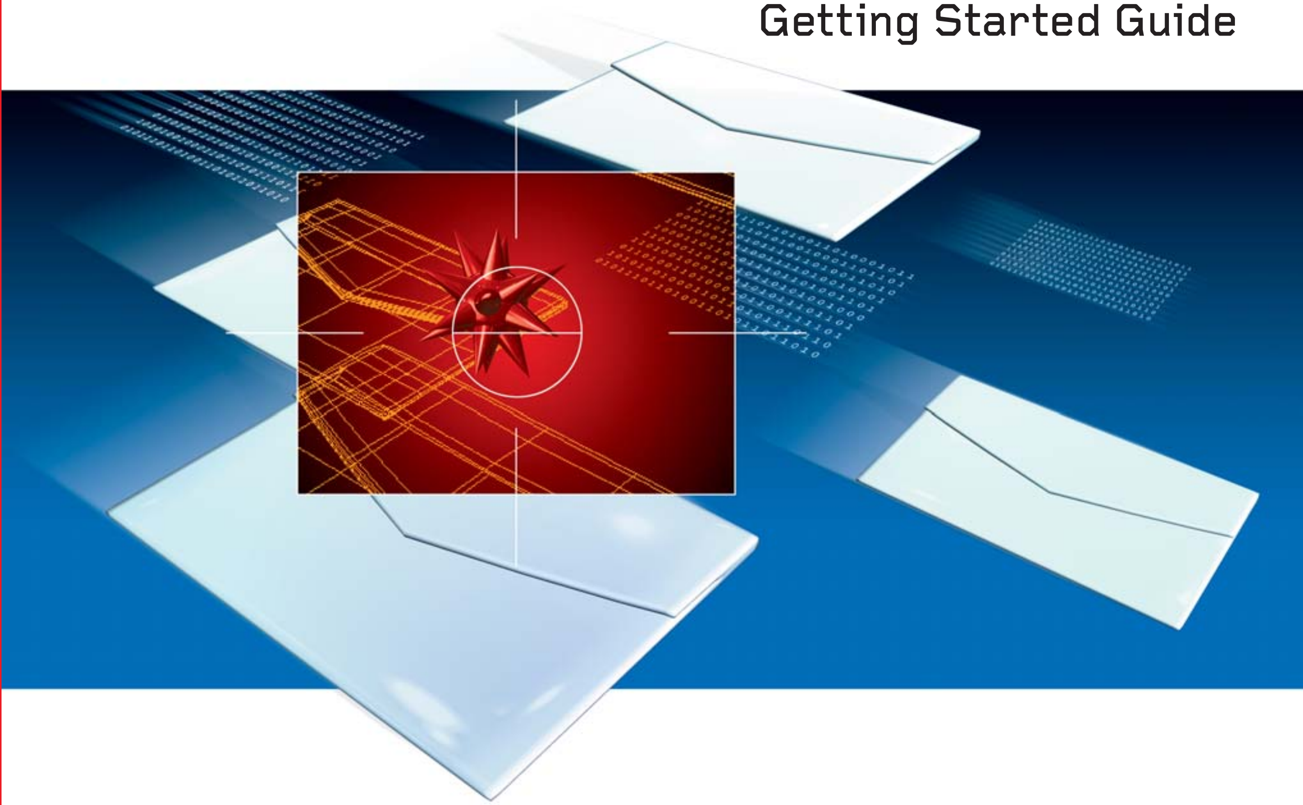
TREND MICRO™

ScanMail™ 8

for Microsoft™ Exchange

Getting Started Guide



TREND MICRO™

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

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

Document Part No. SSEM83030/70117

Release Date: March 2007

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

Document Part No. SSEM83030/70117

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

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

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

```
http://www.trendmicro.com/download/documentation
/rating.asp
```

Contents

Preface

Chapter 1: Introducing Trend Micro ScanMail for Microsoft Exchange

Chapter 2: Installing and Removing ScanMail

Chapter 3: Registering, Activating, and Updating ScanMail

Chapter 4: Managing ScanMail Servers

Chapter 5: Establishing and Maintaining Security for Your Exchange Servers

Chapter 6: Getting Support and Contacting Trend Micro

Chapter 7: Understanding Threats to an Exchange Environment

Appendix D: Glossary of Terms

Index

Preface

Welcome to the Trend Micro™ ScanMail™ for Microsoft™ Exchange version 8.0 Getting Started Guide. This book contains basic information about the tasks you need to perform to deploy ScanMail for protecting your Exchange servers. It is intended for novice and advanced users of ScanMail who want to plan, deploy, and test ScanMail.

This preface discusses the following topics:

- *ScanMail Documentation* on page 2
- *About This Getting Started Guide* on page 3
- *Audience* on page 4
- *Document Conventions* on page 4

ScanMail Documentation

The Trend Micro™ ScanMail™ for Microsoft™ Exchange documentation consists of the following:

- Online Help—Web-based documentation that is accessible from the product console

  The Online Help contains explanations about ScanMail features.

- Getting Started Guide (GSG)—PDF documentation that is accessible from the Solutions CD for ScanMail or downloadable from the Trend Micro Web site

  This GSG contains instructions on deploying ScanMail, a task that includes planning and testing. See *About This Getting Started Guide* for chapters available in this book.

Tip: Trend Micro recommends checking the corresponding link from the Update Center (`http://www.trendmicro.com/download`) for updates to the documentation.

About This Getting Started Guide

The *Trend Micro™ ScanMail™ for Microsoft™ Exchange version 8.0 Getting Started Guide* discusses the following topics:

- *Introducing Trend Micro ScanMail for Microsoft Exchange*—an overview of ScanMail features.
- *Installing and Removing ScanMail*—instructions for installing and removing ScanMail.
- *Registering, Activating, and Updating ScanMail*—instructions for activating and updating ScanMail.
- *Managing ScanMail Servers*—information about managing ScanMail servers.
- *Establishing and Maintaining Security for Your Exchange Servers*—information about how to help keep your Exchange environment safe.
- *Getting Support and Contacting Trend Micro*—information for finding support information.
- *Understanding Threats to an Exchange Environment*—information about security risks.

Audience

The ScanMail documentation assumes a basic knowledge of security systems, including:

- Antivirus and content security protection
- Spam protection
- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Microsoft Exchange Server administration
- Microsoft Exchange Server 2007 server role configurations
- Various message formats

Document Conventions

To help you locate and interpret information easily, the documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

TABLE 1. Conventions used in the documentation

Chapter 1

Introducing Trend Micro ScanMail for Microsoft Exchange

Trend Micro™ ScanMail™ for Microsoft™ Exchange Server version 8.0 protects your Exchange 2000, 2003, and 2007 mail servers. Once installed, ScanMail can protect your servers from viruses/malware, Trojans, worms, spyware/grayware. ScanMail also sustains business and network integrity by screening out spam mail and messages containing undesirable or unwanted content. ScanMail notifications send timely alerts to administrators or other designated individuals whenever significant system events or outbreak activities occur.

In this chapter, you will find information about:

- *Features and Benefits* on page 1-2
- *What's New* on page 1-3
- *ScanMail Technology* on page 1-9

Features and Benefits

ScanMail features provide the following benefits:

Fast and simple installation

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

Powerful and creative antivirus features

- SMTP scanning (Transport scanning) for Exchange 2000, 2003, and 2007 servers
- Leverage Microsoft Virus Scanning API to scan messages at a low-level in the Exchange store
- Quickly scan messages using multi-threaded in-memory scanning
- Detect and take action against viruses/malware, Trojans, and worms
- Detect and take action against spyware/grayware
- Use true file type recognition to detect falsely labeled files
- Use Trend Micro recommended actions or customize actions against viruses/malware
- Detect all macro viruses/malware and remove them or use heuristic rules to remove them

Attachment blocking

- Block named attachments or block attachments by file type

Content filtering

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

Anti-spam rules

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

Quarantine

- Set ScanMail to quarantine suspect email messages

- Query logs for quarantine events and resend quarantined messages when you decide they are safe

Web based product console

- Use SSL to access remote servers through a secure product console

Notifications

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

Informative and timely reports and logs

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

Updates

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

What’s New

The following new features are available in ScanMail version 8.0:

Microsoft™ Operations Manager (MOM) 2005 support

This version of ScanMail supports Microsoft Operations Manager (MOM) 2005 which allows you to manage consolidated information for all applications. ScanMail supports the MOM alert function for critical information.

Control Manager Server 3.0 and 3.5 integration

This version of ScanMail supports the following Control Manager versions:

- Control Manager 3.0 (Build 1417) + Service Pack 6 + Hot fix 5032
- Control Manager 3.5 (Build 1234) + Patch 2 (Build 1408)

The communication between ScanMail 8.0 and Control Manager uses a new protocol called the Trend Micro Control Manager Management Communication Protocol (MCP) agent. ScanMail 8.0 no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of ScanMail and Control Manager. ScanMail 8.0 supports Single sign-on from Control Manager. Access the

ScanMail product console directly from the Control Manager product console without typing a separate user name and password for the ScanMail product console.

Supports End User Quarantine (EUQ) integration with Spam Confidence Level (SCL)

On Exchange 2000 Server and Exchange Server 2003, ScanMail 8.0 provides "Integrate with Outlook Junk E-mail" and "Integrate with End User Quarantine" solutions. You can select either solution during installation.

The Spam Confidence Level (SCL) solution uses rating provided by Intelligent Message Filter (IMF). Intelligent Message Filter (IMF) cannot be installed with Exchange 2000 Server, so "Integrate with Outlook Junk E-mail" is not supported on ScanMail installations with Exchange 2000 Server.

Junk E-mail folder integration

In this version of ScanMail, you can select to send detected Spam messages to the standard Outlook folder. The creation of a separate Spam folder is no longer necessary.

Server names in one-time and scheduled reports

The addition of server names to the one-time and scheduled reports allows you to differentiate the report source when managing multiple servers.

Microsoft Exchange Server 2007 support

This version of ScanMail supports the server roles of Microsoft Exchange Server 2007:

- Edge Transport Server Role
- Hub Transport Server Role
- Mailbox Server Role
- Combo Server Role (Mailbox Server + Hub Transport Server)
- Clustered Mailbox Server Role

ScanMail performs different functions on different server roles.

Note: ScanMail does not support the Client Access Server Role.

Basic installation

ScanMail 8.0 support an upgrade form ScanMail 7.0 to ScanMail 8.0 in addition to standard fresh installation and build upgrade.

Installation enhancement

This version of ScanMail includes installation enhancements to streamline the installation process.

- ScanMail 8.0 includes silent installation which completes with a pre-defined text file requiring no prompts for a hands free local deployment. This feature is not available for cluster server deployment.
- Control Manager Agent and End User Quarantine (EUQ) installation is integrated with the ScanMail installation and uninstallation process.

Note: ScanMail 8.0 only supports End User Quarantine (EUQ) with Exchange 2000 Server and Exchange Server 2003.

- ScanMail 8.0 can be installed with a minimum of local administrator privileges.

A new category for unscannable message parts

ScanMail 8.0 separates the unscannable message count from the virus count. Unscannable files can be files that fall outside of the **Scan Restriction Criteria** you define, encrypted files, or password protected files. This version of ScanMail includes a new category called "Unscannable message parts" for unscannable files in Summary, Logs, Real-time Monitor, Reports, and Notifications.

Provides a new quarantine message part action

You have the option of selecting **Quarantine message part** in Virus Scan, Attachment Blocking, and Content Filtering. In previous version of ScanMail only **Quarantine entire message** was available.

Content filter log enhancement

This version of ScanMail displays the keyword in content filtering logs when there is a match. If the keyword or regular express is too long to display, logs display truncated information.

IntelliTrap

This version of ScanMail incorporates IntelliTrap technology. Use IntelliTrap to scan for packing algorithms to detect packed files. Enabling IntelliTrap allows ScanMail to take user-defined actions on infected attachments and to send notifications to senders, recipients, or administrators.

Trust Scan

Real-time scan is able to skip scanning email messages at the store level when the message has been scanned by ScanMail at the Hub Transport Level. This feature is available for ScanMail with Exchange Server 2007.

Once ScanMail scans a message on an Edge or Hub Transport server, ScanMail adds scan information to the message. When the message reaches the Mailbox, ScanMail evaluates the scan information to prevent redundant use of resources. ScanMail only scans the message if the message was scanned with an older scan engine or pattern file or if ScanMail has not previously scanned the message.

Manual Scan and Scheduled Scan enhancement

In ScanMail 8.0 ActiveUpdate does not interrupt Manual Scan or Scheduled Scan.

For Exchange Server 2007, the Manual Scan and Scheduled Scan pages only appear on Combo Server (Hub Transport + Mailbox server role) and Mailbox server roles. ScanMail 8.0 offers incremental scan options only with Exchange Server 2007. There are three options:

- Scan messages delivered during a time period.
- Scan messages with attachments.
- Scan messages that have not been scanned by ScanMail.

Cluster support

ScanMail supports the shared disk cluster model with Exchange 2000 Server and Exchange Server 2003. ScanMail with Exchange Server 2007 supports Single Copy Cluster (SCC) and Cluster Continuous Replication (CCR) models.

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

Note: The CCR model does not keep data consistent when performing failover to another node.

Version Comparison

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

Support	ScanMail 3.82	ScanMail 6.21	ScanMail 7.0	ScanMail 8.0
OS Version	• Windows NT Server 4.0 with Service Pack 3 or above, • Windows 2000 Server with Service Pack 1 or above	• Windows 2000 Server, with Service Pack 1 or above • Windows Server 2003	• Windows 2000 Server, with Service Pack 2 or above • Windows Server 2003	• Windows 2000 Server with Service Pack 4 or above • Windows 2003 Server with Service Pack 1, Service Pack 2, or R2 (32-bit) • Windows Server 2003 with Service Pack 1, Service Pack 2, or R2 (64-bit)
Minimum Exchange Version	• Exchange 5.5 with Service Pack 2	• Exchange 2000 Server Service Pack 1 • Exchange Server 2003	• Exchange 2000 Server Service Pack 3 • Exchange Server 2003	• Exchange 2000 Server with Service Pack 3 or above • Exchange Server 2003 with Service Pack 2 or above • Exchange Server 2007
Scan mechanism	• ESEAPI	• VSAPI 2.0 • VSAPI 2.5	• VSAPI 2.0 • VSAPI 2.5	• VSAPI 2.0 • VSAPI 2.5 • VSAPI 2.6
Exchange Information Store scanning	• Yes	• Yes	• Yes	• Yes
SMTP (Transport) scanning	• Yes	• Yes	• Yes	• Yes
Quarantine Manager	• Yes	• Yes	• Yes	• Yes

TABLE 1-1. ScanMail version comparison

Support	ScanMail 3.82	ScanMail 6.21	ScanMail 7.0	ScanMail 8.0
Active Message Filter	• Mailstore level (outbound) • SMTP level (inbound and outbound messages)	• Inbound and outbound messages	• Integrated as delete function for inbound and outbound messages	• Integrated as delete function for inbound and outbound messages
Notification	• Dependent on ScanMail profile	• Collaborative Data Object	• Collaborative Data Object	• Collaborative Data Object

TABLE 1-1. ScanMail version comparison

Note: Previous versions of ScanMail offered eManager™ as a separate module add-on. ScanMail 7.0 and 8.0 have fully integrated eManager features so that it is no longer necessary to install eManager separately.

ScanMail Technology

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

The Trend Micro Scan Engine

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

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

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

The scan engine provides:

- Real-time multi-threaded scanning

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

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

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

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

Scan Engine Updates

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

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

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

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

The Trend Micro Pattern Files

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest security risks.

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

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

Pattern file numbering

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

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

For the file pattern number 1.786.01:

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

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

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

How the Scan Engine Works with the Pattern File

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

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

About ActiveUpdate

ActiveUpdate provides up-to-date downloads of all ScanMail components over the Internet. ScanMail components include pattern files for viruses/malware and spyware/grayware.

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

Incremental updates of the pattern file

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

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

Using ActiveUpdate with ScanMail

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

Tip: For a more efficient download in a multi-server environment, configure ScanMail to allow other servers to download updates from it. This makes ScanMail a virtual ActiveUpdate server for other servers in your environment that receive incremental updates.

Trend Micro IntelliScan™

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

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

Trend Micro ActiveAction™

ActiveAction identifies virus/malware 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/malware. When ScanMail detects a virus/malware, it takes the recommended action (clean, quarantine message part, delete entire message) on the virus/malware type to protect your environment's vulnerable points.

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

Using ActiveAction provides the following benefits:

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

Spam engine and spam pattern files

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

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

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

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

Chapter 2

Installing and Removing ScanMail

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

This chapter includes information about:

Minimum Requirements

To install ScanMail with Microsoft™ Exchange 2000 Server or Microsoft Exchange Server 2003 you need the following minimum system requirements:

Processor

Intel™ Pentium II 266 MHz or higher processor

(Intel Pentium or compatible 733MHz processor recommended)

Memory

512MB RAM, 1GB RAM recommended

Disk space

700MB free disk space, 1GB free disk space recommended

(About half of the space is for temporary files.)

Operating System

- Microsoft Windows 2000 Server with Service Pack 4
- Microsoft Windows Server 2003 with Service Pack 1 (32-bit)
- Microsoft Windows Server 2003 R2 (32-bit)
- Microsoft Windows Server 2003 with Service Pack 2 (32-bit)

Mail Server

- Microsoft Exchange 2000 Server with Service Pack 3 or above
- Microsoft Exchange Server 2003 with Service Pack 2 or above

Web Server

- Microsoft Internet Information Services (IIS) 5.0
- Microsoft Internet Information Services (IIS) 6.0
- Apache Web server 2.0

Browser

A Java-enabled Web browser that supports frames.

- Microsoft Internet Explorer 6.0 and 7.0
- Mozilla Firefox™ 2.0

Java™ software

Java 2 Runtime Environment version 1.4.1_02 or above

Note: You can download this software from http://java.sun.com/products/archive/j2se/1.4.1_02/index.html

To install ScanMail with Microsoft Exchange Server 2007 you need the following minimum system requirements:

Processor

- x64 architecture-based processor that supports Intel Extended Memory 64 Technology (Intel EM64T)
- x64 architecture-based computer with AMD 64-bit processor that supports AMD64 platform

Memory

1GB RAM, 2GB RAM recommended (5MB of RAM per mailbox)

Disk space

1GB free disk space, 1.1GB free disk space recommended

(About half of the space is for temporary files.)

Operating System

- Microsoft Windows Server 2003 with Service Pack 1 (64-bit)
- Microsoft Windows Server 2003 R2 (64-bit)
- Microsoft Windows Server 2003 with Service Pack 2(64-bit)

Mail Server

Microsoft Exchange Server 2007

Web Server

- Microsoft Windows Server 2003 requires IIS 6.0
- Apache Web server 2.0

Browser

A Java-enabled Web browser that supports frames, such as

- Microsoft Internet Explorer 6.0 and 7.0
- Mozilla Firefox 2.0

Java software

Java 2 Runtime Environment version 1.4.1_02 or above

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

For cluster installation:

- Shared disk cluster model with Exchange 2000 Server and Exchange Server 2003
- Exchange Server 2007 with Single Copy Cluster (SCC) model
- Exchange Server 2007 with Cluster Continuous Replication (CCR) model

Before you Begin

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

Pilot installation

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

To conduct a pilot installation:

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

Creating an appropriate test site

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

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

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

Preparing a Rollback plan

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

Backing up and restoring ScanMail configurations

Before making any changes, back up ScanMail configurations.

To back up ScanMail and configurations for an Exchange 2000/2003 environment:

1. Stop ScanMail Master Service on the target server which has the database you want to backup.
2. Copy the Conf.mdb, Log.mdb, or Report.mdb file.

To back up ScanMail and configurations for an Exchange 2007 environment:

1. Stop ScanMail Master Service and SQL Server (SCANMAIL) Service on the target server which has the database you want to backup.
2. Copy the Conf.mdf, Log.mdf, or Report.mdf file.

To restore ScanMail configurations for an Exchange 2000/2003 environment:

1. Stop the ScanMail Master Service on the target server which you want to restore the configurations to.
2. Replace the Conf.mdf, Log.mdf, or Report.mdf file.
3. Start ScanMail Master Service.

To restore ScanMail configurations for an Exchange 2007 environment:

1. Stop the ScanMail Master Service and SQL Server (SCANMAIL) Service on the target server which you want to restore the configurations to.
2. Delete Conf.ldf, or Log.ldf, or Report.ldf.
3. Replace the Conf.mdf, Log.mdf, or Report.mdf file.
4. Start SQL Server (SCANMAIL) Service and ScanMail Master Service.

Executing and evaluating your pilot installation

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

Deployment Strategy

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

When deploying and configuring ScanMail on your LAN segments consider:

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

Planning for network traffic

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

ScanMail generates network traffic when it does the following:

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

ScanMail increases the burden on the CPU when it scans email messages arriving at the Exchange server in real time or during scheduled and manual scans. Unlike some other antivirus products, ScanMail uses multi-threaded scanning which reduces the CPU burden.

Deploying ScanMail to multiple servers

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

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

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

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

TABLE 2-1. Deploying ScanMail to Front-End and Back-End Servers

Server Role	Recommendation
Edge Transport server: • No access to Active Directory • XML-based routing • Port 25 SMTP relay • Decentralized management • Message hygiene • Information that defines configuration, connectors, recipients, SMTP settings and agent settings are files that are on the server and are updated to the Edge Transport server role periodically. • Deploys in a standalone manner • There are two primary deployment servers for the Edge Transport server role: (1) In the organization's network perimeter, directly facing the Internet, (2) Behind a third-party mail server directly facing the Internet	• Set Edge Transport servers to perform real-time virus scan • Set Edge Transport servers to update through Trend Micro ActiveUpdate, and to regularly perform scheduled update for protection against new security risks
Hub Transport server: • All transport components, such as Categorizer, can be installed and configured on hardware that is separate from the Mailbox server roles or the Public Folder server role. • Intra-organizational server role for mail transport in an organization and the Internet • Centralized management • Has direct access to Active Directory • Handles all authentications • All routing is based on Active Directory • Uses Port 25 SMTP relay and message relay • Can be load balanced	• Set Hub Transport servers to perform real-time virus scan • Set the Trend Micro ActiveUpdate server as the source of component updates for the Hub Transport server • Set Mailbox servers to use the Hub Transport server as the source of updates, which decreases overall network traffic and reduces exposure to the Internet

TABLE 2-2. Deploying ScanMail to Front-End and Back-End Servers

Server Role	Recommendation
Mailbox server: • Located within the local network, behind the network perimeter and shielded from the Internet • Hosts mailbox databases • Delivers and stores email messages to client mailboxes on the Information Store	• Set Mailbox servers to perform virus scan with vigorous screening options • Regularly perform scheduled scans on Exchange mailboxes to prevent security risks from creeping in from unexpected sources not covered in your configurations

TABLE 2-2. Deploying ScanMail to Front-End and Back-End Servers

Deploying ScanMail to multiple Local Area Network (LAN) segments

Large enterprises might have multiple Exchange servers on different LAN segments separated by the Internet. In these cases, Trend Micro recommends installing ScanMail on each LAN segment separately.

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

Preparing to Install

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

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

The following table displays the minimum privileges required for a ScanMail fresh install.

Exchange Version	Minimum Privileges	Feature Limitation Without Domain Administrator Privileges
Exchange 2000 Server and Exchange Server 2003	Local Administrator and Domain User	Cannot activate EUQ and Server Management
Exchange Server 2007 Edge Transport	Local Administrator	N/A
Exchange Server 2007 Hub/Mailbox/Cluster	Local Administrator and Exchange Organization Administrator	N/A

TABLE 2-3. Fresh Install Minimum Privileges

Configuration Exceptions When You Upgrade

When you upgrade from ScanMail 7.0 to ScanMail 8.0 the installation program uses your previous settings during installation. However, there are three exceptions that behave differently.

End User Quarantine (EUQ)

Once the installation process completes, you cannot switch between **Integrate with Outlook Junk E-mail** and **Integrate with End User Quarantine**. The following table displays the EUQ settings when you use an account with domain administrator privileges to perform an upgrade.

Exchange Version	If you select Integrate with Outlook Junk E-mail during installation	If you select Integrate with End User Quarantine during installation
Exchange 2000 Server	Keep all previous EUQ settings	Keep all previous EUQ settings

TABLE 2-4. EUQ Settings with Domain Administrator Privileges

Exchange Version	If you select Integrate with Outlook Junk E-mail during installation	If you select Integrate with End User Quarantine during installation
Exchange Server 2003	• Remove EUQ mailbox • Remove EUQ account • Merge previous EUQ approved senders list with Junk E-mail safe senders list	Keep all previous EUQ settings

TABLE 2-4. EUQ Settings with Domain Administrator Privileges

The following table displays EUQ settings when you use an account with local administrator privileges to perform an upgrade.

Exchange Version	If you select Integrate with Outlook Junk E-mail during installation	If you select Integrate with End User Quarantine during installation
Exchange 2000 Server	Keep all previous EUQ settings	Keep all previous EUQ settings
Exchange Server 2003	• EUQ mailbox remains because privileges are insufficient for deletion • EUQ account remains because privileges are insufficient for deletion • Spam Maintenance menu does not appear • Merge previous EUQ approved senders list with Junk E-mail safe senders list • Spam Maintenance menu does not appear in the product console	Keep all previous EUQ settings

TABLE 2-5. EUQ Settings with Local Administrator Privileges

Trend Micro Control Manager Agent

This version of ScanMail supports Trend Micro Control Manager™ 3.0 with Service Pack 6 and Hot fix 5032 and Control Manager 3.5 with Patch 2. The communication mechanism between the Control Manager server and Control Manager agent is different from previous versions. The installation process includes settings for migration. The following table displays the Control Manager settings when you perform an upgrade.

Exchange Version	If you select Register ScanMail Agent to Control Manager server	If you select Register ScanMail Agent to Control Manager server
Exchange 2000 Server / Exchange Server 2003	• Unregister from original Control Manager server • Uninstall ScanMail 7.0 Control Manager Agent • Install ScanMail 8.0 Control Manager Agent • Register with new settings • Newly registered ScanMail servers appear in the **ScanMail for Microsoft Exchange** folder. This folder is automatically created by the Control Manager server when the ScanMail agent first registers to the Control Manager server.	• Unregister from original Control Manager server • Uninstall ScanMail 7.0 Control Manager Agent • Remove all Control Manager Agent information from database.

TABLE 2-6. Control Manager Settings

Note: ScanMail 8.0 removes the ScanMail 7.0 Control Manager Agent and installs the Trend Micro Management Communication Protocol (MCP) Agent. The MCP agent and the previous agent use different protocols, so the original hierarchy does not transfer to the MCP agent.

Activation Code

When you perform an upgrade, ScanMail always uses the new activation code.

Pre-Installation Checklist

Item	Notes
Minimum Account privileges	• For Exchange 2000 Server and Exchange Server 2003 you need Local Administrator and Domain User privileges. However, you need to activate End User Quarantine and Server management later with an account with Domain Administrator privileges • For Exchange Server 2007 Hub / Mailbox / Cluster you need Local Administrator and Exchange Organization Administrator privileges. However, you need to activate End User Quarantine later with an account with Domain Administrator privileges • For Exchange Server 2007 Edge Transport you need Local Administrator privileges.
Restart	You do not need to stop Exchange services before installing or restart them after a successful installation. **Warning**: If you are installing ScanMail on a server which is running lockdown tools (such as typically implemented for Windows 2000 server with IIS 5.0), remove the lockdown tool so that it does not disable IIS service and cause the installation to be unsuccessful.
Registration Key and Activation Code	During installation, the setup program prompts you to type an Activation Code. You can use the Registration Key that came with ScanMail to obtain an Activation Code online from the Trend Micro Web site. The setup program provides a link to the Trend Micro Web site. If you do not Activate your product during registration, you can do so at a later time from the product console. However, until you activate ScanMail, ScanMail will only provide a limited service.
Proxy server	During installation, the setup program prompts you to enter proxy information. If a proxy server handles Internet traffic on your network, you must type the proxy server information, your user name, and your password to receive pattern file and scan engine updates. If you leave the proxy information blank during installation, you can configure it at a later time from the product console.

TABLE 2-7. Pre-installation Checklist

Performing a Fresh Install

If you do not have a previous version of ScanMail installed on your Exchange server, then you need to perform a fresh installation. Before beginning your installation, consult the pre-installation checklist, Table 2-7.

Installing on a cluster

You can install ScanMail on Windows 2000 or 2003 clusters.

- Windows 2000 cluster (Single quorum device cluster) with Exchange 2000 Server or Exchange Server 2003
- Windows 2003 cluster (Single quorum device cluster) with Exchange Server 2003 or Exchange Server 2007 SSC model
- Windows 2003 cluster (Majority node set cluster) with Exchange Server 2007 CCR model.

For cluster installation, ScanMail adds a resource for each virtual server and installs all nodes in the cluster simultaneously.

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

ScanMail supports Windows NTFS volume mount points feature, you can surpass the 26-drive-letter limitation. ScanMail can install on the mount point disk. For example, if your shared disk is G, mount point disk is G:\mountpoint disk. You can select mount disk to install data on default path or customized file path.

Upgrading to ScanMail 8.0

To upgrade ScanMail, run the setup program. Before beginning your installation, consult the pre-installation checklist, Table 2-7.

ScanMail for Microsoft Exchange 8.0 supports upgrading from ScanMail version 7.0. If you are currently using ScanMail 7.0, the setup program automatically removes it and installs ScanMail 8.0.

Note: If you have a version of ScanMail that does not support upgrading, remove it using the same version of the uninstallation program that you used to install it. For example, if you are using ScanMail 6.1, uninstall using the ScanMail 6.1 uninstallation program.

When upgrading, if ScanMail 8.0 has configuration settings similar to the previous version, then the upgraded version maintains these customized configurations. However, when ScanMail 7.0 has no equivalent configuration setting, it installs and uses the Trend Micro default configurations.

Upgrade effect on logs and folders

Upgrading to ScanMail 8.0 has the following effects on logs and folders:

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

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

- The quarantine and backup folders are retained during upgrading.

Upgrade effect on configurations and actions

Upgrading to ScanMail 8.0, has the following effects on ScanMail configurations and actions:

- **End User Quarantine**—The approved sender lists are maintained in the upgraded version.
- **Quarantine Message Part**—A new option to quarantine message part is available for selection.

