevention can prevent users from gaining access to network resources. To inform users that Outbreak Prevention has been enabled, display outbreak notifications on clients.

To display outbreak notifications on clients:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.
2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Deploy Now**. The **Outbreak Prevention Settings** screen appears.
4. Select the **When OPP is enabled, display the following message on the OfficeScan client** check box.
5. Accept the default message or type a new message in the text box.
6. Click **Activate Settings** to save your settings.

Restoring network settings to normal

After verifying that an outbreak has been contained and that all infected files have been cleaned or quarantined, restore network settings to normal by disabling Outbreak Prevention.

To restore network settings to normal:

1. On the sidebar, click **Outbreak Prevention**. The domain tree for the **Clients** screen appears.

2. Click the domains or clients on which to enable Outbreak Prevention by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Restore**. The **Restore Outbreak Prevention Settings** screen appears.
4. To inform users that the outbreak has ended, select the **When manual outbreak prevention settings are disabled, display the following message on the OfficeScan clients** check box. Either accept the default message or type a new one in the text box.
5. Click **Restore to normal**.
6. The **Outbreak Prevention** screen displays a message that Outbreak Prevention is disabled on the selected domains and computers.

To verify that Outbreak Prevention is disabled, check if the client icons in the domains you selected no longer appear as .

Note: If you do not restore network settings manually, OfficeScan restores them when the number of hours specified in **Automatically restore network settings to normal after { } hours** on the **Outbreak Prevention Settings** screen passes. The default setting is 48 hours.

Chapter 7

Configuring Virus Outbreak Monitor

This chapter describes how to significantly enhance antivirus initiatives by activating and configuring Virus Outbreak Monitor.

Configuring Virus Outbreak Monitor

After infecting a host on a network, many virus types attempt to drop files on target computers. This action creates a session on the target machine. Therefore, monitoring the number of simultaneous sessions on your network is an effective method of detecting viruses.

OfficeScan clients notify the OfficeScan server when they detect sessions. Whenever the number of concurrent sessions exceeds a specified amount, OfficeScan server can send an alert message to the administrator, who can take proper action.

To configure Virus Outbreak Monitor:

1. Click **Virus Outbreak Monitor** in the sidebar. The **Virus Outbreak Monitor** screen appears.
2. Select the **Enable Virus Outbreak Monitor** check box.
3. Under **Alert Criteria for Virus Outbreak Monitor**, type both the minimum number of network sessions and time period (in minutes) during which they are detected. These criteria will determine when to send an alert message.

Tip: In determining the number of network sessions, Trend Micro suggests taking the number of clients divided by 10 (#clients/10) for every three minutes.

---

4. To send an alert message, select the **Send a notification via email if alert criteria are met** check box.
5. If you enable an alert message, fill in these fields under **Alert message settings**:
   - **SMTP** – type the domain name of the mail server
   - **Port Number** – type the port number that the OfficeScan server uses to communicate with the mail server (default is 25)
   - **To** – type the destination email address
   - **From** – type the name of the sender
   - **Subject** – type the subject of the alert
   - **Message** – type the alert message
6. Click **Save** to save the settings.

To export Virus Outbreak Monitor records

1. Click **Virus Outbreak Monitor** in the sidebar. The **Virus Outbreak Monitor** screen appears.

2. Click the link that displays the **Network sessions recorded** under **Current Status**. The **Virus Outbreak Monitor Records** screen appears.
3. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. A confirmation screen appears.
    - Click **Open** to view the file in your spreadsheet application without saving it.
    - To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use spreadsheet applications to view CSV data files.

Chapter 8

Viewing and Interpreting Logs

This chapter describes how to use OfficeScan logs to monitor your system and analyze your protection.

The topics discussed in this chapter include:

- *Viewing and Interpreting Logs* on page 8-2
- *Managing Logs* on page 8-6

Viewing and Interpreting Logs

OfficeScan keeps comprehensive logs about virus incidents, events, and updates. Use these logs to assess your organization's virus protection policies and to identify clients that are at a higher risk of infection. Also use these logs to check client-server connection and verify that updates were deployed successfully.

OfficeScan maintains the following logs:

- Virus Logs
- Server Update Logs
- Client Update Logs
- System Event Logs
- GateLock IDP Logs (if GateLock devices present)
- Verify Connection Logs

Viewing Virus Logs

OfficeScan records log entries for viruses detected on your clients.

To view virus logs:

1. On the sidebar, click **Logs** > **Virus Logs**. The **Clients** screen appears.
2. Click the domains or clients whose virus logs to view by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **OfficeScan clients**. The **View Virus Logs** screen appears.
4. Under **Time**, click **Select a time period** and make a selection from the list or click **Specify a range** and enter a range of dates.
5. Under **Scan Types**, select the types of logs to display by selecting the corresponding check boxes.
6. Under **Sort by**, click an option to specify how to classify the logs. The options are:
   - Date and time
   - Computer name
   - Virus name
   - Scan type

- Scan result

7. To view the log, click **View logs**.
8. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

Deleting Virus Logs

To conserve disk space on the server, delete virus logs manually.

To delete virus logs:

1. On the sidebar, click **Logs** > **Virus Logs**. The **Clients** screen appears.
2. Click the domains or clients whose virus logs to delete by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. On the sidebar, click **Delete Logs**. The **Delete Logs** screen appears.
4. Under **Select log types**, select the types of logs (based on the type of scan that OfficeScan performed) to delete.
5. Under **Deletion**, specify the logs to delete. The options are:
   - **Delete all log content in the selected log types**
   - **Delete logs older than { } days**

   If you click **Delete logs older than { } days**, type a value for the number of days. For example, if you type '20', OfficeScan deletes logs that you created 20 days ago and earlier.
6. Click **Apply** to delete the logs.

Viewing Server Update Logs

OfficeScan keeps logs for server updates. This helps you keep track of the server's update history and the update methods used.

To view server update logs:

1. Click **Logs** > **Update Logs** > **Server Update** on the sidebar. The **Server Update Logs** screen appears, showing the following information:
   - Time and date of update
   - Result of the update

- Update component
- Update method

2. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

Viewing Client Update Logs

OfficeScan also provides client update logs. Use these logs to verify update deployment.

To view client update logs:

1. Click **Logs** > **Update Logs** > **Client Update** on the sidebar. The **Client Update Logs** screen appears, showing the following information:
   - Date and time of update
   - Update components
   - Progress
   - Details
2. Select the number of results to view on each page from the **Display results per page** list.
3. Click on the column headings **Time/Date** or **Update Components** to sort the table.

To view how many clients were updated for a particular update deployment:

1. Click **View** under the **Progress** column. The **Client Update Progress** screen appears.
2. From this screen, view the number of clients updated for every 15-minute interval and the total number of clients updated.

To view which clients were updated for a particular update deployment:

1. Click **View** under the **Detail** column. The **Client Update Detail** screen appears, showing the names of clients that were updated and the update details.
2. Sort the table by clicking on column headings: **Computer name**, **Notification sent**, **Notification received**, or **Update completed**.
3. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

Viewing System Event Logs

OfficeScan also records events related to the server program, such as shutdown and start-tup. Use these logs to verify that the server is running smoothly and that the services necessary for OfficeScan to work on your network are running.

To view system event logs:

1. Click **Logs** > **System Event Logs** on the sidebar. The **System Event Logs** screen appears, showing recent events on the server.
2. Select the number of results to view on each page from the **Display results per page** list.
3. Sort the table by clicking on column headings: **Time/Date** or **Computer Name**, or **Event Description**.
4. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

Viewing GateLock Intrusion Detection and Prevention (IDP) Logs

OfficeScan allows you to view the GateLock Intrusion Detection and Prevention (IDP) logs for all GateLock devices on your system.

To view GateLock IDP logs:

1. Click **Logs** > **GateLock Clients Logs** on the sidebar. The **GateLock Clients** screen appears, showing recent events on the server.
2. Click the domains or GateLock clients by clicking the corresponding icons in the domain tree. To select all domains and clients, click the root icon.
3. Click **IDP Logs** in the sidebar. **The View Gatelock Clients IDP Logs** screen appears.
4. Select logs based on the time of the log entry. Click the radio button next to the list and select a recent time period from the menu, or click **Specify a range** and type the dates in the **From** and **To** fields.
5. Select a sort criteria from the **Sort** by menu. Sort by the following methods:
   - **Date and Time**
   - **Client Name**
   - **Severity Level**

6. Click **View Logs** to open the **View GateLock Clients IDP Logs** screen.
7. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

Viewing Verify Connection Logs

OfficeScan keeps Verify Connection logs to allow you to determine the connection status between the server and clients.

To view verify connection logs:

1. Click **Logs** > **Verify Connection Logs** on the sidebar. The **Verify Connection Log** screen appears, showing the clients' computer names, domains, IP addresses, and connection status.
2. Select the number of results to view on each page from the **Display results per page** list.
3. Sort the table by clicking on column headings: **Time/Date**, **Computer Name**, **Domain**, **IP Address** or **Status**.
4. To save the log as a comma-separated value (CSV) data file, click **Export to CSV**. Use a spreadsheet application to view CSV data files.

Managing Logs

Manage logs by performing scheduled log maintenance to keep their size from occupying too much space on your hard disk. You can configure OfficeScan to automatically delete the logs based on a schedule.

To perform scheduled log maintenance:

1. On the sidebar, click **Logs** > **Log Maintenance**. The **Log Maintenance** screen appears.
2. Select the **Enable Scheduled Deletion of Logs** check box to perform scheduled maintenance.
3. Under **Log type(s) to delete**, select the logs types to delete automatically. The options are:
4. Under **Log entry deletion criteria**, specify which logs to delete. The options are:
   - **Delete all log content in the selected log types**
   - **Delete logs older than { } days**

If you click **Delete logs older than { } days**, type a value in the text box.

5. Under **Schedule**, specify a frequency when to perform scheduled log maintenance:
   - **Days**
   - **Weekly, every { }**
   - **Monthly, on day { }**

   If you click **Weekly**, select a day from the list.

   If you click **Monthly**, select a date from the list.

   Regardless of the frequency you set, specify when to perform scheduled log maintenance in **Start time**.
6. Click **Save** to save your settings.

Chapter 9

Installing and Launching ScanMail™ for Microsoft™ Exchange

This chapter explains how to install and launch ScanMail for Microsoft Exchange on OfficeScan management consoles. For more information on ScanMail for Microsoft Exchange, see *Introducing Trend Micro ScanMail™ for Microsoft™ Exchange* starting on page 11-1.

System requirements for ScanMail for Microsoft™ Exchange 2000 and 2003

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

Target servers

- Intel™ Pentium™ III 500MHz processor (or higher)
- 256MB RAM minimum (512MB or more recommended)
- 60MB free disk space for the program files
- Microsoft Exchange 2000 or 2003 Server with Service Packs 1 or above
- Microsoft Windows 2000/2003 Server or Advanced Server with Service Pack 1 or above. Either server must be installed on an NTFS partition

- A Java-enabled Web browser that supports frames, such as Microsoft™ Internet Explorer® 5.0 (or above) or Netscape™ Navigator™ 6.0 for Web-based management. If you are using Internet Explorer, make sure you have the Java Virtual Machine installed

Note: For Web-based management, please download and install the latest version (1.3.1 or above) of the Java Virtual Machine (JVM). You can download the JVM from www.sun.com.

System Requirements for ScanMail for Microsoft® Exchange 5.5

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

Target Servers

- 200MHz (or higher) Intel™ Pentium™ processor (or equivalent)
- 256MB RAM minimum
- 50MB free disk space for the program files
- Microsoft Exchange Server 5.5 with Service Pack 4 (or above)
- Windows NT Server version 4.0 (English) with Service Pack 5 (through Service Pack 6a); Microsoft Windows 2000 Server or Advanced Server with Service Pack 1 or above.
- A Java-enabled Web browser that supports frames, such as Microsoft® Internet Explorer® 5.5 (or above) or Netscape™ Navigator™ 6.0 or for Web-based management. If you are using Internet Explorer, make sure you have the Java Virtual Machine installed.

Note: For Web-based management, please download and install the latest version (1.3.1 or above) of the Java Virtual Machine (JVM). You can download the JVM from www.sun.com.

- Microsoft Data Access Components (MDAC) 2.5 and Microsoft Jet 4.0, or MDAC 2.6 (or above) and Microsoft Jet Service Pack 3 for full Quarantine Manager functionality

Note: To determine which versions of MDAC and Microsoft Jet you have installed, see *Determining Your Version of MDAC and Microsoft Jet* starting on page 9-3.

Determining Your Version of MDAC and Microsoft Jet

For Microsoft Exchange 5.5, to use the Quarantine Manager you need to have Microsoft Data Access Components 2.5 and Microsoft Jet 4.0, or MDAC 2.6 (or above) and Microsoft Jet Service Pack 3 installed on your server. MDAC is installed with numerous Microsoft products.

You can determine these version numbers using Microsoft's Component Checker tool, which can be downloaded at:

`http://www.microsoft.com/data/download.htm`

To check your versions of MDAC and Microsoft Jet:

1. Click the file **`cc.exe`** and unzip the contents to a directory, typically **`\comcheck`**.
2. Click **`comcheck.exe`** and select the first option to perform an analysis on your machine.
3. Wait for the scanning to determine your version of MDAC. The MDAC version should be 2.5.
4. Expand the **`OLDDB`** option in the left navigator to determine whether you have Microsoft Jet 4.0 installed.

If you need to install these components:

1. Download the MDAC and Microsoft Jet or Jet SP3 from Microsoft.
2. Install MDAC before Microsoft Jet.
3. Restart the ScanMail_RealTimeScan service if you have already installed ScanMail. Restart the ScanMail Management Console also if you have it open.

System Requirements for ScanMail™ eManager Windows-based Console

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

ScanMail eManager for Microsoft™ Exchange 2000 and 2003

Target Servers

- Microsoft Exchange 2000 Server with Service Pack 1 (or above)
- Windows 2000 Server or Windows 2000 Advanced Server with Service Pack 1 (or above)
- Intel™ Pentium™ III 500MHz or higher processor (or equivalent)
- 256MB RAM minimum (512MB or more recommended)
- 60MB free disk space for the program files
- 100-500MB of free disk space for swap and temporary files
- A monitor with 800x600 or higher resolution

ScanMail™ eManager™ for Microsoft™ Exchange

Target Servers

- Intel Pentium III 500MHz or higher processor (or equivalent)
- 256MB RAM minimum (512MB RAM or more recommended)
- 60MB free disk space for the program files
- Windows NT Server version 4.0 (English) with Service Pack 6 (or above); Windows 2000 Server; Windows 2000 Advanced Server
- Microsoft Exchange Server 5.5 with Service Pack 2 (or above)

For Microsoft Cluster servers, you also need:

Cluster server capabilities are only available in ScanMail enterprise version.

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

Installing and Launching ScanMail for Exchange from the OfficeScan Console

You can use OfficeScan to install ScanMail for Microsoft Exchange on designated servers. You can also launch ScanMail for Exchange consoles to perform ScanMail management.

To install ScanMail for Exchange

1. On the sidebar, click **ScanMail for Exchange**. The **ScanMail for Exchange management** screen appears.
2. Click **Install**. The **Install ScanMail for Microsoft Exchange** screen appears.
3. Specify the server and provide the account and password to install ScanMail for Microsoft Exchange.
4. Click **OK** to install. When the installation is complete, the **ScanMail for Microsoft Exchange Installation** screen appears. You will see the ScanMail server name in the ScanMail for Microsoft Exchange management table, along with the server's IP address and the port number....

To launch ScanMail for Exchange

1. On the sidebar, click **ScanMail for Exchange**. The **ScanMail for Exchange management** screen appears.
2. The name, IP address and port number of each ScanMail server are listed in the **ScanMail for Exchange management** table. Click the name link of the ScanMail server whose console you want to launch.

To remove a ScanMail server from the ScanMail for Microsoft Exchange management table

1. Select the check box next to the server's name or click the top check box to select all servers.
2. Click **Delete**.
3. Click **Refresh** to refresh the table contents. The deleted server will not appear in the **ScanMail for Exchange management** table.

Installing the eManager Windows-based console

If you are using Client Server Messaging Suite for SMB. Client Server Messaging Suite automatically installs the eManager Windows-based console on your administrator server. While you can perform most major eManager functions on the Web-based console, use the Windows-based console to configure the following features:

- Approved/Blocked Senders
- Anti-spam rules
- Notifications

Users can install the Web-based console on designated client machines. Administrators can perform modifications with the Windows-based console on the administrator server. These modifications appear in all web console sessions.

Verifying a successful installation

After installing ScanMail, run a test virus to verify if ScanMail properly installed the scan engine. You can use a harmless "fake" virus developed by the European Institute for Anti Virus Research (EICAR) for this purpose.

Download a copy of the EICAR test file from the Trend Micro website at http://www.trendmicro.com/en/security/test/overview.htm

To make your own test file:

1. Create a file using any text editor; use the following as the content of the file:

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

2. Save the file as Eicar.com

For either option, the mere downloading or creation of the file is enough to trigger Real-time scanning.

Removing ScanMail

Uninstallation removes all components from the selected server(s) — the ScanMail Management Console, ScanMail Web Console, and ScanMail Core Module.

Note: Do not manually uninstall ScanMail. There are many registry entries that the uninstall program automatically removes. Uninstall ScanMail from the Windows Control Panel or the Uninstall program, as described below.

ScanMail's uninstall program removes all program files, and program folders, items, directories, and entries made to the registry. Make sure that you logon using a Windows Administrator account.

Removing ScanMail Using the Windows Control Panel

To remove ScanMail:

1. On the ScanMail server, go to Start > Settings > Control Panel.
2. Click Add/Remove Programs.
3. Select Trend Micro ScanMail for Microsoft Exchange.
4. Click OK when prompted whether you are sure. The ScanMail services stop and the Operating System removes ScanMail.

Removing ScanMail using the Trend Micro Small and Medium Business Solution CD or the Uninstall.exe program

1. If you have the installation CD, run the uninstall program Uninstall.exe located in the \Programs\[product name] directory.

   -or-

   If you downloaded ScanMail for Microsoft Exchange from the Trend Micro Web site, run uninstall.exe to uninstall ScanMail.
2. The Uninstallation screen appears.
3. Click Next. The Select Target Servers screen appears.
4. From the list in the left pane, select the server(s) you want to remove ScanMail from either by highlighting the target server names individually or by highlighting the Domain name to uninstall ScanMail from all servers in a Domain. Double-click a Domain name if you want to view the servers within.
5. Click Add. The selected server(s) appear in the Server name list at the right. If you are uninstalling ScanMail from selected servers within the Domain only, repeat this process until you have added all the servers you want.

6. To remove server(s) from the Server name list, select them and then click Remove or Remove All.
7. Click Next to continue. The Server Logon screen appears.
8. In the User name text box, type the account to log on to the displayed server.
9. In the Password text box, type the password for the specified administrator account.
10. Click Logon to log on the server(s). Setup checks whether or not ScanMail is installed on each server and then displays the results on the next screen.
11. For servers that require different logon credentials, Setup displays the Server Logon screen again.
12. After the logon process, Setup displays the Analyze Selected Server(s) screen. Click Next to continue, then Next on the following screen to start removing the program from the selected servers.
13. On the next two screens, click Next and Finish to complete the uninstallation process. Uninstall automatically updates the Web-based remote server list to remove the corresponding entries for these servers.

Chapter 10

The eManager and ScanMail consoles

This chapter outlines the eManager Web-console features, and describes the differences between the Web-based and Windows-based eManager and ScanMail consoles.

There are a number of ways to manage both ScanMail and ScanMail eManager, including:

- **ScanMail for Exchange Web console**: The Client Server Messaging Suite allows you to perform most major ScanMail and eManager functions from the Web-based console. Trend Micro designed ScanMail so you can use the Web-based console on any computer on the network with a compatible browser.
- **ScanMail for Exchange Windows-based management consol**e: The ScanMail Windows-based management console is a windows-based application for managing ScanMail. When you install ScanMail, the management console automatically installs on the Exchange server. Features available on the management console are virtually the same as those available on the Web console.
- **ScanMail eManager Windows-based management console**: The eManager management console is automatically installed on the Exchange server when you install ScanMail. Several features are only available via the Windows-based eManager console. This chapter describes features available through the ScanMail Web console. Refer to *Content Management with Trend Micro™*

ScanMail™ eManager Windows-based Console starting on page 16-1 for information on the eManager management console.

ScanMail saves all settings you specify in a common configuration file kept on the Microsoft Exchange server. When you use the Windows-based consoles to configure options, configurations in the Web-based consoles update automatically when you log in.

The topics discussed in this chapter include:

- Managing the eManager Web-based console
- Understanding differences between the eManager Windows-based and Web-based consoles
- Understanding differences between the ScanMail Windows-based and Web-based consoles

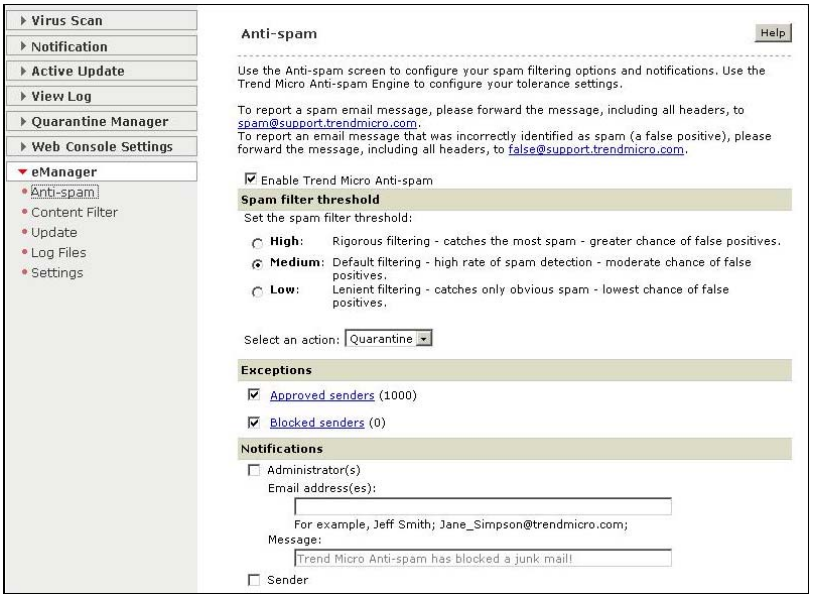

FIGURE 10-1. The ScanMail/eManager Web-based console

Managing the eManager Web-based console

The following sections describe how to perform various tasks on the eManager Web-based console screens.

Anti-spam

Use the Anti-spam screen to configure the following options for your Anti-spam settings. These settings define the detection level eManager uses to filter for unwanted email.

To configure Anti-spam

1. Select Enable Trend Micro Anti-spam to further define the strength eManager uses to detect spam. Select one of these options for your anti-spam mail filter level:
   - High: This is the most rigorous level of spam detection. eManager monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those emails that eManager filters as spam when they are actually legitimate emails.
   - Medium: This is the default setting. eManager monitors at a high level of spam detection with a moderate chance of filtering false positives.
   - Low: This is most lenient level of spam detection. eManager will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.
2. In Select an action, select the action to take when a message meets one of the rules - Delete, Quarantine, or Archive
3. Choose from the following:
   - **Approved Senders**: To enable, select the check box beside Approved Senders. Clicking on the Approved Senders link opens the Approved Senders window. You can use the window to add or remove the addresses/domains of approved senders. Type the email addresses/domains that you want eManager to exempt from blocking and then click Add or click an address/domains from the list and click Remove.
   - **Blocked Senders**: To enable select the check box beside Blocked Senders. Clicking on the Blocked Senders link opens the Blocked Senders window. You can use the window to add or remove the addresses/domains of blocked

senders. Type the email addresses/domains that you want eManager to block and then click Add or click an address/domain from the list and click Remove.

4. In the Notifications section, set notifications to the administrator(s), sender, or recipient(s) when email meets a rule you have defined
5. Select any or all of the following:
   - Administrator(s) - specify the Administrator(s) email addresses in the email addresses text box

     Separate multiple email addresses with semi-colons. Then specify the message text to send, for example,

     "Spam filter has blocked junk mail!"
   - Sender - specify the message text to send
   - Recipient(s) - specify the message text to send

Content Filter

The Content Filter screen provides a means for the administrator to evaluate and control email based on the message text. The content filter can also serve as a more powerful version of Anti-spam — checking inbound and outbound messages for the existence of key words or phrases.

ScanMail eManager comes pre-configured with a list of content filter policies.

- Anti-spam
- Profanity
- Racial Discrimination
- Sexual Discrimination
- Hoaxes
- Chain Mail
- Block HTML script messages

Note: You can only manage the creation or configuration of Content Filter policies from the Windows-based eManager console.

Default Separators

Default separators enable eManager to filter for specific wording. A default separator is comma, or white space that works with keywords specified in content filter rules. When eManager finds a keyword, together with the default separator in a message, eManager performs the user-specified action on the message.

Update Screen

Use the Update screen to schedule the frequency of file updates to your system. Anti-spam uses the file and contains numerous predefined anti-spam rule-sets. The content filter uses Import files and can augment existing policies.

The following information is available in the Information section of the Update screen:

- **Last imported Anti-spam policy:** Used by the content filter, represents the current import file version
- **Last Trend Micro Anti-spam engine**: Used by Anti-spam, represents the current Trend Micro Anti-spam engine version
- **Last Anti-spam rule file:** Used Anti-spam, represents the current rule file version

To schedule automatic update:

1. Click eManager > Update. The Update page appears.
2. Under Scheduled Update section, select Enable automatic update. This enables the Frequency and Start time options.
   a. Select the Frequency:
      - Choose **Update daily** to schedule ScanMail to automatically update the files every day
      - Choose **Update weekly** to schedule ScanMail to automatically update the files every week. Select the day of the week to perform the updates
      - Choose **Update monthly** to schedule ScanMail to automatically update the files every month. Select the day of the month to perform the updates.
   b. Specify the exact time (hour and AM/PM) in Start time

3. Under Proxy Settings, select Use an HTTP proxy server for update to use a proxy server to download updates from the Internet.
4. Type the IP address and port number of your HTTP proxy server. Specify the appropriate proxy authentication (user name and password) if required.
5. Click Apply to save your settings.

Log Files

Use the Log Files screen to view eManager log files.

To view eManager log files:

1. Click eManager > Log Files. The Log Query page appears.
2. In the Display logs for: section, select the log dates you want to view:
   - Select All dates to view the log files for all the dates
   - Select One month to view the log files generated over the past 30 days
   - Select One week to view the log files generated over the past seven days
   - Select Today to view the log file generated since midnight of the current day
   - Select Specified range to view a range of dates, and specify the start and end dates for the log files
3. In the Log type: list, select how you want to view log files in the system. Select whether to view All log files, or select a specific policy to view only the log files that relate to that policy.
4. Type the number of logs that ScanMail will display per page in Results per page.
5. Click View. eManager displays all logs that fit the criteria you specified in the Logs Files page.

Settings

Use the Settings screen to configure other eManager basic settings using the ScanMail Web console. These settings enable further configuration of log maintenance, content filtering, and quarantine, and archive options.

To configure other basic settings for eManager:

1. Click eManager > Settings. The Settings page appears.

2. Under Log Maintenance, select Automatically delete log files and specify number of days.
3. Under Content Filter Global Policy Settings, select any or all of the following:
   - Select Use exact matches only to help prevent eManager from generalizing and refining its searches. A match is valid only when the total number and order of letters in the two words eManager is comparing, are the same
   - Select Case-sensitive comparison so eManager can consider capitalization for the keyword list(s) of all active policies
   - Select Enable scanning the attached file content to evaluate the text in attachments for content violations in addition to the message subject and body text
4. Under Quarantine and Archive Directory Options, set the quarantine and archive directory locations. The default settings are:
   - Quarantine directory:

     c:\Program Files\Trend\SMCF\Quarantine
   - Archive directory:

     c:\Program Files\Trend\SMCF\Archive
5. Click Apply to save your settings.