Upgrading on Clusters

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

WARNING! *Never upgrade a cluster during failover.*

When upgrading on clusters ScanMail does not stop Exchange System Attendant service and IIS admin when you perform a version upgrade or build upgrade.

Running the Setup Program

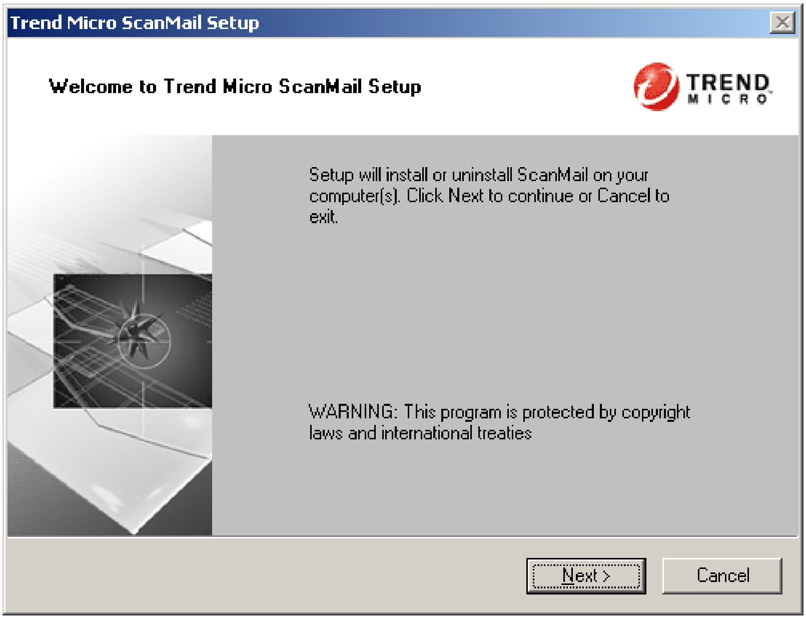
The following sections describe the process for typical installations. At any time, you can click **Cancel** from the setup program. When the "Exit Setup" dialog box displays, click **Yes** to cancel the installation. Canceling the installation removes all files and registry changes from your operating system, except files in the temp directory.

Installation for Exchange 2000 Server and Exchange Server 2003

1. Select a source for the setup program:
   a. Trend Micro Web site.
      i. Download ScanMail from the Trend Micro Web site.
      ii. Unzip the file to a temporary directory
      iii. Run setup.exe to install ScanMail
   b. The Trend Micro Enterprise Solution CD.
      i. Insert the CD and follow the online instructions.

   The **Welcome to Trend Micro ScanMail Setup** screen appears.

2. Click **Next** to continue the installation. The **License Agreement** screen appears.



Trend Micro ScanMail Setup

Welcome to Trend Micro ScanMail Setup

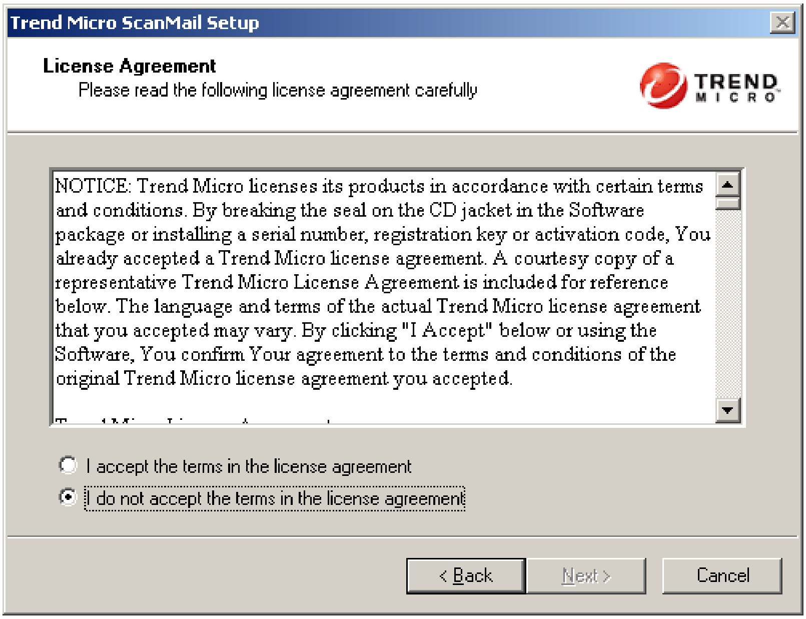
Setup will install or uninstall ScanMail on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties

FIGURE 2-1. Welcome screen

3. Click **I Accept the terms in the license agreement** to agree to the terms of the agreement and continue installation. Click **Next** to continue. The **Select an Action** screen appears.

Note: If you do not accept the terms, click **I do not accept the terms in the license agreement.** This terminates the Setup without modifying your operating system.



Trend Micro ScanMail Setup

License Agreement

Please read the following license agreement carefully

NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or installing a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

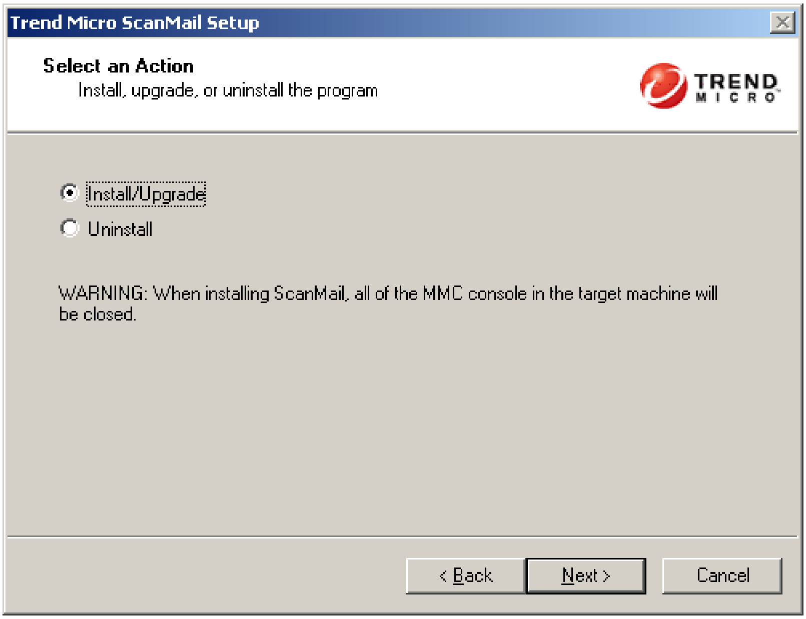
○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

FIGURE 2-2. License Agreement screen

4. Select one of the following actions:
   - Select **Install/Upgrade** to:
     - Perform a fresh install
     - Upgrade ScanMail 7.0 to ScanMail 8.0. For more information about upgrading, see *Upgrading to ScanMail 8.0* starting on page 2-18.
     - Upgrade the ScanMail 8.0 beta version to the ScanMail 8.0 release version.
   - Select **Uninstall** if you want to remove ScanMail from your server. For more information about uninstalling, see *Removing ScanMail* starting on page 2-80.

   Click **Next** to continue. The **Server Role Selection** screen appears.


Trend Micro ScanMail Setup

Select an Action

Install, upgrade, or uninstall the program

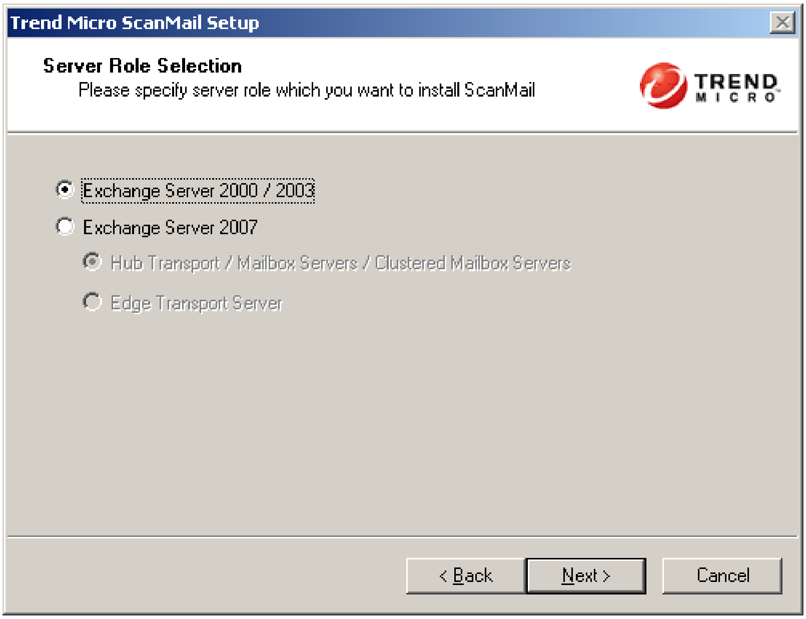
● Install/Upgrade

○ Uninstall

WARNING: When installing ScanMail, all of the MMC console in the target machine will be closed.

FIGURE 2-3. Select an installation action screen

5. Select **Exchange Server 2000/2003** to install ScanMail with Exchange 2000 Server or Exchange Server 2003. Click **Next** to continue. The **Select Target Server(s)** screen appears.



Trend Micro ScanMail Setup

Server Role Selection

Please specify server role which you want to install ScanMail

● Exchange Server 2000 / 2003

○ Exchange Server 2007

● Hub Transport / Mailbox Servers / Clustered Mailbox Servers

○ Edge Transport Server

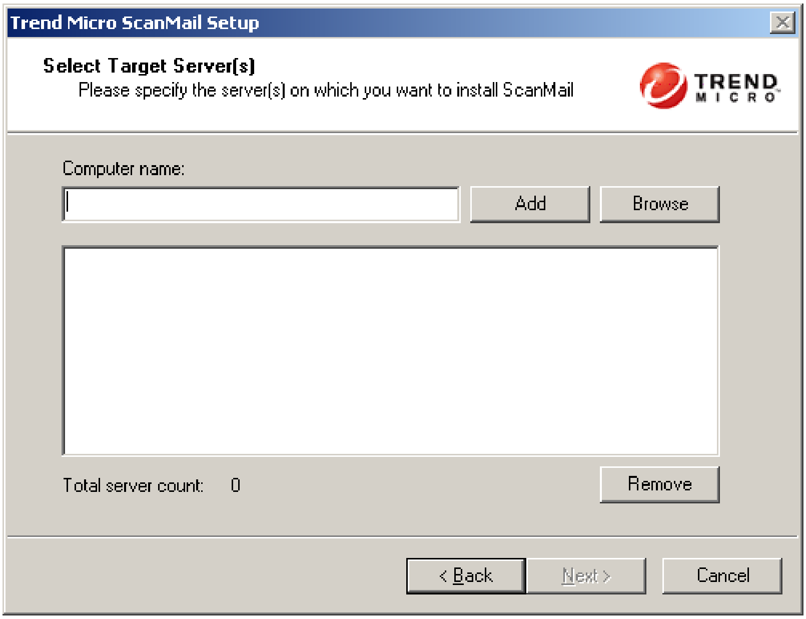
FIGURE 2-4. Server Role Selection for Exchange 2000 Server and Exchange Server 2003 screen

6. Select the computers to which you want to install ScanMail by doing one of the following:

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

   a. Click **Remove** to remove a server from the list.

b. Click **Next** to save your list of target servers and continue the installation. The **Log On** screen appears.



Trend Micro ScanMail Setup

Select Target Server(s)

Please specify the server(s) on which you want to install ScanMail

Computer name:

Total server count: 0

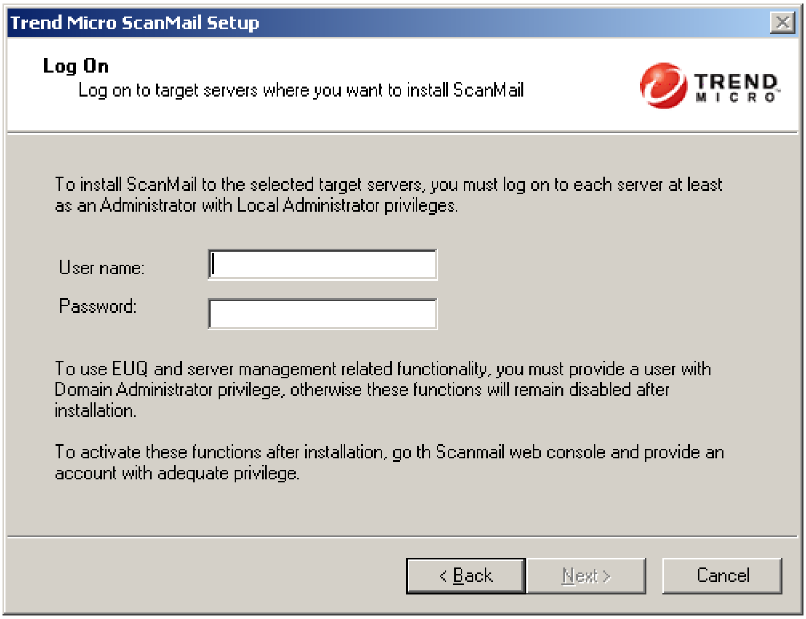
FIGURE 2-5. Select Target Server(s) screen

The setup program can install ScanMail to a number of single servers or to all the computers in a domain. Use an account with the appropriate privileges to access every target server.

Installing to clusters

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

7. Log on to the target servers where you want to install ScanMail. Type the user name and password to log on to the target server to install ScanMail. Click **Next** to continue. The **Configure Shared/Target Directory** screen appears.



Trend Micro ScanMail Setup

Log On

Log on to target servers where you want to install ScanMail

To install ScanMail to the selected target servers, you must log on to each server at least as an Administrator with Local Administrator privileges.

User name:

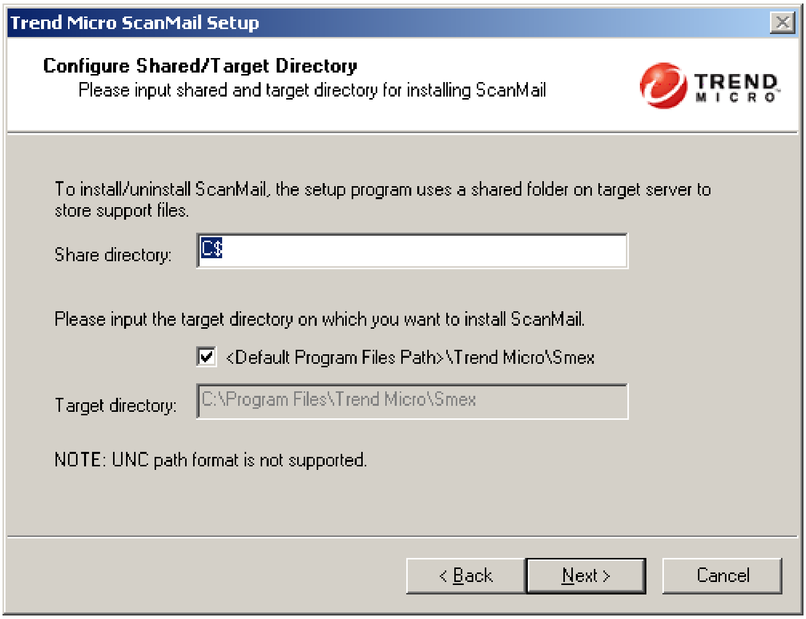
Password:

To use EUQ and server management related functionality, you must provide a user with Domain Administrator privilege, otherwise these functions will remain disabled after installation.

To activate these functions after installation, go th Scanmail web console and provide an account with adequate privilege.

FIGURE 2-6. Log On screen

8. Type the directory share name for which the specified user has access rights or keep the default temporary share directory, C$. The setup program uses the share directory to copy temporary files during installation and is only accessible to the administrator. Type the directory path on the target server where you will install ScanMail. Click **Next** to continue. The **Checking Target Server System Requirements** screen appears.



Configure Shared/Target Directory

Please input shared and target directory for installing ScanMail

To install/uninstall ScanMail, the setup program uses a shared folder on target server to store support files.

Share directory: C$

Please input the target directory on which you want to install ScanMail.

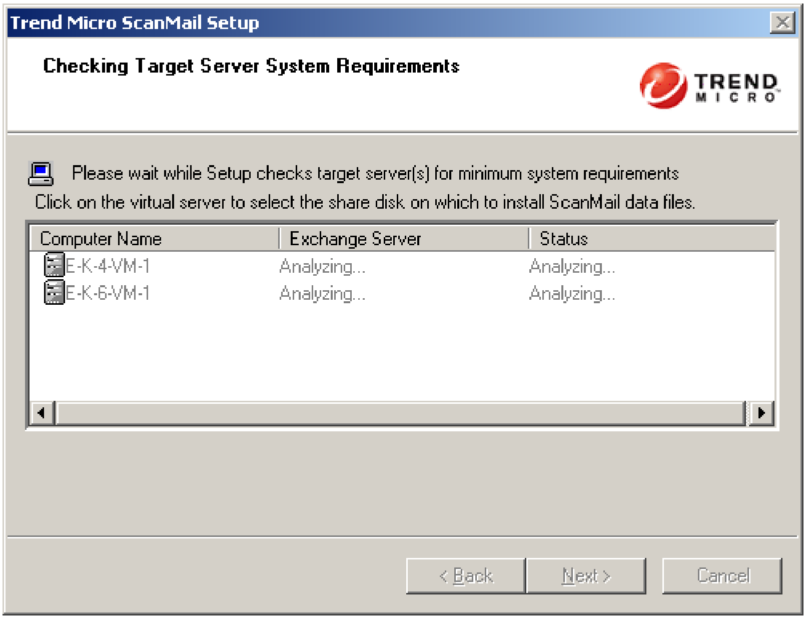
☑ <Default Program Files Path>\Trend Micro\Smex

Target directory: C:\Program Files\Trend Micro\Smex

NOTE: UNC path format is not supported.

FIGURE 2-7. Configure Shared/Target Directory screen

9. Double-click the virtual server on which to install ScanMail data files. Review the settings and click **Next** to continue. The **Select Web Server Type** screen appears.



Trend Micro ScanMail Setup

Checking Target Server System Requirements

Please wait while Setup checks target server(s) for minimum system requirements

Click on the virtual server to select the share disk on which to install ScanMail data files.

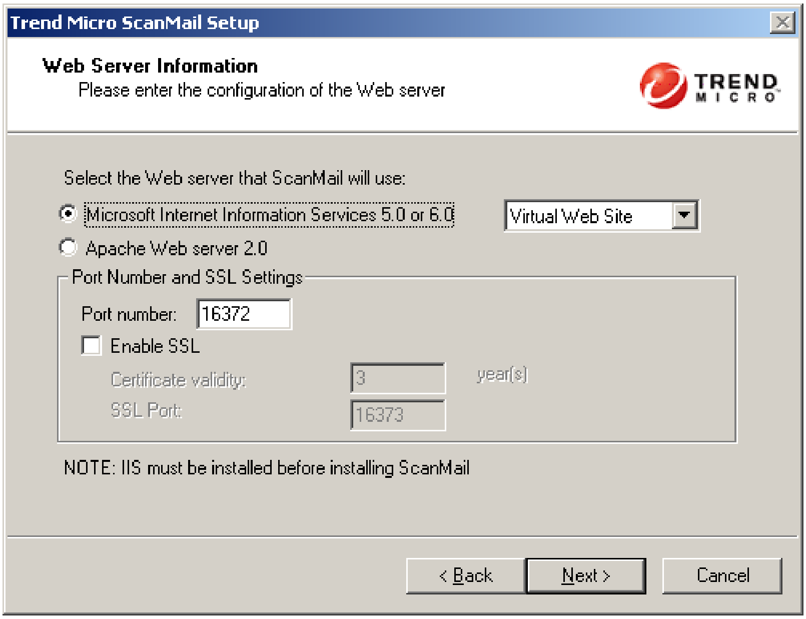
Computer Name	Exchange Server	Status
E-K-4-VM-1	Analyzing...	Analyzing...
E-K-6-VM-1	Analyzing...	Analyzing...

FIGURE 2-8. **Checking Target server System Requirements screen**

10. Select one of following for ScanMail to use as a Web server.

- **Microsoft Internet Information Services (IIS)**—If you are using Windows 2003 Server, you need IIS 6.0. If you are using Windows 2000 Server, you need IIS 5.0. Select **IIS Default Web Site** or **IIS Virtual Web Site**.
- **Apache Web server 2.0**—If an Apache Web server version 2.0 or later is not found, the setup program will automatically install Apache 2.0. IIS Web options are grayed-out.

Next to **Port number** type the port to use as a listening port for this server. You also have the option of enabling Secure Socket Layer (SSL) security. Select **Enable SSL** check box to use this feature. Click **Next** to continue. The **Connection Settings** screen appears.



Trend Micro ScanMail Setup

Web Server Information

Please enter the configuration of the Web server

Select the Web server that ScanMail will use:

● Microsoft Internet Information Services 5.0 or 6.0 — Virtual Web Site

○ Apache Web server 2.0

Port Number and SSL Settings

Port number: 16372

□ Enable SSL

Certificate validity: 3 year(s)

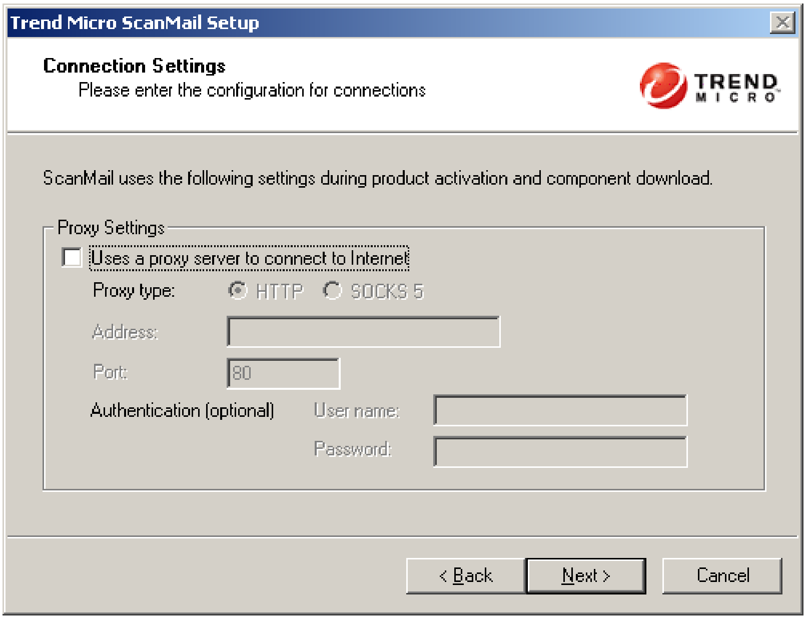
SSL Port: 16373

NOTE: IIS must be installed before installing ScanMail

FIGURE 2-9. Select a Web server screen

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

11. If a proxy server handles Internet traffic on your network, select **Use a proxy server to connect to Internet** and then type the URL address and port number that your proxy uses. By default, the proxy server is disabled. If you want to use SOCKS5 for secure communication behind the proxy, select **Use SOCKS5**. If your proxy requires authentication, type the user name and password used for authentication. Click **Next** to continue. The **Product Activation** screen appears.



Trend Micro ScanMail Setup

Connection Settings

Please enter the configuration for connections

ScanMail uses the following settings during product activation and component download.

Proxy Settings

☐ Uses a proxy server to connect to Internet

Proxy type: ● HTTP ○ SOCKS 5

Address:

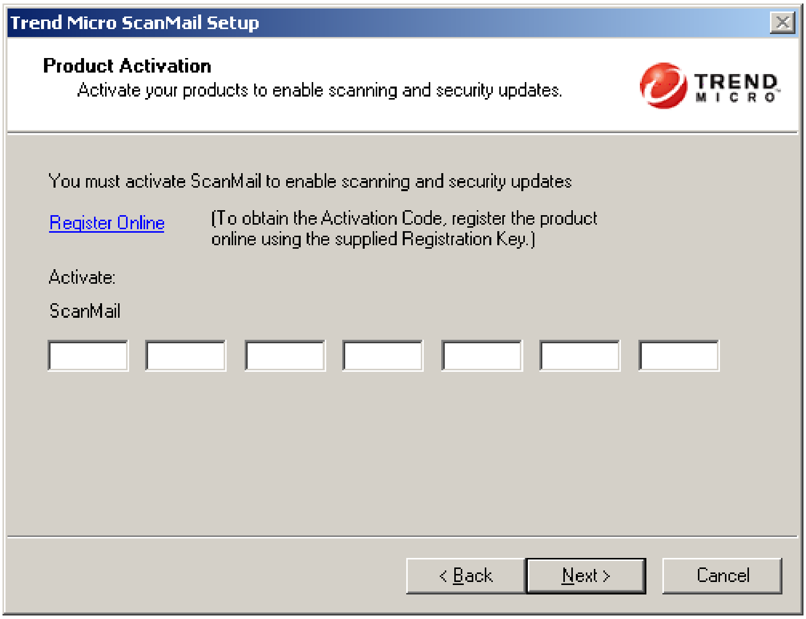
Port: 80

Authentication (optional) User name:

Password:

FIGURE 2-10. Connection settings screen

12. In the **Product Activation** screen, type the full version license for this product's version. Click **Next** to continue. The **World Virus Tracking Program** screen appears.



Trend Micro ScanMail Setup

Product Activation

Activate your products to enable scanning and security updates.

You must activate ScanMail to enable scanning and security updates

Register Online (To obtain the Activation Code, register the product online using the supplied Registration Key.)

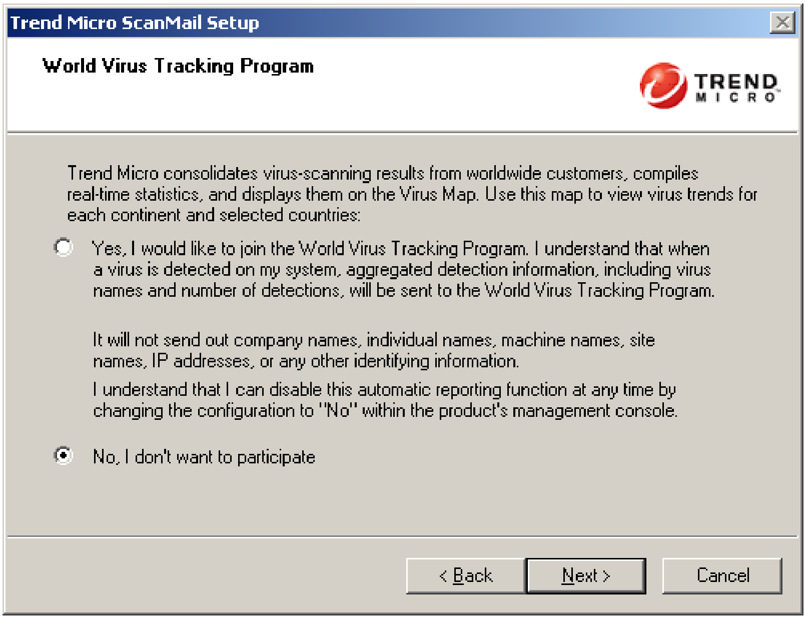
Activate:

ScanMail

FIGURE 2-11. Product Activation screen

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

13. Read the statement and click **Yes** to enroll. If you decline to participate, you can still proceed with the installation. Click **Next** to continue. The **End User Quarantine** screen appears.



Trend Micro ScanMail Setup

World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries:

○ Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, aggregated detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program.

It will not send out company names, individual names, machine names, site names, IP addresses, or any other identifying information.

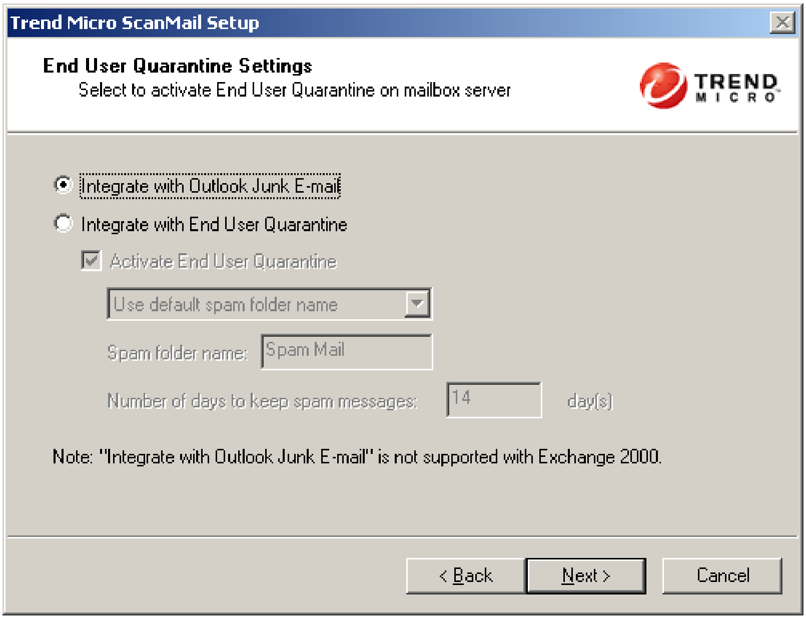
I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

● No, I don't want to participate

FIGURE 2-12. World Virus Tracking Program screen

14. Select one of the following folder options for storing ScanMail detected spam messages:
    - Select **Integrate with Outlook Junk E-mail** to send all ScanMail detected spam messages to the Junk E-mail folder in Outlook.
    - Select **Use Spam Folder** to create a ScanMail Spam Folder in Outlook. You can also specify a different **Spam Folder Name**.

    Click **Next** to continue. The **Control Manager Server Settings** screen appears.


Trend Micro ScanMail Setup

End User Quarantine Settings

Select to activate End User Quarantine on mailbox server

● Integrate with Outlook Junk E-mail

○ Integrate with End User Quarantine

☑ Activate End User Quarantine

Use default spam folder name

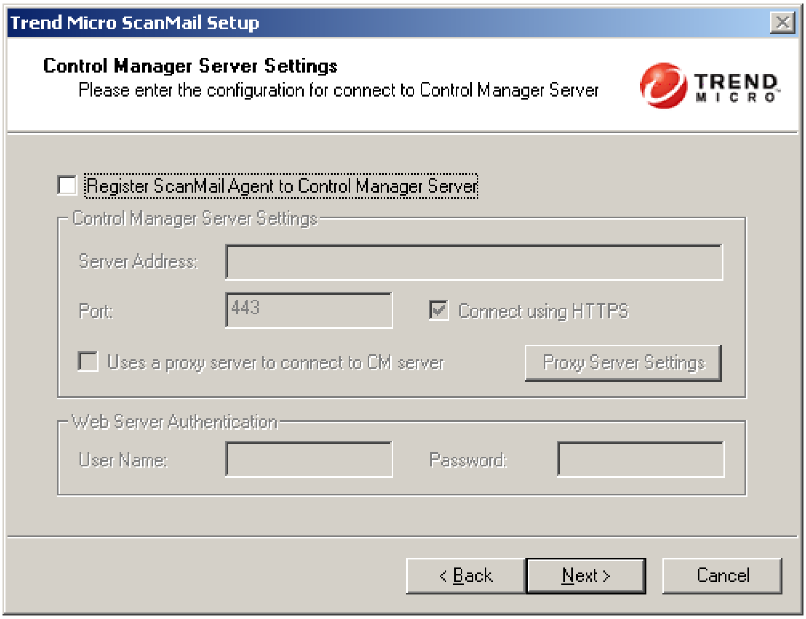
Spam folder name: Spam Mail

Number of days to keep spam messages: 14 day(s)

Note: "Integrate with Outlook Junk E-mail" is not supported with Exchange 2000.

FIGURE 2-13. End User Quarantine Settings screen

15. Specify Control Manager server settings and specify the **Proxy Server Settings** if you use a proxy server between the ScanMail server and Control Manager server. Click **Next** to continue. The **Web Management Console Administrator Account** screen appears.



Trend Micro ScanMail Setup

Control Manager Server Settings

Please enter the configuration for connect to Control Manager Server

□ Register ScanMail Agent to Control Manager Server

Control Manager Server Settings

Server Address:

Port: 443

☑ Connect using HTTPS

□ Uses a proxy server to connect to CM server

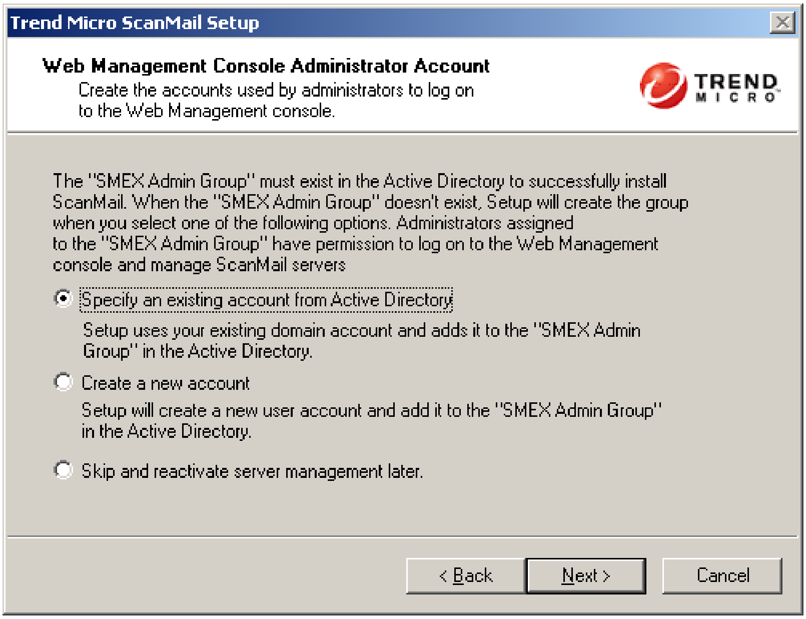
Web Server Authentication

User Name:

Password:

FIGURE 2-14. Control Manager Server Settings screen

16. Use this screen to select whether you want to create a new administrator account or use an existing account from the Active Directory. You can also select **Skip and reactivate server management later**.



Trend Micro ScanMail Setup

Web Management Console Administrator Account

Create the accounts used by administrators to log on to the Web Management console.

The "SMEX Admin Group" must exist in the Active Directory to successfully install ScanMail. When the "SMEX Admin Group" doesn't exist, Setup will create the group when you select one of the following options. Administrators assigned to the "SMEX Admin Group" have permission to log on to the Web Management console and manage ScanMail servers

● Specify an existing account from Active Directory

Setup uses your existing domain account and adds it to the "SMEX Admin Group" in the Active Directory.

○ Create a new account

Setup will create a new user account and add it to the "SMEX Admin Group" in the Active Directory.

○ Skip and reactivate server management later.

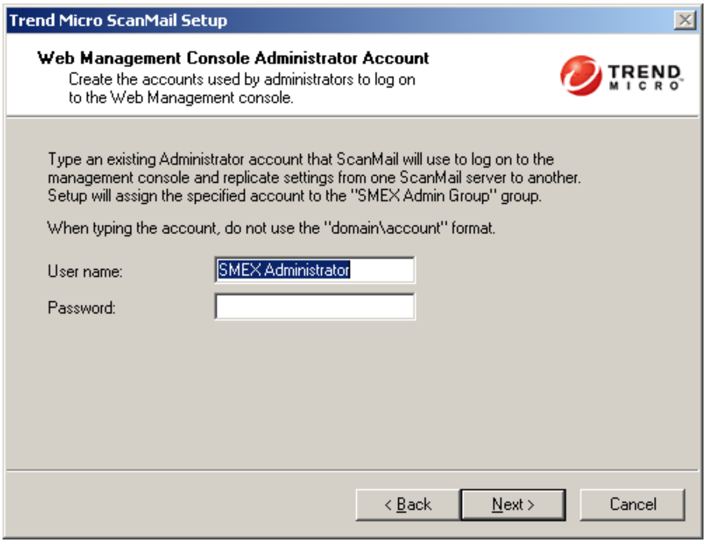
FIGURE 2-15. **Web Management Console Administrator Account screen**

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

You must use a Windows administrator account that has domain administrator privileges on the Log On screen to create the product console log on accounts. If you do not have domain administrator privileges, you can activate it from the ScanMail product console later.

a. Select one of the following to configure a product console account.

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



Web Management Console Administrator Account

Create the accounts used by administrators to log on to the Web Management console.

Type an existing Administrator account that ScanMail will use to log on to the management console and replicate settings from one ScanMail server to another. Setup will assign the specified account to the "SMEX Admin Group" group.

When typing the account, do not use the "domain\account" format.

User name: SMEX Administrator

Password:

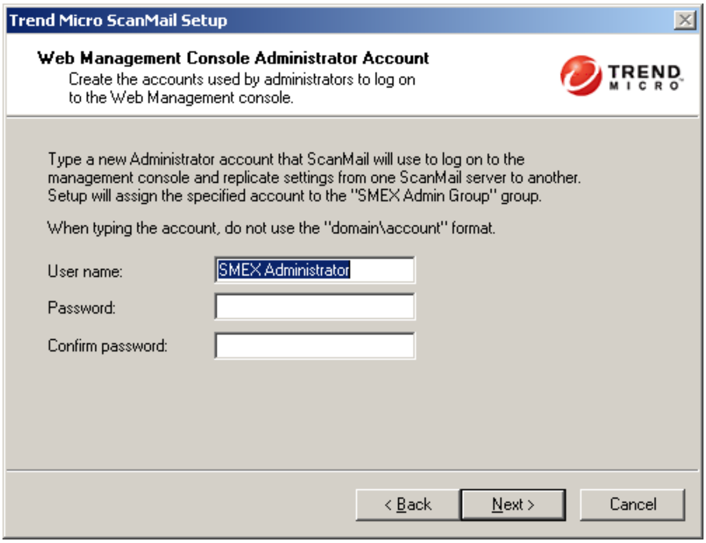
FIGURE 2-16. Specify information about an existing account

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

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

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

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



Trend Micro ScanMail Setup

Web Management Console Administrator Account

Create the accounts used by administrators to log on to the Web Management console.

Type a new Administrator account that ScanMail will use to log on to the management console and replicate settings from one ScanMail server to another. Setup will assign the specified account to the "SMEX Admin Group" group.

When typing the account, do not use the "domain\account" format.

User name: SMEX Administrator

Password:

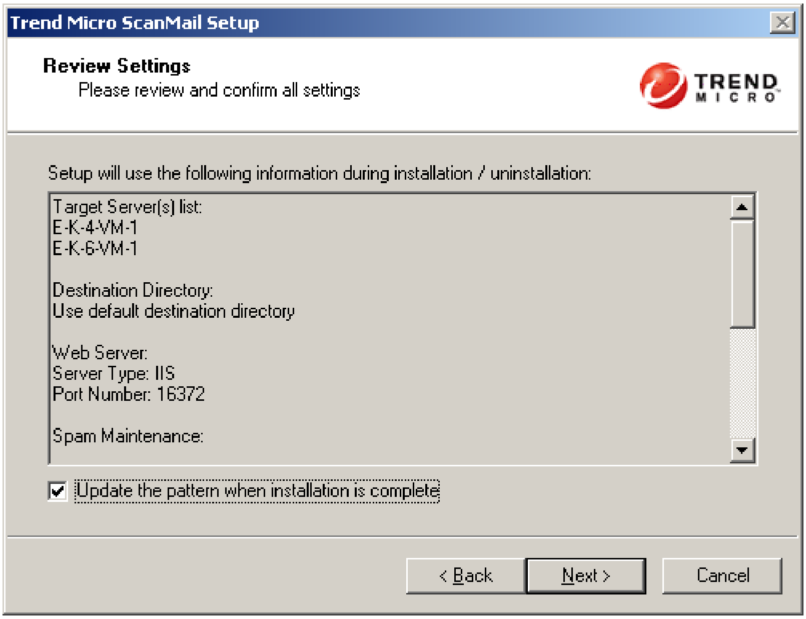
Confirm password:

FIGURE 2-17. Web Management Console Administrator Account screen

- Select **Skip and reactivate server management later**. You can click **Server Management** from the product console to activate this feature.

b. Click **Next** to continue. The **Review Settings** screen appears.

17. Review your settings and click **Next**. The **Installation Progress** screen appears.



Trend Micro ScanMail Setup

Review Settings

Please review and confirm all settings

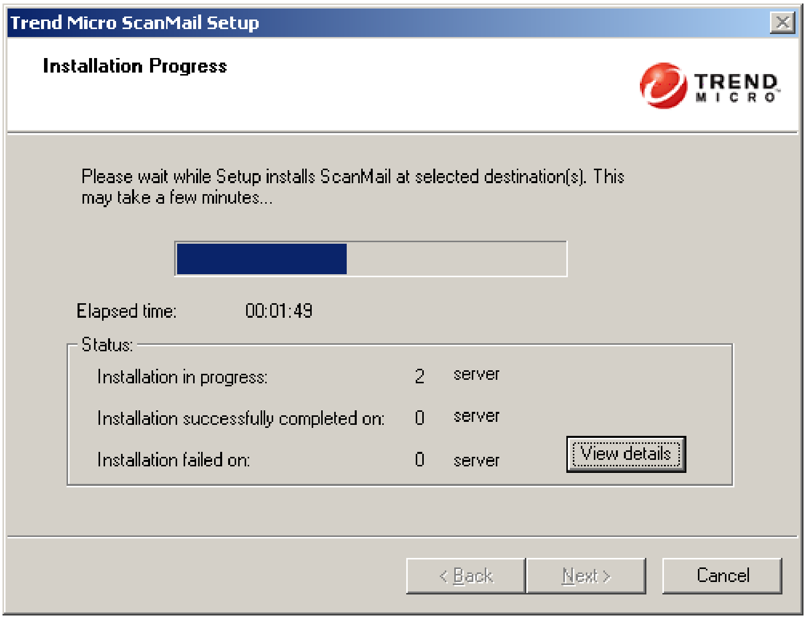
Setup will use the following information during installation / uninstallation:

```
Target Server(s) list:
E-K-4-VM-1
E-K-6-VM-1

Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

Spam Maintenance:
```

☑ Update the pattern when installation is complete

FIGURE 2-18. Review Settings screen

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



Trend Micro ScanMail Setup

Installation Progress

Please wait while Setup installs ScanMail at selected destination(s). This may take a few minutes...

Elapsed time: 00:01:49

Status:

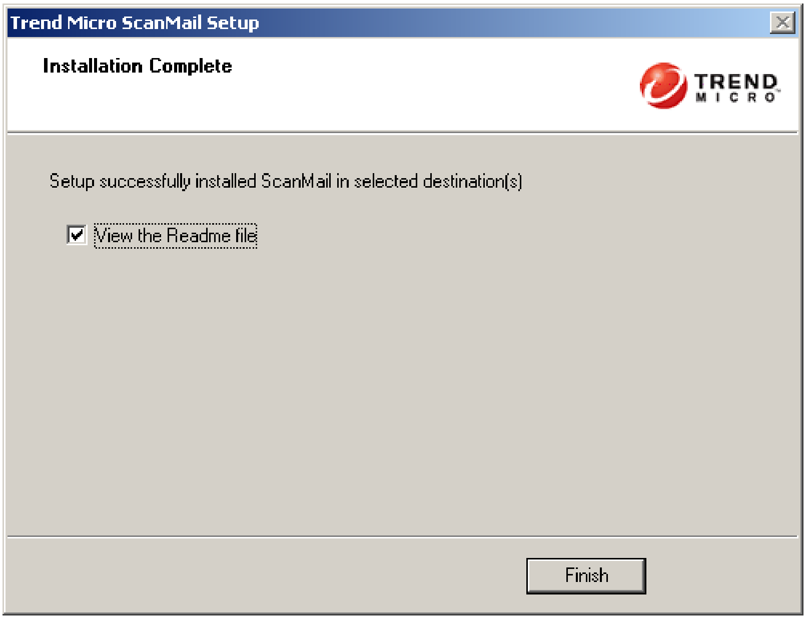
Installation in progress: 2 server

Installation successfully completed on: 0 server

Installation failed on: 0 server

FIGURE 2-19. Installation progress screen

19. This screen informs you that the installation was successful. Click **Finish** to exit the setup program and the Readme file displays.



Trend Micro ScanMail Setup

Installation Complete

Setup successfully installed ScanMail in selected destination(s)

☑ View the Readme file

FIGURE 2-20. Installation Complete screen

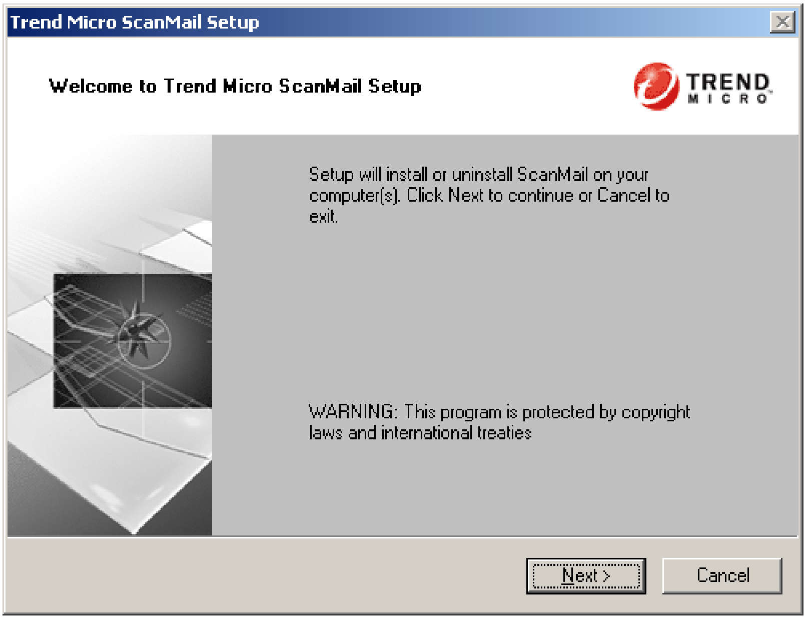
Installation with Exchange Server 2007 Hub Transport / Mailbox Servers

To install ScanMail:

1. Select a source for the setup program:
   - **a.** Trend Micro Web site.
     - **i.** Download ScanMail from the Trend Micro Web site.
     - **ii.** Unzip the file to a temporary directory
     - **iii.** Run setup.exe to install ScanMail
   - **b.** The Trend Micro Enterprise Solution CD.
     - **i.** Insert the CD and follow the online instructions.

   The **Welcome to Trend Micro ScanMail Setup** screen appears.

2. Click **Next** to continue the installation. The **License Agreement** screen appears.


Trend Micro ScanMail Setup
Welcome to Trend Micro ScanMail Setup
TREND MICRO

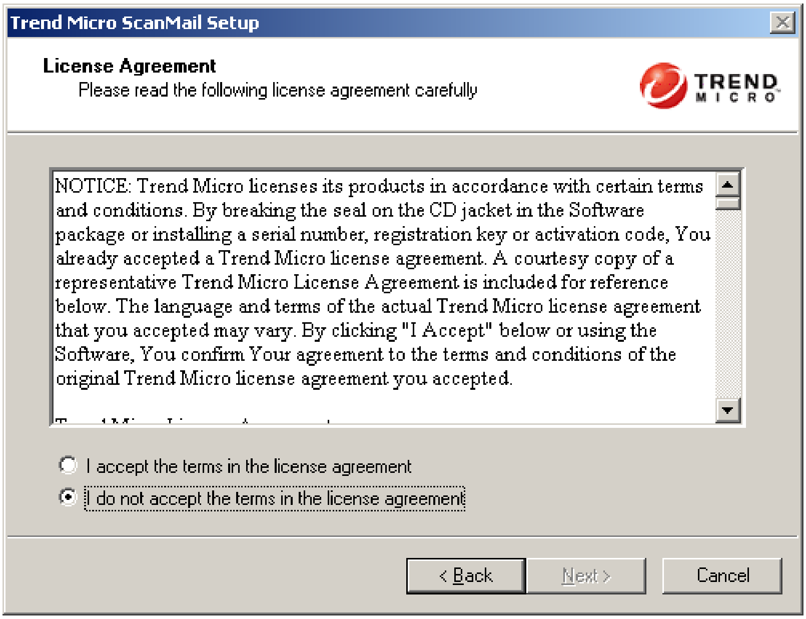
Setup will install or uninstall ScanMail on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties

FIGURE 2-21. Welcome screen

3. Click **I Accept the terms in the license agreement** to agree to the terms of the agreement and continue installation. Click **Next** to continue. The **Select an Action** screen appears.

Note: If you do not accept the terms, click **I do not accept the terms in the license agreement.** This terminates the Setup without modifying your operating system.



License Agreement

Please read the following license agreement carefully

NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or installing a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

Trend Micro License Agreement

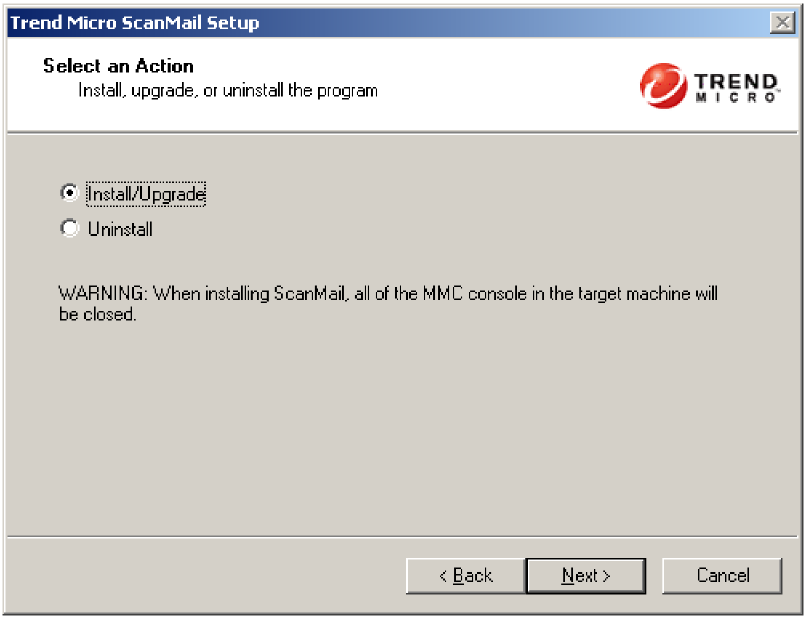
○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

FIGURE 2-22. License Agreement screen

4. Select one of the following actions:
   - Select **Install/Upgrade** to:
     - Perform a fresh install
     - Upgrade the ScanMail 8.0 beta version to the ScanMail 8.0 standard release version.
   - Select **Uninstall** if you want to remove ScanMail from your server. For more information about uninstalling, see *Removing ScanMail* starting on page 2-80.

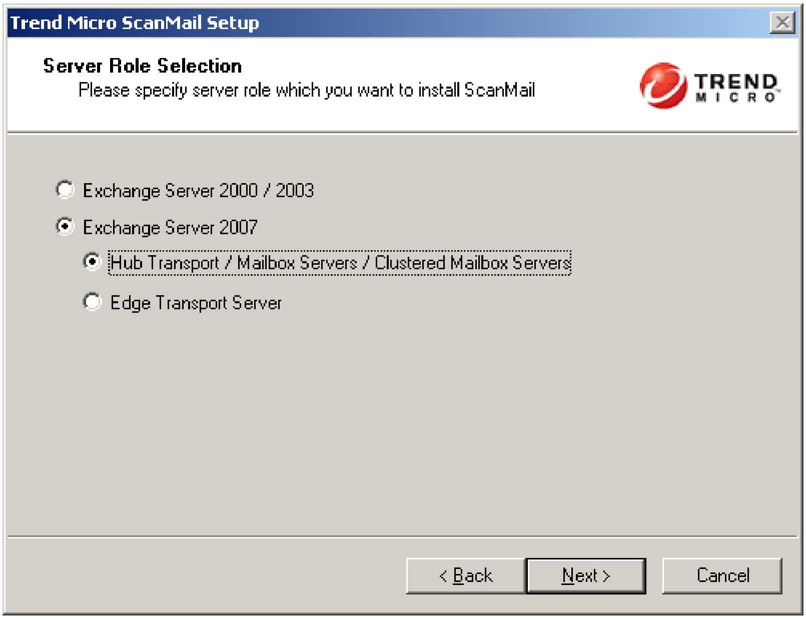
   Click **Next** to continue. The **Server Role Selection** screen appears.



WARNING: When installing ScanMail, all of the MMC console in the target machine will be closed.

FIGURE 2-23. Select an Action screen

5. Select **Hub Transport / Mailbox Servers / Clustered Mailbox Servers** to install ScanMail with the Hub Transport, Mailbox server role, or clustered mailbox server. Click **Next** to continue. The **Select Target Server(s)** screen appears.



Trend Micro ScanMail Setup

Server Role Selection

Please specify server role which you want to install ScanMail

○ Exchange Server 2000 / 2003

● Exchange Server 2007

● Hub Transport / Mailbox Servers / Clustered Mailbox Servers

○ Edge Transport Server

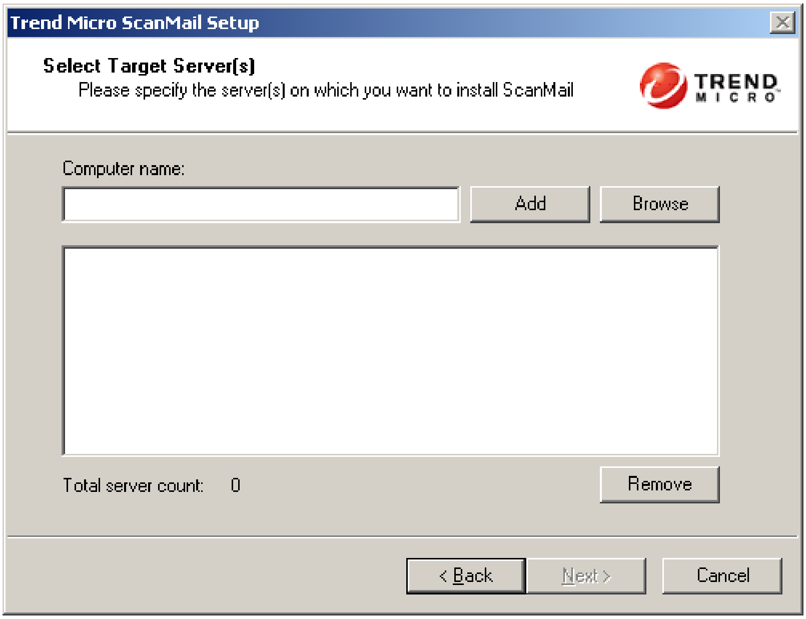
FIGURE 2-24. Server Role Selection screen

6. Select the computers to which you want to install ScanMail by doing one of the following:

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

   a. Click **Remove** to remove a server from the list.

b. Click **Next** to save your list of target servers and continue the installation. The **Log On** screen appears.



Trend Micro ScanMail Setup

Select Target Server(s)

Please specify the server(s) on which you want to install ScanMail

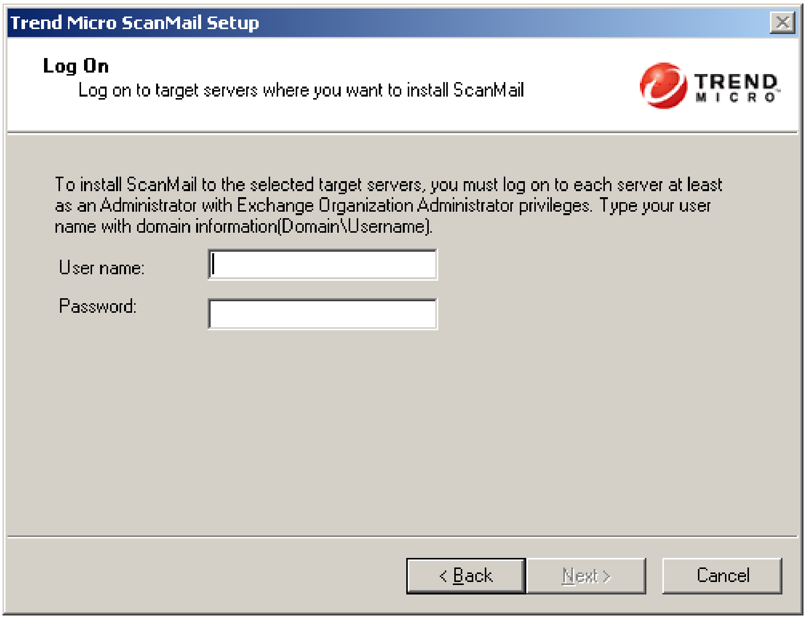
Computer name:

Total server count: 0

FIGURE 2-25. Select Target Server(s)

Note: The setup program can install ScanMail to a number of single servers or to all the computers in a domain. Use an account with the appropriate privileges to access every target server.

7. Log on to the target servers where you want to install ScanMail. Use an account with Exchange Organization Administrator privileges and Local Administrator privileges for the Hub Transport or Mailbox server. Type the user name and password to log on to the target server to install ScanMail. Click **Next** to continue. The **Configure Shared/Target Directory** screen appears.


Trend Micro ScanMail Setup
Log On
Log on to target servers where you want to install ScanMail
TREND MICRO

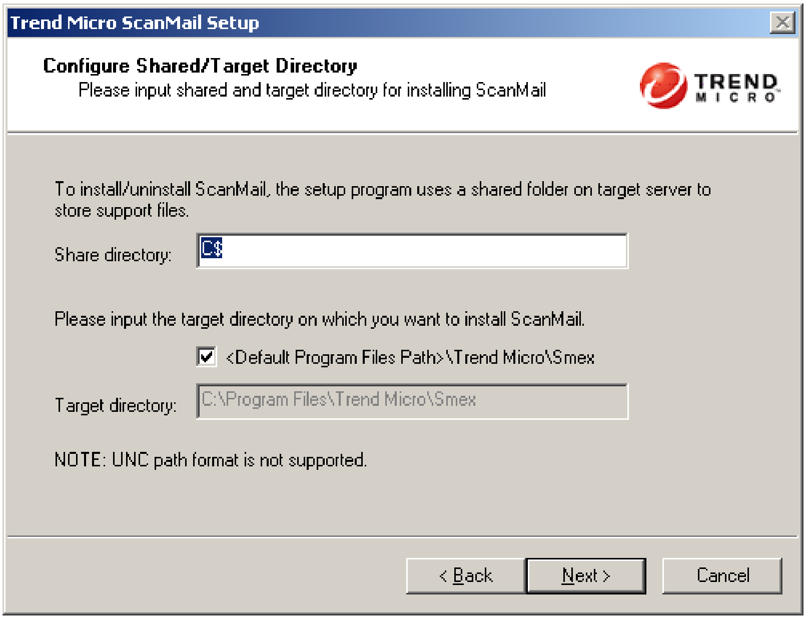
To install ScanMail to the selected target servers, you must log on to each server at least as an Administrator with Exchange Organization Administrator privileges. Type your user name with domain information(Domain\Username).

User name:

Password:

FIGURE 2-26. Log On screen

8. Type the directory share name for which the specified user has access rights or keep the default temporary share directory, C$. The setup program uses the share directory to copy temporary files during installation and is only accessible to the administrator. Type the directory path to where you will install ScanMail on the target server. Click **Next** to continue. The **Checking Target Server System Requirements** screen appears.



Trend Micro ScanMail Setup

Configure Shared/Target Directory

Please input shared and target directory for installing ScanMail

To install/uninstall ScanMail, the setup program uses a shared folder on target server to store support files.

Share directory: C$

Please input the target directory on which you want to install ScanMail.

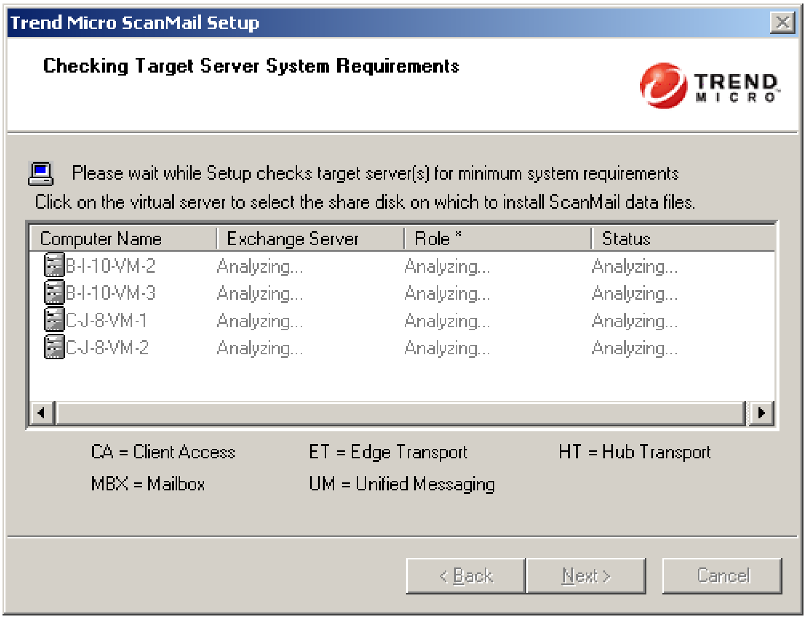
☑ <Default Program Files Path>\Trend Micro\Smex

Target directory: C:\Program Files\Trend Micro\Smex

NOTE: UNC path format is not supported.