Understanding differences between the eManager Windows-based and Web-based consoles

The information below shows the differences between the eManager Windows-based and Web-based consoles

The Windows-based management console provides the following features:

- Anti-spam: create Anti-spam/User Defined rule and Trend Micro Anti-spam
- Content Filter: set Content Filter, Add/Edit/Delete content filter rule
- Update: run Update and set schedule update
- Quarantine: set quarantine and archive location
- Log Files: view and delete log files

The Web-based management console provides the following features:

- Anti-spam: set Trend Micro Anti-spam on or off
- Content Filter: view Content Filter rule
- Update: set scheduled update on/off
- Log Files : view logs
- Settings: set global policy and quarantine/archive location

Note: Quarantine options are the same for both consoles, but the location of the Quarantine options is different; on the Web console, it is located in Settings.

Chapter 11

Introducing Trend Micro ScanMail™ for Microsoft™ Exchange

Trend Micro™ ScanMail™ for Microsoft® Exchange (ScanMail 5.5 or ScanMail 2002 and 2003) stops the spread and acquisition of known and newly detected computer viruses. By combining our award-winning, multi-threading scan engine with the latest macro virus detection technology, Trend Micro MacroTrap™, Trend Micro ScanMail's virus detection rate is one of the most comprehensive in the antivirus industry. ScanMail's scan engine is crucial in a Groupware environment where hundreds of users utilize shared information.

ScanMail protects Microsoft Exchange users from computer viruses in messages and their attachments and documents that are accessed from the Microsoft Exchange shared Information Store databases. Virus scanning is performed in memory, which significantly increases the scanning speed. ScanMail offers flexible, scalable configuration and remote management through the Windows-based ScanMail Management Console, as well as the Web consoles.

Trend Micro ScanMail eManager™ is a plug-in product. It automatically installs when you install ScanMail. ScanMail eManager rejects spam mail for corporate LAN users, and provides a content filter that allows you to check messages for content deemed to be offensive or objectionable.

In this chapter, you will find information about:

- How ScanMail cleans viruses and helps maintain a virus-free environment
- ScanMail's benefits and capabilities
- Management options
- New ScanMail features
- ScanMail eManager

ScanMail for Microsoft Exchange Versions

Trend Micro™ ScanMail™ for Microsoft Exchange contains many new features and tools to make administration of your ScanMail server easier and more comprehensive.

Note: Use the version of the ScanMail Management Console that corresponds with your server version. For example, use 3.52 to manage 3.52 servers, 3.8 to manage 3.8 servers, and 3.81 to manage 3.81 servers.

ESE Version for ScanMail 5.5 users

The most significant enhancement in the ESE version is support for a new scanning API (Application Programming Interface) that enables earlier virus detection and elimination. The new API is called Extensible Storage Engine API (ESE API) and is used in real-time, manual, and scheduled scanning. ESE also supports IMC scanning.

ScanMail for Microsoft Exchange 2000 and 2003 Technology

Microsoft Exchange 2000 or 2003 is not limited to messaging; rather, it is a complete messaging and collaboration platform for business. Exchange 2003 includes advancements in reliability, performance, and openness of Web technology to help businesses effectively use and share information. The new Web store technology built into Microsoft Exchange 2003 enables organizations to store and access email, documents, Web content, and applications from one location.

ScanMail supports Microsoft Exchange 2000 Service Pack 1 (SP1), as well as Microsoft Exchange 2003, which contains the Virus Scanning Application

Programming Interface (VS API) 2.5 that is implemented at a low-level in the Microsoft Exchange store. Microsoft Virus Scan API 2.5 enables early virus detection and elimination; Trend Micro refers to this ScanMail real-time scanning technology as "VS API" in this manual.

ScanMail also includes support for Microsoft® Windows® 2000 Service Pack 2, Service Pack 3, and Service Pack 4. Microsoft Windows 2000 Service Pack 2 and Service Pack 3 are not required for ScanMail but include features that make your system more secure and stable.

ScanMail uses Microsoft Collaboration Objects (CDOs) to send notifications to the ScanMail administrator, senders, and recipients. CDO does not represent a new messaging model, but rather an additional scripting interface to the Messaging Application Programming Interface (MAPI) model used in Microsoft Exchange.

ScanMail provides complete protection for the EDB (Exchange Database) and STM (Exchange Streaming Database).

How viruses spread in a Microsoft 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 virus infections will thrive and persist.

With the capabilities of Microsoft Exchange 2003, there is a greater risk of virus infections and other malicious code entering the Information Store. ScanMail offers improved scalability and tight integration with Windows 2000 and 2003 servers. Figure 11-1 below shows how infected mail spreads in an unprotected enterprise.

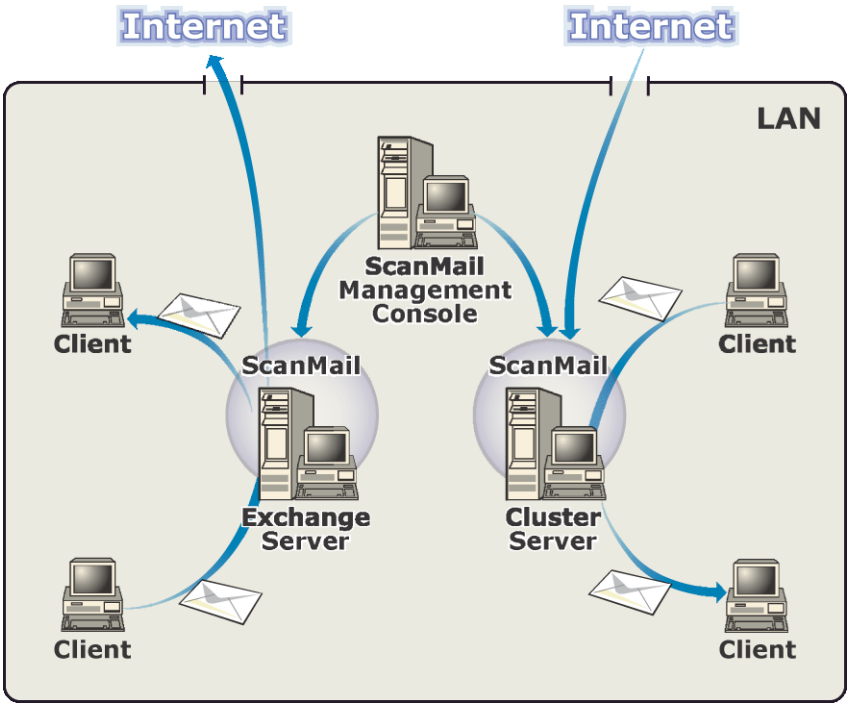

FIGURE 11-1. A Virus Spreading Through Information Sharing.

A virus in one email message spreads quickly through the Exchange network and beyond:

- A Microsoft Exchange user inadvertently attaches an infected Word file and emails it to several local users
- Microsoft Exchange Server 1 receives the message and copies it to the recipients' mailboxes
- A recipient posts the infected attachment to the public folder. Another recipient forwards it to an external user through the Internet. A routine replication of the public folders occurs. The infected document is now on Microsoft Exchange Server 2.
- Users of Microsoft Exchange Server 2 download the infected document

How ScanMail™ works

ScanMail guards all possible virus entry points with real-time scanning of all incoming messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. Once a complete manual or scheduled scan has run, this minimizes the chance of recurring infections from archived documents.

This is an overview of how ScanMail works:

1. The Information Store database verifies whether ScanMail is running as messages and attachments pass through.
2. ScanMail performs virus and malicious code scanning on messages and attachments passing through the system. Not running ScanMail leaves your system vulnerable to virus attacks.
3. After the scanning is complete, ScanMail passes the message and attachments back to the Information Store.
4. 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.

Benefits and capabilities

ScanMail provides many benefits and capabilities, including the following:

- **For ScanMail 5.5 users,** ScanMail now has IMC scanning. ScanMail typically scans messages and attachments at the Information Store level. With Internet Mail Connector (IMC) scanning, you can now also have inbound and outbound messages and attachments scanned at the IMC gateway level. The Scan Options window refers to the Information Store level as the “mailbox level”. By default, ScanMail scans inbound and outbound messages when IMC scanning is selected.
- **For ScanMail 5.5 users,** ScanMail Manual Scan, Scheduled, Real-time Scan, and IMC Scanning, all use ESE technology
- Uses pattern recognition and rule-based technologies to detect known and unknown (new and unidentified) viruses, including macro viruses
- Facilitates management through the Web-based Microsoft Exchange Server List for easy management

- Provides activity logs detailing system, virus, and program update events to keep you updated on ScanMail's latest operations
- Uses a multi-threaded in-memory scanning process for fast performance
- Scans UUENCODE, BINHEX, and MIME encoded attachments; scans a wide variety of compression types for greater ScanMail performance
- Streamlined interface combines manual, scheduled, and real-time scanning in one easy-to-use Virus Scan section; makes it easier to perform all your scans from one module
- Supports RAM Disk and Memory scanning – for fast virus scanning, does not generate a temp file. If the file is larger than a specified setting (3MB by default), a temporary file is generated
- ActiveSupport tool collects Trend Micro product settings and environment setup information (must be installed separately) for easy reinstallation
- Quarantine Manager allows easy viewing of quarantined email and attachments, and resending items that are determined to be safe; check Quarantine Manager for any files that you may not want to delete
- ScanMail offers many customizable scanning options, such as limiting the extracted file size for compressed file scanning and enabling message body scanning. Both virus scanning and attachment blocking support True file formats.
- ScanMail configuration changes take effect immediately, you do not need to shut down the Exchange server and restart it to change the scan options.
- ActiveUpdate of the virus pattern file and scan engine allows you to schedule updates monthly, weekly, daily, or even hourly.
- ScanMail Virus Scan notification options include mail, Simple Network Management Protocol (SNMP) and Windows Event Log. You can configure Outbreak Alert notifications for user-specified limits on numbers of viruses and/or uncleanable viruses within a time period. You can use pager notification for Outbreak Alert.
- ScanMail provides complete logging and reporting capabilities, such as the Scan Event Log, Virus Log, Update Log, Backup Log, Quarantine Log, and Attachment Blocking Log.
- The ScanMail Management Console (SMMC) is the Windows interface used to configure ScanMail. The ScanMail Debugger Console (SMDC) is part of the ScanMail Management Console and is located in the Tools menu. You can debug

the local server or remote servers individually from this screen. ScanMail Server Status Console (SMHB) is a tool that can be used to view the real-time ScanMail status, or "heartbeat" of remote servers from your local server.

- The Windows-based Real-time Scan Monitor includes the ScanMail Performance Monitor, where you can view a snapshot of your local server's performance.

Web console trusted IP zones

ScanMail facilitates management through the Web-based Microsoft Exchange Server List. The Remote Web Console allows you to configure ScanMail from locations that do not have the ScanMail Management Console installed. The "Trusted IP Zones" option allows access to the Web console from specific IP addresses. This adds an additional level of security to the existing administrator password security.

Trend Micro IntelliScan

IntelliScan scans attachments by an intelligent combination of true attachment type scanning and exact extension name filtering. This feature recognizes which files ScanMail can launch into memory and execute even if you change the file extension.

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. For example, ScanMail removes a virus with mass-mailing behavior immediately to prevent network traffic jams.

Typical virus types

Antivirus products evolved from simple DOS virus scanners to multi-platform products that scan for viruses, Trojans, worms, and joke programs. In fact, most of the files that are sent to Trend Micro from corporate customers are Trojans, such as SubSeven, and non-destructive joke programs, such as Flipped, Geschenk, and

Buttons. You can now select separate actions to take when the following types of viruses are found:

- Trojan Horses — a Trojan horse is a program that performs some unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or reformatting a disk. A Trojan horse does not infect other host files, so cleaning is not necessary
- Worms — a computer worm is a self-contained program (or set of programs) that spreads functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments
- Joke Programs — in many corporate environments, a simple joke program can cost as much as a real virus outbreak. This is because joke programs contain payloads and display messages that lead customers to believe that they are infected with an actual virus or Trojan
- Mass-Mailing Viruses — email-aware viruses that automatically spread through a company's messaging system can be expensive to clean up. You can save resources, reduce help desk calls from concerned employees, and eliminate post-outbreak cleanup work by choosing to automatically delete these virus types

Attachment blocking and Active Message filtering

ScanMail can block attachments with specified file names and/or true file extension types from delivery to your system. This feature provides a "Red Alert" Attachment Blocking capability that allows administrators to immediately quarantine or delete potentially destructive files, rather than implementing a complete system shutdown. With VS API technology, inbound and outbound attachments are blocked. You can delete the attachments or place them in the quarantine directory.

Note: For ScanMail 2000 and 2003 users, selecting this option on an Exchange 2003 mailbox server causes ScanMail to scan email twice, at the SMTP transport level, and by default at the mailbox level. Scanning emails twice can seriously degrade mailbox server performance.

Enabling ScanMail's **Active Message Filter** allows you to completely delete messages, rather than just replacing the attachment content. You can delete inbound

and/or outbound messages that meet the attachment blocking, eManager filtering, and/or virus scanning rules.

Information Store database selection

Microsoft Exchange 2003 allows multiple storage groups. In each of these groups, there can be multiple store databases. A typical storage group contains a Mailbox Store and a Public Folder Store. 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.

Quarantine Manager

Quarantine Manager lets the administrator easily view information on quarantined email and attachments. An administrator can determine an item suspect and not deliver it, or delete it individually. Alternatively, you can use the Quarantine Maintenance screen to delete all quarantined files or schedule regular quarantine file deletion.

In addition, when you examine a quarantined item, you may determine that it is actually safe to deliver. You can select and resend an item to the original intended recipient. For example, during a virus outbreak, you may have configured Attachment Blocking to block all attachments. Once the outbreak is over and you have downloaded the latest virus pattern file that detects the new virus threat, you can resend the attachments that were blocked to the original intended recipients.

To facilitate further investigation, quarantine areas are a way to store messages that have triggered filters. For more information, see*Using Quarantine Manager and ScanMail's Log Files* starting on page 15-1.

ScanMail eManager

Trend Micro ScanMail eManager works to reject spam mail bound to and from users of the corporate network. The Microsoft Exchange server does not process rejected spam mail and it does not end up in your clients' mailboxes. ScanMail eManager also supports content filtering.

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

Chapter 12

Configuring Real-time Scanning

For complete protection, Trend Micro recommends that you install one copy of Trend Micro ScanMail on each of your Microsoft Exchange servers. Regardless of which mail client program the sender was using, ScanMail real-time scan examines all messages and public-folder postings, and monitors all server-to-server replications. Trend Micro "IntelliScan" reduces system resource usage by examining all files on your system, but scanning only those types that have the potential to spread viruses. It examines attachments by using an intelligent combination of true attachment type scanning and exact extension name filtering.

Trend Micro "ActiveAction" performs a set of pre-configured, recommended scan actions on viruses and other types of malware. When ScanMail detects a virus, it takes the recommended action (clean, quarantine, delete) on the virus type to protect your environment's vulnerable points.

ScanMail offers file blocking. This “Red Alert” attachment-blocking feature is critical when blocking newly created viruses. To activate this feature, configure the file names and/or extension types to block, and ScanMail quarantines all inbound and outbound files matching your criteria.

The ScanMail Active Message Filter allows you to completely block inbound and/or outbound messages, rather than just the attachments. You can delete messages based on eManager rules, attachment blocking rules, and/or virus detection.

This chapter contains information on:

- Enabling and disabling real-time scanning
- Information Store database selection
- Configuring Real-time scan options
- Configuring the virus scan actions
- Selecting the file attachments to scan
- Configuring the Active Message Filter
- Configuring the virus detection actions
- Monitoring real-time scanning

About real-time scanning

Real-time scanning checks all incoming and outgoing mail for infected message body and attachments, and scans files posted on public folders and replicated from other servers. When ScanMail detects a virus in an attachment, it acts only on the infected file, not the message or other uninfected attached files. You can also configure ScanMail to scan the message body. If ScanMail detects a virus, you can specify one of the following actions: Clean, Quarantine, Delete, or Pass (Ignore).

ScanMail provides full scanning of all protocols passing message content and attachments (such as HTTP, SMTP, MAPI, POP3, IMAP4, IFS and WEBDAV) to the Web Storage Database. ScanMail also supports multi-threading and multi-processors.

ScanMail scans UUENCODE, BINHEX, and MIME encoded attachments and scans a wide variety of compression types. ScanMail recursively scans files containing up to 20 layers of compression; for example, a PKZIP file that has also been LZEXE and ARJ compressed.

You can configure ScanMail to automatically email designated people when it discovers a virus during a real-time scan. For example, the ScanMail administrator, the sender, and/or the recipients can be notified. Alternatively, you can send virus notifications to a Simple Network Management Protocol (SNMP) trap or the Windows Event Log.

Enabling/disabling real-time scanning

After installation, ScanMail automatically enables real-time scanning. ScanMail's real-time scanner starts automatically when the Microsoft Exchange 2000/2003 Information Store database service starts.

ScanMail monitors all email traffic passing to the Microsoft Exchange server. The program saves time and resources by checking mail that users address to multiple recipients only once. ScanMail cleans, deletes, or removes attachments before reaching the recipients.

To enable or disable real-time scanning for ScanMail 2000/2003 users:

1. In the left frame of the ScanMail configuration console, select **Virus Scan**.
2. Click **Options**.
3. Select the **Enable VS API virus scanning** check box to enable real-time scanning, or clear it to disable real-time scanning. VS API is still loaded, even though it is disabled. You cannot enable VS API if it is not loaded.
4. Select **Enable SMTP mail scanning** to scan messages and attachments before they leave the SMTP transport engine. By default, ScanMail scans all Information Store databases. This option is only available for Microsoft Exchange 2003. **This option is only available for Microsoft Exchange 2003**.

To enable or disable real-time scanning for ScanMail for Microsoft Exchange 5.5 users:

1. Select either the **Information Store Scan** or **Internet Mail Connector Scan** tab.
2. In the ScanMail configuration console, select **Real-time Scan**.
3. In the left frame, click **Options**.
4. Select the **Enable real-time scanning** check box to enable real-time scanning, or clear it to disable real-time scanning.

Implementation of the new status is immediate, so you do not need to stop or restart services. You can view the current scanning status in the Windows or Web management console's **Virus Scan > Status** screen.

You can also view the status in the Windows-based **Real-time Scan Monitor**. The **Real-time Scan Monitor** is usually open, but minimized at the bottom of your screen. If you need to re-open it, choose **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > Real-time Scan Monitor**.

Enabling/Disabling ScanMail eManager

ScanMail eManager works to filter out spam and other unwanted content from reaching your Microsoft Exchange server's mailboxes and public folders.

To enable ScanMail eManager, select the **Enable eManager** check box in the ScanMail Windows Console. For ScanMail enterprise version users, this option does not appear if you did not install ScanMail eManager.

Note: When enabled, the ScanMail eManager rules take effect during any current scans. See *Warning on enabling ScanMail eManager while performing manual or scheduled scans* starting on page 13-2 for more information.

Information Store database selection

In each storage group, there can be multiple information store databases. A typical storage group usually contains a Mailbox Store and a Public Folder Store. You can select your entire Microsoft Exchange tree or select individual store databases. For example, you may decide to scan the Public Folder Store on one storage group. If you are replicating the Public Folder Store to another server, you do not need to re-scan it on the second server.

WARNING! *ScanMail stops any ongoing manual or scheduled scans when you apply store database selection changes.*

To select the database stores you want to scan,go to **Virus Scan > Database Selection**. Select the store databases to scan and click Apply.

These selections apply to real-time scanning and future manual and scheduled scan tasks. In addition, these selections also apply to ScanMail eManager.

Configuring virus (real-time) scan options for ScanMail for Exchange 2000 and 2003

You can configure real-time scanning from the ScanMail Management Console or the Web consoles.

To configure virus scan options from the ScanMail Management Console:

1. Select **Virus Scan** > **Options**. The following figure displays the Virus Scan Options screen in the Windows console.

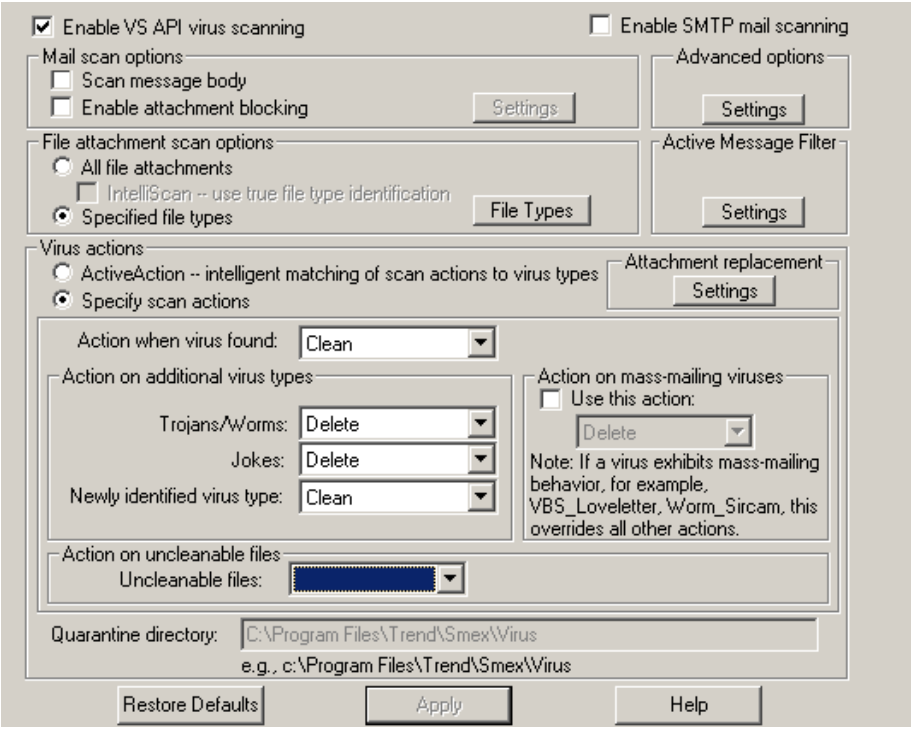

FIGURE 12-1. Virus Scan, Options screen

2. Select the **Enable VS API virus scanning**.

3. Select **Enable SMTP mail scanning** to scan messages and attachments before they leave the SMTP transport engine. By default, ScanMail scans all Information Store databases. **This option is only available for Microsoft Exchange 2003**.
4. If you want to go beyond scanning attachments for viruses and scan the message body for viruses as well, select **Scan message body**. Click **OK** when the warning message appears.

   Note: Scanning the message body can significantly increase scanning time.

5. During outbreak conditions or to conform to company policy, you can block specified attachments from entering or exiting your network by checking **Enable attachment blocking**. Click **OK** when the warning message appears telling you to disable attachment blocking when the outbreak is over. Click **Settings** to configure blocking of attachment types.

Configuring the Real-time Scan Options for ScanMail for Exchange 5.5

You can configure real-time scanning from the ScanMail Management Console or the Web consoles. The instructions do not differ significantly between the consoles. You can click **Copy Scan Options** to automatically transfer all scan options from the Internet Mail Connector Scan to the Information Store Scan screen, and vice versa.

To configure the scan options:

1. Choose **Real-time Scan** > **Options**. The Real Time Scan Options screen appears.

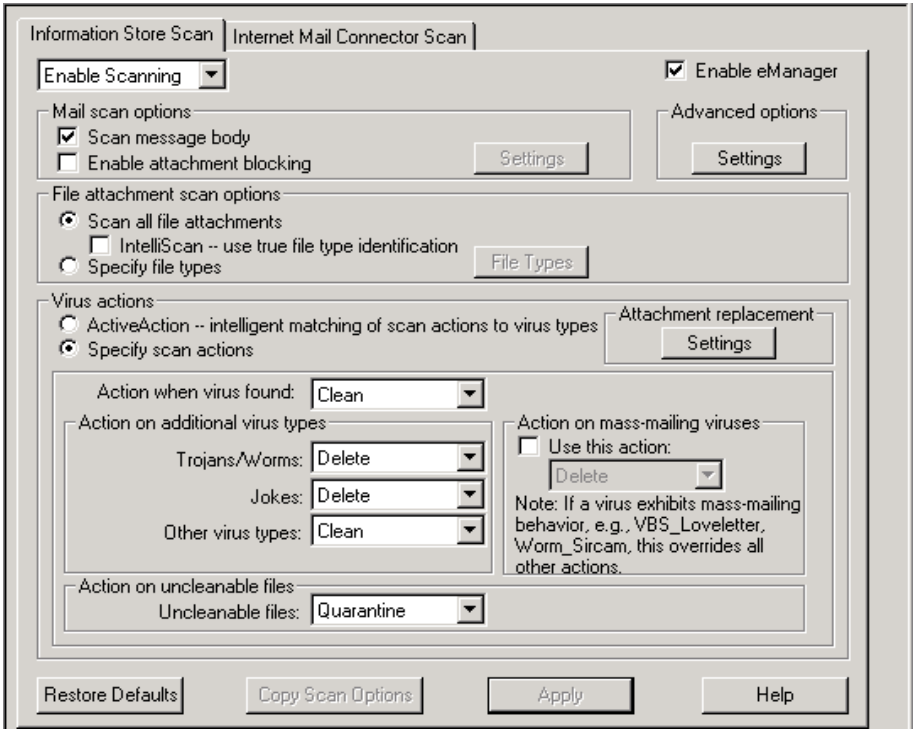

FIGURE 12-2. Real-time Scan, Options screen.

2. Select the **Enable real-time scan**.
3. Select the **Scan message body** if, in addition to scanning attachments, you also want to scan the message body.
4. Click **OK** when the warning message displays.

Note: Scanning the message body can significantly increase scanning time.

---

5. During outbreak conditions or to conform to company policy, select **Enable attachment blocking** to block specified attachments from entering or exiting

your network. A warning message advising you to disable attachment blocking when the outbreak is over displays.

6. Click **OK**, and then click **Settings** to configure which types of attachments to block.

Configuring the virus scan actions

ScanMail contains virus scan actions you can configure to further tailor scanning to your needs. Choose from the following actions:

- **Attachment blocking** block certain file attachments from delivery to your system
- **Advanced options** configure compressed file limits, MacroTrap™ heuristic settings, and whether to back up files before cleaning

Configuring attachment blocking

Attachment blocking prevents certain file attachments from delivery to your system. Specified file attachment types or file names are blocked and do not need to be scanned. This feature is most useful during a new virus outbreak to temporarily block all attachments with a particular file type or file name.

Note: For file attachment scanning and blocking, ScanMail scans all attachments with the same file type. For example, if a user saves Microsoft ® Word ® document with the .rtf extension, ScanMail still scans it. In addition, if a user saves a Word document with the .doc extension, but renames it to .bak, ScanMail still scans it.

Warning on "Red Alert" attachment blocking feature usage

You can either delete unwanted attachments using Active Message Filter or replace them with another file. For example, you can replace them with a note that tells the recipient that ScanMail has replaced the attachment. ScanMail can block attachments based on the attachment type and/or the attachment file name. Attachment blocking supports the wildcard characters"*" and "?".

WARNING! *Use the "Red Alert" Attachment Blocking feature with caution. If you have just installed ScanMail, DO NOT enable attachment blocking until ScanMail completes an initial manual scan or scheduled scan of the Information Store.*

If you enable blocking of all `.exe` files (and select Delete as the action) before all mailboxes have been scanned, it could have unintended results. When a manual or scheduled scan runs, ScanMail deletes all attachments with the .exe extension in the mailboxes and public folders you have selected.

You can delete or replace unwanted attachments by doing one of the following:

- Replace the blocked or uncleanable attachment with a user-specified file name and contents
- Completely block attachments using the Active Message Filter. See *Configuring the Active Message Filter for ScanMail for Exchange 2000 and 2003* starting on page 12-13, or *Using the Active Message Filter for ScanMail for Exchange 5.5* starting on page 12-14

To specify which files to block:

1. Select the file extension and/or full file names that you want to block. A record of blocked files is stored in the Attachment Blocking Log. Choose from the following two options:
   - **Block all attachments** is the most inclusive configuration. If you choose this, the ScanMail blocks all attachments regardless of the file extension.
   - To **Block specified attachments**, specify the file names, file extension names, and/or true file types to block:
     - **File extensions** blocks only specified extension names. Type the extensions you want blocked from delivery, separated by semicolons. ScanMail blocks attached files that match your specifications

     Note: Do not add a period in front of the extension. The wildcard characters "*" and "?" are supported when specifying the file name and file extension fields.

     - **File names** blocks attachments based on the full file name, including the extension. Type the file names you want blocked from delivery,

separated by semicolons. ScanMail blocks attachments that match your specifications

- **True file types** blocks attachments based on their true file type rather than the exact file name. Select from the **Available Types** list and then move the file types to scan to the **Selected Types** list

2. Under **Action on blocked attachments**, choose the option for the blocked files. As a safety measure, select **Quarantine to directory** to block the attachments from delivery and store them in another directory. The default directory is:

   ```
   C:\Program Files\Trend\Smex\Alert
   ```

3. Click **Settings** under **Blocked file replacement** to change the default file name and contents:

   a. Under **Replacement file name**, type a text or html name for the attachment once it has been removed. For example:

   ```
   File Blocked.rem
   ```

   ```
   File_Blocked.htm
   ```

   b. Under **Replacement file contents**, create a text or HTML message to replace the attachment contents.

4. Click **Apply** to save your settings.

Advanced options

Select Advanced options **Settings** to configure compressed file limits, MacroTrap™ heuristic settings, and whether to back up files before cleaning.

The following options are available:

- **Scan compressed attachments** — scans files that are compressed. ScanMail contains a default list of compressed file types to scan. You can select the number of layers of compression to scan by choosing the **Scan compression layer**. For example, if a file has been compressed and then recompressed, the scan compression layer for that file is 2.

  ScanMail must extract compressed files for scanning, which can consume a large amount of disk space. You can specify the **Maximum extracted file size** in megabytes.

- **MacroTrap** (**Heuristic scan**) — scans mail attachments for infected macros. Set the **Scan heuristic level** for the level of security you want. Level 1 uses the most specific criteria, but has the lowest detection rate. Level 4 has the highest detection rate, but uses the least specific criteria and may cause false alarms. Trend Micro recommends a heuristic scan level of 2. This level provides a high detection rate 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 false alarm rate.

- **Enable backing up files before taking action** — to save a copy of the file before cleaning the original file. The default directory is:

  ```
  C:\Program Files\Trend\Smex\Bkup
  ```

  Note: You can change the default backup directory in the Windows console; the Web console also uses this directory.

Selecting the file attachments to scan

You have two options when choosing file attachments to scan. These options further enhance ScanMail's ability to let user's select what file types to scan for infection, and what file types you want to allow as an administrator to enter your system without scanning. Remember that having relaxed file-scanning settings can leave your system vulnerable to malware attacks. Choose from:

- **IntelliScan** scans using true attachment type scanning and exact extension name filtering
- **Specifying the file types to scan** scans a selected subset of file types

Using Trend Micro IntelliScan

IntelliScan scans attachments by using an intelligent combination of true attachment type scanning and exact extension name filtering. This feature recognizes which files you can launch into memory and execute, even if you change the file extension.

In IntelliScan, all files are separated into two types:

- Content-oriented: The file is executed or loaded into memory by an application, which is determined by the file content
- Extension-name oriented: The file is executed or loaded into memory by an application, which is determined by the extension name

IntelliScan uses attachment extension name scanning for unknown application types; or known application types that the system launches by an exact extension name.

Under File attachment scan options, select from the following:

- **All file attachments** — the most secure configuration type. All attached files are scanned for viruses
- **All file attachments** with **IntelliScan** selected — all attached files are examined and those that are currently known to have the capability of harboring viruses are scanned
- **Specified file types** — select only certain attachments to scan

Specifying the file types to scan

Select this option to scan a subset of file types, for example, those most prevalent in your organization.

To specify the file types to scan:

1. Select **File Types** and choose the file types you want to scan. Select from the following two options:
   - **True file types to scan** — When you select the **Documents** and/or **Executables** check boxes ScanMail scans these file types. ScanMail scans other file types by extension name rather than true file type.
   - **File extensions to scan** — a default list of attachments is presented. To define new extensions to scan, type the extension in the new extension box and then click **Add**.
2. Click **OK** when you have made your selections.

Configuring the Active Message Filter for ScanMail for Exchange 2000 and 2003

Rather than delivering the message with the attachment content replaced, the Active Message Filter completely removes messages that:

- Contain attachments that meet the blocking rules
- Contain uncleanable infected attachments
- Meet the eManager rules

ScanMail deletes or quarantines the email as specified for the virus action.

Inbound and outbound mail can be treated separately. You can enable inbound message filtering, outbound message filtering, or both to remove the entire message when infected code is found in the message body or an attachment.

Select one or both of the following:

- **Inbound messages**
- **Outbound messages**

You can also specify which types of messages to exclude from filtering. For example, you can remove attachments that meet the eManager rules through ScanMail eManager, but may not want to remove the entire message. In this case, select the eManager filtering check box.

The options for exclusion from filtering are:

- **eManager filtering** – do not remove the entire email message when part of the email matches eManager rules; remove only the attachment(s) and/or message body that match the rules
- **Attachment blocking** – do not remove the entire email message when an attachment matches the blocking conditions; remove only the attachment(s) that match the specifications
- **Virus scanning** – do not remove the entire email message when part of the email contains a virus; remove only the infected attachment(s) or message body

Using the Active Message Filter for ScanMail for Exchange 5.5

Rather than delivering the message with replaced attachments, the Active Message Filter removes outbound messages that:

- Contain attachments that meet the blocking rules
- Contain uncleanable infected attachments
- Meet the eManager rules

The email is deleted or quarantined as specified for the virus action.

You can specify which types of messages to exclude from the filters. For example, you may decide to remove attachments that meet the eManager rules, but do not want to remove the entire message. Therefore you would select the eManager filtering checkbox. Under the **Outbound Mailbox Message Filter** group box, select filtering options for outbound messages. Under the **Internet Mail Connector Message Filter** group box, select filtering options on inbound and outbound email messages and attachments at the gateway level. The filtering options are:

- **eManager filtering** – do not remove the entire email message when part of the email matches eManager rules; remove only the attachment(s) and/or message body that match the rules
- **Attachment blocking** – do not remove the entire email message when an attachment matches the blocking conditions; remove only the attachment(s) that match the specifications
- **Virus scanning** – do not remove the entire email message when part of the email contains a virus; remove only the infected attachment(s) or message body

Changing the default embedded message deletion layer

Deleting infected messages using the Active Message Filter takes longer if it finds viruses deep in embedded messages. You can now configure how many layers ScanMail processes before it deletes infected messages.

To change the number of layers of embedded messages that ScanMail processes before deleting infected messages:

1. Click **Start > Run** and type `Regedit`.

WARNING! *Using Registry Editor incorrectly can cause serious problems that may require you to reinstall Windows. Microsoft cannot guarantee solving problems resulting from incorrect use of the Registry Editor. Use Registry Editor at your own risk. For information about how to edit the registry, view the "Changing Keys and Values" Help topic in Registry Editor (Regedit.exe) or the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe. Note that you should back up the registry before you edit it.*

2. Go to the following key to change the default embedded message layer:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
Exchange\RealTimeScan\DeleteMail\EmbeddedMsgLayer
```

By default, ScanMail sets the EmbeddedMsgLayer to layer 3. If a virus appears in layer 4 or above, ScanMail detects it and sends notifications, but does not delete the virus.

You can change the embedded layer value here and ScanMail automatically incorporates it in future scans.

Note: ScanMail does not delete uncleanable viruses found in deeper layers, but you can replace them with the text you specify in "Attachment Options".

Uncleanable viruses found in deeper layers are also not deleted, but can be replaced with the text you specify. See *Configuring the attachment replacement settings* starting on page 12-17 for more information.

Configuring the virus detection actions

The following settings enable ScanMail to perform the specified actions when it detects a virus. Configure ScanMail to perform actions automatically, or you can configure virus scan actions manually. Select from the following three actions:

- **ActiveAction** identifies virus types and automatically recommends actions based on how each type invades a computer system or environment
- **Specifying the scan actions** select the action ScanMail takes when a virus is found

- **Configuring the attachment replacement settings** specify the file name and message displayed when ScanMail cannot completely move or delete an infected attachment

Using Trend Micro ActiveAction

ActiveAction identifies virus types and recommends actions based on how each type invades a computer system or environment. ActiveAction categorizes viruses by malicious code, replication, and payload types. When ScanMail detects a virus, it takes the recommended action (clean, quarantine, delete) for the virus category to protect your environment's vulnerable points. For example, ScanMail removes a virus with mass-mailing behavior immediately to prevent network traffic jams.

Specifying the scan actions

In the **Virus Scan** > **Options** screen, you can select the action ScanMail takes when a virus is found.

1. Select **Clean** to automatically clean virus-infected files. The original email message text, any uninfected files, and the cleaned files are delivered to the intended recipient(s).
2. You can select different actions based on the following virus types:

   Trojans/Worms

   A Trojan horse is a program that performs unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files, or formatting a disk. A Trojan horse does not infect other host files, so cleaning is not necessary. To remove a Trojan, delete the program.

   A computer worm is a self-contained program (or set of programs) that spreads functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. To remove a worm, delete the program.

   Jokes

   Joke programs are ordinary executable programs. Trend Micro adds them to the detection list because they are annoying and/or they contain pornographic images. Joke programs cannot spread unless someone distributes them. To remove a Joke program, delete the file.

Other virus types

New virus types may be identified that would benefit from a different default scan action.

3. Due to the rapidity with which they spread, mass-mailing viruses are potentially more damaging than other viruses.
4. Select the **Action on mass-mailing virus** check box and choose the default action.This action takes precedence over any other virus action. For example, if ScanMail detects a virus as a Joke virus and a mass-mailing virus, it executes the mass-mailing action.
5. In the **Action on uncleanable files** section, select the action to take if ScanMail encounters an uncleanable file or cannot clean an infected file. The default is **Quarantine**, which moves the infected files to a specified quarantine directory.

What is the Mass Mailing Pattern?

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. Trend Micro publishes a list of these auto-spamming viruses in the "Mass Mailing Pattern". When such a virus is detected, you can specify an action that's different than the action when a conventional virus is detected. For example, you may want conventional viruses to be quarantined for later inspection, but mass-mailing viruses to be automatically deleted.

Configuring the attachment replacement settings

Click **Attachment Replacement Settings** to specify the file name and message displayed when ScanMail cannot completely move or delete an infected attachment.

1. Under **Replacement file name**, type a text or html name for the attachment once it has been removed. For example,

   ```
   VIRUS_REMOVED.rem
   ```

   ```
   VIRUS_REMOVED.htm
   ```

2. Under **Replacement file contents**, create a text or HTML message to replace the attachment contents.
3. Click **OK** to save your settings.

Specifying the quarantine directory

By default the location for the quarantine directory is:

```
c:\Program Files\Trend\Smex\Virus
```

The quarantine directory can be changed in the Windows or Web consoles. Files that are quarantined can be subsequently viewed, deleted, or resent using the Quarantine Manager.

Configuring virus scan options through the Web console

Select **Virus Scan > Options > Virus Scan** on the Web console to go to the Virus Scan screen. The Virus Scan screen is one of three screens on the Web console that are used to select the options used for real-time, manual, and scheduled scanning:

- **Attachment Blocking** — used to configure attachment blocking and attachment replacement settings. See *Configuring the virus scan actions* starting on page 12-8 for more details
- **Virus Scan** — used to configure the scan options, advanced scan options and virus actions. The options are described below
- **Active Message Filter** — used for removing email (the message and all attachments) that matches eManager filtering, Attachment blocking, or Virus scanning rules.

ScanMail uses the selected options to scan the Information Store databases you have selected (Mailbox store, Public Folder store) on your Microsoft Exchange server. You can change which store databases are scanned in the **Virus Scan > Database Selection** screen.

To configure the scan options on the Virus Scan screen:

1. Under **Select File Attachments to Scan**, select one of the following:
   - **All file attachments —** the most secure configuration type. ScanMail scans all attached files for viruses
   - **IntelliScan —** as an alternative to scanning all files, which can be time-consuming, IntelliScan checks all file types and scans those that have the capacity to contain viruses

- **Specify file types** — specify files to scan by true file format and/or file or extension name

To also scan the body of the message, select **Scan message body**.

Note: Scanning the message body can significantly increase scanning time.

2. Under **Virus Actions**, select one of the following:
   - **ActiveAction** — ActiveAction automatically performs recommended actions based on intelligent virus type/action combinations. If you select this option, you do not need to specify scan actions for different virus types and ScanMail grays these options.
   - **Specify scan actions** — when you select this option, you can configure different actions for different virus categories individually.
     - Regular viruses — the default action is to clean viruses and deliver the cleaned message to the recipient
     - Trojans/Worms — the default action is to simply delete these types of viruses and deliver the cleaned message to the recipient
     - Jokes — the default action is to delete Joke programs, which contain payloads and display messages that lead the recipient to believe they are infected with an actual virus or Trojan
     - Other virus types — used for new types of viruses as they are discovered
     - Mass-mailing viruses — these viruses spread rapidly, Delete is the default action. The action specified here overrides actions specified for any other viruses found in an email message
     - Uncleanable files — when ScanMail encounters an uncleanable virus, Quarantine is the default action
3. If you choose to quarantine infected files that are cleanable and/or the infected files that are uncleanable, specify the **Quarantine directory**. The default directory is:

   ```
   c:\Program Files\Trend\Smex\Virus
   ```

   Users can view, delete, or resend files that ScanMail quarantines using the Quarantine Manager. You can also view the number of quarantined files.

4. Click **Attachment replacement** to select the file name and message that appears when an infected attachment cannot be deleted or moved completely.
5. Under **Advanced Options**, you can configure the following options:
   - Scan options for compressed files
   - MacroTrap and the scan heuristic level to set
   - Whether to back up infected files before taking action

   See *Advanced options* starting on page 12-10 for more details.

Monitoring real-time scanning

Monitor instances of real-time scans using any of the following three options:

- **Virus Scan/Real-time Scan** shows the results of last real-time scan
- **Real-time Scan Monitor screen** displays the current real-time configuration and status of real-time scans
- **Performance Monitor** displays useful information on the aggregate number of virus detections and actions performed since starting the Real-time Scan Monitor service

Displaying the virus scan status for ScanMail for Microsoft Exchange 2000 and 2003

Select **Virus Scan** > **Status** to view the current real-time status:

- Real-time Scan has been running since [date and time]
- Default action taken when virus found
- Number of messages scanned
- Number of attachments infected
- Number of viruses found
- Number of viruses cleaned
- Number of uncleanable viruses
- Number of files moved to quarantine directory

The **Last Virus Found** group box displays the last virus detected by the real-time scanner, including the name, action taken, date, and time.

Note: On the Web console there is a **Messages Scanned** group box, which displays the results of the real-time scan processing. View this information in the Windows-based Real-time Scan Monitor.

Displaying the Real-time Scan Status for ScanMail for Microsoft Exchange 5.5

Select **Real-time Scan** > **Status** to view the current real-time status:

- Real-time Scan has been running since [date and time]
- Default action taken when virus found
- Number of messages scanned
- Number of attachments infected
- Number of viruses found
- Number of viruses cleaned
- Number of uncleanable viruses
- Number of files moved to quarantine directory

The **Last Virus Found** group box displays the last virus detected by the real-time scanner, including the name, action taken, date, and time.

Note: On the Web console there is a **Messages Scanned** group box, which displays the results of the real-time scan processing. This information can also be viewed in the Windows-based Real-time Scan Monitor.

Displaying the Real-time Scan Monitor for ScanMail for Exchange 2000 and 2003

To display the Real-time Scan Monitor screen, you must be physically located at the machine you are administering.

To display the Real-time Scan Monitor screen:

1. If the **Real-time Scan Monitor** is not already displayed on the Windows task bar, click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **Real-time Scan Monitor**.

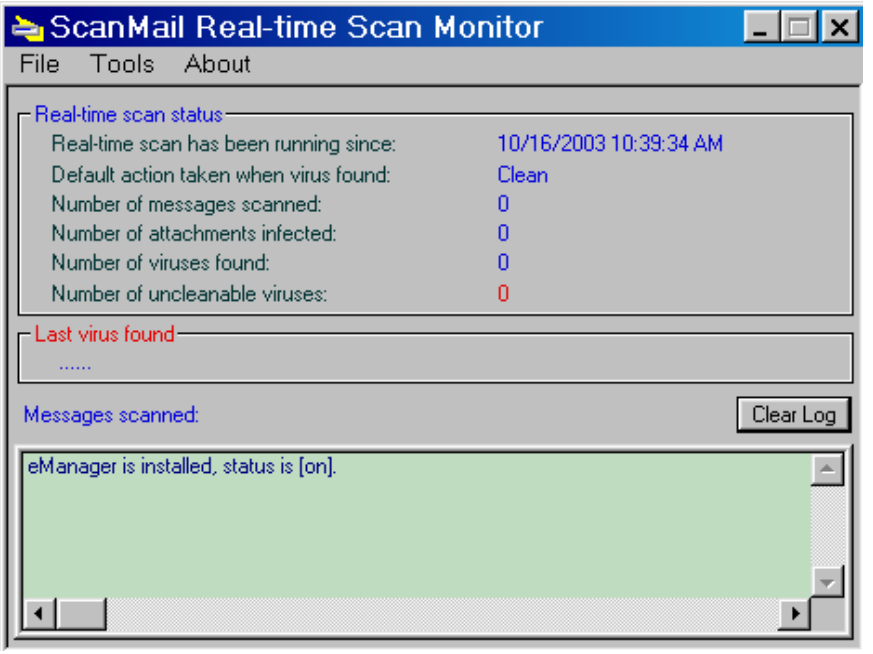

FIGURE 12-3. Real-time Scan Monitor after installation and a pattern download

2. The Real-time Scan Monitor screen displays the current real-time configuration and status. The **Real-time Scan Status** group box displays the current configuration and status of the real-time scanner.

   When real-time scan is enabled, this group box displays the same fields you see in the **Virus Scan > Status** screen, except that the number of viruses cleaned and quarantined is not displayed.

3. The **Messages Scanned** group box displays the results of the real-time, manual, and scheduled scan processes. Click **Clear Log** to clear the messages displayed in the **Messages Scanned** group box.

Displaying the Real-time Scan Monitor for ScanMail for Exchange 5.5

To display the Real-time Scan Monitor screen, you must be physically located at the machine you are administering.

To display the Real-time Scan Monitor screen:

1. If the **Real-time Scan Monitor** is not already displayed on the Windows task bar, click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **Real-time Scan Monitor**.

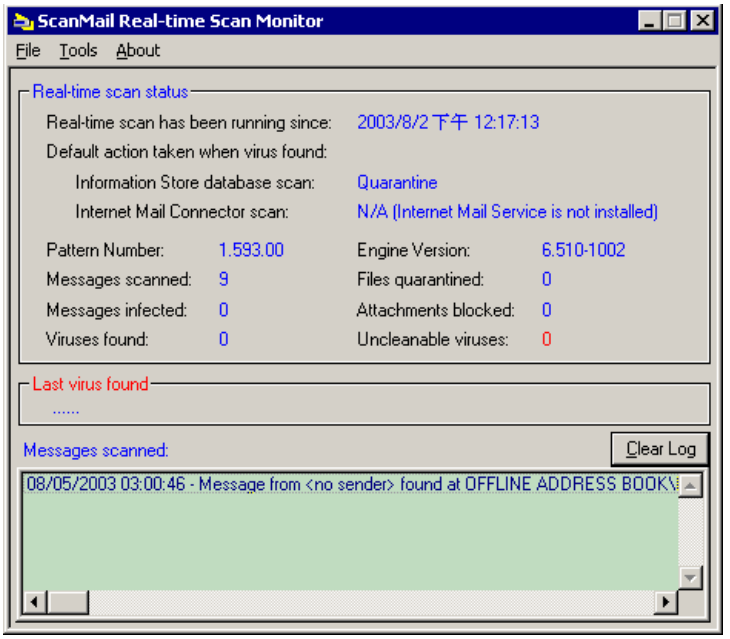

FIGURE 12-4. ScanMail Real-time Scan Monitor screen

2. The Real-time Scan Monitor screen displays the current real-time configuration and status. The **Real-time Scan Status** group box displays the current configuration and status of the real-time scanner.

When real-time scan is enabled, this group box displays the same fields you see in the **Real-time Scan > Status** screen, except that the number of viruses cleaned or quarantined is not displayed.

3. The **Messages Scanned** group box displays the results of the real-time, manual, and scheduled scan processes. To clear the messages displayed in the **Messages Scanned** group box, click **Clear Log**.

Displaying the ScanMail™ Performance Monitor

The ScanMail Performance Monitor displays useful information on the aggregate number of virus detections and actions performed since starting the Real-time Scan Monitor service.

To access the Performance Monitor graph:

1. Click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **Real-time Scan Monitor>Tools > Performance Monitor**.
2. Select **ScanMail**. An instance of the Performance Monitor is displayed below.

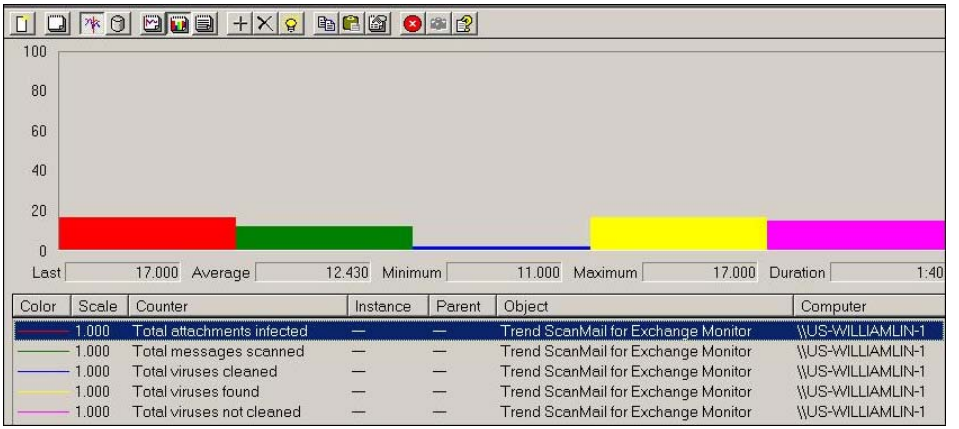

FIGURE 12-5. ScanMail Performance Monitor

The ScanMail Performance Monitor graph shows the following fields:

- Total attachments infected
- Total messages scanned

- Total viruses cleaned
- Total viruses found
- Total viruses not cleaned

Use this information to coordinate virus tracking.

Chapter 13

Configuring Manual and Scheduled Scans

Manual and scheduled scanning of the mailboxes and public folders on the Microsoft Exchange server is similar to traditional hard drive antivirus scanning. Traditional antivirus scanners, however, cannot recognize the Microsoft Exchange database format, and cannot scan files and documents in the Microsoft Exchange environment.

You can run a manual or scheduled scan to ensure that ScanMail scans all attachments once. Scanning the Information Store on the server minimizes the chance of recurring infections from archived documents.

After this initial scan, Trend Micro recommends that you configure ScanMail to automatically scan these locations. Setting regularly scheduled scans helps ensure a virus-free environment.

This chapter contains information on:

- Manual and scheduled scanning
- Setting scheduled scan tasks
- Selecting the Information Store databases to scan

Displaying manual and scheduled scan results

About manual and scheduled scans

When a manual or scheduled scan runs, the ScanMail checks whether there are new (or newly edited) message body contents or unscanned attachments and scans them. The scanner also checks whether your system has an up-to-date pattern file. If it the pattern file is new, the scanner automatically submits existing attachments in the folders that you specified to the scan queue. If there is a new pattern file and you configured ScanMail to scan the message body, it rescans the message body.

When ScanMail detects a virus in an attachment, it acts only on the infected file and leaves the message and any uninfected attachments alone. ScanMail also performs a scan of the message body. When ScanMail detects a virus, it takes the recommended action (clean, quarantine, delete) on the virus type to protect your environment's vulnerable points.

By going to **Notification > Virus Scan**, you can also configure ScanMail to send notification messages to specific people, such as the ScanMail administrator, the sender, and/or the recipients, when a virus is discovered during a scheduled scan. The notification messages contain details about the virus, including the delivery or posting time, name of the virus and the action taken. ScanMail gives you the option to append additional information to the default message (such as the Microsoft Exchange server), or to create a customized message of your own. Alternatively, you can send a virus notification to a Simple Network Management Protocol (SNMP) trap or the Windows Event Log.

You can select any or all of these notification methods. For more information on these notification methods, see *Configuring virus notification messages for ScanMail for Exchange 2000 and 2003* starting on page 14-2, or *Configuring virus notification messages for ScanMail for Exchange 2000 and 2003* starting on page 14-2.

Note: During manual and scheduled scanning, Trend Micro recommends that you disable attachment blocking to prevent the deletion of existing attachments.

Warning on enabling ScanMail eManager while performing manual or scheduled scans

If you install the optional ScanMail eManager plug-in module, the eManager rules and policies take effect after you enable real-time virus scanning. The same set of

eManager rules and policies apply to scanning the Information Store database regardless of the type of scan you are running. This means that when you run a manual scan or a scheduled scan, all real-time scan options currently in effect are used.

You can disable eManager when running a manual scan or scheduled scan to avoid having messages in the Information Store database filtered out. However, remember that this step also disables the real-time scanning eManager filter.

Configuring and running manual scans for ScanMail for Exchange 2000 and 2003

ScanMail scans email attachments, employing Trend Micro MacroTrap™ and its multi-threading, 32-bit scan engine to detect macro, polymorphic, file, boot sector, and other viruses.

ScanMail recursively scans files containing up to 20 layers of compression; for example, a PKZIP file that has also been LZEXE and ARJ compressed. ScanMail also extracts compressed attachments to the first level, scans them, and cleans any viruses that it finds.

You can run manual scans from the ScanMail Management Console or the Web consoles.

Running a manual “Scan Now”

To run a "Scan Now":

1. Select **Virus Scan > Options** to check the current scan options.

   Note: The scan options used for manual scanning are based on the current Virus Scan Options.

2. Select **Virus Scan > Database Selection** to view the databases that will be scanned. Choose the databases to include in your scan.

   Note: The databases scanned are based on the current Database Selection.

3. Select **Scan Tasks** in the left frame.
4. Click **Scan Now** and click **Yes** to continue.

Configuring and Running Manual Scans for ScanMail for Exchange 5.5

ScanMail scans email attachments, employing Trend Micro's MacroTrap™ and its multi-threading, 32-bit scan engine to detect macro, polymorphic, file, boot sector, and other viruses.

ScanMail recursively scans files containing up to 20 layers of compression; for example, a PKZIP file that has also been LZEXE and ARJ compressed. ScanMail also unzips `.zip` attachments to the first level, scans them, and cleans any viruses that are found.

You can run manual scans from the ScanMail Management Console or the Web consoles. Unlike Windows-based management, which allows you to select the public folders to scan, Web-based scans run on all public folders included in the Public Folder List.

To run a manual scan from the ScanMail Management Console:

1. From the ScanMail Management Console, select **Manual Scan > Scan Now**.

   The Manual Scan screen displays the mailboxes and public folders that were detected on the Microsoft Exchange server during the last Mailbox and Public Folder List refresh.
2. To ensure that all mailboxes on the server are included in the above list, click **Refresh Folders**.

   Note: ScanMail only scans those mailboxes that are included in the Mailbox and Public Folder Lists.
3. Select **Enable eManager**. This option enables spam and content filtering.
4. Select the mailboxes and public folders you want to scan.
   a. Select the **Inbox**, **Outbox**, **Sent items**, **Deleted items** and/or **All other folders** check boxes.

b. Select to scan all public folders, or select individual root-level public folders to scan.

Note: On the Web console, you cannot select individual public folders to scan.

5. Select **Scan Options.** The Manual Scan Options screen appears. See *Configuring Real-time Scanning* starting on page 12-1 for more information on setting the scanning options.
6. If you want to use incremental scanning, do the following:
   a. Check **Enable Incremental scanning**.
   b. Under **Scan files updated since**, do one of the following:
      - Select **Last scan** to only scan files that have been modified since the last manual or scheduled scan.
      - Select **Date** to only scan files that have been modified since the date you specify.
   c. Click **OK**.
7. When you have finished making your selections, click **Scan Now**.

Displaying Manual Scan Results

ScanMail provides a Manual Scan Results screen in the Windows console for displaying information about the viruses that were detected during the last manual scan.

To view the results of the last manual scan:

1. From the Windows console, select **Manual Scan** > **Results.**
2. The following fields are displayed:
   - Time — Last performed Manual Scan, Elapsed time
   - Folders (Mailboxes and Public Folders) — Number of folders scanned, Number of folders infected
   - Messages — Number of messages scanned, Number of messages infected
   - Files — Number of infected files, Number of compressed files found, Number of infected files moved to quarantine directory

- Viruses — Number of viruses found, Number of viruses cleaned, Number of uncleanable viruses

Configuring scheduled scans for ScanMail for Exchange 2000 and 2003

When scheduling scans, you should consider the server workload, which is usually heaviest during business hours and lightest during non-business hours. Trend Micro recommends that you schedule scan tasks to run around midnight or during weekends. Do not schedule a scan when your company is doing file backups. By default, ScanMail disables scheduled scans. You need to enable this function and set a date and time to start the periodic scanning of selected mailboxes and public folders on the server.

You can configure scheduled scans from the ScanMail Management Console or the Web consoles.

Configuring scheduled scan options

ScanMail uses the same virus scan options for real-time scanning, manual scans, and scheduled scans. The scan options currently set take effect at the exact time that the manual or scheduled scan runs, because ScanMail detects all open files as real-time scanning events.

Configuring the Information Store databases to scan

ScanMail uses the same Information Store database selection for real-time, manual, and scheduled scanning. Select **Virus Scan > Database Selection** to make sure that the store databases you want to scan are included when the scan runs.

Configuring scheduled scans from the Windows console

To schedule scans from the Windows console:

1. Select **Virus Scan** > **Scan Tasks**.

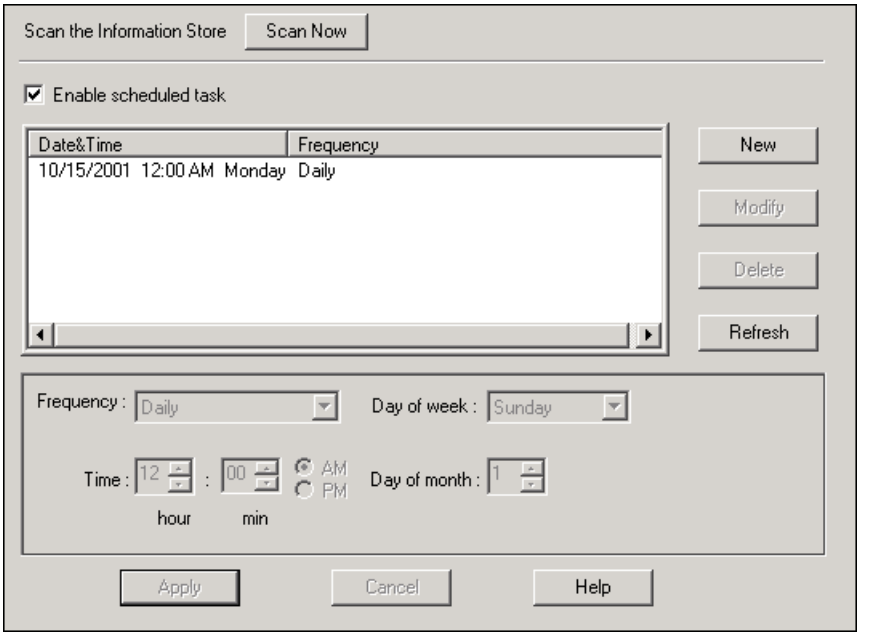

FIGURE 13-1. Virus Scan, Scan Tasks configuration screen

2. To enable scheduled scans, select the **Enable scheduled task** check box. To disable, clear this check box.

   The Scheduled Scan screen displays the current scheduled scans.

3. To add a new entry to the list (i.e., to schedule a new scan),

   a. Click **New**.

   b. Specify when the scan should occur using the **Frequency** and the **Time** drop-down list boxes. Depending on the frequency you select, you may need to select the **Day of week** or the **Day of month**.

   c. Click **Apply**.

4. The scan options are based on the current **Virus Scan Options**.

Configuring scheduled scans from the Web console

To configure a scheduled scan from the Web console:

1. Select **Virus Scan > Scan Tasks** to display the scheduled scan configuration screen.

FIGURE 13-2. Web console, Scheduled Jobs configuration screen

2. The list of scheduled tasks appears. To add a new entry to the list (i.e., to schedule a new scan):
   a. Click **Add**.
   b. Specify when the scan should occur using the **Time** drop-down list boxes and selecting the **Frequency**. Depending on the frequency you select, you may need to select the day of week or the day of month to perform the scan.
   c. Click the option button to enable the scan task and then click **Apply** to save your settings.

Note: The scan options used are based on the current **Virus Scan Options** at the time of the scan.

Configuring Scheduled Scans for ScanMail for Exchange 5.5

When scheduling scans, you should consider the server workload, which is usually heaviest during business hours and lightest during non-business hours. We recommend that you schedule the scan to run around midnight or during weekends. Do not schedule a scan when your company is doing file backups. By default, scheduled scans are disabled. You need to enable this function and set a date and time to start the periodic scanning of selected mailboxes and public folders on the server.

You can configure scheduled scans from the ScanMail Management Console or the Web consoles.

Configuring Scheduled Scans from the Windows Console

To schedule scans from the Windows console:

1. From the ScanMail Management Console, choose **Scheduled Scan**.
2. Select **Scheduled Jobs**.
3. To enable scheduled scans, select the **Enable scheduled task** check box. To disable, clear this check box.
4. If you have installed the ScanMail eManager plug-in, you can select the **Enable eManager** check box in the ScanMail Management Console. This option enables spam and content filtering.
5. The Scheduled Scan screen displays the current scheduled scans. To add a new entry to the list (i.e., to schedule a new scan), click **New**.
6. Click **Select Folders** to select the mailboxes and public folders you want to scan.
   a. Select the **Inbox**, **Outbox**, **Sent items**, **Deleted items** and/or **All other folders** check boxes.
   b. Select to scan all public folders, or select individual root-level public folders to scan.
7. Click **Scan Options** and the Scheduled Scan Options screen is displayed. See *Configuring Real-time Scanning* starting on page 12-1 for more information on setting the scanning options.
8. Click **Incremental Setting** if you want to use incremental scanning.

a. Select **Enable Incremental scanning**.

b. Under **Scan Files Updated Since**, choose one of the following:

- Select **Last scan** to scan only files that have been modified since the last manual or scheduled scan.
- Select **Date** to scan only files that have been modified since the date you specify.

9. Select the time for the Scheduled Scan:

a. Specify when the scan should occur using the **Frequency** and the **Time** drop-down list boxes. Depending on the frequency you select, you may need to select the **Day of week** or the **Day of month**.

b. Click **Apply**.

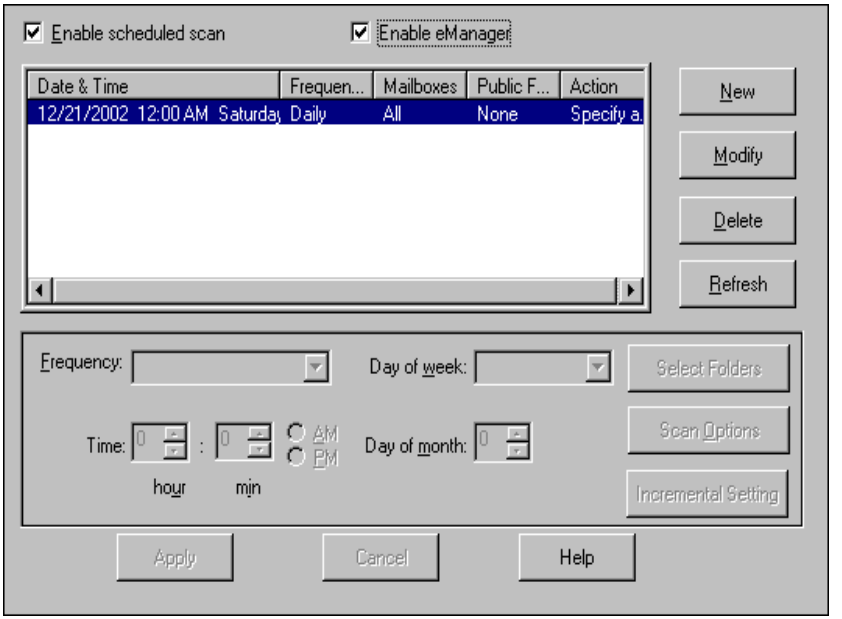

FIGURE 13-3. Scan Tasks configuration screen

Configuring Scheduled Scans from the Web Console

Unlike Windows-based management, which allows you to select the public folders to scan, Web-based scans run on all public folders included in the Public Folder List.

To configure a scheduled scan from the Web console:

1. Select **Scheduled Scan**.
2. Select **Scheduled Jobs** to display the scheduled scan configuration screen.
3. If you have installed the ScanMail eManager plug-in, you can select **Enable** to enable spam and content filtering.

FIGURE 13-4. Web console, Scheduled Jobs configuration screen

4. The list of scheduled tasks is displayed. To add a new entry to the list (i.e., to schedule a new scan), click **Add**.
5. Select the **Folders to Scan**:
   - **All mailboxes**
   - **All public folders**

Note: On the Windows console, you can select individual mailboxes and root-level public folders to scan.

6. Specify when the scan should occur using the **Time** drop-down list boxes and selecting the **Frequency**. Depending on the frequency you select, you may need to select the day of week or the day of month to perform the scan.
7. Set the scheduled scan options.See *Configuring Real-time Scanning* starting on page 12-1 for more information on setting the scanning options.
8. If you want to use incremental scanning, select **Enable Incremental scan**. Under **Scan files updated since**, choose one of the following:
   - Select **Last scan** to scan only files that have been modified since the last manual or scheduled scan.
   - Select **Date** to scan only files that have been modified since the date you specify.
9. Click the option button to enable the scan task and then click **Apply** to save your settings.

Displaying manual and scheduled scan results

You can view the results of each manual and scheduled scan by accessing the **Scan Event Log**. ScanMail logs all events into this log file, including events related to real-time scanning, scheduled scans, and manual scans. Entries include starting time, scan type, and virus action.

To access the Scan Event logs, select **View Logs** and click **Scan Event Log**. For more information about the Scan Event Log, see *ScanMail log files* starting on page 15-8.

Chapter 14

Configuring Notification Messages and ActiveUpdate

You can configure ScanMail to send a notification to users when it detects a virus in their email. The recipient of the notification can be any individual you designate in the configuration (for example, the system administrator or the sender or receiver of the bad email). Notification messages about viruses are fully customizable.

This chapter shows you how to configure notification messages using email, a Simple Network Management Protocol (SNMP) trap, and the Windows Event Log. SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite.

The Outbreak Alert feature allows you to notify administrator(s) when ScanMail finds an unusual number of viruses and/or uncleanable viruses in a user-defined period. The administrator or other designated individuals can receive Outbreak Alert notifications through email, SNMP, pager, or the Windows Event Log.

In ScanMail, you can update the pattern file and/or scan engine automatically from a convenient, easy-to-use ActiveUpdate configuration screen. You can update from the Internet or from another server on your network that has downloaded the update package.

This chapter contains information on:

- Configuring notification messages through the Windows and Web consoles

- Configuring unique Virus Scan, Outbreak Alert, and Attachment Blocking notifications
- Changing notification subject lines through the registry
- Configuring SNMP trap and Windows Event Log notifications
- Updating the pattern file and scan engine from the Trend Micro Web site or another server on your network

Configuring notification messages

In ScanMail, you can customize notification messages for the following categories:

- Virus Notification
- Outbreak Alert Notification
- Attachment Blocking Notification

Configuring virus notification messages for ScanMail for Exchange 2000 and 2003

When ScanMail detects a virus, it can alert designated people using email. The designated people might include the ScanMail administrator, the sender and/or the recipient(s) of the email containing the virus. Notification messages contain details about the virus, such as the name, the delivery or posting time, sender, recipient, subject, mailbox, and the action taken. ScanMail gives you the option to append additional ScanMail fields (such as the Microsoft Exchange server) to the default message or to create a customized message.

You can customize notification messages and send them through a SNMP trap. You can also automatically record Notifications in the Windows Event Log.

To configure virus scan notifications:

1. Select **Notification > Virus Scan**.
2. At the top of the screen, select the **Do not send notification when viruses have been cleaned** check box if you want ScanMail to send notifications only when it finds uncleanable viruses.
3. Select the check box(es) for the types of notification you prefer:
   - **Mail**

- **SNMP**
- **Windows Event Log**

You can select any or all of these notification methods.

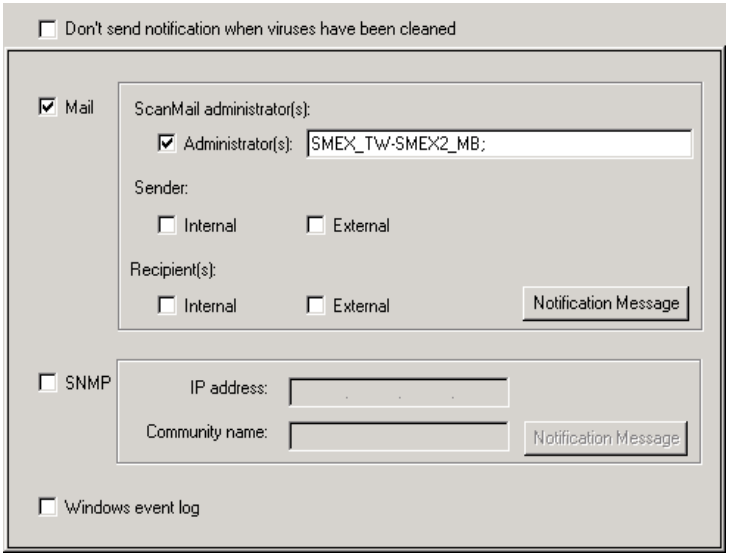

FIGURE 14-1. SMMC Virus Scan notification screen

4. Configure ScanMail to notify the Exchange administrator(s), the sender, and/or the recipient(s) by email when it finds infected files.

   a. Click **Notification Message** to customize the message text. You can edit the provided default messages to the administrator(s), sender, and/or recipient(s).

   b. In the scroll box on the left, you can add the following ScanMail generated fields to your message:

```
Administrator, Date, Exchange Server, File/Action, Recipient,
Sender, Subject, Time
```

5. Select **SNMP** to notify a particular SNMP trap server when ScanMail finds a virus. View the data with a Management Information Base (MIB) browser.

a. Specify the **IP address** host name or number of the SNMP trap server and the **Community name** (Public or Private).

b. Click **Notification Message** and edit the default text message.

c. You can insert the following ScanMail generated fields in the message:

```
Administrator, Date, Exchange Server, File/Action, Recipient,
Sender, Subject, Time
```

6. Select **Windows Event Log** if you want to have all virus events recorded in the standard Windows Event Log.
7. Click **Apply** to save the changes.

Configuring Virus Notification Messages for ScanMail for Exchange 5.5

When ScanMail detects a virus, it can alert designated people using email. The designated people might include the ScanMail administrator, the sender and/or the recipient(s) of the email containing the virus. Notification messages contain details about the virus, such as the name, the delivery or posting time, sender, recipient, subject, mailbox, and the action taken. ScanMail gives you the option to append additional ScanMail fields (such as the Microsoft Exchange server) to the default message or to create a customized message.

Customizable notification messages can be sent through a SNMP trap. Notifications can also be automatically recorded in the Windows Event Log.

To configure virus scan notifications:

1. Select **Notification**.
2. Select **Real-time Scan, Manual Scan,** or **Scheduled Scan**.
3. At the top of the screen, select the **Do not send notification when viruses have been cleaned** check box if you want ScanMail to send notifications only when it finds uncleanable viruses.
4. Select the check box(es) for the types of notification you prefer:
   - **Mail**
   - **SNMP**
   - **Windows Event Log**

You can select any or all of these notification methods.

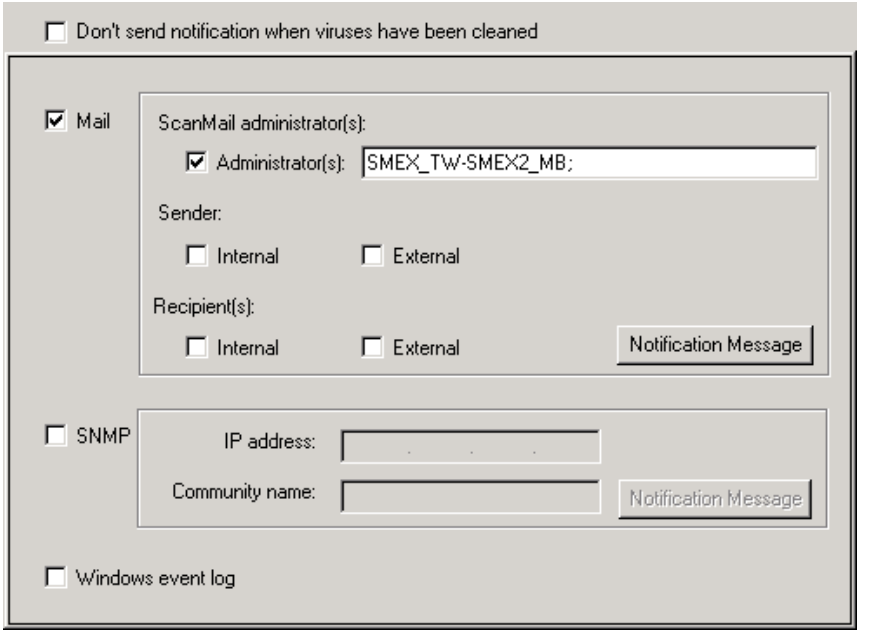

FIGURE 14-2. SMMC Real-time Scan Notification screen

5. Select **Mail** to notify the Exchange administrator(s) or other individuals who need to know when ScanMail finds infected files, or the sender or recipient(s).
   - Select **Internal** if the Sender/Recipient is inside of the organization. For ScanMail for Exchange 5.5 users, an internal recipient is any recipient object in the organization or site, such as the mailbox, or a distribution list.
   - Select **External** if the Sender/Recipient is outside of the organization.

   You can click **Notification Message** to edit the provided default messages to sender, recipient(s), and administrator(s). In the scroll box on the left of the Notification Message screen, you can choose to add ScanMail generated fields to your message.
6. Select **SNMP** to notify a particular SNMP trap server when a virus is found. You can view the data with a Management Information Base (MIB) browser.

a. Specify the **IP address** host name or number of the SNMP trap server and the **Community name** (Public or Private).

b. Click **Notification Message** and edit the default text message.

c. You can insert the following ScanMail generated fields in the message:

```
Administrator, Date, Exchange Server, File/Action, Recipient,
ScanType, Sender, Subject, Time
```

7. Select **Windows Event Log** if you want to have all virus events recorded in the standard Windows Event Log.
8. Click **Apply** to save the changes.

Configuring Outbreak Alert notification messages for ScanMail for Exchange 2000 and 2003

The Outbreak Alert feature allows you to notify administrator(s) when ScanMail finds an unusual number of viruses and/or uncleanable viruses in a user-defined period. The administrator or other designated individuals can receive Outbreak Alert notifications through email, SNMP, pager, or the Windows Event Log.

To configure outbreak alert notifications:

1. Select **Notification > Outbreak Alert**.
2. At the top of the screen, select the **When viruses found exceed** and/or **When uncleanable viruses found exceed** check box(es). Enter the number of viruses and time period in the appropriate fields. If the number of viruses exceed these parameters, it indicates an Outbreak. The default is 25 viruses (cleanable or uncleanable) in 24 hours.
3. Select the check box(es) for the type of notification you prefer:
   - **Mail**
   - **SNMP**
   - **Pager**
   - **Windows Event Log**

   You can select any or all of these notification methods.

.

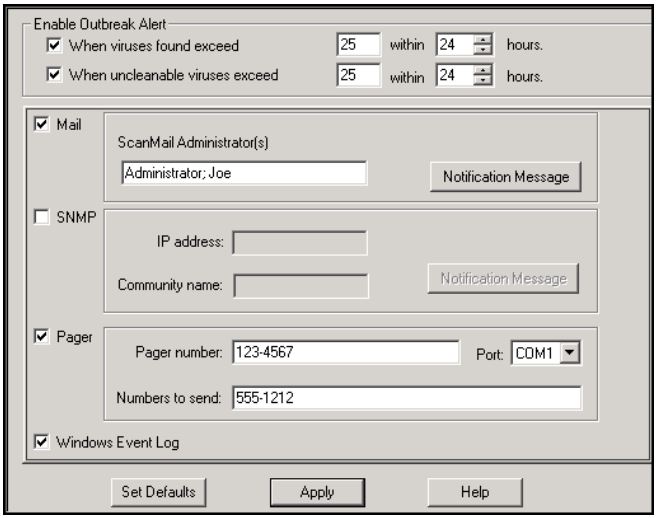

FIGURE 14-3. SMMC Outbreak Alert notification screen

4. Select **Mail** to notify the Exchange administrator(s), the sender, and/or the recipient(s) by email when ScanMail finds infected files. Click **Notification Message** to customize the notification message.

   Type the name of the **ScanMail administrator(s)** mailbox you want to receive the notification messages. If you include more than one administrator's mailbox, use a semicolon as the delimiter between mailbox names.

5. Select **SNMP** to notify a particular SNMP trap server when ScanMail finds a virus. View the data with a Management Information Base (MIB) browser.

6. Specify the **IP address** (name or number) of the SNMP trap server and the **Community name** (Public or Private). For example:

   ```
   IP address: 123.123.123.123
   Community name: Public
   ```

   Click **Notification Message** to customize the notification message.

7. Select **Pager** to have a selected individual paged when ScanMail finds a virus. Enter the **Pager number, Port,** and the **Numbers to send**, including the phone number and any additional codes.

8. Select **Windows Event Log** to record all virus events in the standard Windows Event Log.
9. Click **Apply** to save the changes.

Configuring Outbreak Alert Notification Messages for ScanMail for Exchange 5.5

You can configure Outbreak Alert messages to let the administrator(s) or other designated individuals know when a certain number of viruses and/or uncleanable viruses are found during a user-defined period. You can make Notifications through email, SNMP trap, pager, and/or the Windows Event Log.

To configure outbreak alert notifications:

1. Select **Notification > Outbreak Alert**.
2. At the top of the screen, select the **When viruses found exceed** and/or **When uncleanable viruses found exceed** check box(es). Enter the number of viruses and time period in the appropriate fields. If the number of viruses exceed these parameters, an Outbreak has occurred. The default is 25 viruses (cleanable or uncleanable) in 24 hours.
3. Select the check box(es) for the type of notification you prefer:
   - **Mail**
   - **SNMP**
   - **Pager**
   - **Windows Event Log**

   You can select any or all of these notification methods.

.

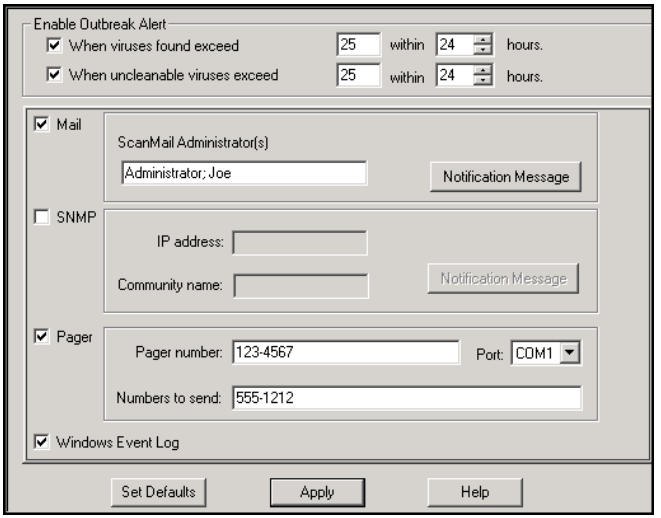

FIGURE 14-4. SMMC Outbreak Alert notification screen

4. Select **Mail** to notify the Exchange administrator(s) or other individuals who need to know when ScanMail finds infected files. Click **Notification Message** to customize the notification message.

   Type the name of the **ScanMail administrator(s)** mailbox you want to receive the notification messages. If you include more than one administrator's mailbox, use a semicolon as the delimiter between mailbox names.

5. Select **SNMP** to notify a particular SNMP trap server when ScanMail finds a virus. You can view the data with a Management Information Base (MIB) browser.

   Specify the **IP address** (name or number) of the SNMP trap server and the **Community name** (Public or Private). For example:

   ```
   IP address: 123.123.123.123
   Community name: Public
   ```

   Click **Notification Message** to customize the notification message.

6. Select **Pager** to page a selected individual when ScanMail finds a virus. Enter the **Pager number**, **Port,** and the **Numbers to send**, which includes the phone number and additional codes, such as "911".
7. Select **Windows Event Log** to record all virus events in the standard Windows Event Log.
8. Click **Apply** to save the changes.

Configuring attachment blocking notification messages for ScanMail for Exchange 2000 and 2003

Attachments can contain viruses. Once you know the name or file extension of an attachment containing a new virus, you can configure ScanMail to block all emails containing attachments of that name and/or extension type. You can also configure ScanMail to notify designated individuals when it blocks specified attachments. You can edit the default notification message and append additional ScanMail fields (such as the Microsoft Exchange server) to create a customized message.

You can send customizable notification messages through an SNMP trap. Alternatively, configure ScanMail to automatically record in the Windows Event Log.

To configure attachment blocking notifications:

1. Select **Notification > Attachment Blocking**.
2. Select the check box(es) for the type of notification you prefer:
   - **Mail**
   - **SNMP**
   - **Windows Event Log**

   You can select any or all of these notification methods. For more information on these notification methods, see *Configuring virus notification messages for ScanMail for Exchange 2000 and 2003* starting on page 14-2, or *Configuring Virus Notification Messages for ScanMail for Exchange 5.5* starting on page 14-4.

ScanMail deletes or moves the attachment contents as specified. However, although it replaces the attachment contents, the attachment icon remains in the original email. You can specify replacement text to notify the recipient that the attachment icon is harmless, see *Configuring the attachment replacement settings* starting on page 12-17

for more details. Alternatively, you can completely block attachments using the Active Message Filter, see *Configuring the Active Message Filter for ScanMail for Exchange 2000 and 2003* starting on page 12-13, or *Using the Active Message Filter for ScanMail for Exchange 5.5* starting on page 12-13.

Note: Disable the file attachment blocking once the virus outbreak is over. Choose **Virus Scan > Options** and clear the **Enable attachment blocking** check box.

See *Configuring the virus scan actions* starting on page 12-8 for more information on file attachment blocking.

Configuring Attachment Blocking Notification Messages for ScanMail for Exchange 5.5

Attachments can contain viruses. Once you know the name or file extension of an attachment containing a new virus, you can configure ScanMail to block all emails containing attachments of that name and/or extension type. You can also configure ScanMail to notify designated individuals when it blocks specified attachments. You can edit the default notification message and append additional ScanMail fields (such as the Microsoft Exchange server) to create a customized message.

ScanMail can send customizable notification messages through an SNMP trap. Notifications can also be automatically recorded in the Windows Event Log.

To configure attachment blocking notifications:

1. Select **Notification > Attachment Blocking**.
2. Select the check box(es) for the types of notification you prefer:
   - **Mail**
   - **SNMP**
   - **Windows Event Log**

   You can select any or all of these notification methods. For more information on these notification methods, see *Configuring virus notification messages for ScanMail for Exchange 2000 and 2003*, or *Configuring Virus Notification Messages for ScanMail for Exchange 5.5*.

ScanMail deletes or moves the attachment contents as specified. However, although it deletes the attachment contents, the attachment icon remains in the original email.

ScanMail deletes or moves the attachment contents as specified. However, although it replaces the attachment contents, the attachment icon remains in the original email. You can specify replacement text to notify the recipient that the attachment icon is harmless, see *Configuring the attachment replacement settings* starting on page 12-17 for more details. Alternatively, you can completely block attachments using the Active Message Filter, see *Configuring the Active Message Filter for ScanMail for Exchange 2000 and 2003* starting on page 12-13, or *Using the Active Message Filter for ScanMail for Exchange 5.5* starting on page 12-13.

Note: Be sure to disable the file attachment blocking once the virus outbreak is over. Choose **Virus Scan > Options** and clear the **Enable attachment blocking** check box.

See *Configuring the virus scan actions* starting on page 12-8 for more information on file attachment blocking.

Changing subject line notifications through the registry

ScanMail configures notifications for the message body through the management consoles, as described above. The subject lines of notification messages are preconfigured, but can be edited in the registry.

WARNING! *Before editing the registry, make sure you understand how to restore it if a problem occurs. For more information, view the "Restoring the Registry" Help topic in Regedit.exe or the "Restoring a Registry Key" Help topic in Regedt32.exe.*

Virus scanning notification subject lines

To modify the subject line of virus notification messages through the registry:

1. Go to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
Exchange\RealTimeScan\Notification\ByMail
```