FIGURE 2-27. Configure Shared / Target Directory

9. Double-click the virtual server on which to install ScanMail data files. Review the settings and click **Next** to continue. The **Select Web Server Type** screen appears.


Trend Micro ScanMail Setup
Checking Target Server System Requirements
TREND MICRO

Please wait while Setup checks target server(s) for minimum system requirements

Click on the virtual server to select the share disk on which to install ScanMail data files.

Computer Name	Exchange Server	Role *	Status
B-I-10-VM-2	Analyzing...	Analyzing...	Analyzing...
B-I-10-VM-3	Analyzing...	Analyzing...	Analyzing...
C-J-8-VM-1	Analyzing...	Analyzing...	Analyzing...
C-J-8-VM-2	Analyzing...	Analyzing...	Analyzing...

CA = Client Access ET = Edge Transport HT = Hub Transport

MBX = Mailbox UM = Unified Messaging

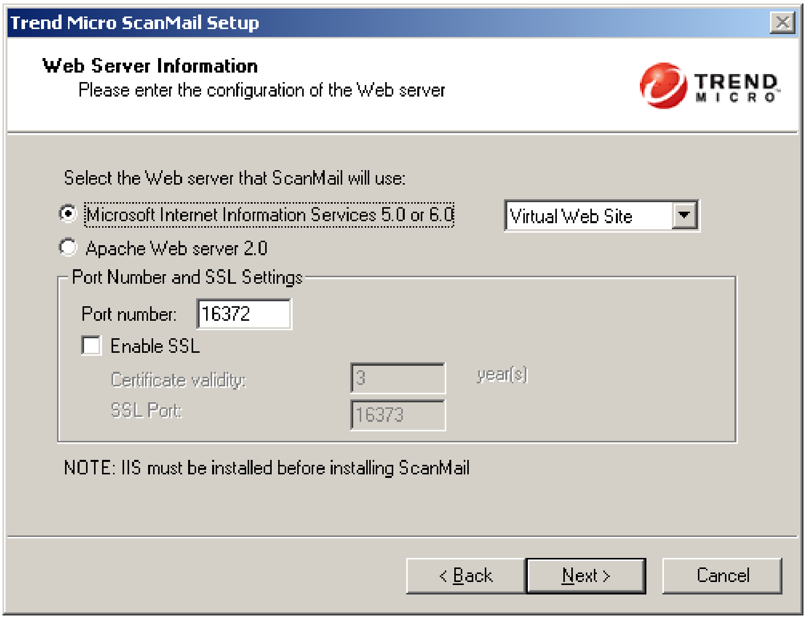
FIGURE 2-28. Checking Target Server System Requirements screen

Note: If the settings are not correct, you can click **Back** to go back to a previous screen in the installation.

10. Select one of following for ScanMail to use as a Web server.

    - **Microsoft Internet Information Services (IIS)**—Ensure that Microsoft Internet Information Services (IIS) 6.0 is installed on the target server(s). Select **IIS Default Web Site** or **IIS Virtual Web Site**.
    - **Apache Web server 2.0**—If an Apache Web server version 2.0 or later is not found, the setup program will automatically install Apache 2.0. IIS Web options are grayed-out.

    Next to **Port number** type the port to use as a listening port for this server. You also have the option of enabling Secure Socket Layer (SSL) security. Select **Enable SSL** check box to use this feature. Click **Next** to continue. The **Connection Settings** screen appears.



Trend Micro ScanMail Setup

Web Server Information

Please enter the configuration of the Web server

Select the Web server that ScanMail will use:

● Microsoft Internet Information Services 5.0 or 6.0 — Virtual Web Site

○ Apache Web server 2.0

Port Number and SSL Settings

Port number: 16372

□ Enable SSL

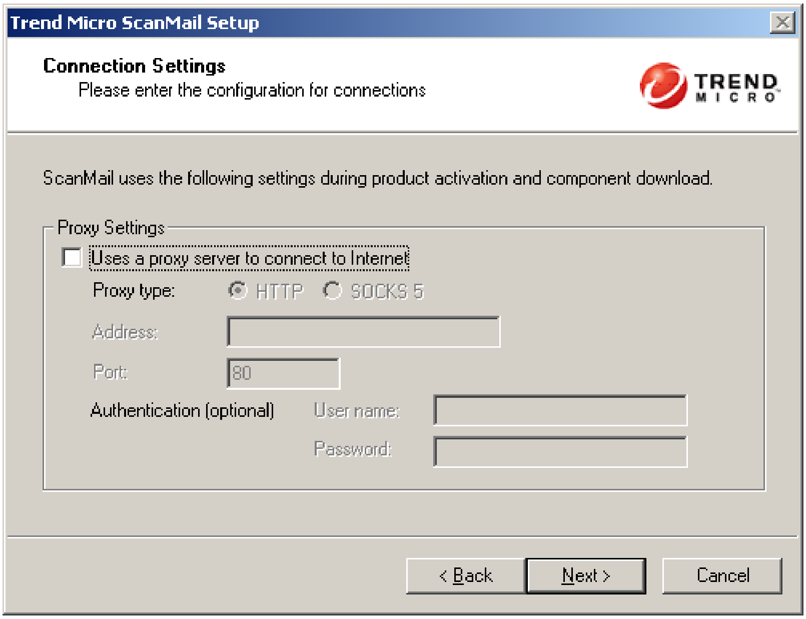
Certificate validity: 3 year(s)

SSL Port: 16373

NOTE: IIS must be installed before installing ScanMail

FIGURE 2-29. Select Web Server Type screen

11. If a proxy server handles Internet traffic on your network, select **Use a proxy server to connect to Internet** and then type the URL address and port number that your proxy uses. By default, the proxy server is disabled. If you want to use SOCKS5 for secure communication behind the proxy, select **Use SOCKS5**. If your proxy requires authentication, type the user name and password used for authentication. Click **Next** to continue. The **Product Activation** screen appears.



Trend Micro ScanMail Setup

Connection Settings

Please enter the configuration for connections

ScanMail uses the following settings during product activation and component download.

Proxy Settings

□ Uses a proxy server to connect to Internet

Proxy type: ● HTTP ○ SOCKS 5

Address:

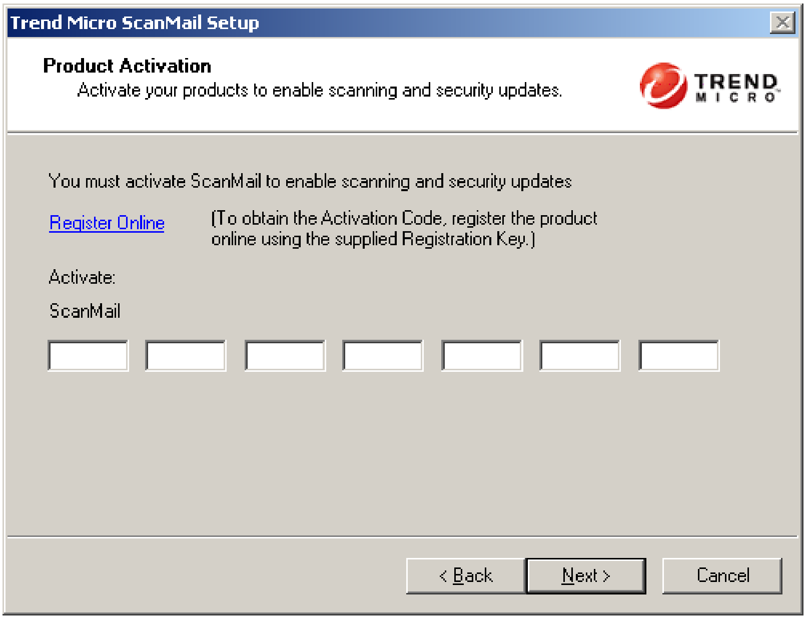
Port: 80

Authentication (optional) User name:

Password:

FIGURE 2-30. Connection Settings screen

12. In the **Product Activation** screen, view the full version license for this product's version. Click **Next** to continue. The **World Virus Tracking Program** screen appears.



Trend Micro ScanMail Setup

Product Activation

Activate your products to enable scanning and security updates.

You must activate ScanMail to enable scanning and security updates

Register Online (To obtain the Activation Code, register the product online using the supplied Registration Key.)

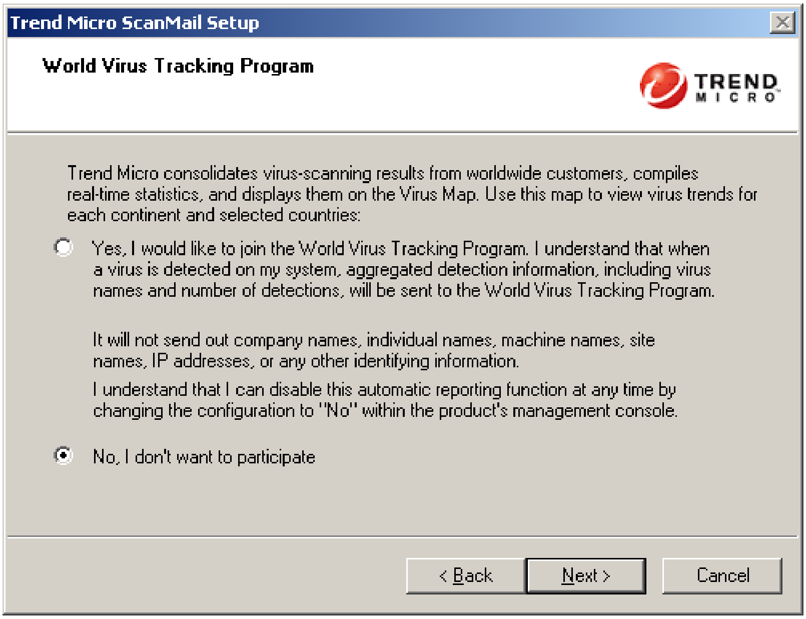
Activate:

ScanMail

FIGURE 2-31. Product Activation screen

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

13. Read the statement and click **Yes** to enroll. If you decline to participate, you can still proceed with the installation. Click **Next** to continue. The **Control Manager Server Settings** screen appears.



Trend Micro ScanMail Setup

World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries:

○ Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, aggregated detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program.

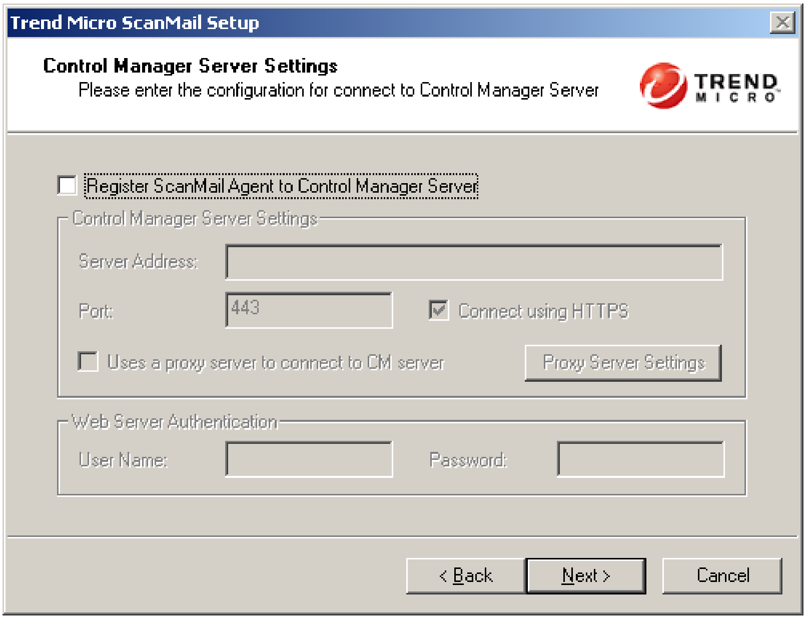
It will not send out company names, individual names, machine names, site names, IP addresses, or any other identifying information.

I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

● No, I don't want to participate

FIGURE 2-32. World Virus Tracking Program screen

14. Specify the Control Manager server settings and specify the **Proxy Server Settings** if you use a proxy server between your ScanMail server and Control Manager server. Click **Next** to continue. The **Management Group Selection** screen appears.



Trend Micro ScanMail Setup

Control Manager Server Settings

Please enter the configuration for connect to Control Manager Server

□ Register ScanMail Agent to Control Manager Server

Control Manager Server Settings

Server Address:

Port: 443

☑ Connect using HTTPS

□ Uses a proxy server to connect to CM server

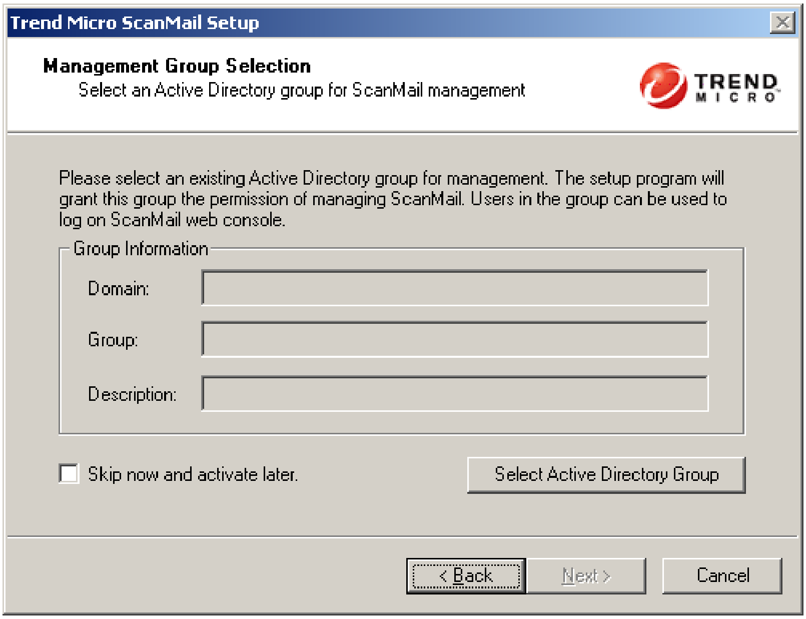
Web Server Authentication

User Name:

Password:

FIGURE 2-33. Control Manager Server Settings screen

15. Configure an Active Directory Group to have ScanMail management privileges by clicking **Select Active Directory Group** or select **Skip now and activate later** to configure this feature after installation. Click **Next** to continue. The **Review Settings** screen appears.



Trend Micro ScanMail Setup

Management Group Selection

Select an Active Directory group for ScanMail management

Please select an existing Active Directory group for management. The setup program will grant this group the permission of managing ScanMail. Users in the group can be used to log on ScanMail web console.

Group Information

Domain:

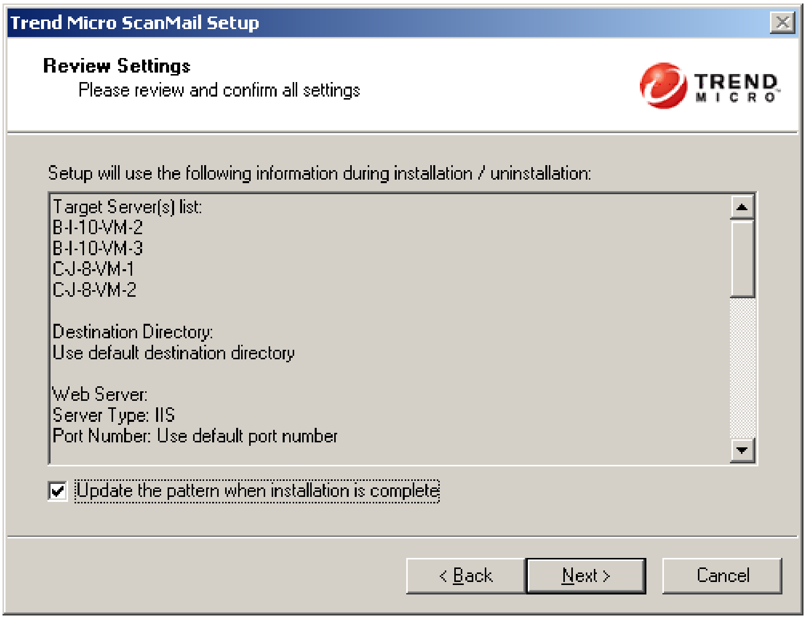
Group:

Description:

□ Skip now and activate later.

FIGURE 2-34. Management Group Selection screen

16. Review your settings and click **Next** to continue. The **Installation Progress** screen appears.



Trend Micro ScanMail Setup

Review Settings

Please review and confirm all settings

Setup will use the following information during installation / uninstallation:

Target Server(s) list:
B-I-10-VM-2
B-I-10-VM-3
C-J-8-VM-1
C-J-8-VM-2

Destination Directory:
Use default destination directory

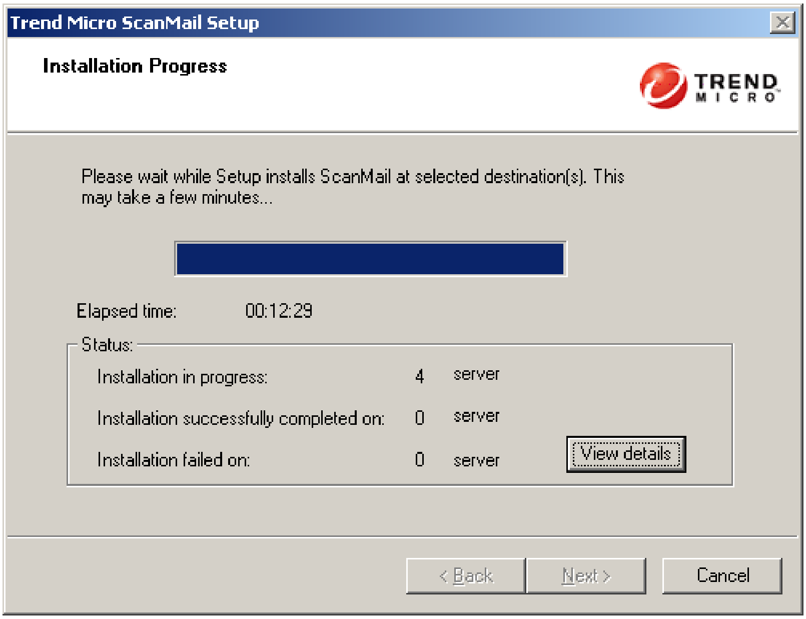
Web Server:
Server Type: IIS
Port Number: Use default port number

☑ Update the pattern when installation is complete

FIGURE 2-35. Review Settings screen

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

Note: ScanMail installs Microsoft™ SQL Server 2005 Express for configurations, logs, and reports on 64-bit computers. ScanMail sets the Microsoft SQL Server 2005 Express security level to the highest.


Trend Micro ScanMail Setup

Installation Progress

Please wait while Setup installs ScanMail at selected destination(s). This may take a few minutes...

Elapsed time: 00:12:29

Status:

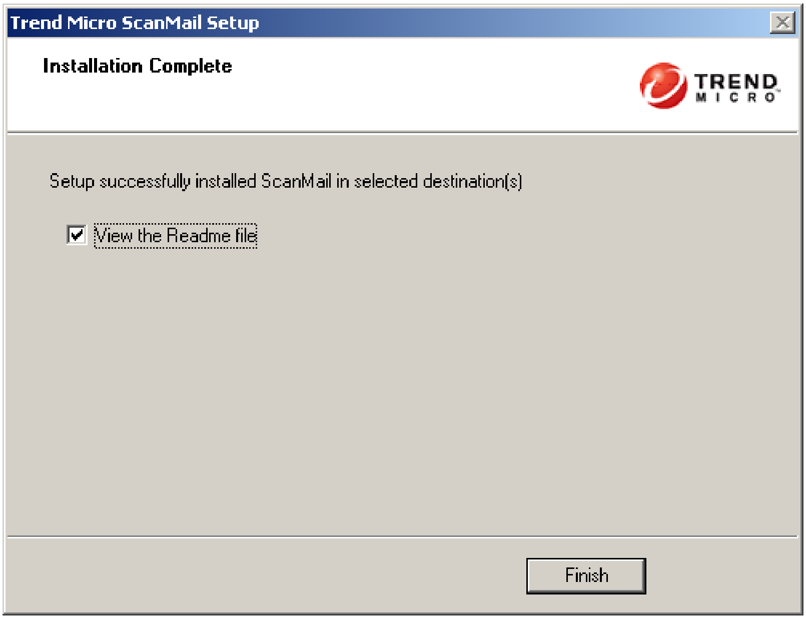
Installation in progress: 4 server

Installation successfully completed on: 0 server

Installation failed on: 0 server

FIGURE 2-36. Installation Progress screen

18. This screen informs you that the installation was successful. Click **Finish** to exit the setup program and the Readme file displays.



Setup successfully installed ScanMail in selected destination(s)

☑ View the Readme file

FIGURE 2-37. Installation Complete screen

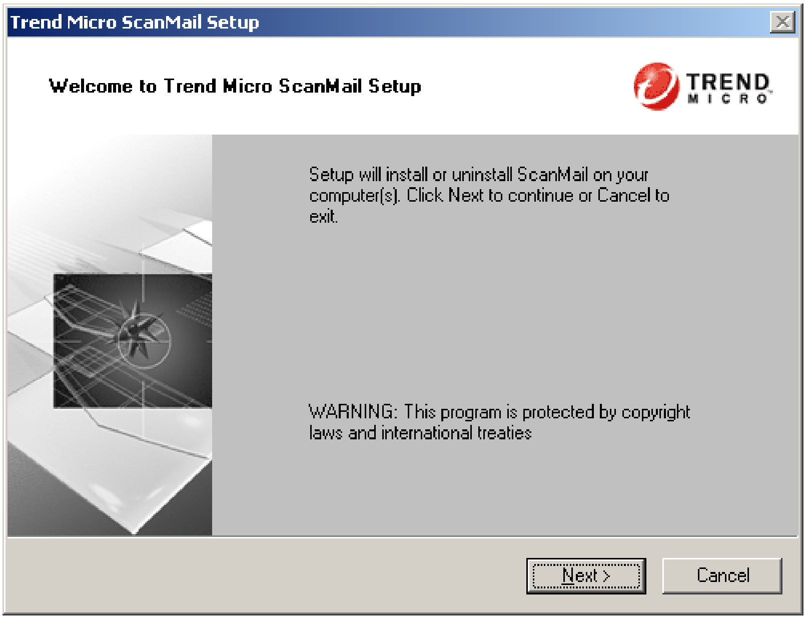
Installation with Exchange Server 2007 Edge Transport Servers

To install ScanMail:

1. Select a source for the setup program:
   - **a.** Trend Micro Web site.
     - **i.** Download ScanMail from the Trend Micro Web site.
     - **ii.** Unzip the file to a temporary directory
     - **iii.** Run setup.exe to install ScanMail
   - **b.** The Trend Micro Enterprise Solution CD.
     - **i.** Insert the CD and follow the online instructions.

   The **Welcome to Trend Micro ScanMail Setup** screen appears.

2. Click **Next** to continue the installation. The **License Agreement** screen appears.



Trend Micro ScanMail Setup

Welcome to Trend Micro ScanMail Setup

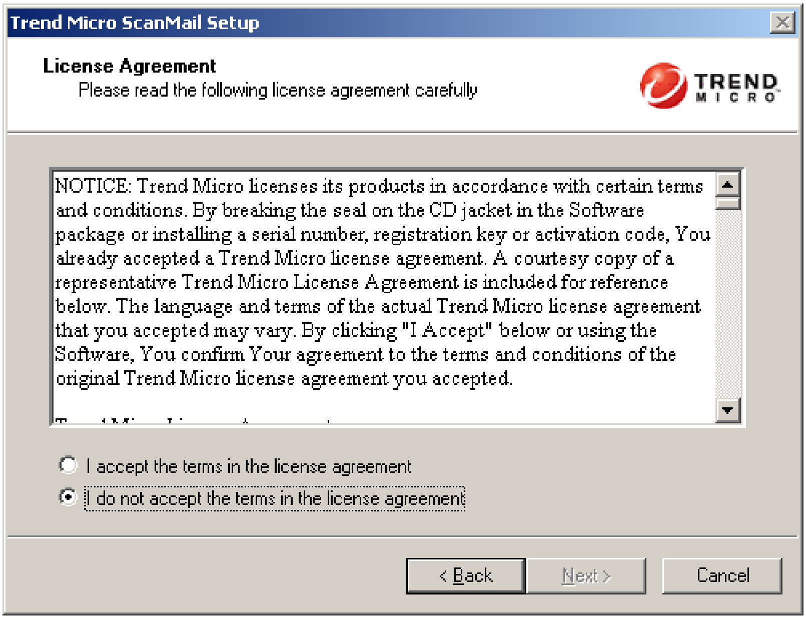
Setup will install or uninstall ScanMail on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties

FIGURE 2-38. Welcome screen

3. Click **I Accept the terms in the license agreement** to agree to the terms of the agreement and continue installation. Click **Next** to continue. The **Select an Action** screen appears.

Note: If you do not accept the terms, click **I do not accept the terms in the license agreement.** This terminates the Setup without modifying your operating system.



Trend Micro ScanMail Setup

License Agreement

Please read the following license agreement carefully

NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or installing a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

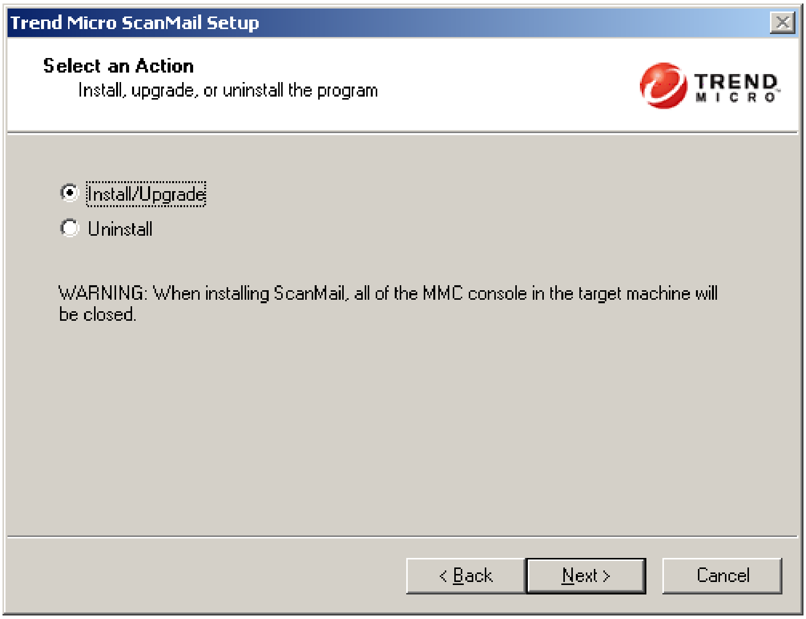
○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

FIGURE 2-39. License Agreement screen

4. Select one of the following actions:
    - Select **Install/Upgrade** if you want to:
        - Perform a fresh install
        - Upgrade the ScanMail 8.0 beta version to the ScanMail 8.0 standard release version.
    - Select **Uninstall** if you want to remove ScanMail from your server. For more information about uninstalling, see *Removing ScanMail* starting on page 2-80.

    Click **Next** to continue. The **Server Role Selection** screen appears.


Trend Micro ScanMail Setup

Select an Action

Install, upgrade, or uninstall the program

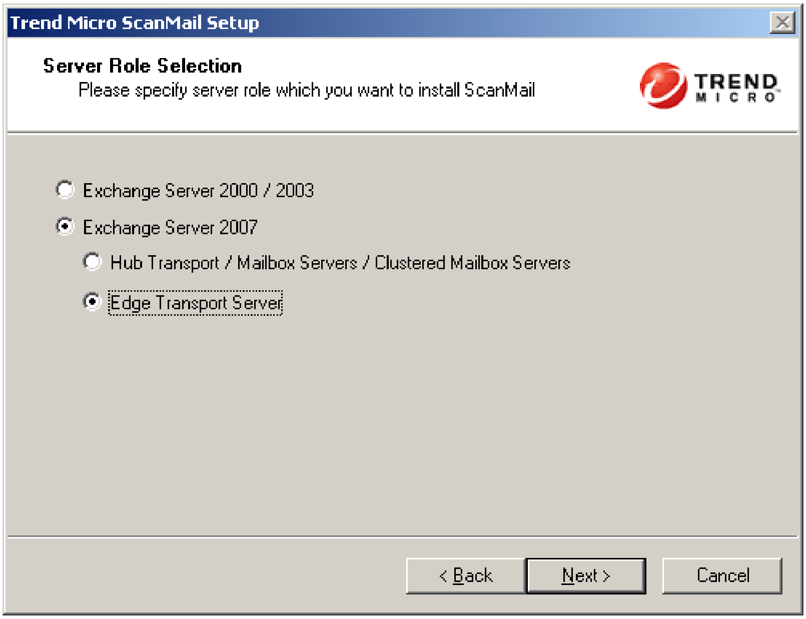
● Install/Upgrade

○ Uninstall

WARNING: When installing ScanMail, all of the MMC console in the target machine will be closed.

FIGURE 2-40. **Select an Action screen**

5. Select **Edge Transport Server** to install ScanMail with the Edge Transport server role. Click **Next** to continue. The **Select Target Server(s)** screen appears.