2. Edit the subject line for the following keys:
   - CustSubA — administrator
   - CustSubR — recipient
   - CustSubS — sender

Attachment blocking notification subject lines

To modify the subject line of attachment blocking notification messages through the registry:

1. Go to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for
Exchange\AttachmentBlockingNotify\Notification\ByMail
```

2. Edit the subject line for the following keys:
   - CustSubA — administrator
   - CustSubR — recipient
   - CustSubS — sender

About ActiveUpdate technology

New virus pattern files are available at least weekly. If you have enabled automatic virus pattern file downloads, each time ScanMail runs a scheduled scan you are guarding against the latest types of viruses discovered.

New virus pattern files are available weekly or more often, so Trend Micro recommends scheduling daily automatic pattern file updates. New scan engine updates are available periodically, so Trend Micro recommends that you schedule regular scan engine updates also. Updates are available free for one year to registered users. Download updates automatically using the ScanMail's built-in "ActiveUpdate" technology.

By default, ScanMail disables the scheduled program update of ScanMail's pattern file and scan engine. Enable this function and set the schedule to have your copy of the virus pattern file and scan engine automatically updated.

Virus pattern file

ScanMail draws upon an extensive database of virus "signatures," commonly called the virus pattern file. ScanMail uses this file to detect viruses in email traffic, folder replications, and archived documents.

If a particularly damaging virus is discovered "in the wild", Trend Micro releases a new pattern file when there is a detection routine.

Scan Engine

ScanMail uses the virus scan engine to scan files and detect viruses. Trend Micro releases new engine versions for many reasons, including:

- New virus types that may not be detected by the old engine
- Enhanced scanning performance and detection rates
- Added support for virus detection to additional formats, such as the newest Microsoft® Word® or Microsoft® Excel® types
- Modified the scan engine to detect and remove malicious Java and ActiveX® code

Configuring pattern file and Scan Engine updates

As writers release new viruses, Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file. New virus pattern files are available at least every week, so Trend Micro recommends that you schedule frequent updates.

If there is a new virus outbreak, you can also perform a manual update to get the latest virus protection.

Configuring "Update Now"

Use the **Update Now** screen to update the ScanMail pattern file and/or scan engine. Use Update Now from the ScanMail Management Console or the Web consoles.

To configure "Update Now":

1. Select **Active Update** > **Update Now** to display the **Update Now** screen.
2. The current pattern file, scan engine, and program (SMMC, ScanMail core module, and Web program files) versions appear at the top of the screen.
3. In the Update Components section, select the check box(es) for the type of update you want to perform:
   - **Pattern file**
   - **Scan engine**

   .

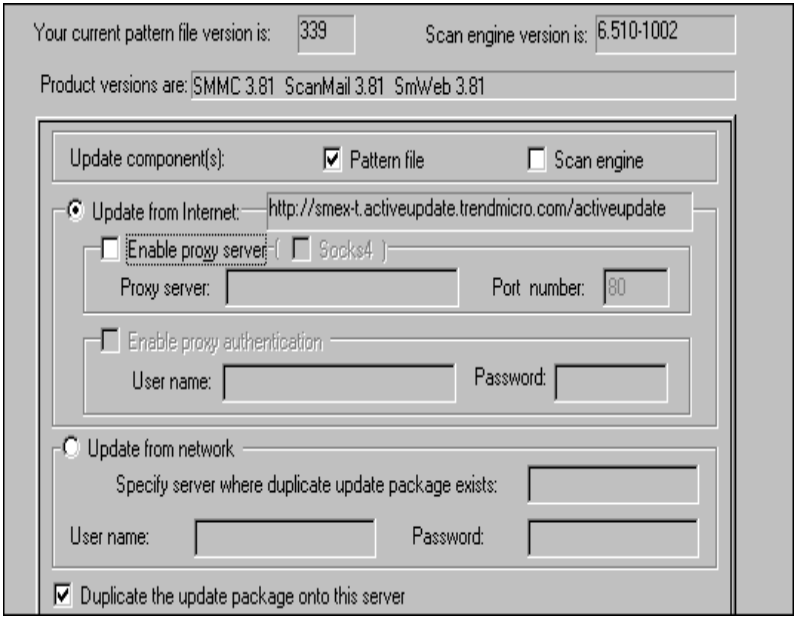

FIGURE 14-5. SMMC Update Now screen

4. Select the location from which you want to download the new updates:
   a. If this is your only ScanMail server, select **Update from Internet** to download the latest updates from the Trend Micro Web site.

b. If you use a proxy server to access the Internet, select the **Enable proxy server** check box, and type the **Proxy server** IP host name or number, and the **Port number**.

c. If your proxy server uses the Socks 4 protocol, select the **Socks4** check box.

d. If your proxy server requires proxy authentication, select the **Enable proxy authentication** check box and type the **User name** and **Password** used to access it.

e. Select **Update from Network** to download the updates from an update package on another ScanMail server on your network.

f. In the **Specify server where duplicate update package exists** text box, type the server name from which you want to download the updates and enter the **User name** and **Password** to access the updates.

Note: The server you are updating from must already have a copy of the update package downloaded from the Internet, or from another ScanMail server.

5. Select **Duplicate the update package onto this server** to keep a copy of the update package on the server. This option makes a complete copy of the pattern file and scan engine download package. Other servers can then connect to this server using **Update from Network** to receive updates.

Note: If you have several ScanMail servers, Trend Micro recommends that you select this option for one central server. Then configure your other servers to update from this server, which decreases Internet traffic.

6. Click **Update Now** to update the program files. ScanMail logs the event into the Update Logs.

Configuring scheduled updates

Schedule ScanMail to automatically download the latest program file updates from Trend Micro or from another server on your network. Configuration is similar whether you use the ScanMail Management Console or the Web consoles.

To configure a scheduled update:

1. Select **ActiveUpdate** > **Scheduled Update** to display the **Scheduled Update** screen.

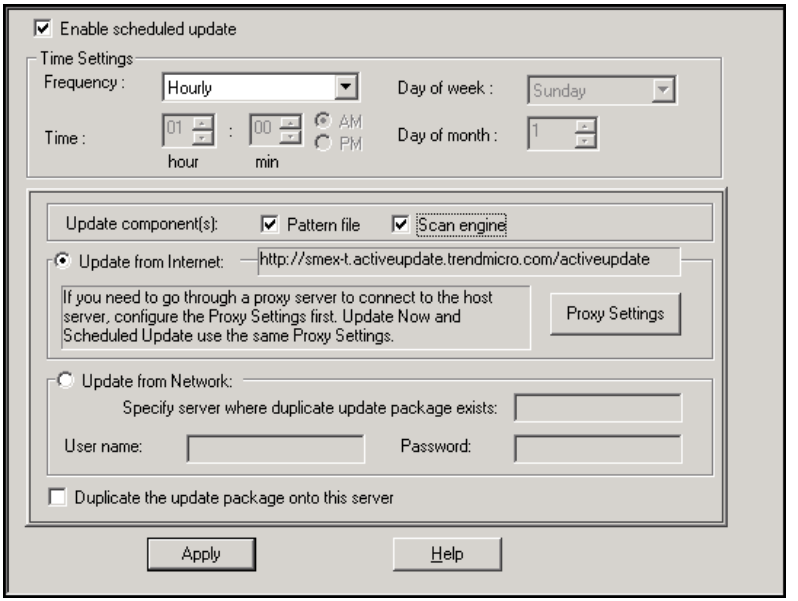

FIGURE 14-6. ActiveUpdate, Scheduled Update screen

2. Select the **Enable scheduled update** check box.

3. In the **Time Settings** group box, select the update frequency. Use the pull-down menu to select **Hourly, Daily, Weekly, or Monthly**.

Select which components you want to update and configure your update settings, as described in the previous section. Click **Apply** to save the new configuration. ScanMail retains the new update schedule on the **Scheduled Update** screen.

Chapter 15

Using Quarantine Manager and ScanMail's Log Files

ScanMail has a Quarantine Manager that lets you easily view information on quarantined email and attachments. If you determine that an item is suspect and should be quarantined, you can:

- Delete it individually
- Use the Quarantine Maintenance screen to delete all quarantined files
- Schedule regular quarantine file deletion

You can examine a quarantined email and delete the item or resend it once you feel it is safe. Alternatively, you can resend the item to other individuals. For example, you may have set up an eManager rule to block anyone other than the Human Resources department from sending specific email messages. If you examine an email attachment and discover that non Human Resource employees are sending out these specified documents or attachments, you may want to notify certain individuals of this behavior.

ScanMail also keeps logs of scan events, viruses deleted, program updates, files backed up before cleaning, quarantined files, and attachments blocked. These logs are a valuable source of system information. ScanMail provides a Log Maintenance screen where you can configure how long to keep the log files and schedule regular log maintenance.

This chapter contains information on ScanMail's Quarantine Manager and Log Files, including the following sections:

- Resending Quarantined Email and Attachments
- Quarantine Maintenance
- Viewing ScanMail's log files
- Scheduling regular log file deletion

Quarantine Manager

The quarantine directory on the ScanMail server is where messages are moved as the result of a processing action.

You can use Quarantine Manager to:

- Reduce the chance of important messages being deleted, if they are erroneously detected by the eManager or VirusWall 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

The Quarantine Manager consists of the following screens:

- **Quarantined Email** — query quarantined email, including attachments
- **Quarantined Attachments** — query quarantined attachments
- **Quarantine Maintenance** — select how long to keep the quarantine log files and whether to compact the quarantine database

Quarantined email and attachments

Use the **Quarantined Email** and **Quarantined Attachments** screens to view quarantine information such as **Date & Time**, **Sender**, **Recipients**, and **Subject**.

View quarantined attachments in the **Quarantined Attachments** screen. This option shows cases where ScanMail blocks only a specific attachment in an email, rather than the entire email. You can examine quarantined email information, delete an item, or resend it when you are sure it is safe. Alternatively, you can send the item to other individuals.

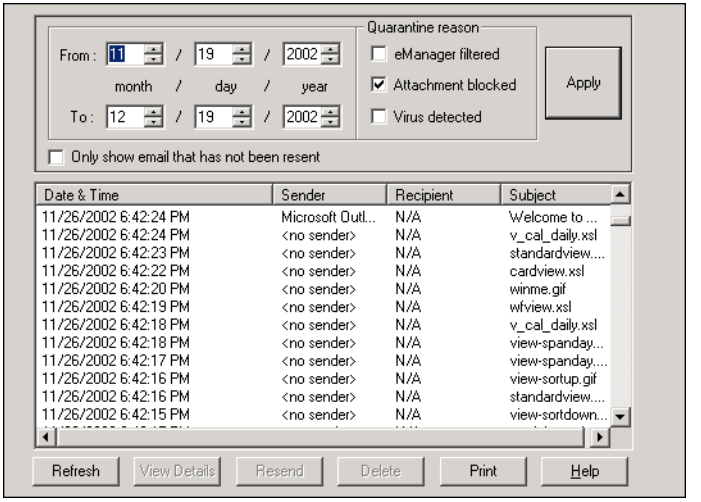

FIGURE 15-1. Quarantined Email screen

To select the quarantine records to view:

1. In the left frame, click **Quarantine Manager** > **Quarantined Email**.
2. Select the range of dates for the quarantine records you want to view. The dates are in the mm/dd/yyyy format.
3. Select one or more of the quarantine reasons:
   - **eManager filtered** — view the messages that met the filter conditions (if the ScanMail eManager plug-in is installed)
   - **Attachment blocked** — shows the messages that contain attachments that met the file-blocking rules
   - **Virus detected** — shows messages that were quarantined because they contain viruses
4. To view the messages that have only been quarantined, select **Only show email that has not been resent**.
5. Click **Apply** to view the records.

To see more information on a quarantined message, select the message and click **View Details**.

Viewing quarantined email and attachment information

To view details about a quarantined email message, select the item and click **View Details**.

The following information is presented:

- **Received on** — the time the email was quarantined
- **Resend status** — the status is False if you have not sent the message to the recipient or others. The status is True if the message was examined, determined to be safe for delivery, and sent to the original intended recipient or others specified

> **Note:** Resend each item individually using the **Quarantined Attachments** details screen. In the **Quarantined attachments** section, the **Resent** field shows the resend status of each attachment.

- **Sent at** — the time the message was sent
- **From** — the sender
- **To** — the recipient
- **Subject** — the original email subject line without a quarantine warning appended
- **Quarantined attachments** — the quarantined attachment file name, size, and quarantine reason appear

Resending quarantined email

To resend a quarantined email message and/or attachments, select the item you have determined is safe and click **Resend**.

To resend a quarantined email

1. To specify the delivery options, fill in the following fields:
   - **Send to** — select the check box to send the message to the original recipients

- **Forward to** — enter the email addresses of people you want to receive the message

2. Edit the default **Subject** text. You can also append the original subject line to the end of the message.
3. In the **Message Body** field, enter the text that will be inserted in the message body.
4. Select the attachments to include:
   - **Quarantined email** — sends the entire email, including the quarantined attachments
   - **Message content only** — sends the message body of the quarantined email without any attachments
   - **Quarantined attachments only** — sends the quarantined attachment(s) without the original message text
5. If you want to permanently delete the quarantined documents after the resend completes, click **Delete**.

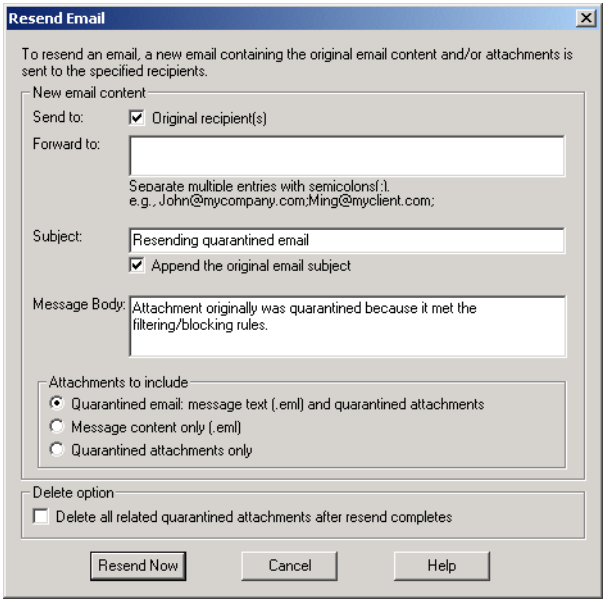

FIGURE 15-2. Resend Email screen

Quarantine Maintenance

Use the Quarantine Maintenance screen to set up automatic quarantine file deletion at certain intervals, or to perform manual quarantine log deletion. Rather than deleting quarantined items individually, this option allows you to automatically delete all files, or all resent files.

Deleting quarantined files regularly helps prevent your quarantine database from becoming too large. To free up server disk space, compact the quarantine database periodically to reuse the space occupied by the deleted files.

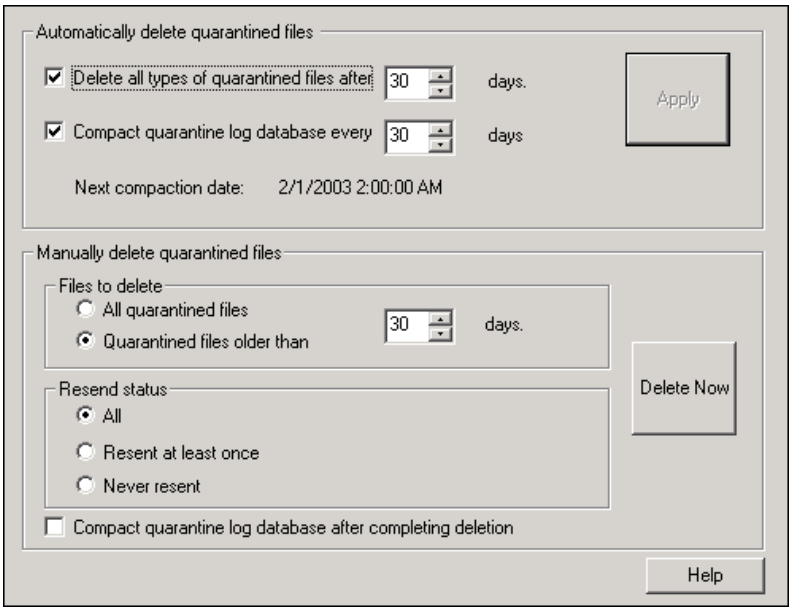

FIGURE 15-3. Quarantine Maintenance Screen

Automatic quarantine file deletion

ScanMail stores information on quarantine files to help control the amount of disk space used. You can automatically delete quarantine files after a specified time.

In the **Delete all types of quarantined files after** text box, specify the number of days you want to save the log files. You can keep quarantined files for a maximum of 180 days. If you want to keep the files for a longer time, clear the check box and manually delete your logs.

To save space on the server's hard disk, you can select **Compact quarantine log database every __ days**. Enter the number of days to wait until compacting the database again. The interval start date is the date of installation or the date this setting is selected/updated. The next compaction date appears.

Manual quarantine file deletion

To delete only specific log files or delete them only at a specific time, fill in the manual deletion section. You can also delete log files individually by navigating to the Quarantine directory.

To manually delete log files using the ScanMail console:

1. In the **Quarantine Maintenance** screen, select whether to delete all files now or the age of the files to delete. The default is to keep the logs 30 days before allowing deletion.
2. Select the **Resend status** for the logs you want to delete:
   - **All** – delete all files, whether or not they have been sent to the recipient
   - **Resent at least once** – delete only the files that have been sent to the recipient at least once
   - **Never resent** – delete only the files that have never been sent to the recipient
3. To reduce the size of the quarantine database, select **Compact quarantine log database after completing deletion**.
4. Click **Delete Now**.

ScanMail log files

ScanMail keeps the following log files to document various events:

- **Scan Event Log** — manual and scheduled scan events
- **Virus Log** — virus events, such as the date and time the virus was detected, the virus name, and the action that was taken
- **Update Log** — program updates of the pattern file and scan engine
- **Backup Log** — files that have been backed up before virus cleaning
- **Quarantine Log** — infected messages that have been quarantined
- **Attachment Blocking Log** — attachments that have been blocked from delivery

Use Log Maintenance to purge log records that you no longer want to keep.

Viewing log file entries

You can view the log files from the Windows or Web consoles.

To view log file entries from the Windows console:

1. Select **View Log**.
2. The options are:
   - **Scan Event Log**
   - **Virus Log**
   - **Update Log**
   - **Backup Log**
   - **Quarantine Log**
   - **Attachment Blocking Log**

Note: To update the displayed results, click **Refresh Log** at the bottom of the screen.

---

3. To view specific entries in the logs, in the **From** and **To** text boxes, specify the time period you want. (The Update log does not contain these fields).
4. Click **Apply** and the results appear in the screen below.
   - To save the list, click **Export** and enter the file name with a .csv extension
   - To print the log, click **Print**

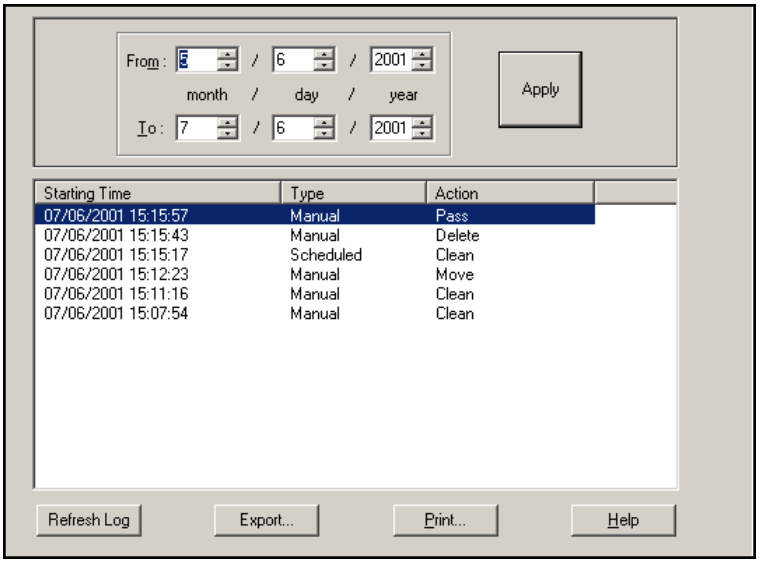

FIGURE 15-4. SMMC Scan Event Log screen

The **Virus Log** screen contains one additional button—**Virus Information**. See the **Log Screen Details** section below for more information on this option.

Log screen details

Each of the log screens displays a different set of log details:

Scan Event Log

The Scan Event Log shows a history of scan events that occurred during manual and scheduled scans. The following fields are displayed:

`Starting Time, Type, Action`

Virus Log

The Virus Log displays information on viruses found during real-time, manual, and scheduled scans. The following fields are displayed:

```
Date & Time, Found At, Sender, Recipient, Subject, Scanning Time,
File, Virus, Action
```

If ScanMail finds malicious code in a public folder, the folder name appears in the **Found At** field, preceded by a backslash. Mailbox names are not preceded by a "\". For example:

```
\Public Folder1

mailbox1

mailbox2
```

For details about a virus, select an entry from the list and click **Virus Info**. You can also double-click the target entry and the Virus Information screen appears.

For the most up-to-date virus information, in the ScanMail top menu bar, click **Help > Web Virus Encyclopedia**.

Update Log

The Update Log records events related to software program updates. The following fields appear:

```
Starting Time, Ending Time, Method, Result, Description
```

Use this log to view whether pattern file and scan engine updates are occurring automatically as scheduled. The Method can be Internet or Replication. In the Method field, **/S** means that a scheduled update was performed, and **/M** means that a manual update was performed.

Backup Log

The Backup Log displays a list of infected files ScanMail backed up before taking the selected action. The following fields appear:

```
Date & Time, Found At, Sender, Recipient, Virus Name, Original File,
Backup File
```

Quarantine Log

The Quarantine Log displays a list of files ScanMail quarantined after finding a virus during real-time, manual, and scheduled scans. The following fields appear:

```
Date & Time, Found At, Sender, Recipient, Virus Name, Original
File, Quarantined File
```

If ScanMail finds malicious code in a public folder, the folder name appears in the **Found At** field, preceded by a backslash. Mailbox names are not preceded by a "\".

Depending on how you configure your virus scan options, you can choose to quarantine all files that contain viruses, or just uncleanable virus-infected files.

Attachment Blocking Log

The Attachment Blocking Log displays a list of files that were blocked based on attachment file name and/or extension. The following fields appear:

```
Date & Time, Found At, Sender, Recipient, Subject, Scanning Time,
Original File, Quarantined File, Action
```

Maintaining the log files

ScanMail stores date information on the scan event, virus log, attachment blocking, update, backup, and quarantine files to assist in controlling their sizes. You can automatically delete entries in these files that are older than a specified number of days.

In addition, you can delete the log files manually whenever you want to free up more space on your server.

Automatically deleting log files

If you want ScanMail to automatically delete the log files to free additional space on your server, fill in the automatic log deletion section in the Windows or Web console.

To automatically delete log files:

1. In the left frame, click **View Log**.
2. Click **Log Maintenance** to display the Log Maintenance screen:

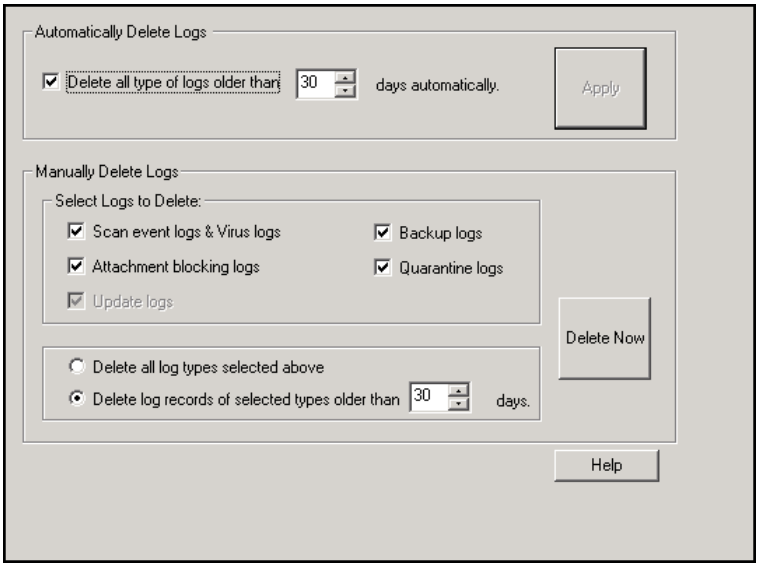

FIGURE 15-5. SMMC Log Maintenance screen

In the **Delete all types of logs older than** text box, specify the number of days you want to save the log files. The maximum number of days to keep the log files is 180 days. If you want to keep logs for a longer time, clear the check box and delete your logs manually.

3. Click **Apply**.

Manually deleting log files

If you want to delete only specific log file types or delete them at specific times, enter information in the manual log deletion section. You can also individually delete log files by navigating to the `\Log` directory.

To manually delete log files through the ScanMail configuration consoles:

1. In the **Log Maintenance** screen, select the check boxes for the types of logs you want to delete:
   - Scan event logs & Virus logs
   - Attachment blocking logs
   - Update logs
   - Backup logs
   - Quarantine logs

   Note: You can delete the Scan Event & Virus logs from the Windows console only.

2. Select the number of days to keep the logs:
   - To delete the selected log files for all dates, select the **Delete all log types selected above**
   - To delete the logs only if they are a certain age, select the **Delete log records of selected types older than** text box, and type the number of days to keep the log files. The maximum number of days is 180
3. Click **Delete Now**.

ScanMail keeps the log files in the **`\Log`** directory of ScanMail using the file names, **`ScanSum.log`** for the Scan Event log file and **`TmUpdate.log`** for the Update log file.

To delete log records individually on the server:

1. Navigate to the **`\Program Files\Trend\SMEX\Log`** directory.
2. You can delete the scan event, update, and attachment blocking logs completely or open them and delete individual records.
3. The backup, quarantine, and virus logs are stored as individual log records for each day, in the yyyymmdd.ext format.

where the extension (.ext) is **.b** for the backup log files, **.q** for the quarantine log files, **.r** for virus scan log files, or **.f** for attachment blocking log files. You can delete these logs individually.

Note: These files do not appear until you have backed files up for cleaning, quarantined virus-infected files, or run a scan.

Chapter 16

Content Management with Trend Micro™ ScanMail™ eManager Windows-based Console

Trend Micro ScanMail eManager for Microsoft Exchange works to reject spam mail bound to or sent from users of the corporate LAN. The Exchange server does not process rejected spam mail so it does not end up in your clients' mailboxes. Trend Micro monitors new spam, collects telltale blocking information from the new spam and incorporates the blocking information into new Anti-spam Rule and Import files.

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

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

filtered for content violations as well. You can use the included content filter policies and also define policies of your own.

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

This chapter introduces ScanMail eManager and describes how eManager interfaces with ScanMail for Microsoft Exchange. The topics include:

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

Content Management

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

Spam Filtering

ScanMail eManager's spam filter quickly evaluates the header and/or content of messages. In particular, it checks the origin of messages to assess whether they are spam (unsolicited commercial email, or UCE), by comparing the header information to a set of user-defined rules. When eManager finds messages that match the spam filter rules, it **deletes** or **quarantines** those messages. It does not pass deleted or quarantined messages to ScanMail for Microsoft Exchange for virus checking.

Alternatively, eManager **archives** (copies to the archive directory) messages, and passes them to ScanMail for Microsoft Exchange for virus checking.

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

Content Filtering

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

What is Spam Mail?

Spam is unsolicited commercial email (UCE). The purpose of spam is to promote a business or idea. However, spam is email that is unrequested and unwanted by the recipient.

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

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

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

Why is Spam Mail Bad?

Spam wastes people’s time and resources. At a corporate level, it reduces productivity and creates a burden for MIS staff.

Consider the following points when you consider whether spam is harmful or not.

- Spam is often annoying, offensive, wasteful and sometimes illegal
- Spam blasts can slow down your network, as bandwidth is consumed in the delivery of hundreds of unwanted email messages
- Spam mail wastes time and is distracting. Just to delete spam, email clients must first identify who the messages are from and what they are about. Even careful users risk deleting legitimate messages while trimming spam from their inbox
- Spam mail serves no corporate interest, yet uses the corporate Exchange server(s) for processing and delivery. It uses CPU, takes up space on the server hard drive, and on the hard drives of countless end-users. Even after you delete spam, it persists in memory as deleted files and backups until your computer permanently removes it from your system
- Spam mail multiplies the risk of widespread virus attacks by simultaneously exposing many people to the same infected file or URL containing a malicious Java or ActiveX application

For more information about the cost of spam to your company, Trend Micro invites you to visit our website. You can find a useful tool, the Trend Spam ROI Calculator, and links to spam activity reports

Click on the following to open the website in your browser:

http://www.trendmicro.com/form/spam/default.asp

Tracking Spammers

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

Anti-spam Rules

Anti-spam Rules can be defined by entering criteria in any one or all of the following fields in the Anti-spam screen of the Windows-based Console:

- To

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

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

Anti-spam Rules Strategy

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

Content Filter Policies

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

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

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

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

Example "Free offer" Policy

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

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

The following paragraph matches the rule-sets above:

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

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

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

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

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

Boolean Expressions Implied in the Content Filter

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

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

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

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

ScanMail for Microsoft Exchange and ScanMail eManager Processing Order

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

1. ScanMail for Microsoft Exchange receives inbound mail and redirects it to ScanMail eManager. This action occurs before virus scanning.
2. In a quick operation, ScanMail eManager performs a spam/not-spam evaluation.
3. ScanMail eManager compares the message information to the user-defined list of current rules. When it finds mail that matches any one of the specified criteria, that mail is **Deleted, Archived,** or **Quarantined**. It does not compare the message further. It does not forward deleted and quarantined messages to ScanMail for Microsoft Exchange. It copies archived messages to the archive directory and then forwards as usual to ScanMail for Microsoft Exchange.

4. The processing order is shown below:

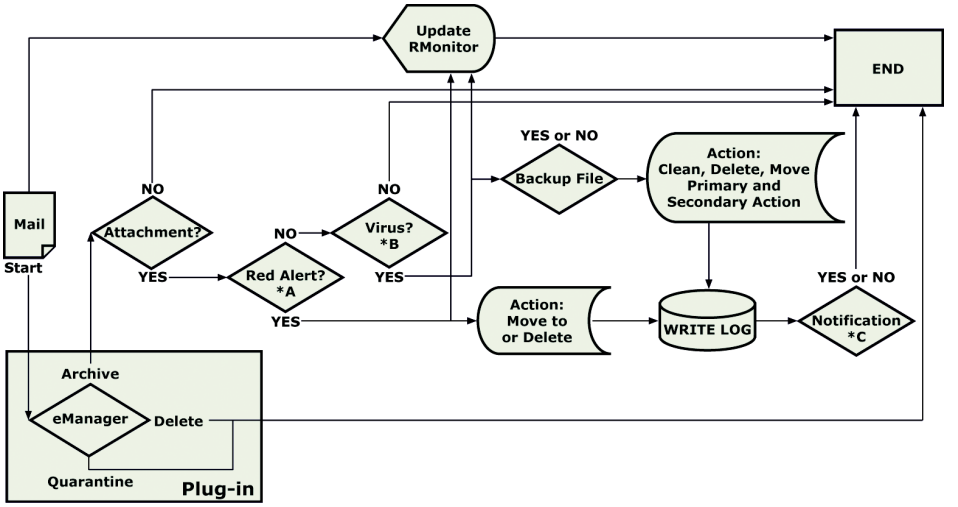

FIGURE 16-1. Email process flow through ScanMail eManager to ScanMail for Microsoft Exchange

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

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

Control Manager™ Agent for ScanMail eManager

Trend Micro Control Manager is only available in ScanMail enterprise version.

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

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

Trend Micro Control Manager is sold separately. Once you have purchased and installed the Control Manager server software, you can install the Control Manager agent for ScanMail eManager for Microsoft Exchange. Control Manager allows you to configure groups of ScanMail servers from one convenient Web console.

Summary of New Features

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

- Trend Micro Anti-spam Engine

  The Trend Micro Anti-spam Engine is a module (or plug-in) that provides spam detection capabilities for the product into which it is integrated.

  The anti-spam engine examines the header and content of the email message and intelligently determines if the mail is spam.
- Configure ScanMail eManager options from a ScanMail for Exchange Local or Remote Web console

Chapter 17

Introducing Trend Micro™ ScanMail™ eManager

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

- Starting and stopping eManager
- Starting the eManager Windows-based Management console
- Viewing the ScanMail eManager processes
- Removing ScanMail eManager
- ScanMail eManger Files

Starting and stopping eManager

ScanMail eManager can now be conveniently stopped and started directly from the ScanMail Web console.

To enable ScanMail eManager:

1. Start the ScanMail Web console .
2. Enable real-time virus scanning.

Note: In ScanMail for Microsoft Exchange 2000, if you enable eManager on the Virus Scan > Options screen, eManager is enabled for all types of scans, i.e., real-time scan, scheduled scan, and manual scan. However, in ScanMail for Microsoft Exchange 5.5, you can separately enable or disable eManager for real-time scan, scheduled scan, and manual scan.

Restarting ScanMail™ for Microsoft™ Exchange and eManager™

ScanMail eManager only processes messages while ScanMail Exchange is running. Restart ScanMail to reactivate ScanMail eManager.

To restart the ScanMail for Microsoft Exchange services:

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

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

ScanMail eManager services start along with ScanMail Exchange.

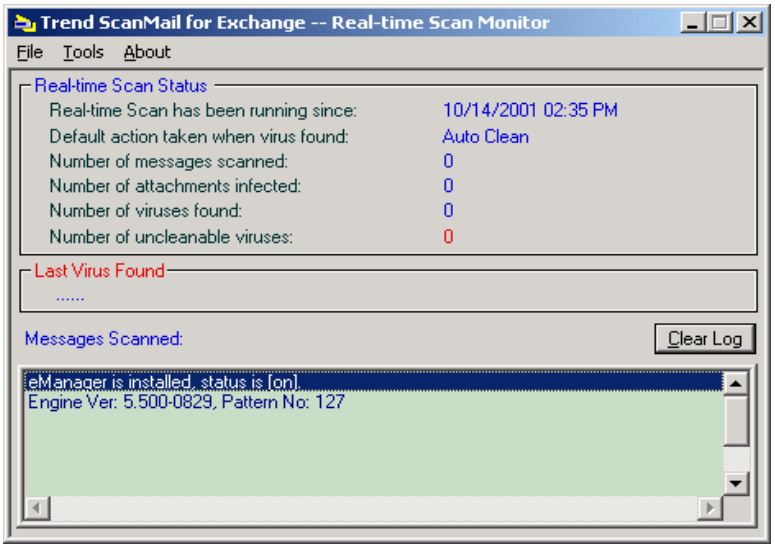

FIGURE 17-1. Real-time Scan Monitor, Messages Scanned section shows that the ScanMail eManager Content Filter has been loaded.

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

Stopping ScanMail™ for Microsoft™ Exchange and eManager™

To stop ScanMail and eManager:

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

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

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

Starting the ScanMail™ eManager Console

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

To start ScanMail eManager:

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

Note: You must use a Windows Administrator account.

Selecting the Server to Administer

When you originally start eManager, you log onto the local server. The server you are currently logged on appears in the **Current server** line.

To log on to a server:

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

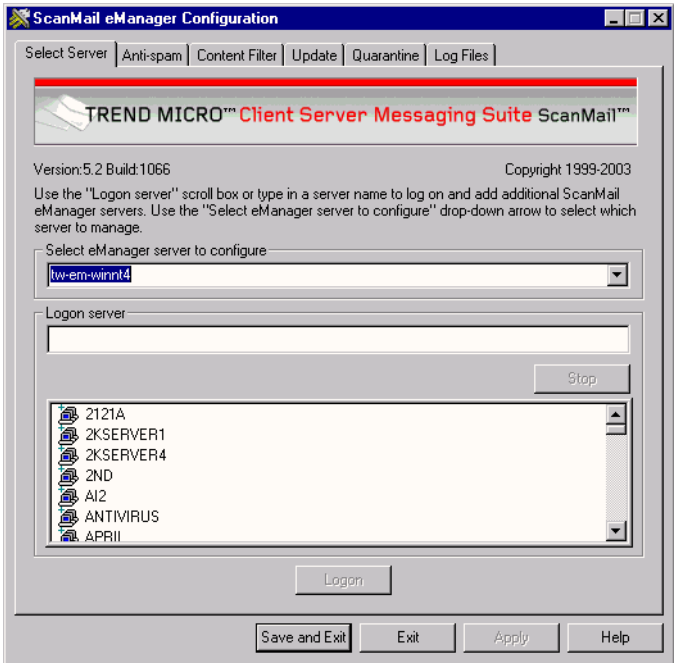

FIGURE 17-2. ScanMail eManager Select Server screen

2. Click **Logon**.

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

---

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

You can change to any server to which you have already logged on without logging on again. You do not need to re-enter your user name and password each time you

change servers. Select the server name in the Select eManager Server to Configure text box and it becomes the current server to configure.

Viewing the ScanMail™ eManager™ Processes

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

To view whether the eManager process is loaded by opening the Windows Task Manager:

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

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

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

Removing ScanMail eManager

To remove ScanMail eManager, you must first stop the ScanMail for Microsoft Exchange real-time scanning services (ScanMail_Monitor, ScanMail_RealTimeScan, and ScanMail_Web).

Removing ScanMail eManager Using the Windows™ Start Menu

To remove ScanMail eManager from the local server's Windows Start menu:

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

ScanMail™ eManager Files

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

```
Spamptn, SpamRule, Tempdir, WebRoot, Quarantine, Archive
```

ScanMail eManager also adds the following entry to your registry:

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

Chapter 18

Spam Filtering

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

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

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

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

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

- Rules strategies
- Creating anti-spam rules
- Creating global exception rules
- Operators
- Notification messages
- Action on unwanted email

Viewing Email Headers

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

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

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

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

Example Message Header

Return-Path: <dgq7@botmail.ro>
Received: from *rly-yes01.mx.aol.com* (rly-yes01.mail.aol.com [123.18.144.193])
by air-yes05.mx.aol.com (v47.2) with SMTP; Fri, 07 Aug 1999 07:20:53 -0400
Received: from mail1.starfordnet.com (mail1.staffassoc.com [123.10.128.47]
(may be forged)) **by** *rly-yes01.mx.aol.com* (8.8.8/8.8.5/AOL-4.0.0) with
ESMTP id HAA20159; Fri, 7 Aug 1999 07:20:41 -0400 (EDT)

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

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

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

Configuration Files

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

```
\Program Files\Trend\SMCF

    contscan.ini
    csconfig.dat

\Program Files\Trend\SMCF\spamrule

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

\Program Files\Trend\SMCF\spamptn

    Tm####.exp
    Tm####.rul
    Tm####.sig
```

Using the Spam Filter

The spam filter starts and stops with ScanMail for Microsoft Exchange. You cannot run the spam filter independently.

You can view the operational status of the spam filter (i.e., eManager) in one of several ways:

1. Open the ScanMail Management Console and go to the **Virus Scan > Options** (Exchange 2000) or **Real-time Scan > Options** (Exchange 5.5) screen. **Enable eManager** should be selected.
2. Open the Real-time Scan Monitor on the ScanMail eManager machine to see real-time virus and filter processing. The Real-time Scan Monitor, Messages Scanned section should list that eManager is loaded.

   Or,

   open the Windows task manager and make sure that the process **Cm_smex.exe** is loaded.

See Chapter 17, "Introducing Trend Micro™ ScanMail™ eManager", for more details on stopping and starting ScanMail for Microsoft Exchange and ScanMail eManager.

Creating Anti-spam Rules

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

The two types of rules are:

- Regular rules
- Exception rules

Each type of rule uses the same configuration options. The only difference is the action taken when a message matches the conditions. A message matching a regular rule condition can be Deleted, Quarantined, or Archived. Exception rules allow messages matching the condition to pass through completely, rather than being Archived as well.

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

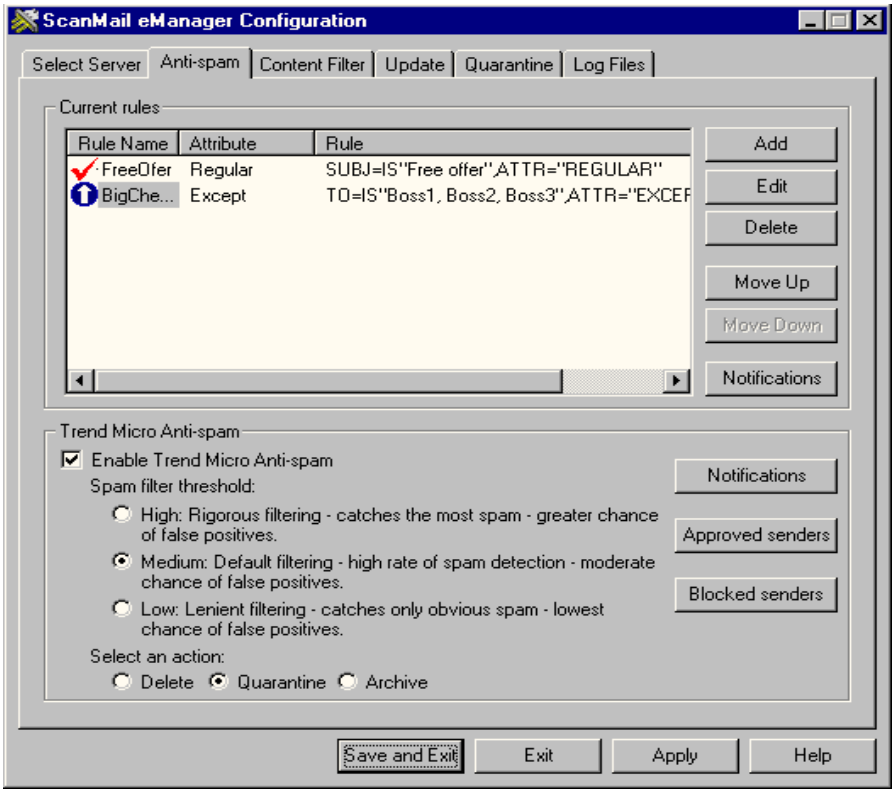

FIGURE 18-1. This eManager spam filter shows anti-spam in effect.

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

Current Rules Strategy

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

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

Rules Strategy Example

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

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

For example, if you analyze your incoming messages and discover that for every 10,000 messages processed by the Exchange server, 42 are sent by *SpamKing*, 500 contain the phrase "Free Offer" in the subject line, 18 are sent to *SpamLover*, and 196 contain the term "SeXXX" in the subject line.

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

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

When ordered as above, 500 of every 10,000 incoming messages can be eliminated in the first round of evaluation because they match the "Free Offer" rule. If, the order were reversed and "SpamLover" was the first rule and a "Free Offer" message arrived, the message would be evaluated four times (1. check for "SpamLover," 2.

check for "SpamKing," 3. check for "SeXXX," 4. check for "Free Offer") before finally matching on "Free Offer" and being rejected.

User-defined Current Rules

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

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

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

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

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

Add-Edit Rule Options Screen

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

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

Note: The **Routing domain** and **Reply-to** fields are not available in this version and are grayed out, as shown in Figure 18-2 below.

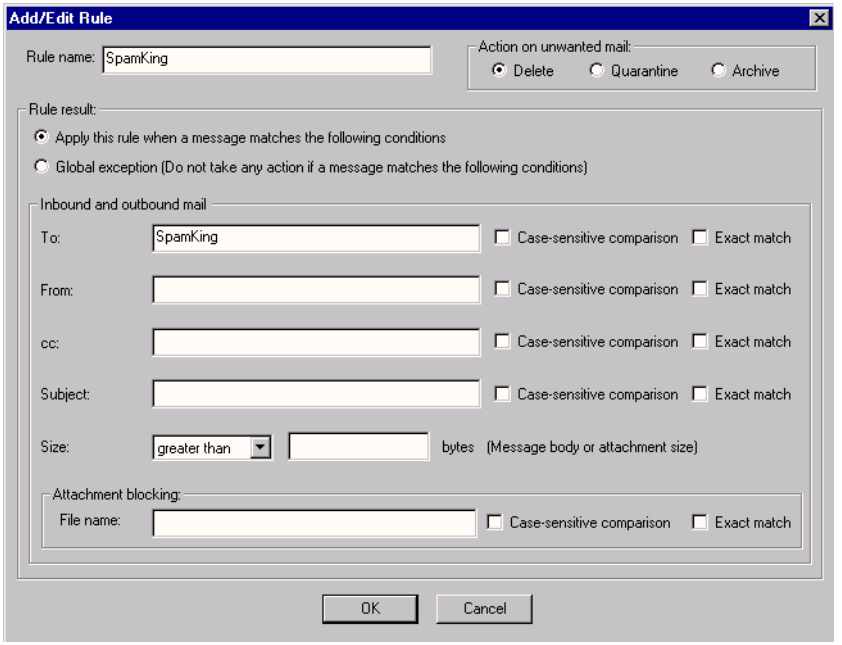

FIGURE 18-2. This rule blocks inbound messages sent to SpamKing.

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

Rule Name

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

Action on Unwanted Mail

Messages that ScanMail finds to match the filter rules are deleted or quarantined and are not passed to ScanMail for Microsoft Exchange for virus scanning. Alternatively, it can copy messages to the archive directory, and then pass them to ScanMail for Microsoft Exchange for virus checking.

ScanMail records all blocked actions in the log file.

Quarantined. ScanMail moves email messages to the quarantine directory that the user has specified on the Quarantine screen.

Archived. ScanMail forwards email messages to the intended recipient, but it also renames and moves the messages to the archive directory that the user has specified on the Quarantine screen.

Deleted. eManager keeps the log file for deleted mail.

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

Rule Result

Based on the rule results, you can designate rules as Regular rules or Exception rules. By default, ScanMail considers rules Regular and applies the rule to any email message when it matches the specified conditions.

Alternatively, you can create a Global Exception rule that takes effect regardless of what other rules you have configured. ScanMail applies this rule when an email message matches the conditions you specify. However, messages that match the Global Exception conditions are exempt from any further comparisons. ScanMail passes it to ScanMail for Microsoft Exchange for virus scanning.

Address and Subject Fields

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

To, From, cc, Subject

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

Blind Carbon Copies (email addresses appearing in the **bcc** field). ScanMail does not consider information included in this field as part of the header. Therefore, when taking action on an email, it does not filter information in the bcc through its anti-spam rules.

Case-Sensitive Comparisons

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

You can configure ScanMail to apply case-sensitivity on a field-by-field basis when it filters email. To do so, individually select the Case-sensitive comparison check boxes for the To, From, cc, and Subject fields.

Exact Matches

ScanMail considers anti-spam keywords a match if the specified word matches any part of the mail header, i.e., To, From, cc, and Subject fields. For example, if you specify "Free" as the keyword in the Subject field, ScanMail considers an occurrence of "Freezer" in the mail header, specifically the Subject field, a valid match.

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

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

Message or Attachment Size

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

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

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

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

Attachment Blocking

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

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

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

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

Anti-spam Notifications

You can configure separate notifications for the user-defined Current Rules section. Just select the corresponding **Notifications** option.

Current Rules Notifications

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

- Notify the following administrator(s) — enter the Administrator(s) email addresses in the **Email address(es)** text box. Multiple email addresses should be delimited with semi-colons. Then enter the message text to send, for example:
  "Note: Spam filter has blocked junk mail!"
- Notify sender — enter the message text to send.
- Notify recipient(s) — enter the message text to send.

Chapter 19

Content Filtering

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

There is no limit to the number or type of content policies you can create, enable, or disable. The content filter also provides a synonym checking feature that allows you to extend the reach of your policies.

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

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

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

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

The topics include:

- Understanding ScanMail eManager Content Filter

- Creating content filter policies
- Understanding ScanMail eManager's content filter policies
- Using the content filter policies to block spam
- Using the Quarantine Screen
- Reporting spam messages to Trend Micro

Understanding ScanMail™ eManager Content Filter

The ScanMail eManager Content Filter starts and stops with ScanMail for Microsoft Exchange. You cannot run eManager independently. Chapter 17, "Introducing Trend Micro™ ScanMail™ eManager" describes starting and stopping ScanMail eManager for Microsoft Exchange.

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

Creating Content filter policies

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

Content filter comparisons use only the email message text and non-encoded text/Word attachments. They do not consider binary email attachments.

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

Selecting an individual policy from a Policies list enables that policy. There is no limit to the total number of policies that can be engaged by the content filter. One rule

of thumb, however, is that the more active policies there are, the longer it takes to evaluate a given email message.

The Content Filter screen is displayed in the figure below.

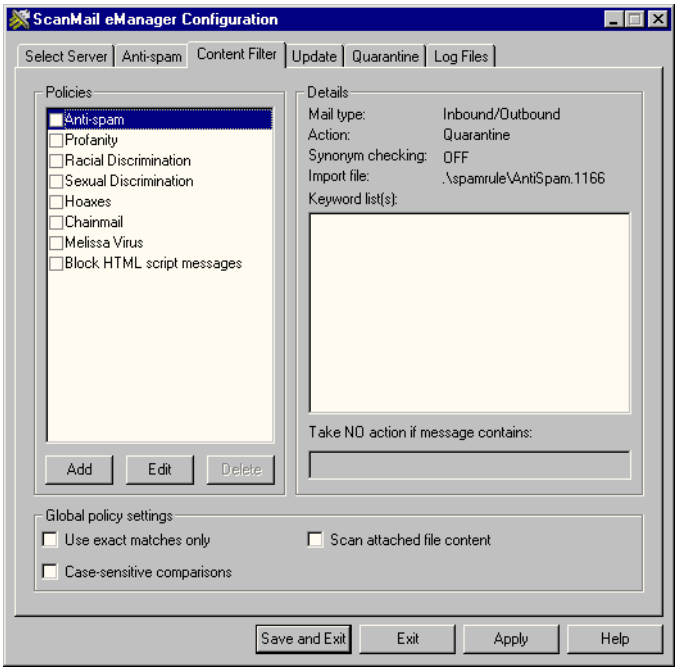

FIGURE 19-1. Content filtering is policy-based and user-configurable.

Creating Keyword Lists

The **Keyword List** for a given **Policy** contains the words and phrases that the content filter uses to check email message contents. The filter makes a match only when the message it evaluates contains *all* of the keywords. For example, you can add the following keywords to the list (perform four separate **Add**s).

Example 1:

free, money
free, gift

free, parking
free, college diploma

Notice that this example uses four related words instead of just one. Basing the policy solely upon the word *free* is not likely to produce reliable results because the word can have several different meanings in different contexts (*free* - meaning something that costs nothing - *and free* - to release*)* To minimize the chance of such false positives, qualify the primary word, *free*, with additional words typically associated with it in a spam message (*money, gift, parking* and *college diploma)*. Including several keyword groups increases the reach of the filter.

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

Example 2:

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

free, money, gift, parking, college diploma

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

Example 3:

In this example we construct a policy wherein the occurrence of any one of the related words from example 2, triggers a match.

free
gift
money
parking
college diploma

Use this technique to filter out other offensive or unwanted content. You decide whether or not the occurrence of any one of the words on your list is sufficient to warrant tracking (**Archive** option), further investigation (**Quarantine** option), or immediate deletion.

Understanding ScanMail™ eManager's Content Filter Policies

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

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

Anti-spam

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

See Update starting on page 10-5 for more information on updating the Import file.

Profanity and Discrimination Lists

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

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

The Sexual Discrimination list stores words that are sexually harassing and inappropriate. This is a starter list of words that are offensive and is intentionally brief. The keywords listed are words that generally do not have alternate meanings that are not offensive.

Hoaxes and Chain mail Lists

The Hoax list contains keywords and phrases that identify some of the most common hoax email messages. Use this list to have ScanMail block Hoax emails.

What is a Hoax email? It is an email message that warns the recipient of some false danger and encourages them to forward the message to others. Forwarding the hoax messages perpetuates the problem.

Example: The Hoax describes a fantastic or impossible virus or Trojan program. It advises you to forward the warning to friends and co-workers. Other hoaxes offer bogus free gifts or other items not appropriate for a corporate environment.

The Chain mail list contains keyword phrases that identify some of the most common Chain mail messages. Use this list to have ScanMail block Chain mail.

What is a Chain mail? It is a message that encourages the recipient to forward the message to others. Some Chain mails encourage the recipient to add to or edit the message. There are several problems with chain letters. Chain mail can slow down networks and contribute to a spam mail problem. Chain mail can be offensive and may threaten recipient who do not forward the Chain mail. In some countries they are illegal if they request money or other items of value and promise a substantial return to the participants.

Example: A typical chain letter includes names and addresses of several individuals whom you may or may not know. They instruct you to send money or valuables to the person at the top of the list, and then eliminate that name and add yours to the bottom. They instruct you to mail copies of the letter to a few more individuals. Sometimes the Chain mail contains threats to the recipient if they refuse to forward the message (for example, they claim you will have bad luck if you fail to forward the message).

Blocking HTML Script Messages

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

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

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

Note: You cannot customize the Anti-spam policy. It is based on the Import File that is downloaded from Trend Micro. The default action of the policy is to **Quarantine** all messages matching the anti-spam rules. However, you can change this default action to **Archive** or **Delete**.

Creating content filter policies

Do not include more than four or five values for keywords linked on the same line or you risk making them overly restrictive. If only one keyword is included on any given line, you risk making the policy too permissive—ScanMail will find too many email messages to match.

ScanMail evaluates the criteria you specify exactly as you enter them. This includes any quotes, spaces and punctuation. It treats phrases, delimited by commas as single units. Only when it finds that each word, space, etc. in the phrase also appear in the message, and it appears in the order in which it was entered, is a match triggered.

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

Step-by-Step Example

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

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

To create a new policy:

1. In eManager, click the **Content Filter** tab, then the **Add** option that appears below the Policies list.
2. In the **Policy name** field, enter a name for the policy, in this example, **Sex**.

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

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

   Because of the sensitive nature of this policy, neither the message sender nor intended recipient are informed of the action. Alternatively, you can have a mild warning automatically sent to the **Recipient**:

   A message you received appears to violate the company email policy. We do not condone the use of company time and equipment for viewing sexual

material; please refrain from this behavior in the future. If you feel that you've received this message in error, email your concerns to the following address: admin@yourcompany.com.

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

Using the Content Filter to block spam

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

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

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

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

Content Filter Options

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

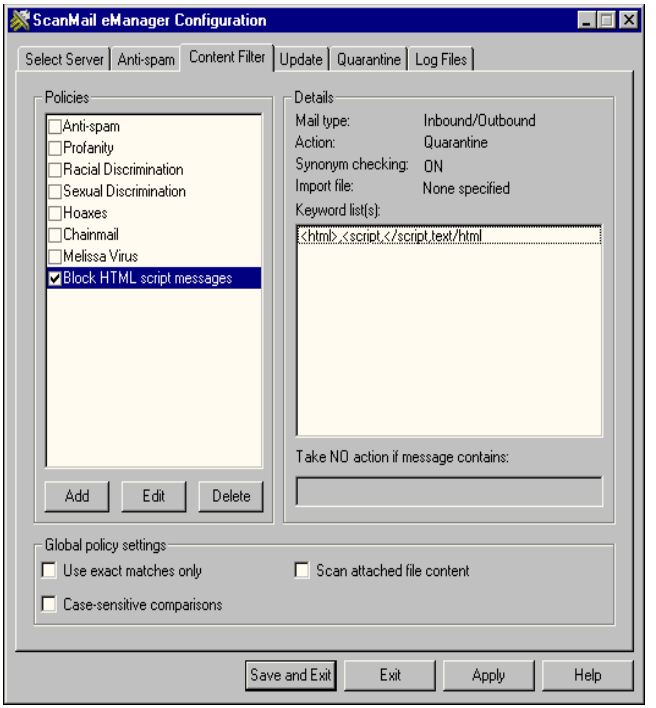

FIGURE 19-2. Content filter policies can include multiple keyword sets, synonyms, import files, and anti-keywords.

Policies

The **Policies** list shows the individual rules by which ScanMail evaluates inbound and outbound messages.

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

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

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

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

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

Details

The **Details** area provides more detailed summary information about how a policy functions. When you highlight a policy, the Details of that policy appear. The Details provide a summary of such information as the type of mail eManager checks for the policy, the action eManager takes when it finds a match and the keywords for which it searches.

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

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

Keyword Lists

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

Add/Edit Policy Options

ScanMail evaluates the criteria you specify for content filter policies exactly as you entered them, including any quotes, spaces and punctuation. It treats phrases as single

units. Matches occur only when each word, space, comma, etc. in the phrase is found to appear in the message.

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

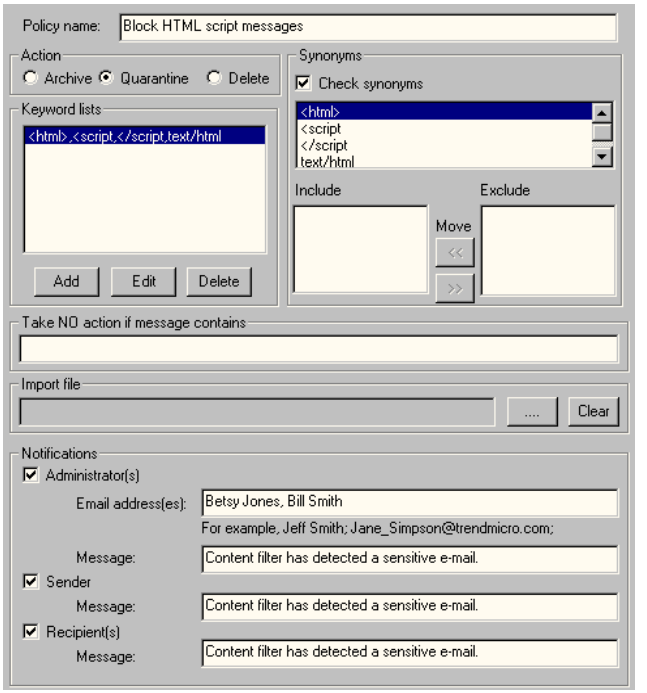

FIGURE 19-3. Add/Edit Policy Screen

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

Policy Name

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

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

Action

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

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

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

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

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

Keyword List(s)

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

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

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

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

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

The following paragraph matches the rule-set above:

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

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

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

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

Using Synonym Checking

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

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

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

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

Keyword List Example

Case 1. Keywords appear on a single line

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

Case 2. Keywords each appear on their own individual lines