Trend Micro ScanMail Setup

Server Role Selection

Please specify server role which you want to install ScanMail

○ Exchange Server 2000 / 2003

● Exchange Server 2007

○ Hub Transport / Mailbox Servers / Clustered Mailbox Servers

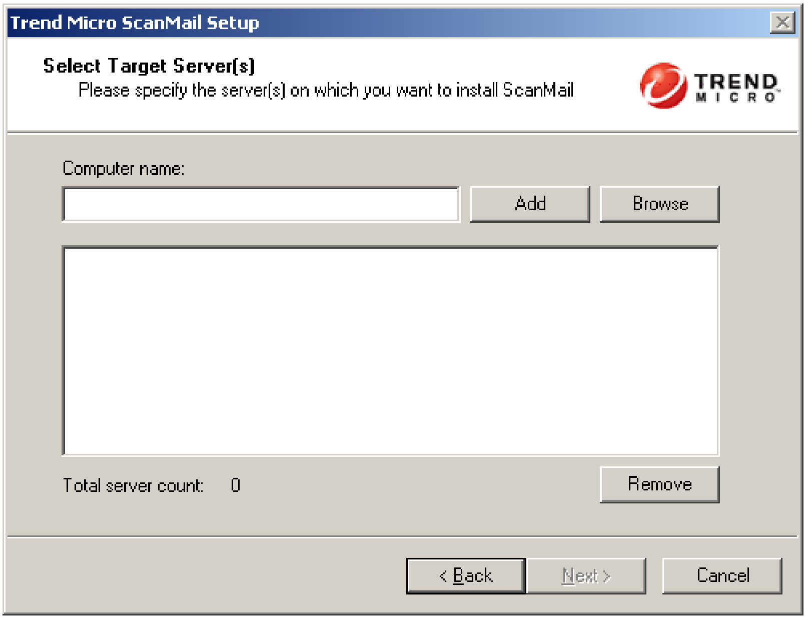
● Edge Transport Server

FIGURE 2-41. Server Role Selection screen

6. Select the computers to which you want to install ScanMail by doing one of the following:
   - Type the name of the server to which you want to install in the **Computer name** field and click Add to add the computers to the list of servers.
   - Click **Browse** and browse the computers that are available on your network, double-click the domain or computers you want to add to the list.

a. Click **Remove** to remove a server from the list.

b. Click **Next** to save your list of target servers and continue the installation. The **Log On** screen appears.



Trend Micro ScanMail Setup

Select Target Server(s)

Please specify the server(s) on which you want to install ScanMail

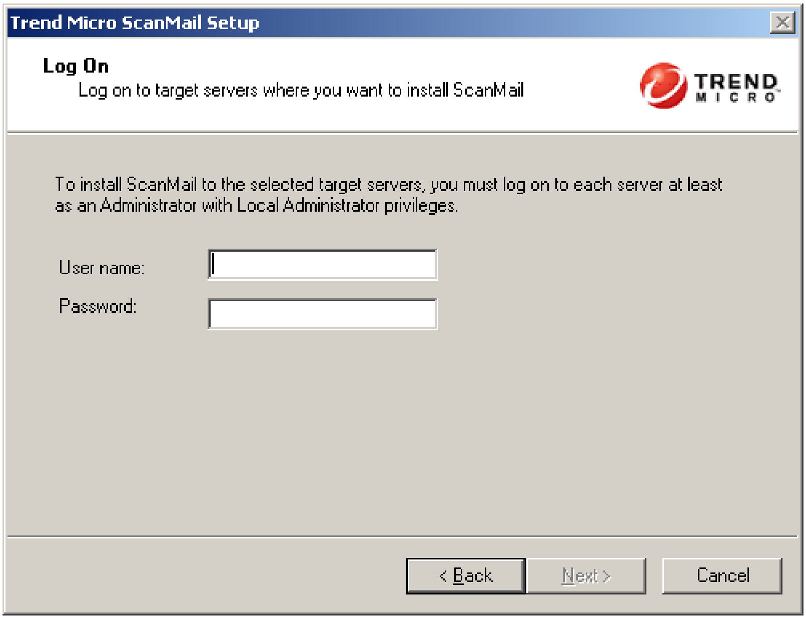
Computer name:

Total server count: 0

FIGURE 2-42. Select Target Server(s)

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

7. Log on to target servers where you want to install ScanMail. Use an account with Local Administrator privileges. Type the user name and password to log on to the target server to install ScanMail. Click **Next** to continue. The **Configure Shared/Target Directory** screen appears.



Trend Micro ScanMail Setup

Log On

Log on to target servers where you want to install ScanMail

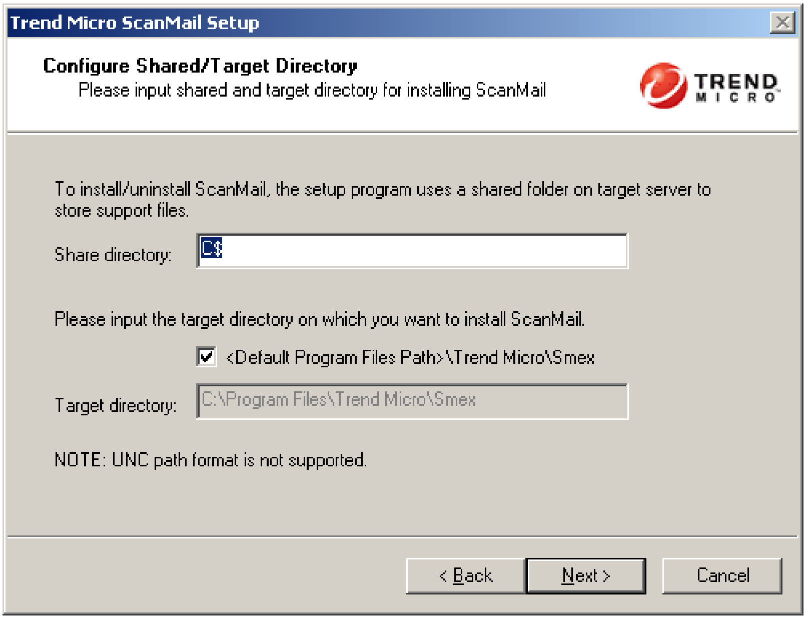
To install ScanMail to the selected target servers, you must log on to each server at least as an Administrator with Local Administrator privileges.

User name:

Password:

FIGURE 2-43. Log On screen

8. Type the directory share name for which the specified user has access rights or keep the default temporary share directory, C$. The setup program uses the share directory to copy temporary files during installation and is only accessible to the administrator. Type the directory path to where you will install ScanMail on the target server. Click **Next** to continue. The **Checking Target Server System Requirements** screen appears.


Trend Micro ScanMail Setup

Configure Shared/Target Directory

Please input shared and target directory for installing ScanMail

To install/uninstall ScanMail, the setup program uses a shared folder on target server to store support files.

Share directory: C$

Please input the target directory on which you want to install ScanMail.

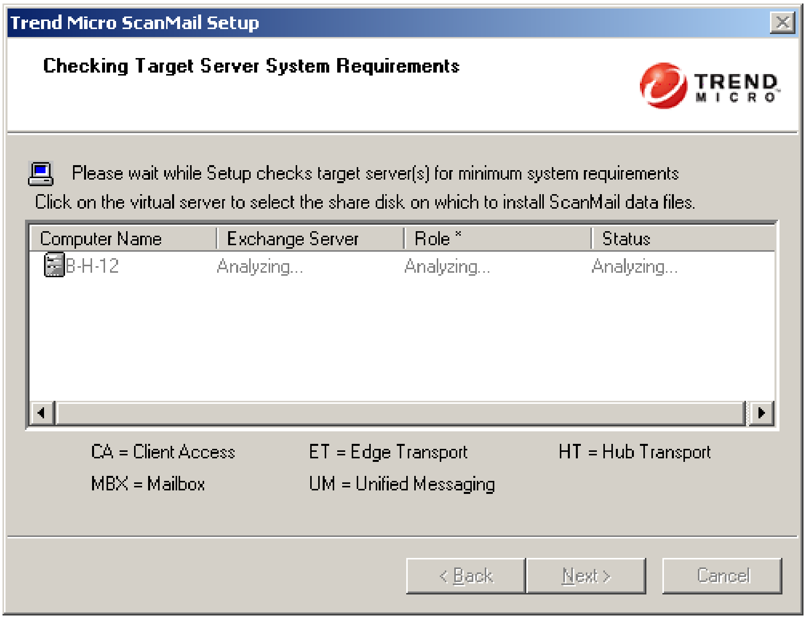
☑ <Default Program Files Path>\Trend Micro\Smex

Target directory: C:\Program Files\Trend Micro\Smex

NOTE: UNC path format is not supported.

FIGURE 2-44. Configure Shared / Target Directory

9. Double-click the virtual server on which to install ScanMail data files. Review the settings and click **Next** to continue. The **Select Web Server Type** screen appears.



Trend Micro ScanMail Setup

Checking Target Server System Requirements

Please wait while Setup checks target server(s) for minimum system requirements

Click on the virtual server to select the share disk on which to install ScanMail data files.

Computer Name	Exchange Server	Role *	Status
B-H-12	Analyzing...	Analyzing...	Analyzing...

CA = Client Access   ET = Edge Transport   HT = Hub Transport

MBX = Mailbox   UM = Unified Messaging

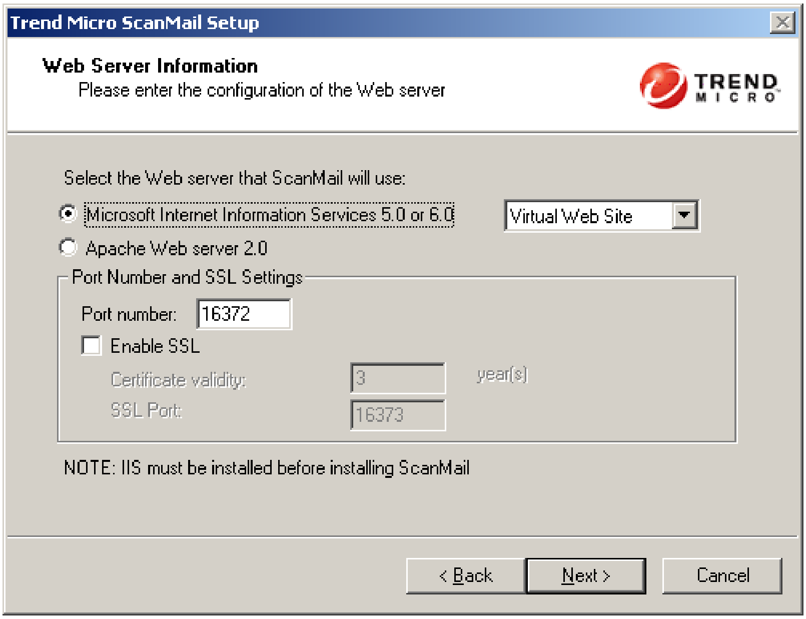
FIGURE 2-45. Checking Target Server System Requirements screen

Note: If the settings are not correct, you can click **Back** to go back to a previous screen in the installation.

10. Select one of following for ScanMail to use as a Web server.

- **Microsoft Internet Information Services (IIS)**—Ensure that Microsoft Internet Information Services (IIS) 6.0 is installed on the target server(s). Select **IIS Default Web Site** or **IIS Virtual Web Site**.
- **Apache Web server 2.0**—If an Apache Web server version 2.0 or later is not found, the setup program will automatically install Apache 2.0. IIS Web options are grayed-out.

Next to **Port number** type the port to use as a listening port for this server. You also have the option of enabling Secure Socket Layer (SSL) security. Select **Enable SSL** check box to use this feature. Click **Next** to continue. The **Connection Settings** screen appears.



Trend Micro ScanMail Setup

Web Server Information

Please enter the configuration of the Web server

Select the Web server that ScanMail will use:

● Microsoft Internet Information Services 5.0 or 6.0 — Virtual Web Site

○ Apache Web server 2.0

Port Number and SSL Settings

Port number: 16372

□ Enable SSL

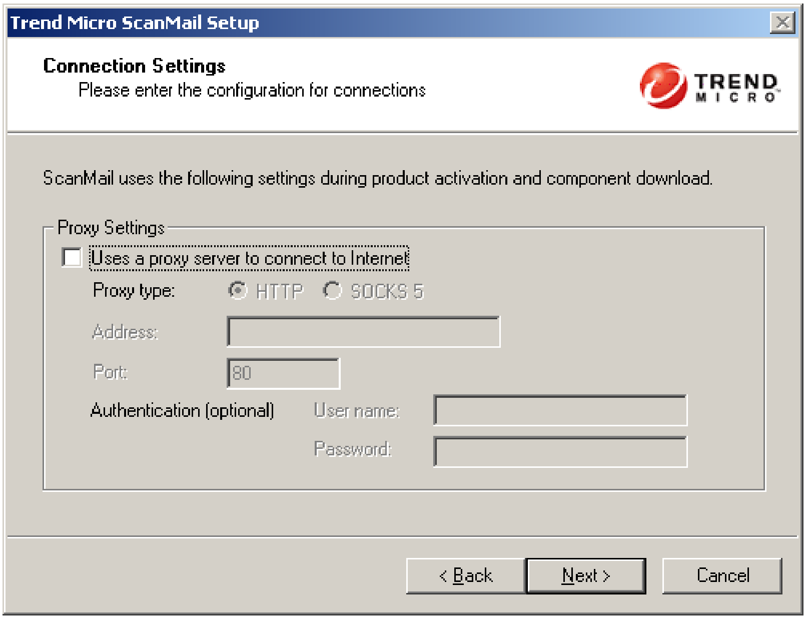
Certificate validity: 3 year(s)

SSL Port: 16373

NOTE: IIS must be installed before installing ScanMail

FIGURE 2-46. Select Web Server Type screen

11. If a proxy server handles Internet traffic on your network, select **Use a proxy server to connect to Internet** and then type the URL address and port number that your proxy uses. By default, the proxy server is disabled. If you want to use SOCKS5 for secure communication behind the proxy, select **Use SOCKS5**. If your proxy requires authentication, type the user name and password used for authentication. Click **Next** to continue. The **Product Activation** screen appears.



Trend Micro ScanMail Setup

Connection Settings

Please enter the configuration for connections

ScanMail uses the following settings during product activation and component download.

Proxy Settings

□ Uses a proxy server to connect to Internet

Proxy type: ● HTTP ○ SOCKS 5

Address:

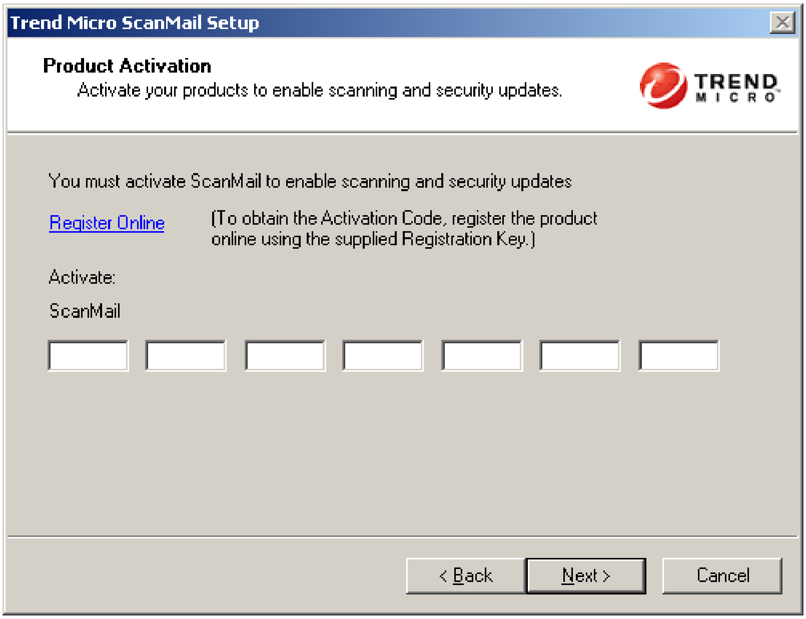
Port: 80

Authentication (optional) User name:

Password:

FIGURE 2-47. Connection Settings screen

12. In the **Product Activation** screen, type the full version license for this product's version. Click **Next** to continue. The **World Virus Tracking Program** screen appears.



Trend Micro ScanMail Setup

Product Activation

Activate your products to enable scanning and security updates.

You must activate ScanMail to enable scanning and security updates

Register Online (To obtain the Activation Code, register the product online using the supplied Registration Key.)

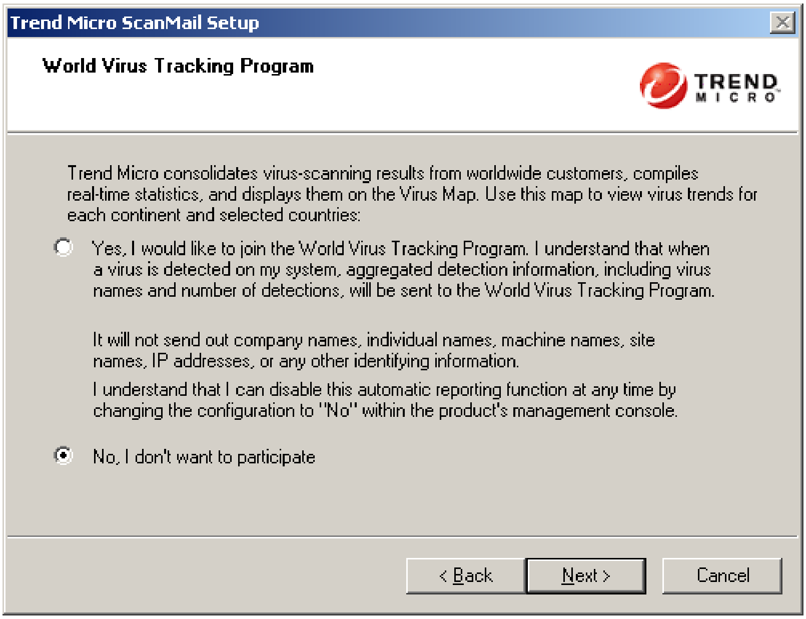
Activate:

ScanMail

FIGURE 2-48. Product Activation screen

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

13. Read the statement and click **Yes** to enroll. If you decline to participate, you can still proceed with the installation. Click **Next** to continue. The **Control Manager Server Settings** screen appears.



Trend Micro ScanMail Setup

World Virus Tracking Program

Trend Micro consolidates virus-scanning results from worldwide customers, compiles real-time statistics, and displays them on the Virus Map. Use this map to view virus trends for each continent and selected countries:

○ Yes, I would like to join the World Virus Tracking Program. I understand that when a virus is detected on my system, aggregated detection information, including virus names and number of detections, will be sent to the World Virus Tracking Program.

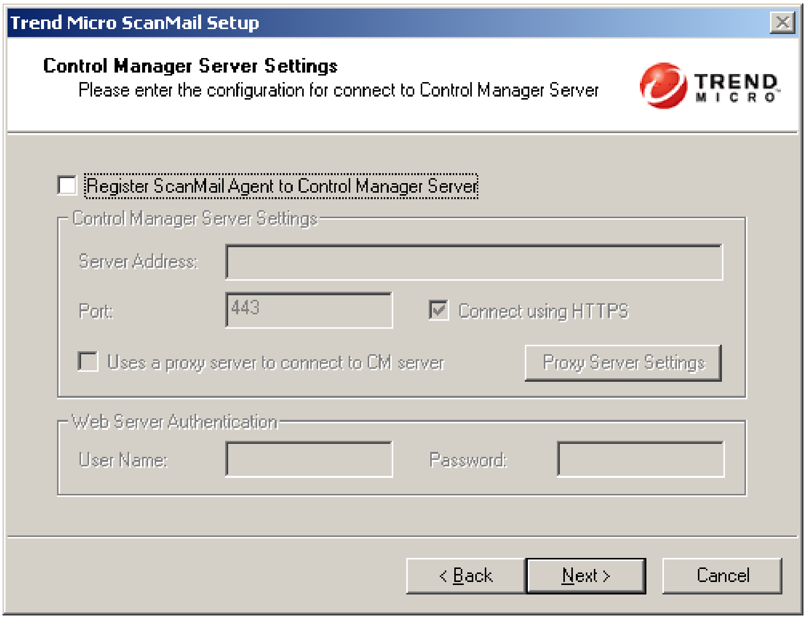
It will not send out company names, individual names, machine names, site names, IP addresses, or any other identifying information.

I understand that I can disable this automatic reporting function at any time by changing the configuration to "No" within the product's management console.

● No, I don't want to participate

FIGURE 2-49. World Virus Tracking Program screen

14. Specify the Control Manager server settings and specify the **Proxy Server Settings** if you use a proxy server between your ScanMail server and Control Manager server. Click **Next** to continue. The **Review Settings** screen appears.



Trend Micro ScanMail Setup

Control Manager Server Settings

Please enter the configuration for connect to Control Manager Server

□ Register ScanMail Agent to Control Manager Server

Control Manager Server Settings

Server Address:

Port: 443

☑ Connect using HTTPS

□ Uses a proxy server to connect to CM server

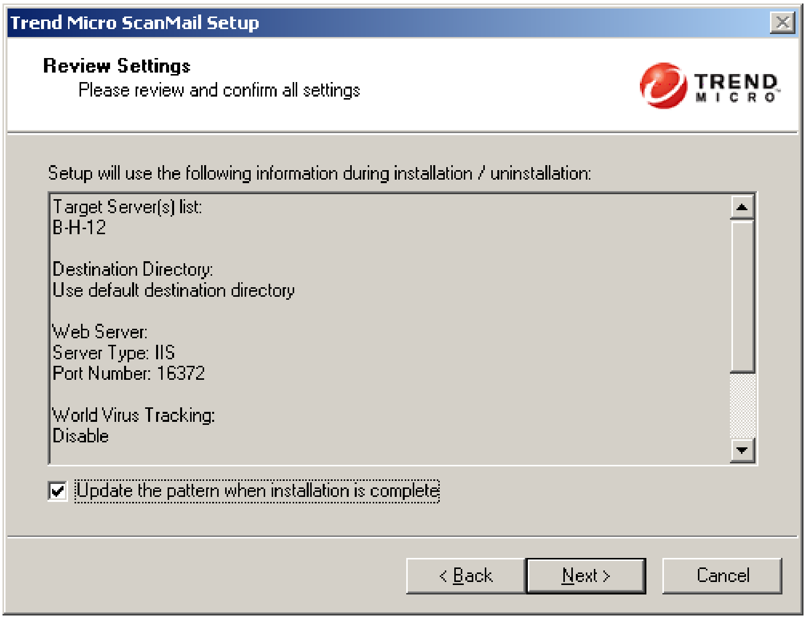
Web Server Authentication

User Name:

Password:

FIGURE 2-50. Control Manager Server Settings screen

15. Review your settings and click **Next**. The **Installation Progress** screen appears.



Review Settings

Please review and confirm all settings

Setup will use the following information during installation / uninstallation:

Target Server(s) list:
B-H-12

Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

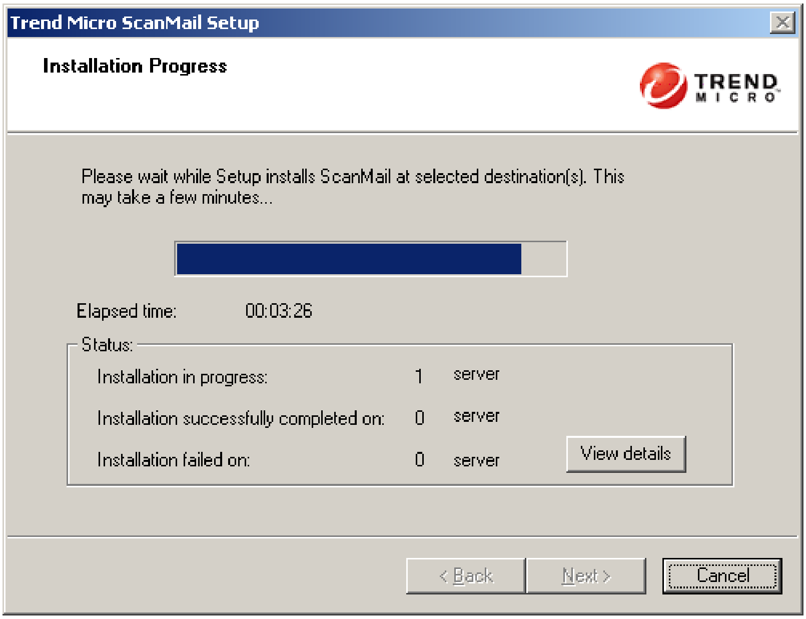
World Virus Tracking:
Disable

☑ Update the pattern when installation is complete

FIGURE 2-51. Review Settings screen

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

Note: ScanMail installs Microsoft™ SQL Server 2005 Express for configurations, logs, and reports on 64-bit computers. ScanMail sets the Microsoft SQL Server 2005 Express security level to the highest.



Trend Micro ScanMail Setup

Installation Progress

Please wait while Setup installs ScanMail at selected destination(s). This may take a few minutes...

Elapsed time: 00:03:26

Status:

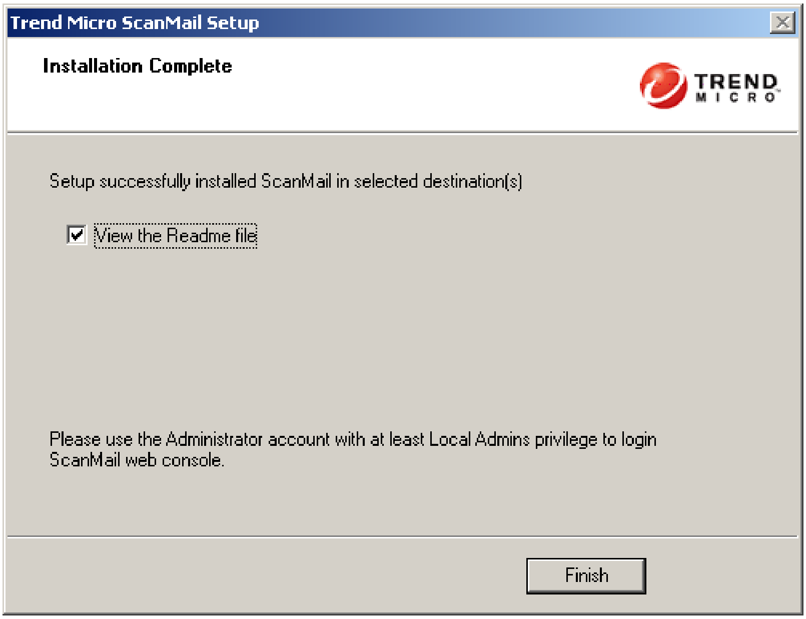
Installation in progress: 1 server

Installation successfully completed on: 0 server

Installation failed on: 0 server

FIGURE 2-52. Installation Progress screen

17. This screen informs you that the installation was successful. Click **Finish** to exit the setup program and the Readme file displays.



Trend Micro ScanMail Setup

Installation Complete

Setup successfully installed ScanMail in selected destination(s)

☑ View the Readme file

Please use the Administrator account with at least Local Admins privilege to login ScanMail web console.

FIGURE 2-53. Installation Complete screen

18. Use an administrator account with local administrator privileges to log on to the ScanMail product console.

Cluster installation

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

The instructions to install ScanMail from a cluster server are nearly identical to the non-cluster installation instructions. See *Running the Setup Program* starting on page 2-20 for instructions for installing ScanMail to a cluster server environment.

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

For more information about manually installing a cluster server, see *Manually Creating a ScanMail Resource for Virtual Servers* on page 4-13.

Post-Installation

Verifying a Successful Installation

ScanMail is installed to the following directory:

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

ScanMail adds the following services:

```
ScanMail for Microsoft Exchange Master Service
```

```
ScanMail for Microsoft Exchange Remote Configuration Server
```

Note: This service is not added for ScanMail with Exchange Server 2007 Edge Transport server roles.

```
ScanMail for Microsoft Exchange System Watcher
```

ScanMail adds the following keys to the registry:

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

Note: The following keys are added to ScanMail with Exchange 2000 Server, Exchange Server 2003, Exchange Server 2007 Hub Transport Server with Mailbox Server, and Exchange Server 2007 Mailbox Server. The following keys are not added to ScanMail with Exchange Server 2007 Edge Transport Server and Exchange Server 2007 Hub Transport Server.

```
HLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan

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

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

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

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

Testing Your Installation

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

Visit http://www.eicar.org for more information.

The EICAR test script is a text file with a *.com extension. It is inert. It is not a virus/malware, it does not replicate, and it does not contain a payload.

WARNING! *Never use real viruses/malware to test your antivirus installation.*

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

To test real-time scanning:

1. Ensure you have a valid email client connected to the Exchange 2000, 2003, or 2007 you are testing.
2. Go to `http://www.antivirus.com/vinfo/testfiles/index.htm` and download a copy of the standard industry test file EICAR for testing.
3. Verify that the Real-time Scan and Real-time Monitor are running correctly. On the Real-time Monitor screen, check to see if you can read the message **Real-time scan has been running since**.
4. Open your mail client and create a test message called Test ScanMail. Attach a copy of the EICAR test file to your email and send that email to your test mailboxes.
5. After the message is sent to the mailboxes, switch back to the Real-time Monitor screen. You will see the message being scanned as it passes through the Real-time monitor. You will also see the test file being detected in the Real-time Monitor. In addition to the Real-time monitor you can also review the virus detection result in the Virus Log from the ScanMail Management console.

To test virus notification:

1. Configure virus scan to detect the virus/malware and notify the administrator.
   - **a.** Click **Virus Scanning > Target**. Select IntelliScan if necessary.
   - **b.** Click **Action**. Select **ActiveAction** and select **Notify** from the drop-down list.
   - **c.** Click **Notification**. Click **Notify administrator** and then click the icon to expand the page. Select **To** and type the email address where you want to send the notification.
   - **d.** Click **Save**.
2. Send an email containing the EICAR test script and verify that the administrator received the email.
   - **a.** Create a test message called "Test ScanMail" and attach a copy of the EICAR test script to your email.
   - **b.** Send the email to your test mailboxes.
   - **c.** Go to the administrator mailbox and view the notification.

Silent Installation

This version of ScanMail supports silent installation.

The following lists the general steps required to perform silent installation:

1. Launch Windows command prompt.
2. Locate the ScanMail for Exchange directory.
3. Type `Setup /R` to start recording mode.
4. Copy the pre-configured file (`setup-xxx.iss`) to the ScanMail for Exchange directory when the recording completes.
5. Type `Setup /S <pre-configured filename>` to perform silent installation.

If you do not want to record a new pre-configured file, you can use parameters to override user names and passwords in an existing pre-configured file. The following table displays the parameters you can use to configure silent installation settings.

Parameter	Description
Setup /H |Help| ?	Displays the Help screen.
Setup /R <pre-configured file path>	Start recording mode. If the path is empty, the default path is the Windows directory
Setup /S <pre-configured filename>	Perform silent installation with the file name you specify.
Setup /USER <user name>	Specify a different user name to override the log on user name and password that is defined in the pre-configured file. You need to provide a password before silent installation begins.
Setup /CONSOLEUSER <user name>	Specify a different user to override the console user name and password defined in the pre-configured file. You need to provide a password before silent installation begins.
Setup /PROXYUSER <user name>	Specify a different user to override the ScanMail proxy user name and password defined in the pre-configured file. You need to provide a password before silent installation begins.

TABLE 2-8. Silent Installation setting parameters

Parameter	Description
Setup /CMPROXYUSER <user name>	Specify a different user to override the Control Manager Agent proxy user name and password defined in the pre-configured file. You need to provide a password before silent installation begins.
Setup /CMWEBUSER <user name>	Specify a different user to override the Control Manager Agent Web user name and password defined in the pre-configured file. You need to provide a password before silent installation begins.
Setup /MV	Switch to “Verbose mode” to display the progress in a Command Prompt window. The default setting is concise mode which does not display the process and only records to a log file.
Setup /L <log file path>	Specify the log file path. The default path is the ScanMail source files folder.

TABLE 2-8. Silent Installation setting parameters

Silent Installation Limitations

The following lists the limitations for silent installation:

- Silent installation is only for local computers.
- Silent installation does not support cluster servers.
- Generate the pre-configured file by using recording mode the first time. Then, modify settings in the pre-configured file. However, do not modify settings in the **Do not edit** sections.
- Record settings using the latest version when performing an upgrade. Previous settings remain when performing an upgrade.
- Record settings separately for target servers with different languages. Do not apply pre-configured files recorded on an English operating system to a target server with a German operating system.

Performing Silent Installation

The steps in silent installation follow the same steps as regular installation. Refer to the corresponding installation sections for the different server roles. See *Installation for Exchange 2000 Server and Exchange Server 2003* starting on page 2-20, *Installation with Exchange Server 2007 Hub Transport / Mailbox Servers* starting on page 2-41, or *Installation with Exchange Server 2007 Edge Transport Servers* starting on page 2-58.

The differences are between the standard installation process and silent installation are:

- The Welcome screen displays a message reminding you that ScanMail records the installation process into a pre-configured file.
- In recording mode, ScanMail only records the user name and password and does not log on to target server(s).
- Once the recording completes, the file name and location information is listed on the setup screen.
- **Checking Target Server System Requirements** and **Selecting an Action** screens do not display.

Removing ScanMail

Uninstallation removes the following components:

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

Uninstallation of ScanMail 8.0 with Exchange Server 2007 does not remove the following components:

- Microsoft Visual C++ 2005 Redistributable
- Microsoft Visual C++ 2005 Redistributable (X64)

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

The following table displays the minimum privileges required for uninstalling ScanMail.

Exchange Version	Minimum Privileges	Feature Limitation Without Domain Administrator Privileges
Exchange 2000 Server and Exchange Server 2003	Local Administrator and Domain User	Cannot remove the EUQ mailbox. Manual removal of EUQ mailbox required.
Exchange Server 2007 Edge Transport	Local Administrator	N/A
Exchange Server 2007 Hub/Mailbox/Cluster	Local Administrator and Exchange Organization Administrator	N/A

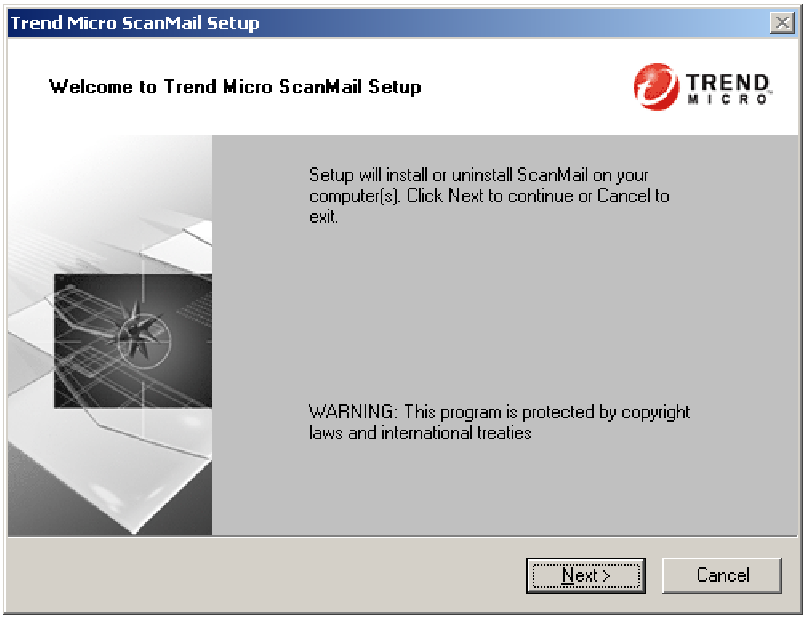
TABLE 2-9. Minimum privileges required for uninstalling ScanMail

Removing ScanMail using the Trend Micro™ Enterprise Solution CD

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

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

2. The **Welcome to Trend Micro ScanMail Setup** screen appears. Click **Next** to continue with the uninstallation.



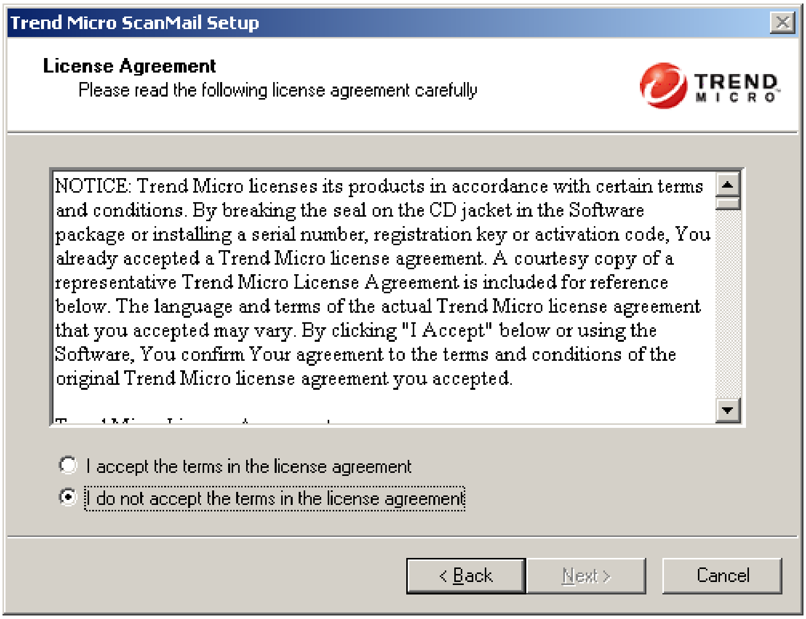
Trend Micro ScanMail Setup
Welcome to Trend Micro ScanMail Setup
TREND MICRO

Setup will install or uninstall ScanMail on your computer(s). Click Next to continue or Cancel to exit.

WARNING: This program is protected by copyright laws and international treaties

FIGURE 2-54. Welcome screen

3. The **License Agreement screen** appears. If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the process without modifying your operating system. Agree to the terms of the agreement by selecting **I Accept the terms in the license agreement** and click **Next** to continue with the uninstallation. The **Select an Action** screen appears.



Trend Micro ScanMail Setup

License Agreement

Please read the following license agreement carefully

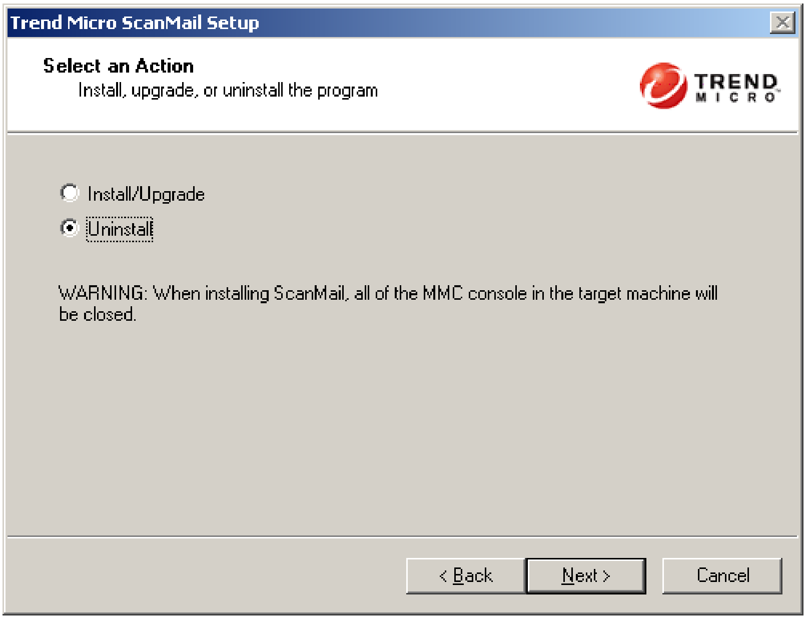
NOTICE: Trend Micro licenses its products in accordance with certain terms and conditions. By breaking the seal on the CD jacket in the Software package or installing a serial number, registration key or activation code, You already accepted a Trend Micro license agreement. A courtesy copy of a representative Trend Micro License Agreement is included for reference below. The language and terms of the actual Trend Micro license agreement that you accepted may vary. By clicking "I Accept" below or using the Software, You confirm Your agreement to the terms and conditions of the original Trend Micro license agreement you accepted.

○ I accept the terms in the license agreement

● I do not accept the terms in the license agreement

FIGURE 2-55. License Agreement screen

4. Select **Uninstall** to remove ScanMail from your server(s). The **Select Target Server(s)** screen appears.



Trend Micro ScanMail Setup

Select an Action

Install, upgrade, or uninstall the program

○ Install/Upgrade

● Uninstall

WARNING: When installing ScanMail, all of the MMC console in the target machine will be closed.

FIGURE 2-56. Select an Action screen

To uninstall ScanMail from a server:

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

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

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

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

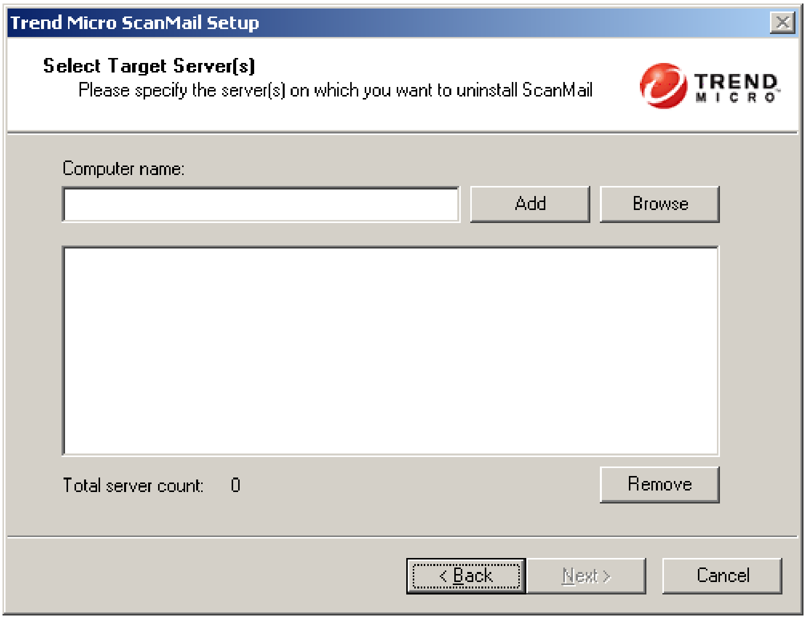
5. To uninstall ScanMail from a server:

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

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

   b. Click **Remove** to remove a server from the list.

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


Trend Micro ScanMail Setup

Select Target Server(s)

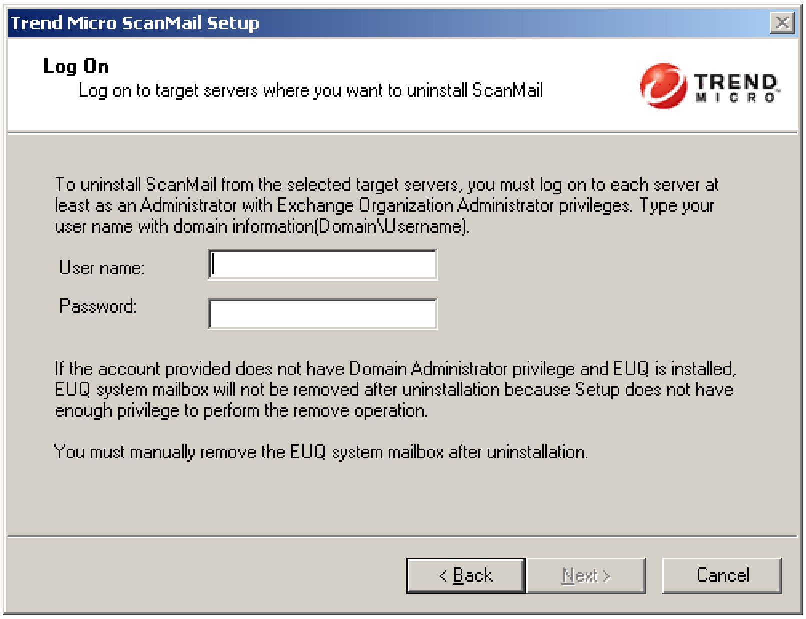
Please specify the server(s) on which you want to uninstall ScanMail

Computer name:

Total server count: 0

FIGURE 2-57. Select Target Server(s) screen

6. The **Log On** screen appears. Type the user name and password to log on to the target server to uninstall ScanMail. Click **Next** to continue. The **Configure Shared Directory** screen appears.



Trend Micro ScanMail Setup

Log On

Log on to target servers where you want to uninstall ScanMail

To uninstall ScanMail from the selected target servers, you must log on to each server at least as an Administrator with Exchange Organization Administrator privileges. Type your user name with domain information(Domain\Username).

User name:

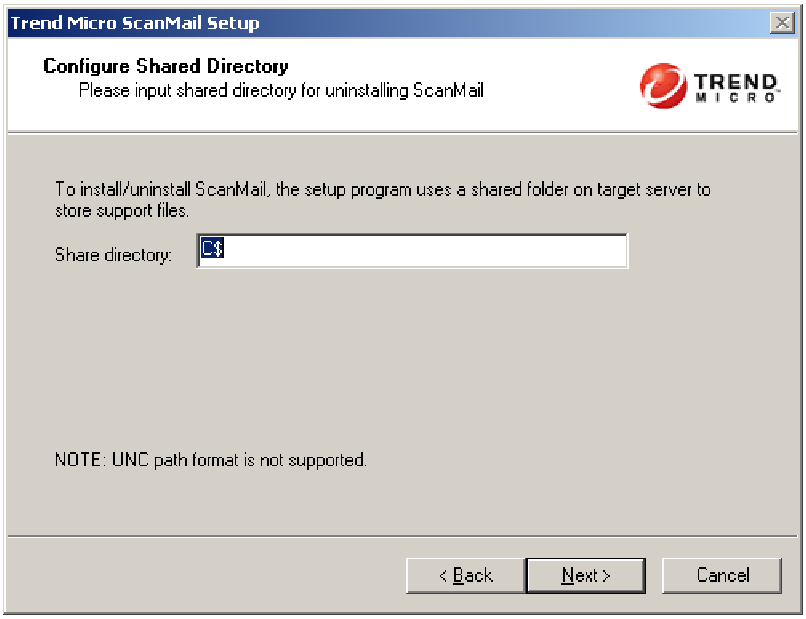
Password:

If the account provided does not have Domain Administrator privilege and EUQ is installed, EUQ system mailbox will not be removed after uninstallation because Setup does not have enough privilege to perform the remove operation.

You must manually remove the EUQ system mailbox after uninstallation.

FIGURE 2-58. Log On screen

7. The **Configure Shared Directory** screen appears. Use this screen to specify the shared directory for the target servers from where you will uninstall ScanMail.



Trend Micro ScanMail Setup

Configure Shared Directory

Please input shared directory for uninstalling ScanMail

To install/uninstall ScanMail, the setup program uses a shared folder on target server to store support files.

Share directory: C$

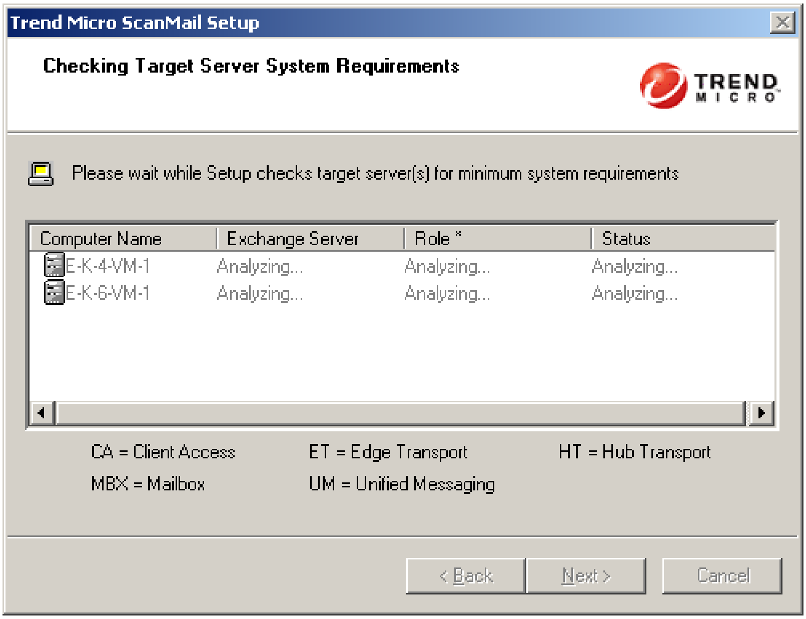
NOTE: UNC path format is not supported.

FIGURE 2-59. Configured Shared Directory screen

a. Specify a folder on the target server for storing support files for the uninstallation process.

b. Click **Next**.

8. The **Checking Target System Requirements** screen appears. View the screen and ensure the settings for the uninstallation are correct and click **Next** to continue.



Trend Micro ScanMail Setup

Checking Target Server System Requirements

Please wait while Setup checks target server(s) for minimum system requirements

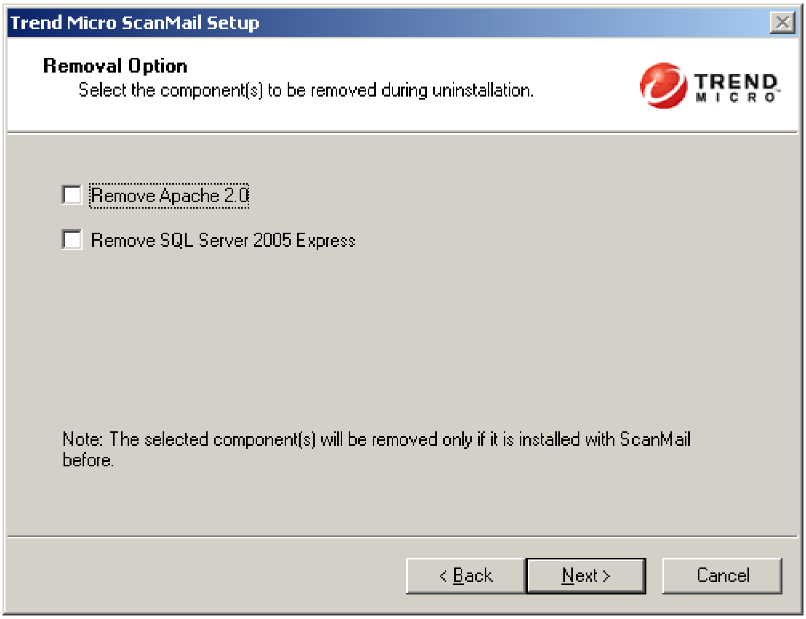
Computer Name	Exchange Server	Role *	Status
E-K-4-VM-1	Analyzing...	Analyzing...	Analyzing...
E-K-6-VM-1	Analyzing...	Analyzing...	Analyzing...

CA = Client Access   ET = Edge Transport   HT = Hub Transport

MBX = Mailbox   UM = Unified Messaging

FIGURE 2-60. Checking Target Server System Requirements screen

9. The **Removal Option** screen appears. Select the components to remove and click **Next**.



Trend Micro ScanMail Setup

Removal Option

Select the component(s) to be removed during uninstallation.

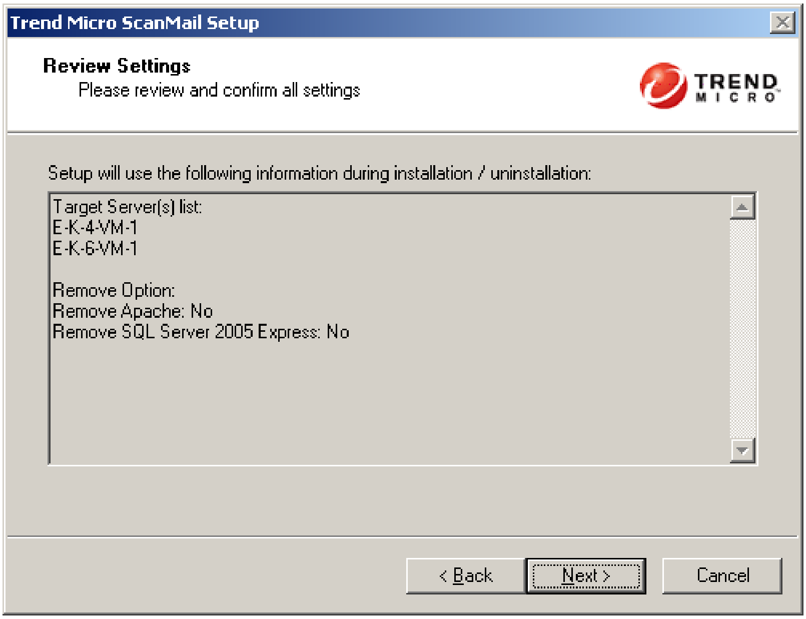
□ Remove Apache 2.0

□ Remove SQL Server 2005 Express

Note: The selected component(s) will be removed only if it is installed with ScanMail before.

FIGURE 2-61. Removal Option screen

10. The **Review Settings** screen appears. Review your settings and click **Next** to begin the uninstallation progress.



Trend Micro ScanMail Setup
Review Settings
Please review and confirm all settings
TREND MICRO
< Back
Next >
Cancel

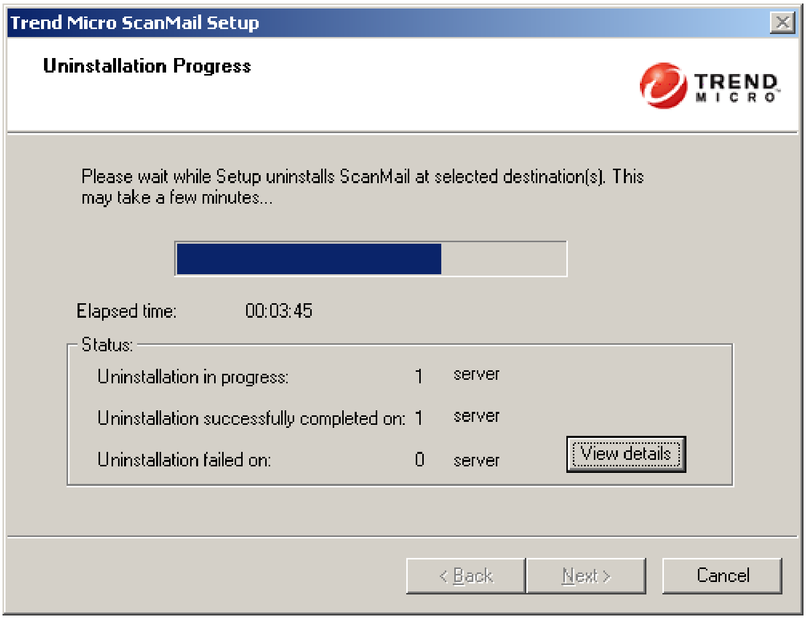
Setup will use the following information during installation / uninstallation:

Target Server(s) list:
E-K-4-VM-1
E-K-6-VM-1

Remove Option:
Remove Apache: No
Remove SQL Server 2005 Express: No

FIGURE 2-62. Review Settings screen

11. The **Uninstallation Progress** screen appears. When the uninstallation is complete, click **Next** to proceed.



Trend Micro ScanMail Setup

Uninstallation Progress

Please wait while Setup uninstalls ScanMail at selected destination(s). This may take a few minutes...

Elapsed time: 00:03:45

Status:

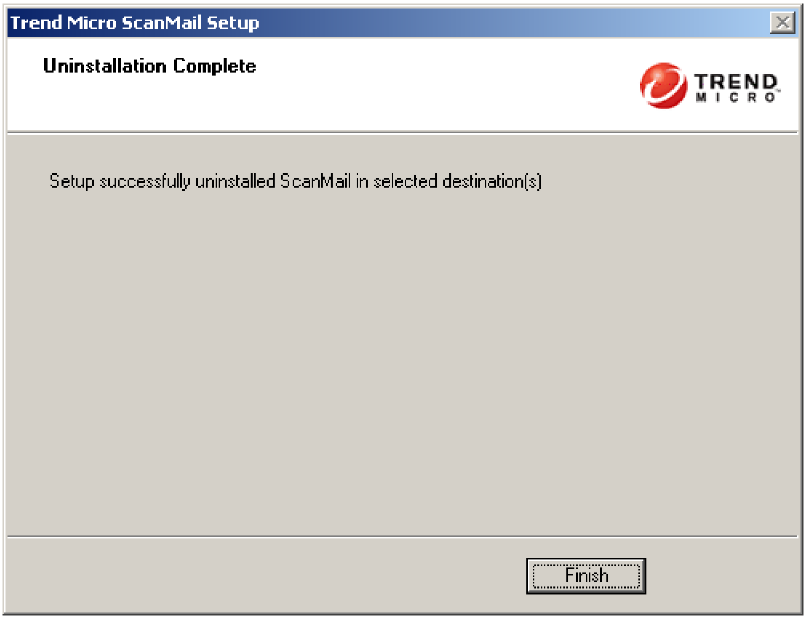
Uninstallation in progress: 1 server

Uninstallation successfully completed on: 1 server

Uninstallation failed on: 0 server

FIGURE 2-63. Uninstallation Progress

12. The **Uninstallation Complete** screen appears to inform you that the servers successfully uninstalled. Click **Finish** to exit the setup program. The setup program removes ScanMail from the selected servers.



Setup successfully uninstalled ScanMail in selected destination(s)

FIGURE 2-64. Uninstallation Complete screen

Removing ScanMail Using the Windows Control Panel

You can remove ScanMail using the Windows Control Panel, but you must remove Microsoft SQL Server 2005 Express and Apache separately. Using the setup program to uninstall ScanMail removes all related components and programs. Trend Micro recommends using the Setup.exe program to uninstall ScanMail.

To uninstall ScanMail:

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

Note: For Exchange Server 2007, ScanMail 8.0 installs Microsoft Visual C++ 2005 Redistributable and Microsoft Visual C++ 2005 Redistributable (X64) and they are not uninstalled when you uninstall ScanMail.

Removing ScanMail from Clusters

The instructions to uninstall ScanMail from clusters are similar to the non-cluster uninstallation instructions. For more information on removing non-clustered ScanMail, see *Removing ScanMail using the Trend Micro™ Enterprise Solution CD* on page 2-81.

To remove ScanMail from clusters

Run `setup.exe` again and uninstall ScanMail.

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

To manually remove ScanMail from a cluster:

1. Use **Add or Remove Programs** to uninstall on each node.
2. Use **Windows Cluster Administrator** to delete ScanMail resources.
3. Use one of the following commands unregister ScanMail cluster resource type:
   - Microsoft Exchange 2000 Server/Exchange Server 2003/Exchange Server 2007 SCC: **cluster restype clusRDLL /delete /type**

- Microsoft Exchange 2007 CCR: **cluster restype clusRDLLCCR /delete /type**

Note: For Exchange Server 2007, ScanMail 8.0 installs Microsoft Visual C++ 2005 Redistributable and Microsoft Visual C++ 2005 Redistributable (X64) and they are not uninstalled when you uninstall ScanMail.

Chapter 3

Registering, Activating, and Updating ScanMail

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

In this chapter, you will find information about:

Registering ScanMail

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

When you register, you receive an Activation Code (AC) that you can use to activate ScanMail. For more information, see *Activation Codes* on page 3-4.

To register your product:

Use one of the following methods to register:

- During installation

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

- Online

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

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

- Contact Trend Micro directly

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

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

For more information, see *Contacting Technical Support* on page 6-2.

Activating ScanMail

The following conditions require Activation.

- Installing ScanMail for the first time

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

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

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

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

Activation Codes

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

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

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

Standard Activation Code

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

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

TABLE 3-1. Standard Activation Code features

Suite Activation Code

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

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

TABLE 3-2. Suite Activation Code features

Activation Code Comparison

The following table illustrates the features available for each type of activation code.

Feature	Suite AC		Standard AC	
	Full	Trial	Full	Trial
Management console	Yes	Yes	Yes	Yes
Anti-Spam and Content Filtering items on Reports, Logs, and Quarantine Manager	Yes	Yes	No	No
Virus Scan	Yes	Yes	Yes	Yes
Attachment Blocking	Yes	Yes	Yes	Yes

TABLE 3-3. Features available for each type of activation code

Feature	Suite AC		Standard AC	
	Full	Trial	Full	Trial
Anti-Spam	Yes	Yes	No	No
Content Filtering	Yes	Yes	No	No
Manual Scan / Scheduled Scan	Yes	Yes	Yes	Yes
Active Update	Yes	Yes	Yes	Yes
End User Quarantine	Yes	Yes	No	No
Control Manager Support	Yes	Yes	Yes	Yes

TABLE 3-3. Features available for each type of activation code

You can activate ScanMail by one of the following methods:

To activate ScanMail during installation:

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

To activate ScanMail after installation using the product console:

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

Updating ScanMail

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

- Virus pattern
- Additional threat pattern
- IntelliTrap pattern
- IntelliTrap exception pattern
- Scan engine
- Spam pattern
- Spam engine

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

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

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

Updating Components on Clusters

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

Note: On Microsoft Exchange Server 2007 CCR model, ScanMail automatically updates when the ScanMail resource is online.

Setting Your Proxy Server

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

The following features use Proxy servers:

- ActiveUpdate
- Product registration
- World Virus Tracking

To set the Internet proxy:

1. Log on to the ScanMail product console.
2. On the sidebar, click **Administration** > **Proxy**. The **Proxy** screen appears.
3. Select **Use a proxy server for update and product license notification**.
4. Type the server name or IP address of the proxy server and its port number.
5. Select **Use SOCKS 5 proxy protocol** to use SOCKS 5 protocol.
6. If your proxy server requires a password, type your user name and password in the fields provided.
7. Click **Save** to save your settings.

Manually Updating Your Components

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

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

To manually install your components:

1. Log on to the ScanMail product console.
2. Click **Updates** > **Manual**.
3. Select the component that you wish to update.
4. Click **Update**. ScanMail begins downloading the components and displays a progress bar that shows you the elapsed time and the percentage of the download remaining.

Setting a scheduled Update

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

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

To configure scheduled updates:

1. Select a source from which your updates will be downloaded.
   a. Click **Updates** > **Download Source**. The **Source** screen appears.
   b. Select a download source.
   c. Click **Save**.
2. Set up your schedule.
   a. Click **Updates** > **Scheduled**.
   b. Click **Enable schedule updates** to have ScanMail begin to update according to your schedule.
   c. Set the **Update Schedule**.
      i. Select an update frequency: by minute, hour, day, or week.
      ii. Set the start time for the schedule by selecting the hour and minute. Each time the update occurs, the download begins at this time.
3. Select the components for downloading from the update source.
   a. Select the components that ScanMail downloads during each scheduled update.

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

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

Download Source

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

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

- Trend Micro ActiveUpdate Server

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

  For more information, see *About ActiveUpdate* starting on page 1-12

- Intranet location containing a copy of the current file

  Download components from an Intranet source that receives updated components.

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

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

- Other update source

  Download components from an Internet or other source.

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

Allowing Other Servers to Download Updates from a ScanMail Server

Click **Allow other servers to download updates from this server** to set ScanMail to create a duplicate copy of the update package on the current server. Normally, ScanMail only downloads components that the user has set it to download or the increments of the components that it needs. See *Incremental updates of the pattern file* on page 1-12. When you set ScanMail to duplicate the update package, it will download all the components that are available for downloading.

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

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

Rolling Back a Component Update

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

To manually roll back to a previous component:

1. Stop the following ScanMail services:
   - ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail_RemoteConfig)
   - ScanMail for Microsoft Exchange Master Service (ScanMail_Master)
2. Delete all the files in:
   - `"<Install folder>\AU_Data\AU_Cache\"`
   - `"<Install folder>\AU_Data\AU_Temp\"`
   - `"<Install folder>\AU_Data\AU_Storage\"`
   - `"<Install folder>\web\activeupdate\"`
3. Roll back the Virus pattern file, Additional Threats pattern file, IntelliTrap pattern file, and the IntelliTrap exception pattern file.

   a. Remove the most recently downloaded pattern files from this location:

   `"<Install folder>\engine\vsapi\latest"`

   b. Remove the following files. Verify that ScanMail has already downloaded an older version of these files to which you can roll back.

   - The Virus pattern file:

     `ex: lpt$vpn.xxx`
   - The Additional Threats pattern file:

     `ssaptn.xxx`
   - The IntelliTrap pattern file:

     `tmblack.xxx`
   - The IntelliTrap exception file:

     `tmwhite.xxx`

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

   For example: If you have recently downloaded Virus pattern file `ex:lpt$vpn.345` and you want to roll back to a previous download pattern, `ex:lpt$vpn.344`, then delete `ex:lpt$vpn.345` and ScanMail will begin to use `ex:lpt$vpn.344`.

   c. Delete all files in:
   - `"<Install folder\engine\vsapi\primary\pattern\"`
   - `"<Install folder\engine\vsapi\secondary\pattern\"`

4. To roll back the anti-spam pattern file:

   a. Remove the latest pattern in:
   - `"<Install folder>\engine\TMASE\latest\rule"`
     `ex:tmxxxxxx.*`
     `"xxxxxx" means the latest version.`

   b. Delete all files in:
   - `"<Install folder>\engine\TMASE\primary\rule\"`
   - `"<Install folder>\engine\TMASE\secondary\rule\"`
   - `"<Install folder>\engine\TMASE\latest\rule\cache\"`
   - `"<Install folder>\engine\TMASE\primary\rule\cache\"`
   - `"<Install folder>\engine\TMASE\secondary\rule\"`

5. Start the following ScanMail services again:
   - ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail_RemoteConfig)
   - ScanMail for Microsoft Exchange Master Service (ScanMail_Master)

Chapter 4

Managing ScanMail Servers

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

In this chapter, you will find information about:

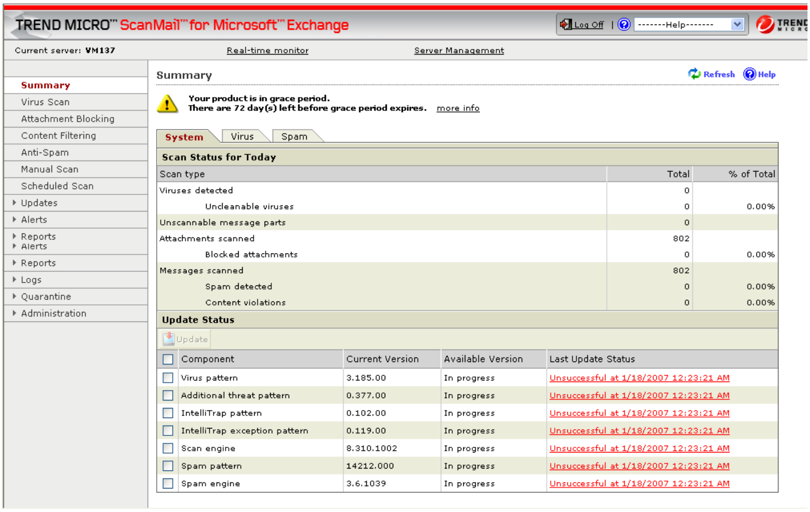
Using the Product Console

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

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

Management Console Main View

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



Your product is in grace period.
There are 72 day(s) left before grace period expires. more info

Scan Status for Today

Scan type	Total	% of Total
Viruses detected	0	
Uncleanable viruses	0	0.00%
Unscannable message parts	0	
Attachments scanned	802	
Blocked attachments	0	0.00%
Messages scanned	802	
Spam detected	0	0.00%
Content violations	0	0.00%

Update Status

□	Component	Current Version	Available Version	Last Update Status
□	Virus pattern	3.185.00	In progress	Unsuccessful at 1/18/2007 12:23:21 AM
□	Additional threat pattern	0.377.00	In progress	Unsuccessful at 1/18/2007 12:23:21 AM
□	IntelliTrap pattern	0.102.00	In progress	Unsuccessful at 1/18/2007 12:23:21 AM
□	IntelliTrap exception pattern	0.119.00	In progress	Unsuccessful at 1/18/2007 12:23:21 AM
□	Scan engine	8.310.1002	In progress	Unsuccessful at 1/18/2007 12:23:21 AM
□	Spam pattern	14212.000	In progress	Unsuccessful at 1/18/2007 12:23:21 AM
□	Spam engine	3.6.1039	In progress	Unsuccessful at 1/18/2007 12:23:21 AM

FIGURE 4-1. The product console

Product Console Elements

Banner

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

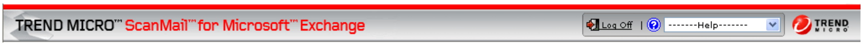


FIGURE 4-2. Product console banner

The banner displays the following:

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

  For more information, see *Understanding Real-time Monitor* on page 4-8.
- **Server Management** console—click to access the Server Management console.

  For more information, see *Understanding the Server Management Console* on page 4-9.
- **Log Off**—click this to end your session and close the product console. Logging off the product console prevents unauthorized users from modifying the settings.
- **Help**—get support by selecting an option from the drop-down list

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

- **Sidebar** — provides access to the main menu items for ScanMail

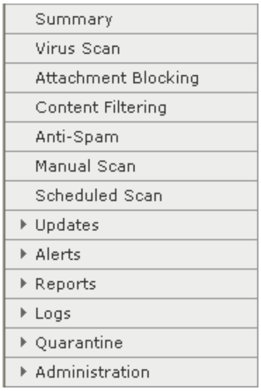
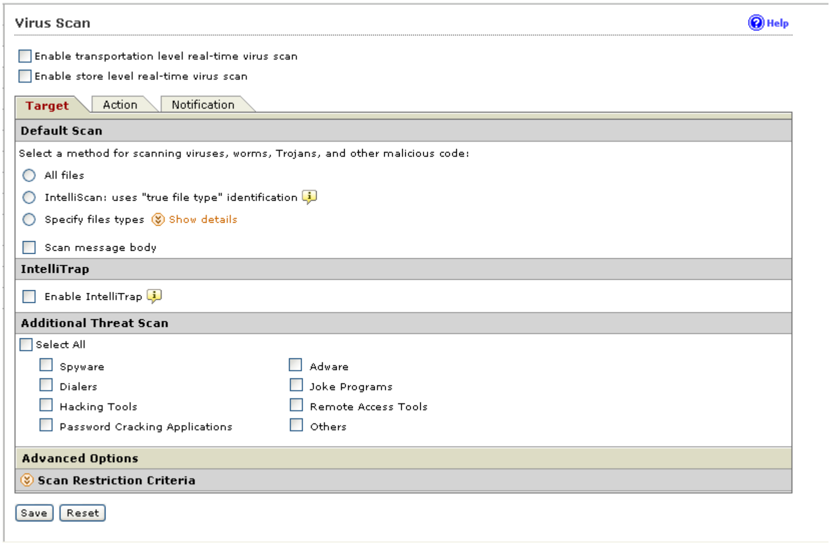


FIGURE 4-3. Product console sidebar

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



Virus Scan — Help

□ Enable transportation level real-time virus scan

□ Enable store level real-time virus scan

Target | Action | Notification

Default Scan

Select a method for scanning viruses, worms, Trojans, and other malicious code:

○ All files

○ IntelliScan: uses "true file type" identification

○ Specify files types Show details

□ Scan message body

IntelliTrap

□ Enable IntelliTrap

Additional Threat Scan

□ Select All

□ Spyware	□ Adware
□ Dialers	□ Joke Programs
□ Hacking Tools	□ Remote Access Tools
□ Password Cracking Applications	□ Others

Advanced Options

Scan Restriction Criteria

Save | Reset

FIGURE 4-4. **Product console configuration area**

Getting Help While Using the ScanMail Product Console

ScanMail offers the following types of help:

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

Viewing Servers from the Product Console

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

Note: Use an account with local administrator privileges and/or an account that belongs to the ScanMail administrative group. For ScanMail with Exchange 2000/2003 you can use an account that is part of the "SMEX Admin Group". For ScanMail with Exchange 2007 you can use an account that is part of the Active Directory group or any Active Directory group that is part of the forest that was used to activate Server Management.

To view the product console for a local server

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

To view the product console from a remote server:

Use a Java-enabled Web browser that supports frames and access one of the following:

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

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

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

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

Viewing Virtual Servers on a Cluster

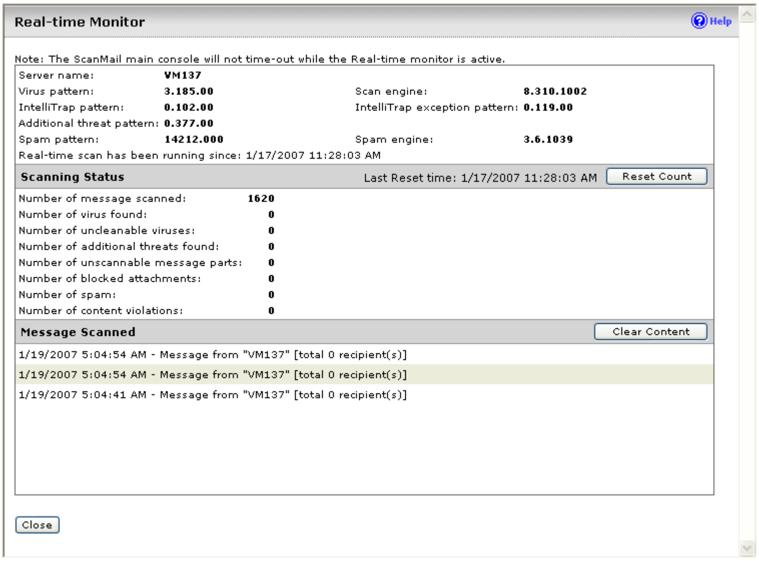
Each Exchange virtual server is an independent management unit and must have its own configuration and log storage, no matter how many virtual servers are on one single cluster node. The product console should use the network name/IP address associated with the specified Exchange virtual server to control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

Each node has a ScanMail shortcut to allow you to view all virtual servers link. Click **All programs** > **Trend Micro ScanMail for Microsoft Exchange** > **ScanMail Management Console** to view all virtual servers.

Note: The virtual server links are not updated when you create or delete the ScanMail resource manually.

Understanding Real-time Monitor

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



Note: The ScanMail main console will not time-out while the Real-time monitor is active.