```
Apple Juice
Pear
Orange
```

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

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

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

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

Notes:

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

The capitalization and exact-match properties of synonyms are consistent with those defined on the **Content Filter** tab. In other words, if the word *red* appears in the

synonyms list, it only triggers a match with the word ***red****undant* if **Exact Match** is not selected; likewise, the word *red* only triggers a match with the word *Red* in the message text if **Case-sensitive comparison** is not selected.

Creating exception keyword lists

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

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

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

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

Example

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

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

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

Import File

Trend Micro provides special keyword lists designed to efficiently filter out certain types of spam and other unwanted email based on message content. Contained in

"Import files", these policies go beyond the quick header checking used by the spam filter, and instead filter messages based on an analysis of the actual message content. Import files, like the Rule-file, are updated monthly by Trend Micro and you can download it "on demand" or scheduled for automatic downloads.

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

Import File Format

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

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

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

Notifications

Whenever the content filter acts upon an email message, ScanMail can notify the email administrator and others of the action.

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

You can set policy specific notifications as follows:

1. With eManager running and the **Content Filter** tab active, click the **Add** or **Edit** option that appears below the Policies window.
2. Select **Notify the following administrator(s)**, **Notify sender**, and/or **Notify recipient(s)**.

3. If you selected to notify the administrators, specify the email addresses of the parties to whom you want a notification sent in the **Email address(es)** field.

   Multiple email addresses should be delimited with semicolons.

4. In the **Message text** field, enter the message text you want the notification recipient to receive, for example:

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

Using Global Policy Settings

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

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

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

Exact Matches

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

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

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

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

Case-Sensitive Comparisons

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

Enable Scanning the Content of Attached Files

You can select **Enable scanning the content of attached files** if you want to evaluate the text in attachments for content violations. You can scan non-encoded text files and Word documents for their contents.

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

Using the Quarantine Screen

You can use the Quarantine Screen to set the quarantine and archive directory locations. The default settings are:

Quarantine directory:

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

Archive directory:

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

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

Quarantine and Archive Directory Structure

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

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

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

Reporting spam messages to Trend Micro

To report a spam email message, please forward the message, including all headers, to:

spam@support.trendmicro.com

To report an email message that eManager incorrectly identified as spam (a false positive), please forward the message, including all headers, to:

false@support.trendmicro.com

Trend Micro regularly updates the anti-spam rules file and anti-spam engine with information from the messages you provide. Your assistance helps reduce future spam and false positive messages.

Chapter 20

Troubleshooting

This chapter describes how to troubleshoot problems that may arise with OfficeScan.

In this chapter, you will learn about potential issues regarding the following:

- *Client-server communication* on page 20-2
- *Incorrect number of clients on the Web console* on page 20-2
- *Incorrect client status on the Web console* on page 20-3
- *Incorrect component versions* on page 20-4
- *Unsuccessful installation from the Web page or with Remote Install* on page 20-5
- *Client icon does not appear on the Web console after installation* on page 20-5
- *Issues during migration from third-party antivirus software* on page 20-6

Contact information

- *Contacting the Trend Micro Virus Information Center* on page 20-9
- *Contacting Technical Support* on page 20-9
- *Contacting Trend Micro Knowledge Base* on page 20-11
- *Contacting TrendLabs™* on page 20-11

Client-server communication

This section explains some key points about OfficeScan client-server communication. Understating the client-server communication will help you more quickly troubleshoot problems and take advantage of the Web console's central management capabilities.

Figure 20-1 illustrates the flow of communication between the server and the clients.

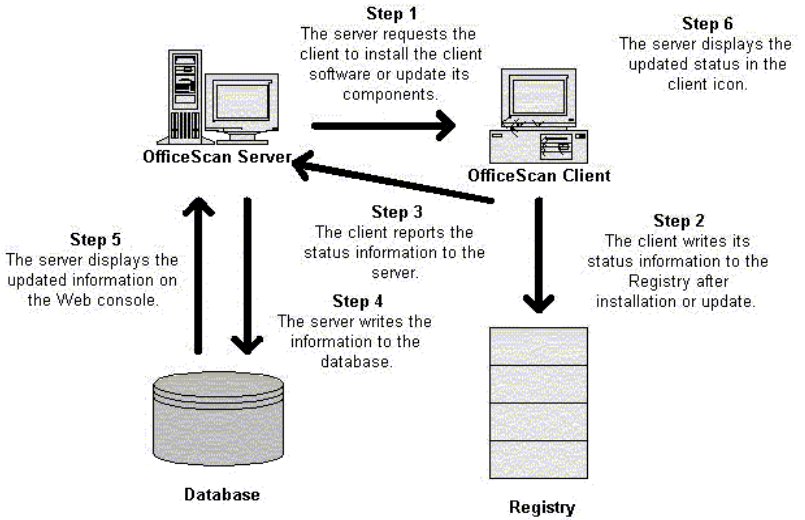

FIGURE 20-1. Client Server Communication flow

If you see an error message stating "the actual status and the reflected status of the client on the management console are not synchronized," this is primarily because the server database records do not match with the values in the client's registry.

Incorrect number of clients on the Web console

You may see that the number of clients reflected on the Web console is incorrect.

This happens if you retain client records in the database after client program removal. For example, if client-server communication is lost while removing the client, the server will not know about the client removal. The server retains client information in the database and still shows the client icon on the console. When you reinstall the client, the server creates a new record in the database and displays a new icon on the console.

This error can occur in steps 4 and 5 of the client-server communication flow (see *Client-server communication* on page 20-2).

Use the Verify Connection feature to check for duplicate client records. See *Verifying client-server connection* on page 5-23 for more information.

Incorrect client status on the Web console

You may see that OfficeScan does not synchronize the actual client status and the client status on the console. This happens if the client is unable to launch the client program or if, at startup, the client loses connection to the server before it could report its status.

This error can occur in steps 4 and 5 of the client-server communication flow (see *Client-server communication* on page 20-2).

To resolve this, try the following:

- Use the OfficeScan Verify Connection feature of the server to check if client-server communication exists. See *Verifying client-server connection* on page 5-23 for more information. If the server can communicate with the client, it will display the client status as Online.
- Check if the client computer is off or if the client program has been unloaded, removed, or stopped. These conditions will cause the server to display the client status as Off. If there was an error during any of these processes, it is possible that the client was not able to inform the server that it is shutting down or that it is being unloaded, removed, or stopped. As a result, the server did not know to change the status of the client from On to Off. On the client, check if the OfficeScan icon appears as . If it does, the client has switched to roaming mode.

Note: If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from both the server and client. Then contact Trend Micro technical support. See the OfficeScan client help for information on running Active Support.

Incorrect component versions

OfficeScan may incorrectly display the version number of the client components. This happens when the client is unable to write its status information to the registry and send this information to the server.

For example, you updated the pattern file of a client from 411 to version 413. However, after updating, the console still shows 411. It is possible that you updated the client but the client was unable to write its updated information to the registry.

To resolve the incorrect display problem, try the following:

- Use ping or telnet to verify that client-server communication still exists
- If you have limited bandwidth, check for connection timeouts between the server and the client
- If you are using a proxy server for client-server communication, check that the proxy settings are correct
- Open a Web browser on the client, type `http://{Server name}:{Server port}/officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client. In this case, please contact Trend Micro support.
- Check if the user has local administrator rights to the client computer to write to the registry. OfficeScan writes client information, including the version of the pattern file, scan engine, and program, to the registry.
- Check if the user modified files or registry values but forgot to restart the `Tmlisten.exe` service on the client for Windows XP/2000/NT/Server 2003 or `Pccwin97.exe` on the client for Windows Me/98/98 SE.
- Check if the client has two or more Network Interface Cards (NICs). If a client has two NICs, it will also have two IP addresses. The server may not be able to

communicate with the client because it does not know which IP address to use. You may be able to install the client, but may not be able to update it.

Note: If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from both the server and client. Then contact Trend Micro technical support. See the OfficeScan client help for information on running Active Support.

Unsuccessful installation from the Web page or with Remote Install

If users report that they cannot install from the internal Web page or if installation with Remote Install is unsuccessful, try the following:

- Verify that client -server communication exists by using ping and telnet
- Verify that you have administrator privileges to the target computer where you want to install the client
- Check if TCP/IP on the client is enabled and properly configured
- Check if the target computer meets the minimum system requirements
- Check if any file has been locked
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- If you are using a proxy server for client-server communication, check if the proxy settings are configured correctly
- Open a Web browser on the client, type `http://{Server name}:{server port} /officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.

Client icon does not appear on the Web

console after installation

You may discover that the client icon does not appear on the console after you install the client. This happens when the client is unable to send its status to the server.

To resolve this, do the following:

- Verify that client-server communication exists by using ping and telnet
- If you have limited bandwidth, check if it causes connection timeout between the server and the client
- Check if the \PCCSRV folder on the server has shared privileges and if all users have been granted full control privileges
- Verify the OfficeScan server proxy settings to ensure they are correct
- Open a Web browser on the client, type `http://{OfficeScan_Server_Name}:{port number}/officeScan/cgi/cgionstart.exe` in the address text box, and then press ENTER. If the next screen shows -2, this means the client can communicate with the server. This also indicates that the problem may be in the server database; it may not have a record on the client.

Note: If this does not help you find the real cause of the issue, use ActiveSupport to collect `Ofcdebug.log` from both the server and client. Then contact Trend Micro technical support. See the OfficeScan client help for information on running Active Support.

Issues during migration from third-party antivirus software

This section discusses some issues you may encounter when migrating from third-party antivirus software.

Client migration

The setup program for the OfficeScan client utilizes the third-party software's uninstallation program to automatically remove it from your users' system and

replace it with the OfficeScan client. If automatic uninstallation is unsuccessful, users get the following message:

```
Uninstallation failed.
```

There are several possible causes for this error:

- The third-party software's version number or product key is inconsistent
- The third-party software's uninstallation program is not working
- Certain files for the third-party software are either missing or corrupted
- The registry key for the third-party software cannot be cleaned
- The third-party software has no uninstallation program

There are also several possible solutions for this error:

- Manually remove the third-party software
- Stop the service for the third-party software
- Unload the service or process for the third-party software

Manually remove the third-party software

If the third-party software is registered to the Add/Remove Programs

1. Open the Control Panel.
2. Double-click **Add/Remove Programs**.
3. Select the third-party software from the list of installed programs.
4. Click **Remove**.

If the third-party software is not registered to the Add/Remove Programs

1. Open the Windows registry.
2. Go to `HKEY_LOCAL_MACHINES\Software\Microsoft\Windows\CurrentVersion\Uninstall`.
3. Locate the third-party software and run the uninstall string value.
4. If the third-party software's setup program is in MSI format:
   - Locate the product number
   - Verify the product number
   - Run the uninstall string

Note: Some products' uninstallation keys are in the Product Key folder.

Modify the service for the third-party software

1. Restart the computer in safe mode.
2. Modify the service startup from automatic to manual.
3. Restart the system again.
4. Manually remove the third-party software.

Unload the service or process for the third-party software

WARNING! *This procedure may cause undesirable effects to your computer if performed incorrectly. Trend Micro highly recommends backing up your system first.*

1. Unload the service for the third-party software.
2. Open the Windows registry, then locate and delete the product key.
3. Locate and delete the run or run service key.

Verify that the service registry key in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` has been removed.

Contacting the Trend Micro Virus Information Center

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

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

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

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

Contacting Technical Support

A license to Trend Micro software includes the right to product updates, pattern file updates, and basic technical support for one (1) year, after which you must purchase renewal maintenance on an annual basis to continue receiving these services.

You can contact Trend Micro via fax, phone, and email, or visit us at www.trendmicro.com. Evaluation copies of all Trend Micro products can be downloaded from our Web site.

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

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

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

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

  +1-408-257-1500 (main)

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

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

If you interested in learning about the benefits of Premium Support, contact:

Email:sales@trendmicro.com
Phone: (877) TRENDAV (877-873-6328)

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

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

Speeding Up Your Support Call

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

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

- Exact text of any error message given
- Steps to reproduce the problem

Contacting Trend Micro Knowledge Base

On the Trend Micro Web site, you can visit the Knowledge Base, an online database of common answers to technical questions, at:

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

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

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

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

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

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

Contacting TrendLabs™

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

You can rely on the following post-sales service:

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

TrendLabs has achieved ISO 9002 quality assurance certification.

Appendix A

Using OfficeScan Tools

OfficeScan includes a set of tools that can that can help you easily accomplish various OfficeScan tasks, including server configuration and client management.

These tools are classified into two categories:

- **Administrative tools** – developed to help configure the server and manage clients
- **Client tools** – developed to help enhance the performance of the client program

Refer to Table 1-1 for a complete list of tools included in this version of OfficeScan.

Administrative Tools	Client Tools
Database Backup	Client Packager
Login Script Setup	Image Setup Utility
Vulnerability Scanner	Remote Agent
	Restore Encrypted Files

TABLE 1-1. OfficeScan tools

Note: You must run OfficeScan tools separately from the Web console.

Administrative Tools

This section contains information about the following OfficeScan administrative tools:

- Database Backup
- Login Script Setup
- Vulnerability Scanner

Database Backup

The database on the server contains all OfficeScan settings, including scan settings and privileges. Backing up the OfficeScan database is a routine task that Trend Micro recommends you perform. If the server database becomes corrupted, you can easily restore it if you have a stored copy of the database.

Database Backup requires the following files:

- Main file: `DBBackup.exe`
- Required DLL file: `svcmgr.dll`

To back up a database:

1. On the server, open Windows Explorer and go to the `\PCCSRV\Admin\Utility\DBBackup` folder of OfficeScan.
2. Double-click `DBBackup.exe` to start Database Backup. The tool's icon appears in the Windows system tray.
3. Right-click the Database Backup icon in the system tray. A pop-up menu appears.
4. Click **DB Backup Settings**. The Database Backup console appears.
5. In **Source database**, click to browse for the database folder of OfficeScan.

   The database files of the HTTP-based server are in `\PCCSRV\HTTPDB`.

6. In Backup path, click to browse for the folder where you want to store the backup. Trend Micro recommends creating the backup folder on another drive or folder other than the OfficeScan folder.
7. Under **Backup Schedule**, select a frequency with which Database Backup will run:
   - **No Action** - select if you do not want to back up the database
   - **Daily** - select to back up the database daily. Select a time when Database Backup will run from the **Time** spin boxes. Use the first spin box to specify the hour and the second to specify the minute. Database Backup uses the 24-hour format. For example, to back up the database at 8:35 pm, select 20 in the first spin box and then select 35 in the second spin box.
   - **Weekly** - select to back up the database once every week. Select the day and time when to Database Backup will run from the **Day of the week** box and **Time** spin boxes, respectively.
   - **Monthly** - select to back up the database once every month. Select the date and time when to Database Backup will run from the **Day of the month** box and **Time** spin boxes, respectively.
8. Click **Apply** to save your settings.

Login Script Setup

With Login Script Setup, you can automate the installation of the OfficeScan client to unprotected computers when they log on to the network. Login Script Setup adds a program called autopcc.exe to the server login script. The program `autopcc.exe` performs the following functions:

- Determines the operating system of the unprotected computer and installs the appropriate version of the OfficeScan client
- Updates the virus pattern file and program files

For instructions on installing clients, see *Installing with Login Script Setup* on page 4-16.

Vulnerability Scanner

Use Vulnerability Scanner to detect installed antivirus solutions and to search for unprotected computers on your network. To determine if computers are protected, Vulnerability Scanner pings ports that are normally used by antivirus solutions. Vulnerability Scanner can perform the following functions:

- Ping computers on your network to check their status and retrieve their computer names, platform versions, and descriptions
- Determine the antivirus solutions installed on the network. It can detect Trend Micro products (including, OfficeScan, ServerProtect for Windows NT and Linux, ScanMail for Microsoft Exchange, InterScan Messaging Security Suite, and PortalProtect) and third-party antivirus solutions (including, Norton AntiVirus Corporate Edition v7.5 and v7.6 and McAfee VirusScan ePolicy Orchestrator).
- Display the server name and the version of the pattern file, scan engine and program for OfficeScan and ServerProtect for Windows NT
- Send scan results via email
- Run in silent mode (command prompt mode)
- Install OfficeScan client remotely on computers running Windows 2003/XP (Professional only) /NT/2000

You can also automate Vulnerability Scanner by creating scheduled tasks. For information on how to automate Vulnerability Scanner, see the TMVS online help.

You can run Vulnerability Scanner on the server or on any Windows 2000 computer on the network. To run Vulnerability Scanner on a computer other than the server, copy the TMVS folder from the \PCCSRV\Admin\Utility folder of the server to the computer.

WARNING! *You cannot run Vulnerability Scanner on computers running Windows 2003/XP/NT/Me/98.*

To run Vulnerability Scanner:

1. Open the TMVS folder and double-click `TMVS.exe`. The Vulnerability Scanner console appears.
2. Click **Settings**. The **Settings** screen appears.

3. Under **Product Query**, select the products that you want to check for on your network. To prevent false alarms, Trend Micro recommends selecting all check boxes. For example, if you have ServerProtect installed on a server but did not select the ServerProtect (NT/Linux) check box, Vulnerability Scanner will report that your server is unprotected.

   If you have Trend Micro InterScan and Norton AntiVirus Corporate Edition installed on your network, click **Settings** next to the product name to verify the port number that Vulnerability Scanner will check.

4. Under **Description Retrieval Settings**, click the retrieval method that you want to use. Normal retrieval is more accurate, but it takes longer to complete.

   If you click **Normal retrieval**, you can set Vulnerability Scanner to try to retrieve computer descriptions, if available, by selecting the **Retrieve computer descriptions when available** check box.

5. Do the following:

   - To automatically send the results to yourself or other administrators, under **Alert Settings** select the **Email results to the system administrator** check box, and then, click **Configure** to specify your email settings.

     i. In the **To** text box, type the email address of the recipient.

     ii. In the **From** text box, type your email address. This will let the recipient know who sent the message, if you are not only sending it to yourself.

     iii. In the **SMTP server** text box, type the address of your SMTP server. For example, you can type smtp.company.com. The SMTP server information is required.

     iv. In the **Subject** text box, type a new subject for the message or accept the default subject.

     v. Click **OK** to save your settings.

   - To display an alert on unprotected computers, select the **Display alert on unprotected computers** check box. Then, click **Customize** to set the alert message. The **Alert Message** screen appears. You can type a new alert message or accept the default message. Click **OK**.
   - To save the results as a comma-separated value (CSV) data file, select the **Automatically save the results to a CSV file** check box. By default, CSV data files are saved to the TMVS folder. If you want to change the default CSV

folder, click **Browse**. The **Browse for folder** screen appears. Browse for a target folder on your computer or on the network and then click **OK**.

6. Under **Ping Settings**, specify how Vulnerability Scanner will send packets to the computers and wait for replies. Accept the default settings or type new values in the **Packet size** and **Timeout** text boxes.
7. To remotely install OfficeScan Client and send a log to the server, type the OfficeScan server name and port number. If you want to automatically remotely install OfficeScan client, select the **Auto-install OfficeScan Client for unprotected computer** check box.
8. Click **Install Account** to configure the account. The **Account Information** screen appears. Type user name and password that permits installation. Click **OK**.
9. If you want to send log to server, select the **Report log to OfficeScan server** check box.
10. Click **OK** to save your settings. The **Trend Micro Vulnerability Scanner** console appears.
11. In **IP Range to Check**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers. Note that the Vulnerability Scanner only supports class B IP addresses.
12. Click **Start** to begin checking the computers on your network. The results are displayed in the Results table.

Note: You can also run Vulnerability Scanner at the command prompt. For more information, see the Vulnerability Scanner online help.

To create scheduled tasks

1. Under **Scheduled Tasks**, click **Add/Edit**. The **Scheduled Task** screen appears.
2. Under **Task Name**, type a name for the task you are creating.
3. Under **IP Address Range**, type the IP address range that you want to check for installed antivirus solutions and unprotected computers.
4. Under **Task Schedule**, click a frequency for the task you are creating. You can set the task to run **Daily**, **Weekly**, or **Monthly**. If you click **Weekly**, you must

select a day from the list. If you click **Monthly**, you must select a date from the list.

5. In the **Start time** spin boxes, type or select the time when the task will run. Use the 24-hour clock format.
6. Under **Settings**, click **Use current settings** if you want to use your existing settings, or click **Modify settings**.

   If you click **Modify settings**, click **Settings** to change the configuration. For information on how to configure your settings, refer to steps 4 and 5 in the "To run Vulnerability Scanner:" procedure.
7. Click **OK** to save your settings. The task you have created appears under **Scheduled Tasks**.

Other Settings

To configure the following settings you need to modify `TMVS.ini`:

- **Debug** – enable or disable the debug log
- **EchoNum** – set the number of computers that Vulnerability Scanner will simultaneously ping
- **ThreadNumManual** – set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software
- **ThreadNumSchedule** – set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks
- **ThreadNumSilent** – set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running the tool at the command prompt

To modify these settings:

1. Open the TMVS folder and locate the `TMVS.ini` file.
2. Open `TMVS.ini` using Notepad or any text editor.
3. Do the following:
   - To enable the debug log, change the value from `Debug=0` to `Debug=1`.

- To set the number of computers that Vulnerability Scanner will simultaneously ping, change the value for `EchoNum`. Specify a value between 1 and 64.

  For example, type `EchoNum=60` if you want Vulnerability Scanner to ping 60 computers at the same time.

- To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software, change the value for `ThreadNumManual`. Specify a value between 8 and 64.
- For example, type `ThreadNumManual=60` to simultaneously check 60 computers for antivirus software.
- To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running scheduled tasks, change the value for ThreadNumSchedule. Specify a value between 8 and 64.

  For example, type `ThreadNumSchedule=60` to simultaneously check 60 computers for antivirus software whenever Vulnerability Scanner runs a scheduled task.

- To set the number of computers that Vulnerability Scanner will simultaneously check for antivirus software when running the tool at the command prompt, change the value for `ThreadNumSilent`. Specify a value between 8 and 64.

  For example, type `ThreadNumSilent=60` to simultaneously check 60 computers for antivirus software whenever you run Vulnerability Scanner at the command prompt.

4. Save `TMVS.ini`.

Client Tools

This section contains information about the following OfficeScan client tools:

- Client Packager
- Image Setup Utility
- Remote Agent
- Restore Encrypted Files

Client Packager

Client Packager is a tool that can compress setup and update files into a self-extracting file to simplify delivery via email, CD-ROM, or similar media. It also includes an email function that can access your Microsoft Outlook address book and allow you to send the self-extracting file from within the tool's console.

Users just need double-click the file to run the setup program. OfficeScan clients that are installed using Client Packager report to the server where the setup package was created.

For instructions on how to use Client Packager, *Installing with Client Packager* on page 4-19.

Image Setup Utility

Disk imaging technology allows you to create an image of an OfficeScan client and make "clones" of it to other computers on your network.

Each client installation needs to a Globally Unique Identifier (GUID), so that the server can identify your clients individually. Use an OfficeScan program called imgsetup.exe to create a different GUID for each clone.

Image Setup Utility helps you use hard drive imaging technology to deploy the OfficeScan client software.

For instructions on how to use Image Setup Utility, see *Installing from a client disk image* on page 4-23.

Remote Agent

OfficeScan clients in remote offices sometimes have problems connecting to the server in the main office because of low-bandwidth connections. This can prevent the proper deployment of OfficeScan components, especially the pattern files, which help keep the clients protected against the latest virus threats.

To help ensure that clients (especially those in low-bandwidth remote offices) are always updated, Trend Micro developed Remote Agent. Remote Agent allows clients in low-bandwidth remote offices to get updated pattern files and scan engine directly from the Trend Micro update server, instead of only from the OfficeScan server. With

this tool, clients are more likely to get program updates, even if deployment of new pattern files from the server is not possible because of bandwidth limitations.

Although clients by themselves can download updates directly from the Trend Micro update server with Update Now (if you grant them this privilege), using Remote Agent minimizes bandwidth consumption. You only need to configure a single client to download updates and share these with other clients in the low-bandwidth office. Other clients no longer have to download the updates themselves, thereby helping optimize bandwidth usage in low-bandwidth offices.

You can get the Remote Agent files from the following folder on the OfficeScan server:

`\PCCSRV\Admin\Utility\RemoteAgent`

What you can do with Remote Agent

With Remote Agent, you can perform the following tasks:

- Allow your mobile clients to get updates from the Trend Micro update server, instead of only from the OfficeScan server
- Allow you to assign a client in the remote office to download updates from both the server in the main office and the Trend Micro update server and to share these updates with the other clients in the remote office. This reduces network traffic because the other clients no longer have to connect to the server in the main office to get updates.
- Configure the agent to periodically verify its connection status with the server
- Schedule an update
- View update results from the agent log
- Configure the settings and update sources
- Perform a manual update (Update Now)

See the Remote Agent (OSRA) Configuration Guide for information on installing and using Remote Agent.

Restore Encrypted Files

Whenever OfficeScan detects an infected file, it encrypts this file and stores it in the `\Suspect` folder of the client, normally in `C:\Program Files\Trend`

`Micro\OfficeScan Client\Suspect`. The infected file is encrypted to prevent users from opening it and spreading the virus to other files on the computer.

However, there may be some situations when you have to open the file even if you know it is infected. For example, an important document has been infected and you need to retrieve the information from the document, you will need to decrypt the infected file to retrieve your information.

You can use Restore Encrypted Files to decrypt infected files from which you want to open.

WARNING! *Decrypting an infected file may spread the virus to other files.*

Restore Encrypted Files requires the following files:

- Main file: `VSEncode.exe`
- Required DLL file: `Vsapi32.dll`

To decrypt files in the Suspect folder:

1. On the client where you want to decrypt an infected file, open Windows Explorer and go to the `\PCCSRV\Admin\Utility\VSEncrypt` folder of OfficeScan.
2. Copy the entire `VSEncrypt` folder to the client computer.

Note: Do not copy the `VSEncrypt` folder to the OfficeScan folder. The `Vsapi32.dll` file of Restore Encrypted Files will conflict with the original `Vsapi32.dll`.

---

3. Open a command prompt and go to the location where you copied the VSEncrypt folder.
4. Run Restore Encrypted Files using the following parameters:
   - `no parameter` - encrypt files in the Suspect folder
   - `-d` - decrypt files in the Suspect folder
   - `-debug` - create debug log and output in the root folder of the client
   - `/o` - overwrite encrypted or decrypted file if it already exists

- `/f {filename}` - encrypt or decrypt a single file
- `/nr` - do not restore original file name

For example, you can type `VSEncode [-d] [-debug]` to decrypt files in the Suspect folder and create a debug log. When you decrypt or encrypt a file, the decrypted or encrypted file is created in the same folder.

Note: You may not be able to encrypt or decrypt files that are locked.

Restore Encrypted Files provides the following logs:

- `VSEncrypt.log` - contains the encryption or decryption details. This file is created automatically in the root system drive (normally, on the C: drive).
- `VSEncDbg.log` - contains the debug details. This file is created automatically in the root folder if you run `VSEncode.exe` with the -debug parameter.

To encrypt or decrypt files in other locations:

1. Create a text file and then type the full path of the files you want to encrypt or decrypt.

   For example, if you want to encrypt or decrypt files in `C:\My Documents\Reports`, type `C:\My Documents\Reports\*.*` in the text file. Then save the text file with an INI or TXT extension, for example, you can save it as ForEncryption.ini on the `C: drive`.

2. At a command prompt, run Restore Encrypted Files by typing `VSEncode.exe -d -i` {location of the INI or TXT file}, where {location of the INI or TXT file} is the path of the INI or TXT file you created (for example, `C:\ForEncryption.ini`).

Appendix B

Configuring OfficeScan with Add-ons and Third-party Software

Configuring OfficeScan Wireless Protection Manager

As personal digital assistants (PDAs) and other handheld computing devices increase the number of ways for communicating with other devices, the chances of becoming infected also increase. These days, it is common for PDAs to feature Internet connectivity.

Note: In this quick start guide, the term "PDA" is used to describe personal digital assistants and other handheld computing devices.

OfficeScan for Wireless provides portable, easy-to-use virus protection for wireless devices to defend against potential threats. Malicious code or other threats specifically designed for portable platforms can enter your Palm, Pocket PC, or EPOC device during beaming, synchronization, or Internet access.

This section contains the following:

- About Wireless Protection Manager
- PDA System Requirements

- Installing Wireless Protection Manager
- Opening Wireless Protection Manager
- Using Wireless Protection Manager
- Updating OfficeScan for Wireless
- Downloading Update Components
- Enabling and Configuring Proxy Settings
- Synchronizing with Your PDA
- Working with Logs

About Wireless Protection Manager

You need to install Wireless Protection Manager on your desktop or laptop PC to help manage OfficeScan for Wireless files that are installed, synchronized, or updated on your PDA device. It also receives information in the form of logs from the PDA devices.

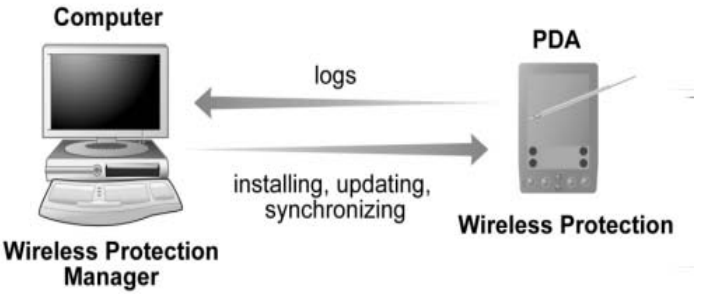

FIGURE 2-1. Relationship between Wireless Protection Manager on your computer and wireless protection on your PDA

Note: Wireless Protection Manager does not provide any virus protection for your desktop or laptop PC.

PDA System Requirements

Your PDA requires the following to run Trend Micro OfficeScan for Wireless.

Palm

- Palm™ OS 3.x or 4.x
- 2MB of memory
- 100KB of available memory for program installation
- Desktop computer must have Palm Desktop™ 3.1 or above and HotSync™ applications

Pocket PC

- Windows CE 3.0
- 16MB of RAM
- 1MB of available memory for program installation
- Desktop computer must have Microsoft ActiveSync™ 3.1 or above application

EPOC

- Psion Revo™ or Revo™ Plus
- 8MB of RAM
- 200KB of available memory for program installation
- Desktop computer must have PsiWin 2.3.2 application

Installing Wireless Protection Manager

You need to install the following to provide virus protection on your PDA.

- Wireless Protection Manager on your computer
- OfficeScan for Wireless on your PDA

Before you install Wireless Protection Manager, make sure you have already installed your synchronization software (for example, Palm Desktop) and your PDA is firmly and correctly seated in its cradle.

To install Wireless Protection Manager:

1. In the system tray, right-click the OfficeScan Client icon, and then click **OfficeScan Main**. The OfficeScan client window appears.
2. Under the **Toolbox** tab, click **Install/Upgrade Wireless Protection**. A message box appears. Click **Yes** to install. The setup wizard appears.
3. Click **Next**. The **License Agreement** screen appears.
4. Click **I accept the terms in the license agreement**, and then click **Next**. You must agree to continue installation. The **Customer Information** screen appears.
5. Make sure the information is correct, and then click **Next**. The **Destination Folder** screen appears. You can choose where to install Wireless Protection Manager or use the default location. To change the location click **Change**, and then browse to the desired location.
6. Click **Next**. Select the check box of the platform of your PDA, depending on the synchronization software you have already installed (for example, Palm Desktop).
7. Click **Next**, and then click **Install**.
8. Click **Finish**.

After you have chosen the synchronization software platform and installed Wireless Protection Manager on your computer, OfficeScan for Wireless is automatically installed on your PDA.

Note: For Palm OS-based PDAs, the next time you perform a HotSync, OfficeScan for Wireless is installed on your PDA. In addition, after installing OfficeScan for Wireless, you need to manually close and re-open HotSync Manager. Reloading HotSync Manager is needed to successfully obtain virus logs from Palm OS-based devices.

Opening Wireless Protection Manager

After you have installed Wireless Protection Manager, you need to open it to access the functions.

To open Wireless Protection Manager:

- Click **Start** > **Trend Micro Wireless Protection Manager** > **Trend Micro Wireless Protection Manager**. The Wireless Protection Manager appears.

Using Wireless Protection Manager

Use Wireless Protection Manager to update your pattern file and scan engine on PDAs. You can specify the download location to get the update components, set proxy settings, and synchronize files between the main program and the files on your PDA.

Updating OfficeScan for Wireless

To protect your PDA against the latest threats, you need to update your scan engine and virus pattern files. Although all components can be updated, new pattern files are released on at least a weekly basis. Updating your pattern file provides you with the most up-to-date protection and lets OfficeScan for Wireless scan for the latest viruses or other malicious programs.

Trend Micro recommends regular updates to your virus pattern file to maintain a high-level of virus protection.

In addition, as new viruses are discovered and existing ones evolve, it becomes necessary to update certain program files and add new functionality to the scan engine. Updating your scan engine ensures OfficeScan for Wireless can act on the new instructions in the virus pattern to detect and remove viruses.

Updating your wireless protection involves the following steps:

1. Manually downloading the files from either the Trend Micro ActiveUpdate Server or another specified source
2. Synchronizing the files with your PDA

Downloading Update Components

You need to download the update components from the Trend Micro ActiveUpdate Server or another specified update source. These components include the virus pattern file, scan engine, and other program files.

To ensure you have the latest Trend Micro virus protection technology, you need to keep your files updated.

To download update components:

1. Open Wireless Protection Manager.
2. Click the **Manual Update** tab.
3. Under **Component Download Source**, confirm the update source is correct. If not, do one of the following:
   - Click **Trend Micro ActiveUpdate Server** to download from Trend Micro
   - Click **Other source** to download from another specified location (default)
4. Click **Update Now**.

Enabling and Configuring Proxy Settings

If you use a proxy server on your network, you need to type the IP address and port number of this proxy server. You may also need to supply the appropriate logon credentials.

To enable and configure proxy settings:

1. Open Wireless Protection Manager.
2. On the menu bar, click **Option** > **Proxy Settings**. The **Proxy Settings** window appears.
3. Under **Proxy server**, select the **Use a proxy server...** check box.
4. In **Host name**, type the IP address or name of the proxy server (for example, proxy.yourcompany.com).
5. In **Port**, type the port number of the proxy server (for example, 80).
6. In **Protocol**, click the protocol your proxy server uses (**HTTP** or **Socks**).
7. Under **Authentication**, in **User name** and **Password**, type your proxy server logon credentials.
8. Click **OK**.

Synchronizing with Your PDA

To make sure the latest update components are on your PDA, you need to synchronize the updated files on your computer with your PDA.

Before manually synchronizing through Wireless Protection Manager, please do the following:

- Make sure your PDA is firmly and correctly seated in its the cradle
- Close any antivirus software running on your PDA

Note: This function currently only works with PDAs running on Pocket PC and EPOC platforms. For Palm-based PDAs, you need to manually synchronize using the Palm HotSync function.

To synchronize with your PDA:

1. Open Wireless Protection Manager.
2. Click the **Manual Synchronize** tab.
3. Click **Synchronize**.

Working with Logs

All virus events are recorded as log entries. Log entries contain useful information about virus events that have occurred including the type of virus scan, the date and time the virus was detected, the file and virus name, and the performed action.

Viewing logs

If you have detected a virus, view virus logs stored on Wireless Protection Manager to get more information. Before you view logs, remember to synchronize Wireless Protection Manager with your PDA to make sure you are viewing the most updated logs.

To view logs:

1. Open Wireless Protection Manager.
2. Click the **Virus Log** tab.

3. Under **Select log range**, select the PDA type check box for the log you want to view.
4. Do the following:
   - To view all logs, in the **Log for** list select **All dates**.
   - To view logs within a specific date range, in the **Log for** list select **Specified date range**, and choose the date range.
5. Click **View Log**.

Managing logs on your PDA

The virus log stores information about viruses detected during previous scans and the actions taken against them.

To view the log, tap **Log** on the main screen of your PDA.

The **Virus Scan Log** screen displays information about detected viruses as well as the size of the log in bytes. Tap **Back** to return to the main screen.

To delete the log entries, tap **Clear Log**. A message box appears to confirm log deletion. Tap **Yes** to remove log entries, or **No** to abort the operation.

Deleting logs

Delete Wireless Protection Manager log entries if the information they provide is no longer useful. If the number of logs is taking up too much disk space, you may also want to delete log entries for certain dates.

To delete logs:

1. Open Wireless Protection Manager.
2. Click the **Virus Log** tab.
3. Under **Delete logs manually**, in the **Delete logs before** list, select a date.
4. Click **Delete Log**. A confirmation message appears. Click **Yes** to delete all logs before and including the date you selected.

Index

A

Action on unwanted mail
  content filter 19-13
  spam filter 18-9
Activate Now 5-3, 5-7–5-8
ActiveAction 5-29, 11-7, 12-16
ActiveUpdate 14-13
ActiveX 2-2
Add/Edit screen
  specifying evaluation criteria 18-7
adding a domain 5-15
Administrative Tools 5-6
Advanced Options 12-10
antivirus policy
  enforcing 2-5
architecture 2-11
archived messages
  location 19-13
Attachment Blocking 12-8
  Notifications 14-10–14-11
Attachment Replacement Settings 12-17
Attachments
  evaluating ASCII 18-7
  evaluating binary 18-7
Automatic Deployment 5-20
automatic updates
  client 5-20
autopcc.exe *See* Login Script Setup

B

Backing up files 12-11
Backup Log 15-8
bcc field
  support for 18-10
blocking ports 6-3
blocking shared folders 6-2
Bulk-mail, example rates 16-3

C

Case-sensitive comparisons
  content filter 19-19
client 2-12
  automatic updates 5-20
  classifications 2-13
  disconnected 2-14
  granting privileges
    client privileges 5-41
  installation path 4-4
  installing to 4-14
  managing 2-6
  network traffic 3-5
  normal 2-13
  removing 4-31
  removing using Uninstall Now 4-31
  roaming 2-14
  updating 5-20
  updating manually 5-21
  virus alert 4-4
client installation
  client disk image 4-23–4-24
  Client Packager 4-19
  internal Web server 4-15
  Login Script Setup 4-16
  testing with the EICAR test script 4-29
  using Microsoft SMS 4-25–4-27
  Windows NT remote install 4-22
client installation path 4-4
Client Update 5-4–5-6
ClnPack.exe *See* Client Packager
Compressed attachments 12-10
conducting a pilot 4-9
Configuration files
  spam filter 18-3
configuring 5-25–5-26
configuring outbreak notifications 6-7
console 4-4
Contacting Trend Micro
  in the U.S. 20-9
  main U.S. address 20-10
  outside the U.S. 20-10
Content filter
  criteria 19-11
  encoded attachments not evaluated 19-2
  explained 19-1
  illustration 19-3
  policy illustration 19-10
  policy types 19-1

step-by-step example 19-7
viewing operations of 19-2
controlling
virus outbreak 2-6
Current rules
no limit 18-7
screen 18-7

D

Damage 2-15
Damage Cleanup Services 2-15–2-16
DCS 2-15
DCS *See* Damage Cleanup Services
dedicated server 3-5
deleting a domain 5-15
denying write access to files and folders 6-5
deployment
pilot 4-9
domain 4-6
adding 5-15
creating 5-12
deleting 5-15
managing 2-6
moving clients from 5-15
renaming 5-16
selecting from 5-12
working with 5-14
domain tree 5-11
icons 5-14
refreshing 5-13
selecting from 5-12

E

EICAR test script 4-30
Email headers
example 18-2
viewing 18-2
eManager 12-14
Content filtering efficacy 19-13
efficacy 16-8
services processing order 16-7
starting 17-1
Embedded Message Deletion Layer 12-14
Encoded attachments
not evaluated 18-7
ESE Version 11-2
Event log file
scanning 15-8
events 2-12
Exact Match
content filter 19-18
spam filter 18-10
exclusion list 5-37

F

False positives
and spam rules 18-10
reducing, in content filter 19-4
file-based server 2-12
filtering 12-14
FQDN 4-6
full pattern file 3-5
fully qualified domain name 4-6

G

Gateway 11-5
Global policy settings, content filter 19-11
granting privileges to clients 5-41
GUID 4-24

H

hacker attacks 4-5
Help 5-10
Heuristic scan level 12-11
HTTP communication 4-5
HTTP server 4-7
HTTP. *See* HyperText Transfer Protocol
HTTP-based server 2-11
HyperText Transfer Protocol 2-12

I

IIS 2-11
IMC 11-5
Import file
format 19-17
obtaining 19-16
Incremental Scan
manual scans 13-5, 13-10, 13-12
incremental update 3-5
infected files
sending to the quarantine folder 2-6

Installing 4-19
installing
clients 4-14–4-27
IntelliScan 5-29, 11-7, 12-11
Internet email, percent spam 16-4
Internet Information Server. *See* IIS
Internet Mail Connector 11-5
Internet Mail Connector Message Filter 12-14

J

Java applet 2-2
Joke Programs 11-8
Jokes/Worms 12-16

K

Keyword list 19-3
explained 19-13
Keywords
delimiting multiple 19-7
example creating 19-3
example matching paragraph 19-14
multiple on same line 19-3
operators linking 19-7
using phrases in 19-7
Knowledge Base 20-11

L

Log files 15-8
Attachment blocking 15-12
Backup 15-11
directory 15-14
file names 15-14
maintaining 15-12
Quarantine 15-12
Scan Event 15-10
Update 15-11
Virus 15-11
Login Script Setup 4-16
Logs 5-5, 5-8–5-9

M

macro virus 2-2
MacroTrap
heuristic scan 12-11
technology 11-1
Mailbox and Public Folder List
refreshing 13-4
management console
functions 2-16
Web console 2-16
managing
domains and clients 2-6
Manual Deployment 5-21
Manual Outbreak Prevention 5-7, 6-1
blocking ports 6-3
configuring outbreak notifications 6-7
denying write access to files and folders 6-5
restoring network settings to normal 6-7
shared folder blocking 6-2
Manual scan 5-35, 13-1
results 13-5
running 13-3–13-4
manual update
clients 5-21
server 5-18
Mass-Mailing Pattern (MMP) 12-17
Mass-mailing viruses 11-8, 12-17
master setup 4-4
client installation path 4-4
proxy information 4-4
required information 4-4
required protocols 4-3
required restarts 4-3
required rights 4-3
shared directory 4-4
starting 4-5
virus alert message 4-4
Windows licenses 4-5
Microsoft Exchange
how viruses spread 11-3
Microsoft Exchange 2000 11-2
Microsoft SMS 4-25
MIME 18-7
moving clients from a domain 5-15

N

name 4-6
network traffic
pattern updates 3-5
planning for 3-4
server 3-4–3-5

normal clients 2-13
Notification messages 14-1
  additional text 14-2, 14-4
  changing subject line through the registry 14-12
  content filter 19-17

O

OfficeScan
  architecture 2-11
  client 2-12
  domain 5-12
  management console 2-11, 2-16
  server 2-11
  three-tier application 2-11
OfficeScan for Wireless 2-6
Outbound Mailbox Message Filter 12-14
outbreak
  controlling 2-6
  using Manual Outbreak Prevention 6-1
Outbreak alert 5-26, 14-8
  email 5-27
  pager 5-28
  SNMP Trap 5-28
  Windows NT Event Log 5-28
outbreak alert 14-6

P

package description file. *See* PDF
password 4-4
pattern file
  compressed 3-5
  extracted 3-5
  full 3-5
  incremental update 3-5
pattern updates
  network traffic 3-5
PDF 4-26
performing scans 2-5
pilot deployment 3-7, 4-9
planning
  network traffic 3-4
Policy
  defined 19-2, 19-10
  enable/disable 19-2
  example 16-6
  explained 16-1, 16-5
  naming 18-8, 19-13
  spam-blocking example 19-9
preparing for
  server installation 4-2
protection
  analyzing using logs 2-5
  updating 2-5
protocols 4-3
proxy 4-4
Proxy server 14-16
Pyramid model
  a rules strategy 16-5, 18-6

Q

Quarantine
  automatic file deletion 15-7
  Directory 12-18
  log 15-8
  maintenance 15-2, 15-6
  Manager 15-1
  manual file deletion 15-8
Quarantined items
  attachments 15-2
  Email 15-2
  location of messages 18-9, 19-13
Quarantined messages
  location of 18-9

R

Real-time scan 5-32, 12-2
  monitor 12-21, 12-23
  uncleanable files 12-17
Red Alert File Blocking 12-8
removing
  client 4-31
renaming a domain 5-16
required protocols 4-3
required restarts 4-3
required rights 4-3
requirements
  server 4-2
  Web console 4-2
Resending Quarantined Email 15-4
Restore to Normal 5-8–5-9

restoring network settings to normal 6-7
roaming clients 2-14
  privileges 2-14
  updating 2-14
rollback plan 3-7
Rule name
  spam filter 18-7

S

Scan compression layer 12-10
Scan Engine 11-1, 14-14
Scan Now 13-3
  running 5-38, 13-4
scan options 5-29
scan settings
  configuring 5-29
  excluding files and folders 5-37
  Manual scan 5-35
  scheduled scan 5-35
ScanMail
  eManager 11-9
  how it works 11-5
  manual and scheduled scan limitations 13-4
  Performance Monitor 12-24
scanning
  excluding files and folders 5-37
  from one location 2-5
  Scan Now 5-38
Scheduled scan 5-35
  configuring 13-6, 13-9
  displaying results 13-12
Scheduled Update
  pattern file and scan engine 14-16
  server updates 5-17
server
  configuring scheduled updates 5-17
  dedicated 3-5
  file-based 2-12
  HTTP-based 2-11
  network traffic 3-4
  preparing for installation 4-2
  system requirements 4-2
  updating 5-16
  updating manually 5-18
Server Administration 5-4
server installation
  preparing 4-2
  verifying 4-9
Service Pack 11-3
Set Password 5-4
Set Scan Options 5-3
setting client privileges 5-41
Settings
  content filter 19-11
shared directory 4-4
single site deployment 3-4
SMTP mail scanning 12-6
Spam
  defined 16-3
  filtering explained 16-2
  using the content filter to block 19-9
Spam filter
  creating rules 16-5
  illustration 18-5
  viewing operations of 18-4
Spam rules
  creating 18-1
  illustration 18-8
Spammers
  tracking 16-4
standard alert 5-25
  email 5-23, 5-25
  pager 5-26
  SNMP Trap 5-26
Starting the eManager services 17-2
Storage groups 11-9
Synonym checking
  content filter 19-14
  example 19-15
System requirements 9-1–9-2
  Win 2000/NT client 4-13
  Win Me/98/95 client 4-13
  Win XP client 4-13
system requirements
  Web console 4-2

T

Take 19-16
TCP 4-5
TCP port 4-5, 4-7

TCP/IP 2-12, 4-3
Technical support 20-9
testing
  with EICAR test script 4-29
three-tier application 2-11
Transmission Control Protocol. *See* TCP
TrendLabs 20-11
Trojans 2-15, 11-8, 12-16
Trusted IP Zones 11-7

U

U.S. Federal Trade Commission's "dirty-dozen" list 19-17
understanding architecture 2-11
Uninstall Now 4-31
uninstalling
  client program 4-31
  ScanMail 9-7
update
  Update Log 15-8
  Update Now 14-14
  updating from Internet 14-15
  updating from network 14-16
  verifying 5-23
Update Now 2-14, 5-22
updating clients 5-20
  roaming clients 2-14
  using Automatic Deployment 5-20
  using Manual Deployment 5-21
  using Update Now 5-22
updating the server 5-16
  using Manual Server Update 5-18
  using scheduled update 5-17
UUencode 18-7

V

Verify Connection Logs 5-8–5-9
verifying
  server installation 4-9
  updates 5-23
virus alert message 4-4
Virus log file 15-8
virus outbreak
  controlling 2-6
Virus pattern file 14-14
Virus Scan
  Status 12-20–12-21
Virus Scan Application Programming Interface (VS API) 11-2
virus scanning 2-5
Vulnerability Scanner 4-36

W

Web console 2-16
  domain tree 5-11
  getting around 5-2
  Logs 5-5, 5-8–5-9
  Manual Outbreak Prevention 5-7
  opening 5-2
  other links 5-10
  Server Administration 5-4
  system requirements 4-2
  updating 5-4
Web-based Server List 11-7
Wildcards
  use in content filter policies 19-12
Windows licenses 4-5
Wireless Protection Manager 2-6
Worms 11-8