```
Server name:               VM137
Virus pattern:             3.185.00        Scan engine:                   8.310.1002
IntelliTrap pattern:       0.102.00        IntelliTrap exception pattern: 0.119.00
Additional threat pattern: 0.377.00
Spam pattern:              14212.000       Spam engine:                   3.6.1039
Real-time scan has been running since: 1/17/2007 11:28:03 AM
```

Scanning Status Last Reset time: 1/17/2007 11:28:03 AM

```
Number of message scanned:            1620
Number of virus found:                   0
Number of uncleanable viruses:           0
Number of additional threats found:      0
Number of unscannable message parts:     0
Number of blocked attachments:           0
Number of spam:                          0
Number of content violations:            0
```

Message Scanned

```
1/19/2007 5:04:54 AM - Message from "VM137" [total 0 recipient(s)]
1/19/2007 5:04:54 AM - Message from "VM137" [total 0 recipient(s)]
1/19/2007 5:04:41 AM - Message from "VM137" [total 0 recipient(s)]
```

FIGURE 4-5. The Real-time monitor

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

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

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

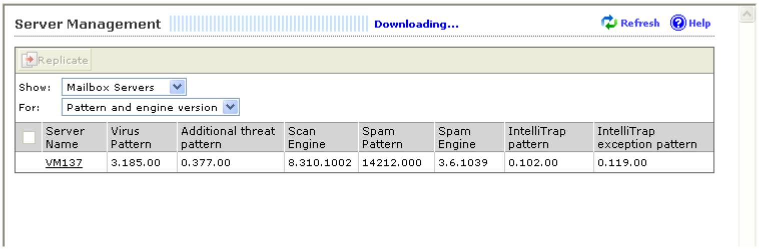
Understanding the Server Management Console

The ScanMail Server Management console enables you to view all of the ScanMail servers on a network. In Exchange 2000 Server and Exchange Server 2003 environments, special permissions are required to be able to view and replicate settings to servers belonging to different domains within the same domain forest.

To grant access rights to other domains in the same forest for Exchange 2000 and Exchange 2003:

1. Run regedit. (regedt32 on Windows 2000.)
2. From `HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL SECUREPIPESERVERS\winreg` right click **winreg** > **Permissions** from the popup menu (for Windows 2000, select **Security** > **Permissions**.)
3. Add the "SMEX Admin Group"of the domain the controlling Server Management console belongs to and allow Read.
4. From `HKLM\SOFTWARE\TRENDMICRO\ScanMail for Exchange` right click **ScanMail for Exchange** > **Permissions** from the popup menu (for Windows 2000 select **Security** > **Permissions**.)
5. Add the "SMEX Admin Group" of the domain the controlling Server Management console belongs to and allow **Full Control**.

Note: This procedure is not required for Exchange 2007.



Show: Mailbox Servers

For: Pattern and engine version

□	Server Name	Virus Pattern	Additional threat pattern	Scan Engine	Spam Pattern	Spam Engine	IntelliTrap pattern	IntelliTrap exception pattern
	VM137	3.185.00	0.377.00	8.310.1002	14212.000	3.6.1039	0.102.00	0.119.00

FIGURE 4-6. The Server Management console

Use the Server Management console to do the following:

Feature	Description
View pattern and engine version	View information about current scan engine, virus pattern file, additional threat pattern, IntelliTrap pattern, IntelliTrap exception pattern, spam engine, and spam pattern files.
View scanning result	View information about the total messages scanned and the scan results. Scanning results also shows the number of detected virus/malware, uncleanable virus/malware, blocked attachments, spam, content violations, and unscannable message parts.
View scanning status	On Exchange 2000 Server and Exchange Server 2003 you can view the scan status for virus scan, attachment blocking, content filtering, and anti-spam. On Exchange Server 2007 you can view the scan status for Store virus scan, Transport virus scan, Store attachment blocking, Transport attachment blocking, Store content filtering, Transport content filtering, and anti-spam.
View last replication	View the status of the last replication and the duration of the last replication.
Replicate settings to remote servers	Replicate settings to one or multiple remote servers in the list.

TABLE 4-1. Server Management console features

Activating Server Management

The Server Management Console displays remote server status and allows you to replicate settings to remote servers. If you did not activate Server Management during the ScanMail installation process, you need to activate Server Management before you use the Server Management Console. You must log on using an account with local administrator privileges to activate Server Management. Then click the Server Management link at the top of the product console.

- To activate Server Management for ScanMail with Exchange 2000 Server or Exchange Server 2003—Select to Specify an existing account from Active

Directory or Create a new account. The activation wizard prompts you through the steps required to activate Server Management.

- To activate Server Management for ScanMail with Exchange Server 2007—Specify an existing group in Active Directory and the activation wizard prompts you through the steps required to activate Server Management.

Using Server Management to Replicate Configurations

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

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

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

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

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

Manually Creating a ScanMail Resource for Virtual Servers

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

To create a ScanMail resource for a virtual server:

1. Create a ScanMail resource manually. Select the ScanMail resource type:
   - Microsoft Exchange 2000 Server: ScanMail for Exchange Cluster Agent
   - Microsoft Exchange Server 2003: ScanMail for Exchange Cluster Agent
   - Microsoft Exchange Server 2007 SCC: ScanMail for Exchange Cluster Agent for Single Copy Cluster
   - Microsoft Exchange Server 2007 CCR: ScanMail for Exchange Cluster Agent for MNS Cluster.
2. Create a ScanMail resource on the server group for the target’s virtual server.

   The new resource will have a dependency on resource types.

   The following lists the ScanMail resource dependencies:
   - Microsoft Exchange 2000 Server— Physical Disk, Network Name, and Microsoft Exchange Information store.
   - Microsoft Exchange Server 2003—Physical Disk/Mount-point Disk, Network Name, and Microsoft Exchange Information store.
   - Microsoft Exchange Server 2007 SCC—Physical Disk/Mount-point Disk, Network name, and Microsoft Exchange Information store
   - Microsoft Exchange Server 2007 CCR— Network Name and Microsoft Exchange Information Store.

   ScanMail puts data on the disk created for your **Physical Disk** resource. Do not move or modify the data on the disk. If you want to install on a mount-point disk, select a mount-point disk’s resource.

3. Clear **Affect the group** in the SMEX resource properties. Right click the **SMEX resource > properties > Advanced > Uncheck** and clear the **Affect the group** check box.
4. Create a virtual directory for viewing reports about the target server on each node where a virtual server is installed. Before doing this step, ensure that the target virtual server is on the current node. Depending on your installation options, you can create the virtual directory using Internet Information Services (IIS) or Apache.
   - Using IIS Web server to create the virtual directory:

     i. To open IIS click the following path:

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

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

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

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

     For example: G:\SMEX\data\report
   - Using Apache Web server to create the virtual directory:

     i. To open `Httpd.conf`, click the following path from the **Start** menu:

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

     ii. Find the following text string:

     ```
     # SMEX Virtual Path -- Start
     ```

     iii. Type the following:

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

     For example:

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

```
    Allow from all
</DirectoryMatch>
```

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

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

Type the following in the area provided for virtual servers:

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

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

5. On Exchange 2000 and Exchange 2003, create an account and mailbox for End User Quarantine functions as follows:

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

For example:

```
EUQ_VirtualServer1
```

Chapter 5

Establishing and Maintaining Security for Your Exchange Servers

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

In this chapter you will find information about:

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

Establishing a Security Baseline

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

1. Update ScanMail.

   Update components immediately following installation to gain optimal protection for ScanMail. Refer to *Updating ScanMail* starting on page 5-4.

2. Verify that ScanMail is running and functioning correctly.

   From the product console, click **Real-time monitor**. The Real-time monitor page opens and shows ScanMail activities in real time. **Real-time scan has been running since** indicates that ScanMail is performing scans.

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

   Trend Micro recommends you perform a manual scan of your entire Information Store following installation. When ScanMail detects viruses/malware or other malicious code it takes action against them according to Trend Micro defaults.

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

Note: ScanMail uses Trend Micro default values to filter undesirable content, block potentially harmful attachments and scan for viruses/malware and other security threats in real time. Customize ScanMail configurations to gain the optimal protection and efficiency.

Maintaining Security

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

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

Refer to *Setting a scheduled Update* starting on page 3-9.

2. Viruses/malware and other security risks can attack your Exchange servers from unexpected sources such as local unprotected computers and servers or by bypassing too lenient configurations. Run regular scheduled scans to significantly reduce this risk.
3. Select **Enable action on Mass-mailing behavior** from the Virus Scan page to provide early warning of virus outbreaks.
4. When an attack occurs, it is vital that administrators receive early warning to prevent the attack from spreading. Trend Micro recommends setting ScanMail to send alerts to key network security professionals when outbreak conditions threaten your network. You can use Outbreak Alert to set ScanMail to automatically notify designated individuals.
5. Consider your overall network security. ScanMail for Microsoft Exchange is designed to guard your Exchange mail servers. ScanMail does not provide protection to non-Exchange mail servers, file servers, desktops, or gateway devices. ScanMail protection is enhanced when used together with other Trend Micro products such as Trend Micro OfficeScan™ to protect your file servers and desktops, and Trend Micro InterScan VirusWall™ or InterScan™ Messaging Security Suite to protect your network perimeter.

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

   `http://www.trendmicro.com/en/products/global/enterprise.htm`
6. File-based antivirus software usually allows you to set up folders to exclude from scanning. Trend Micro recommends setting up the following folders to exclude from scanning when using ScanMail with other antivirus software:
   - SMEX/storage/quarantine
   - SMEX/storage/backup folder
   - SMEX/storage/archive
   - SMEX/temp
   - SMEX/debug

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

Updating ScanMail

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

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

1. Register your software. See *Registering ScanMail* on page 3-2.
2. If a proxy server handles Internet traffic on your network, you must set the proxy server information. See *Setting Your Proxy Server* on page 3-7
3. Configure your update method and source. Methods include **Manual Update** and **Scheduled Update**. Sources include the ActiveUpdate server, the Internet, and the Intranet UNC path. See *Manually Updating Your Components* on page 3-9 and *Setting a scheduled Update* on page 3-9.

Managing Outbreak Situations

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

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

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

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

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

      `http://www.trendmicro.com/vinfo/`
    - Check ScanMail notifications. ScanMail can be set to automatically send alerts when outbreak conditions exist. In addition, ScanMail can be set to notify administrators or other designated individuals when ScanMail takes actions against detected threats.
    - For a quick analysis of the security incident, view the ScanMail Summary screen or create a one-time report. For more detailed information about the security incident, query the logs.

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

     Refer to *Updating ScanMail* starting on page 5-4.
   - Follow-up the update with a manual scan of the entire information store. Use the Trend Micro recommended defaults such as IntelliScan and ActiveAction or set even more aggressive scanning filters. If you know exactly what you are scanning for, select **Specified files** from the Virus Scan screen and type the name of the file for ScanMail to detect.
3. Analyzing
   - Perform a Log Query to discover information about the attack. The log contains such useful information as the time and date, sender and receiver, and infected attachment names.
   - If you need some assistance to help analyze the security problem, send your virus/malware case to the Trend Micro Virus Response Service.

     `https://premium.trendmicro.com/virusresponse/en/us/VRS/logon/logon.asp`
   - If you need more assistance, contact Trend Micro support. See *Contacting Technical Support* on page 6-2.
4. Recovering

   When you have restored your Exchange environment, consider changing your configurations and security policies. Consider the following points:
   - Set ScanMail to backup files before taking action and then set very aggressive configurations. This allows ScanMail to detect and eliminate many threats without taking irreversible actions.
   - Monitor the results using the real-time monitor or by generating logs and reports.
   - Use the Server Management tool to quickly and easily replicate configurations from one secure and tested ScanMail server to another.

Chapter 6

Getting Support and Contacting Trend Micro

This chapter discusses how to perform miscellaneous administrator tasks as well as how to get technical support.

In this chapter, you will find information about:

- *Contacting Technical Support* starting on page 6-2
- *Before Contacting Technical Support* on page 6-3
- *Contacting Trend Micro* starting on page 6-4
- *Known Issues* starting on page 6-5

Contacting Technical Support

There is an abundance of security information and support available through the Web site. You can find the following:

- Downloadable product upgrades, component updates and hot fix patches
- Security advisories on the latest outbreaks
- Downloadable trial versions of Trend Micro products
- Expert advise on specific viruses/malware in the wild and computer security in general
- An encyclopedia of computer security information, white papers, and virus/malware statistics
- Free downloadable software for virus scans, web feeds, and security testing

To contact Trend Micro technical support:

1. Visit the following URL:
   `http://kb.trendmicro.com/solutions/`
2. Click the link for the region you want to contact and follow the instructions for contacting support in that region.

You can find Trend Micro contacts in the following regions:

- Asia/Pacific
- Australia and New Zealand
- Latin America
- United States and Canada.

Before Contacting Technical Support

While our basic technical support staff is always pleased to handle your inquiries, there are a couple things you can do to quickly find the answer you are seeking.

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

  The documentation set for this product includes the following:

  Getting Started Guide. The Getting Started Guide introduces ScanMail and provides instructions for upgrading and installing. The latest version of the Getting Started Guide is available in electronic form:

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

  Online help—The purpose of online help is to provide conceptual and procedural information. Online help is accessible from the ScanMail Web management console.

  Readme file—The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and release history.

  Knowledge Base

  `http://esupport.trendmicro.com`

  This site contains the most up-to-date information about all Trend Micro products. Other inquiries that were already answered are also posted and a dynamic list of the most frequently asked questions is also displayed.

- To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:
  - Product serial number
  - ScanMail program, scan engine, pattern file, version number
  - OS name and version
  - Internet connection type
  - Exact text of any error message given
  - Steps to reproduce the problem

Contacting Trend Micro

Trend Micro Incorporated has its world headquarters at:

Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku, Tokyo 151-0053 Japan.

In the United States, Trend Micro is located at:

10101 N. De Anza Blvd.
Cupertino, CA 95014-9985
Tel: +1-408-257-1500
Fax: +1-408-257-2003

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

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

Note: The information on this Web site is subject to change without notice.

The Trend Micro Web site has a wealth of sales and corporate information available.

- Corporate information includes our company profile, international business office contacts, and partnering and alliance information.
- Sales information includes product evaluation information and trial downloads, reseller contacts, and virus/malware research information.

TrendLabs[SM]

TrendLabs is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Irvine, CA, to mitigate outbreaks and provide urgent support.

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

Known Issues

Known issues document unexpected ScanMail behavior that might require a temporary workaround. Trend Micro recommends always checking the Readme file for information about system requirements and known issues that could affect installation or performance. Readme files also contain a description of what's new in a particular release, and other helpful information.

The latest known issues and possible workarounds can also be found in the Trend Micro Knowledge Base:

`http://esupport.trendmicro.com`

Chapter 7

Understanding Threats to an Exchange Environment

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

In this chapter, you will find information about:

What Do the Terms Mean?

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

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

Viruses/Malware

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

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

Generally, there are three kinds of viruses/malware:

- File

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

- Boot

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

- Script

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

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

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

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

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

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

Worms

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

Trojan Horse Programs

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

Joke Programs

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

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

About Mass-Mailing Attacks

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

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

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

About Compressed Files

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

ScanMail currently supports the following compression types:

- Extraction–used when multiple files have been compressed or archived into a single file: PKZIP, LHA, LZH, ARJ, MIME, MSCF, TAR, GZIP, BZIP2, RAR, and ACE.
- Expansion–used when only a single file has been compressed or archived into a single file: PKLITE, PKLITE32, LZEXE, DIET, ASPACK, UPX, MSCOMP, LZW, MACBIN, and Petite.
- Decoding–used when a file has been converted from binary to ASCII, a method that is widely employed by email systems: UUENCODE and BINHEX.

Note: When ScanMail does not support the compression type, then it cannot detect viruses/malware in compression layers beyond the first compression layer.

When ScanMail encounters a compressed file it does the following:

1. ScanMail extracts the compressed files and scans them.

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

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

   ScanMail performs the same action against infected files detected in compressed formats as for other infected files. For example, if you select **Quarantine entire message** as the action for infected files, then ScanMail quarantines entire messages in which it detects infected files.

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

About Macro Viruses/Malware

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

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

How ScanMail prevents macro viruses/malware from infecting your Exchange server:

- Detects malicious macro code using heuristic scanning

  Heuristic scanning is an evaluative method of detecting viruses/malware. This method excels at detecting undiscovered viruses/malware and threats that do not have a known virus signature
- Strips all macro code from scanned files.

Spyware/Grayware

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

Types of spyware/grayware

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

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

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

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

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

Hacking Tools: helps hackers enter computers.

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

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

Potential Risks and Threats

The existence of spyware/grayware on your network have the potential to introduce the following:

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

How ScanMail Protects the Exchange Environment

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

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

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

- Anti-spam

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

- Content filtering

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

- Attachment blocking

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

- Virus scan

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

Appendix A

Windows Event Log Codes

Event Identifications for notifications written into windows event logs have changed a lot from previous versions of ScanMail. This change might impact your monitoring efforts. Consult the following table to understand the Windows event logs.

Event ID	Facility	Type/ Severity	Category	Description
3	Application	Error	None	ScanMail service started successfully.
4	Application	Error	None	ScanMail service stopped successfully.
5	Application	Warning	None	Virus scanning notification.
6	Application	Warning	None	Attachment blocking notification.
7	Application	Warning	None	Content filtering notification.
16	Application	Warning	None	Alert. Manual update unsuccessful.
17	Application	Information	None	Alert. Manual update successful.
18	Application	Warning	None	Alert. Last update time is older than specified time.
19	Application	Information	None	Alert. Manual scan successful.

TABLE A-1. ScanMail Windows Event Log Codes

Event ID	Facility	Type/ Severity	Category	Description
20	Application	Error	None	Alert. Manual scan unsuccessful.
21	Application	Warning	None	Alert. Scan time exceeds specified time.
22	Application	Warning	None	Alert. The disk space on the local drive (volume) of the backup, quarantine, or archive directory is less than specified size.
23	Application	Warning	None	Alert. The size of database to keep quarantine and logs exceeds specified size.
24	Application	Information	None	Alert. Scheduled scan successful.
25	Application	Error	None	Alert. Scheduled scan unsuccessful.
32	Application	Error	None	Alert. Scheduled update unsuccessful.
33	Application	Information	None	Alert. Scheduled update successful.
80	Application	Information	None	Alert. Outbreak Prevention Mode started.
82	Application	Information	None	Alert. Outbreak Prevention Mode stopped and restored configuration.
257	Application	Warning	None	Virus Outbreak Alert.
258	Application	Warning	None	Uncleanable virus Outbreak Alert.
259	Application	Warning	None	Blocked attachment Outbreak Alert.
513	Application	Error	None	Filter loading exception.
514	Application	Error	None	Adapter loading exception.
4097	Application	Warning	None	Alert. The disk space on the local drive of the MS Exchange transaction log is less than specified size.
4098	Application	Warning	None	Alert. The Microsoft Exchange mail store size exceeds specified size
4099	Application	Warning	None	Alert. The Microsoft Exchange SMTP messages queued continuously exceeds the specified number

TABLE A-1. ScanMail Windows Event Log Codes

Event ID	Facility	Type/ Severity	Category	Description
4112	Application	Error	None	ScanMail Master Service stopped due to insufficient disk space. Please free up some disk space and restart ScanMail Master Service.
8193	Application	Information	None	EUQ. Processing manual End User Quarantine maintenance task started.
8194	Application	Information	None	EUQ. Processing of manual End User Quarantine maintenance task ended.
8195	Application	Information	None	EUQ. Processing of schedule End User Quarantine maintenance task started.
8196	Application	Information	None	EUQ. End of processing schedule End User Quarantine maintenance task.
8197	Application	Information	None	EUQ. Start to process enable End User Quarantine task.
8198	Application	Information	None	EUQ. End of processing enable End User Quarantine task.
8199	Application	Information	None	EUQ. Start to process disable End User Quarantine task.
8200	Application	Information	None	EUQ. End of processing disable End User Quarantine task
12289	Application	Error	None	The transport scan module was unable to load the ScanMail transport hook. This could be caused by improper COM registration, missing DLL files, or privilege issues with the hookSMTP.dll. Check if the required files are complete, manually register hookSMTP.dll, and restart ScanMail Master Service.
12290	Application	Error	None	The ScanMail transport scan module is unable to send IPC requests to the ScanMail Master service. Check Windows event log for system errors.

TABLE A-1. ScanMail Windows Event Log Codes

Event ID	Facility	Type/ Severity	Category	Description
12291	Application	Error	None	The transport scan module is unable to detect ScanMail or it does not have proper permission to access ScanMail related files or registries. ScanMail Master Service is not started. Please restart ScanMail Master Service.
12292	Application	Error	None	Another transport scan module may be active. Please check if a transport scan module has already been loaded by the Exchange transport service. Another transport scan module has been running already.
12293	Application	Error	None	The ScanMail transport scan module is unable to create a transport agent object. Make sure the ScanMail DLL files are complete.
12294	Application	Warning	None	Transport scan has been disabled and messages have been passed through without being scanned by ScanMail. To enable transport scanning, please open ScanMail Management Console and enable any of transport level real-time virus scan, transport level attachment blocking, transport level content filtering, or Anti-spam.
12545	Application	Error	None	The MCP agent between ScanMail and Control manager is stopped unexpectedly.

TABLE A-1. ScanMail Windows Event Log Codes

Pre-configured Files

Pre-configured files are used for Silent Installation. To perform silent installation, record a new pre-configured file. There are twelve sections in each pre-configured file. The following table lists the different sections. Use the following table as a reference if you want to manually modify a pre-configured file.

Section	Contents
Log on	• LogonUserDomain=User's configuration • LogonUserName= User's configuration • LogonPassword= User's configuration Password should be encrypted.
Directory	• TempDir=smex80temp • ShareName=C$ Default is C$, user can configure. • TargetDir=C:\Program Files\Trend Micro\Smex This is default setting, user can configure. • UseDefaultProgPath=0 or 1 0 is using user's configuration, 1 is using default
Activation	MasterACCode=User's configuration

TABLE 2-1. Pre-configured files

Section	Contents
Proxy	• UseProxy=0 or 1 0 is disable, 1 is enable • DoAUAfterInstall=0 or 1 0 is disable, 1 is enable • ProxyURL=User’s configuration • ProxyPort=User’s configuration The range is 1 to 65535 • ProxyUsername=User’s configuration • EnableSocks5=0 or 1 0 is disable, 1 is enable
Web	• WebServerType=0 or 1 0 is IIS, 1 is Apache • IISSiteType=0 or 1 0 is Virtual Web Site, 1 is Default Web Site. This setting is only effected when user select IIS server. • WebPort=User’s configuration The range is 1 to 65535 • EnableSSL=0 or 1 0 is disable, 1 is enable • SSLPort=User’s configuration The range is 1 to 65535 • SSLValidPeriodCertificate=User’s configuration
WTC	WTCEnable=0 or 1 0 is disable, 1 is enable
ServerManagement	• CreateNewConsoleAccount=0 or 1 0 is use existent or skip, 1 is creating new account • ConsoleUsername= User’s configuration • ActivateServerManagement=0 or 1 0 is deactivate, 1 is activate
SMTP	EnableSMTPScanning=1 0 is disable, 1 is enable

TABLE 2-1. Pre-configured files

Section	Contents
EUQ	• ActivateEUQ=0 or 1 0 is deactivate, 1 is activate • IntegrateWithOutook2K3JunkMailFolder=0 or 1 0 is disable, 1 is enable • UseDefaultSpamFolderName=0 or 1 0 is using user’s configuration, 1 is using default • SpamFolderName=Spam Mail This is default folder name, user can configure it • SpamMsgRetainDay=14 This is default setting; user can configure it, the range is 0 to 30
CMAgent	• RegisterCMAgent=0 or 1 0 is disable, 1 is enable • CMServerAddress=User’s configuration • CMServerPortNumber=443 This is default setting; user can configure it, the range is 1 to 65535 • ConnectCMServerUsingHTTPS=0 or 1 0 is disable, 1 is enable • ConnectCMServerUsingProxy=0 or 1 0 is disable, 1 is enable • ConnectCMServerProxyAddress=User’s configuration • ConnectCMServerUseSOCKS5=0 or 1 0 is disable, 1 is enable • ConnectCMServerProxyUserName=User’s configuration • CMServerWebUserName= User’s configuration • ConnectCMServerProxyPortNumber=80 This is default setting; user can configure it, the range is 1 to 65535

TABLE 2-1. Pre-configured files

Section	Contents
Do NOT edit these settings	• LogonPassword= User's configuration Password should be encrypted. • ExchangeType=1, 2 or 3 1 is "Exchange 2007 Edge Transport Server" 2 is "Exchange 2007 Hub Transport Server / Mailbox Server" 3 is "Exchange 2000/2003 Server" • ProxyPassword= User's configuration Password should be encrypted. • ConsolePassword= User's configuration Password should be encrypted. • EUQInstallLangID=1033 Please don't change this setting. • EUQDefaultLangID=9 Please don't change this setting. • ConnectCMServerProxyPassword= User's configuration Password should be encrypted. • CMServerWebPassword= User's configuration Password should be encrypted. • ConsoleGroup= "SMEX Admin Group" for 2000/2003 (Please don't modify the group name) "User's configuration" for 2007 (For example: DomainName\Group, please don't change the group name) • ServerManagementGroupSid= (Please don't modify the SID)
InstallOption	WaitIISAdminToUnloadSMTPHook=-1 • This setting is effected on migration case only. • -1: It's the default setting. SMEX installation program is restarting IIS service during upgrade normal server(s) but waiting 20 minutes for cluster server(s). The migration includes build and version upgrade. • 0: Restart IIS service without waiting 20 minutes for normal and cluster server(s). • 1: Waiting 20 minutes for normal and cluster server(s).

TABLE 2-1. Pre-configured files

Appendix C

Introducing Trend Micro Control Manager

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based product console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager allows system administrators to monitor and report on activities such as infections, security violations, or virus entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up-to-date. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

This chapter discusses the following topics:

- *Control Manager Basic Features* on page C-2
- *Understanding Trend Micro Management Communication Protocol* on page C-3
- *Control Manager Agent Heartbeat* on page C-7
- *Registering ScanMail for Microsoft Exchange to Control Manager* on page C-9
- *Managing ScanMail for Microsoft Exchange From Control Manager* on page C-11

Control Manager Basic Features

Control Manager is designed to manage antivirus and content security products and services deployed across an organization's local and wide area networks.

Feature	Description
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console This helps ensure consistent enforcement of your organization's virus and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus outbreak
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure management console access and component download
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage via user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager management console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control ScanMail for Microsoft Exchange servers in real-time. Control Manager immediately sends configuration modifications made on the management console to the ScanMail for Microsoft Exchange servers. System administrators can run manual scans from the management console. This command system is indispensable during a virus outbreak.

TABLE C-1. Control Manager Features

FEATURE	DESCRIPTION
Centralized update control	Update virus patterns, anti-spam rules, scan engines, and other antivirus or content security components to help ensure that all managed
Centralized reporting	Get an overview of the antivirus and content security product performance using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

TABLE C-1. Control Manager Features

Understanding Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with ScanMail for Microsoft Exchange servers. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and Two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

XML parsing requires more system resources compared to the other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your server or device).

The agent footprint required to transfer information is much larger in XML compared with other data formats.

Data processing performance is slower due to the larger data footprint.

Packet transmissions take longer and the transmission rate is less than other data formats.

With the issues mentioned above, MCP's data format is devised to resolve these issues. The MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length and value. This BLOB format has the following advantages:

- **Smaller data transfer size compared to XML:** Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.
- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
- **Improved design flexibility:** Design flexibility is also been considered since each item is composed of name ID, type, length and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with/or without compression. With this type of data transfer strategy, network bandwidth can be preserved and improved scalability is also created.

NAT and Firewall Traversal Support

With limited addressable IPs on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with TMCM 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks when agent sits behinds a NAT device (or TMCM server sits behind a NAT device) since the connection can only route to the NAT device, not the product behind the NAT device (or the TMCM server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

The MCP deals with this issue by introducing a one-way communication model. With one-way communication, only the agent initiates the network connection to the server. The server cannot initiate connection to the agent. This one-way communication works well for log data transfers. However, the server dispatching of commands occurs under a passive mode. That is, the command deployment relies on the agent to poll the server for available commands.

HTTPS Support

The MCP integration protocol applies the industry standard communication protocol (HTTP/HTTPS). HTTP/HTTPS has several advantages over TMI:

- A large majority of people in IT are familiar with HTTP/HTTPS, which makes it easier to identify communication issues and find solutions those issues
- For most enterprise environments, there is no need to open extra ports in the firewall to allow packets to pass
- Existing security mechanisms built for HTTP/HTTPS, such as SSL/TLS and HTTP digest authentication, can be used.

Using MCP, Control Manager has three security levels:

- **Normal security:** Control Manager uses HTTP for communication
- **Medium security:** Control Manager uses HTTPS for communication if HTTPS is supported and HTTP if HTTPS is not supported
- **High security:** Control Manager uses HTTPS for communication

One-Way and Two-Way Communication Support

MCP supports one-way and two-way communication.

One-Way Communication

NAT traversal has become an increasingly more significant issue in the current real-world network environment. In order to address this issue, MCP uses one-way communication. One-way communication has the Control Manager agent initiating the connection to and polling of commands from the server. Each request is a CGI-like command query or log transmission. In order to reduce the network impact, the connection is kept alive and open as much as possible. A subsequent request uses an existing open connection. Even if the connection is dropped, all connections involving SSL to the same host benefit from session ID cache that drastically reduces re-connection time.

Two-Way Communication

Two-way communication is an alternative to one-way communication. It is still based on one-way communication, but has an extra channel to receive server notifications. This extra channel is also based on HTTP protocol. Two-way communication can improve real time dispatching and processing of commands from the server by the Control Manager agent. The Control Manager agent side needs a Web server or CGI compatible program that can process CGI-like requests to receive notifications from Control Manager server.

Single Sign-on (SSO) Support

Through MCP, Control Manager 3.5 now supports single sign-on (SSO) functionality for Trend Micro products. This feature allows users to sign in to Control Manager and access the resources of other Trend Micro products without having to sign in to those products as well.

Cluster Node Support

Under varying cases administrators may like to group certain product instances as a logical unit, or cluster (for example products installed under a cluster environment present all installed product instances under one cluster group). However, from the

Control Manager server's perspective, each product instance that goes through the formal registration process is regarded as an independent managed unit and each managed unit is no different from another.

Through MCP, Control Manager supports cluster nodes.

Control Manager Agent Heartbeat

To monitor the status of ScanMail for Microsoft Exchange servers, Control Manager agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the ScanMail for Microsoft Exchange server and to check for commands to the ScanMail for Microsoft Exchange server from Control Manager. The Control Manager product console then presents the product status. This means that the ScanMail for Microsoft Exchange server status is not a real-time, moment-by-moment reflection of the network’s status. Control Manager checks the status of each ScanMail for Microsoft Exchange server in a sequential manner in the background. Control Manager changes the status of ScanMail for Microsoft Exchange servers to offline, when a fixed period of time elapses without a heartbeat from the ScanMail for Microsoft Exchange server.

Active heartbeats are not the only means Control Manager has for determining the status of ScanMail for Microsoft Exchange servers. The following also provide Control Manager with the ScanMail for Microsoft Exchange server status:

- Control Manager receives logs from the ScanMail for Microsoft Exchange server. Once Control Manager receives any type of log from the ScanMail for Microsoft Exchange server successfully, this implies that the ScanMail for Microsoft Exchange server is working fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the ScanMail for Microsoft Exchange server to retrieve the pending command. If server connects to the ScanMail for Microsoft Exchange server successfully, it also indicates that the product is working fine and this event will be counted as a heartbeat.
- In one-way communication mode, the Control Manager agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The Control Manager agent heartbeats implement with the following ways:

- **UDP:** If the product can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. Also the transmitting client cannot make sure that the server does indeed receive the request.
- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the ScanMail for Microsoft Exchange server applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains ScanMail for Microsoft Exchange server activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots denote Working status or the hours that the Communicator sends information to the Control Manager server. White slots indicate Idle time. Define Working or Idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 3:00 PM, and from 6:00 P.M. to 12:00 P.M.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend

Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

TABLE C-2. Heartbeat Recommendations

Registering ScanMail for Microsoft Exchange to Control Manager

The ScanMail for Microsoft Exchange server is a standalone product and you do not need to register to Control Manager. However, by registering to Control Manager you gain the benefits explained earlier in this appendix. All features are managed using the ScanMail for Microsoft Exchange server product console.

To register a ScanMail for Microsoft Exchange server to Control Manager:

1. Log on to the ScanMail product console.
2. Click **Administrator** > **Control Manager Settings**. The Control Manager Settings screen displays.

Note: Control Manager uses the name specified in the **Entity display name** field to identify ScanMail for Microsoft Exchange servers. The name appears in the Product Directory of Control Manager.

3. Under **Connection settings**, type the name of the ScanMail server in the **Entity display name** field.

4. Under **Control Manager Server Settings** specify the following:

   a. Type the Control Manager server IP address or host name in the Server FQDN or IP address field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

   c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products), select **Connect through HTTPS**.

   d. If your network requires authentication, type the user name and password for your IIS server in the **Username** and **Password** fields.

   e. If you use a NAT device, select **Enable two-way communication port forwarding** and type the NAT device's IP address and port number in **IP address** and **port number**.

   Refer to the *Trend Micro Control Manager Administrator's Guide* for more information about managing products in Control Manager.

5. From the Control Manager management console **Main Menu**, click **Products**.

6. On the left most menu, select **Managed Products** from the list and then click **Go**.

7. Check to see that the ScanMail for Microsoft Exchange server displays.

Managing ScanMail for Microsoft Exchange From Control Manager

A managed product refers to a ScanMail for Microsoft Exchange server, an antivirus, a content security or third party product represented in the Product Directory. The Control Manager management console represents managed products as icons. These icons represent ScanMail for Microsoft Exchange servers, other Trend Micro antivirus and content security products, as well as third party products.

Indirectly administer the managed products either individually or by groups through the Product Directory. Use the Directory Manager to customize the Product Directory organization.

Understanding Product Directory

Take care when planning the structure of the Product Directory, a logical grouping of managed products, because it affects the following:

- **User access:** When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. Carefully plan the Product Directory since you can only grant access to a single segment. For example, granting access to the root segment grants access to the entire Directory. On the other hand, granting access to a specific ScanMail for Microsoft Exchange server only grants access to that specific product.
- **Deployment planning:** Control Manager deploys virus pattern, scan engine, spam rule, and program updates to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory will therefore simplify the designation of recipients.
- **Outbreak Prevention Policy and Damage Control Template deployments:** OPP and DCS deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

As shown in this sample Product Directory, managed products identify the registered antivirus or content security product, as well as provide the connection status.

Product Directory icons:

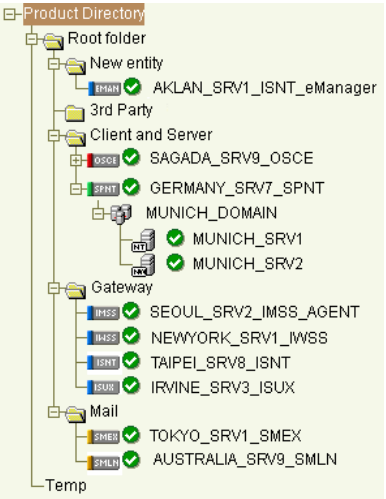
PRODUCT DIRECTORY TREE	ICON	DESCRIPTION
 Product Directory Root folder New entity EMAN ✓ AKLAN_SRV1_ISNT_eManager 3rd Party Client and Server OSCE ✓ SAGADA_SRV9_OSCE SPNT ✓ GERMANY_SRV7_SPNT MUNICH_DOMAIN NT ✓ MUNICH_SRV1 NW ✓ MUNICH_SRV2 Gateway IMSS ✓ SEOUL_SRV2_IMSS_AGENT IWSS ✓ NEWYORK_SRV1_IWSS ISNT ✓ TAIPEI_SRV8_ISNT ISUX ✓ IRVINE_SRV3_ISUX Mail SMEX ✓ TOKYO_SRV1_SMEX SMLN ✓ AUSTRALIA_SRV9_SMLN Temp	📁 📂	New entity or user-defined folder name
	EMAN	InterScan eManager
	OSCE	OfficeScan Corporate Edition
	SPNT	ServerProtect Information Server
	🖥	ServerProtect Domain
	NT	ServerProtect for Windows (Normal Server)
	NW	ServerProtect for NetWare (Normal Server)
	IMSS	InterScan Messaging Security Suite
	IWSS	InterScan Web Security Suite
	ISNT	InterScan VirusWall for Windows
	ISUX	InterScan VirusWall for UNIX
	SMEX	ScanMail for Microsoft Exchange
	SMLN	ScanMail for Lotus Notes
	NVW NVW NVW	Network VirusWall
	FW	NetScreen Global PRO Firewall
	✓	Managed Product connection status icon

TABLE C-3. Managed Product Icons

Arrange the Product Directory using the Directory Manager. Use descriptive folders to group your ScanMail for Microsoft Exchange servers according to their protection type and the Control Manager network administration model. For example, grant access rights to mail administrators to configure the Mail folder.

Accessing a ScanMail for Microsoft Exchange Default Folder

Newly registered ScanMail for Microsoft Exchange servers usually appear in the ScanMail for Microsoft Exchange folder after installation completes. Control Manager creates this folder when the ScanMail agent first registers to the Control Manager server. However, Control Manager segregates managed products handled by Trend VCS agents under the Trend VCS agents folder.

Access Product Directory

Use the Product Directory to administer ScanMail for Microsoft Exchange servers registered with the Control Manager server.

Note: Viewing and accessing the folders in the Product Directory depends on the Account Type and folder access rights used to log on to the management console.

To access the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.

Manually Deploy New Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your ScanMail for Microsoft Exchange servers and other managed products on demand. This is useful especially during virus outbreaks.

Download new components before deploying updates to specific or groups of ScanMail for Microsoft Exchange servers or managed products.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired folder or ScanMail for Microsoft Exchange server.

4. On the working area, click the **Tasks** tab.
5. Select **Deploy <component>** from the Select task list.
6. Click **Next>>**.
7. Click **Deploy Now** to start the manual deployment of new components.
8. Monitor the progress via Command Tracking.
9. Click the **Command Details** link to view details for the Deploy Now task.

View ScanMail for Microsoft Exchange Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Spyware/Grayware summaries for all managed products present in the Product Directory tree.

There are two ways to view the ScanMail for Microsoft Exchange servers status summary:

- Through Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or ScanMail for Microsoft Exchange server.
   - If you click a ScanMail for Microsoft Exchange server or managed product, the Product Status tab displays the ScanMail for Microsoft Exchange server or managed product's summary
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Spyware/Grayware summaries

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the Display summary for list.

Configure ScanMail for Microsoft Exchange and Managed Products

Depending on the product and agent version:

- You can configure devices or products either individually or in groups according to folder division

  Perform group configuration using the folder Configuration tab.

Note: When performing a group configuration, verify that you want all ScanMail for Microsoft Exchange server in a group to have the same configuration. Otherwise, add devices or managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration tab shows the product console

To configure a product:

1. Click **Products** on the main menu.
2. On the left most menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired ScanMail for Microsoft Exchange server, managed product or folder.
4. On the working area, click the **Configuration** tab.
5. Select the product to configure from the Select product list.

Note: Step 4 is necessary when you use the folder Configuration tab.

6. At the Select configuration list, select the product feature to access or configure.
7. Click **Next**. The ScanMail product console appears.

Issue Tasks to ScanMail for Microsoft Exchange and Managed Products

Use the Tasks tab to invoke available actions to a group or specific ScanMail for Microsoft Exchange server or managed product. You can perform the following tasks on ScanMail for Microsoft Exchange servers:

- Configuration Replication
- Deploy anti-spam rules
- Deploy engines
- Deploy license profiles
- Deploy pattern files/cleanup templates
- Enable Real-time Scan
- Start Scan Now

Deploy the latest pattern file, or scan engine to ScanMail for Microsoft Exchange servers with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to ScanMail for Microsoft Exchange servers:

1. Access the Product Directory.
2. On the left-hand menu, select the desired ScanMail for Microsoft Exchange server or folder.
3. On the working area, click the **Tasks** tab.
4. Select the task from the Select task list.
5. Click **Next**.
6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View ScanMail for Microsoft Exchange and Managed Product Logs

Use the Logs tab to query and view logs for a group or specific ScanMail for Microsoft Exchange server.

To query and view ScanMail for Microsoft Exchange server logs:

1. Access the Product Directory.
2. On the left-hand menu, select the desired ScanMail for Microsoft Exchange server or folder.
3. On the working area, click the **Logs** tab.
4. Select the client log type:

Event Logs:

a. Provide the following search parameters:

PARAMETER	DESCRIPTION
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Unusual network virus behavior
Product	If you select a folder, this list shows the managed products belonging to the folder. To view information on all products, select All. Otherwise, query logs of a specific managed product
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE C-4. Search Parameters for Event Logs

b. Click **Display Logs** to begin the query and display the query results.

Security Logs:

a. Select All virus log incidents or a specific security logs type and then click **Query**.

b. Provide the following search parameters:

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE C-5. Search Parameters for Security Logs

c. Click **Display Logs** to begin the query.

Note: eManager managed products records content security violations in the Security Logs, not in the Virus Logs.

5. The Query Result screen displays the results in a table format.
6. The Generated at entity column of the result table indicates the Control Manager server time.

Recover ScanMail for Microsoft Exchange Removed from the Product Directory

The following scenarios can cause Control Manager to delete ScanMail for Microsoft Exchange servers from the Product Directory:

- Reinstalling the Control Manager server and selecting Delete existing records and create a new database option

  This option creates a new database using the name of the existing one.
- Replacing the corrupted Control Manager database with another database of the same name
- Accidentally deleting the ScanMail for Microsoft Exchange server using the Directory Manager

If a Control Manager server's ScanMail for Microsoft Exchange server records are lost, the agents on the products still "know" where they are registered to. The product agent will automatically re-register itself after 8 hours or when the service is restarts.

To recover ScanMail for Microsoft Exchange servers removed from the Product Directory:

- Restart the ScanMail for Microsoft Exchange service.
- Re-register the ScanMail agent to the Control Manager server.

Search for ScanMail for Microsoft Exchange, Product Directory Folders or Computers

Use the Search button to quickly:

- Add a specific or a group of ScanMail for Microsoft Exchange servers to Temp
- Find and locate a specific ScanMail for Microsoft Exchange server in the Product Directory

To search for a folder or ScanMail for Microsoft Exchange server:

1. Access Product Directory.
2. On the left menu, click **Search**.
3. On the working area, provide the following search parameters:

PARAMETER	DESCRIPTION
Search for	Select the object of the search from the drop down list Search for managed products or Communicators based on their name, folder name, or computer name.
Keyword	This allows you to search for the object by name Select **Case sensitive** to narrow down the search results.
Managed product status / Communicator status	Select the appropriate connection status, for the Communicator or managed product The options are: All, Active, Inactive, Abnormal, Product Active, and Product Inactive. Choose All to search for objects regardless of the connection status.

TABLE C-6. Search Parameters

PARAMETER	DESCRIPTION
Product	Select the appropriate product from the list. Choose **All** to search for all products.

TABLE C-6. Search Parameters

4. Click **Begin Search** to start searching.
5. Control Manager presents the search results in a table format. You may opt to directly create the temp sub-folder where the search results will be grouped.

Refresh the Product Directory

To refresh the Product Directory:

- In the Product Directory, click the **Refresh** icon on the upper right corner of the left menu.

Understanding Directory Manager

After the registering to Control Manager, the ScanMail for Microsoft Exchange server first appears in the Product Directory under the default folder.

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs. For example, you can group products by location or product-type   messaging security, web security, file storage protection, and so on.

The Directory allows you to create, modify, or delete folders, and move ScanMail for Microsoft Exchange servers between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the ScanMail for Microsoft Exchange servers belonging to each folder. Consider the following factors when planning and implementing your folder and ScanMail for Microsoft Exchange server structure:

- Product Directory
- User Accounts
- Deployment Plans

Group ScanMail for Microsoft Exchange servers according to geographical, administrative, or product specific reasons. In combination with different access rights used to access ScanMail for Microsoft Exchange servers or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages:

Grouping Type	Pro's	Con's
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

TABLE C-7. Product Grouping Comparison

Using the Directory Manager Options

Directory Manager provides seven options: New Folder, Delete, Rename, Undo, Redo, Cut, and Paste.

Use these options to manipulate and organize ScanMail for Microsoft Exchange servers in your Control Manager network.

To use and apply changes in the Directory Manager:

- Right-click a folder or ScanMail for Microsoft Exchange server to open a pop-up menu that presents a list of actions you can perform
- Click **+** or the folder to display the ScanMail for Microsoft Exchange servers belonging to a folder
- Press **Enter** or click anywhere when you rename a folder
- Click **Save** to apply your changes and update the Directory Manager organization
- Click **Reset** to discard changes that are not yet saved

Access Directory Manager

Use Directory Manager to group ScanMail for Microsoft Exchange servers together.

To access the Directory Manager:

1. Access Product Directory.
2. On the left-hand menu, click **Directory Manager**.

Create Folders

Group ScanMail for Microsoft Exchange servers into different folders to suit your organization's Control Manager network administration model.

To create a folder:

1. Access the Directory Manager.
2. On the working area, right-click where you want to create a new folder. If you are building the tree for the first time, right-click the Root folder.
3. Select **New folder** from the pop-up menu. Control Manager creates a new sub-folder under the main folder.
4. Type a name for the new folder or use the default name and then press **Enter**.
5. Click **Save**.

Except for the New entity folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabet characters (a/A to z/Z).

Renaming Folders or ScanMail for Microsoft Exchange

To rename a folder or ScanMail for Microsoft Exchange server:

1. Access Directory Manager.
2. On the working area, right-click the folder or ScanMail for Microsoft Exchange server you want to rename and then select **Rename** from the pop-up menu. The folder/ScanMail for Microsoft Exchange server name becomes an editable field.
3. Type a name for the new folder or use the default name and then press **Enter**.
4. Click **Save**.

Note: Renaming a ScanMail for Microsoft Exchange server only changes the name stored in the Control Manager database there are no effects to the product.

Move Folders or ScanMail for Microsoft Exchange

To transfer or move a folder or ScanMail for Microsoft Exchange server to another location:

1. Access Directory Manager.

2. On the working area, select the folder or ScanMail for Microsoft Exchange server you want to move.
3. Do one of the following:
    - Drag-and-drop the folder or ScanMail for Microsoft Exchange server to the target new location
    - Cut and paste the folder or ScanMail for Microsoft Exchange server to the target new location
4. Click **Save**.

Delete User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a ScanMail for Microsoft Exchange server which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

1. Access the Directory Manager.
2. On the working area, right-click the folder you want to delete and then select **Delete** from the pop-up menu.
3. Click **Save**.

Note: You cannot delete the New entity folder

Use caution when deleting user-defined folders, you may accidentally delete a ScanMail for Microsoft Exchange server.

Understanding Temp

Temp, a collection of ScanMail for Microsoft Exchange server shortcuts, allows you to focus your attention on specific products without changing the Product Directory organization. Use Temp for deploying updates to groups of products with outdated components.

Consider the following issues when using Temp:

- Control Manager deletes all ScanMail for Microsoft Exchange server shortcuts when you log off the management console.
- You can only add the ScanMail for Microsoft Exchange servers to Temp if you can see them in the Product Directory, you cannot make shortcuts to products that you cannot access.

Using Temp

You can manipulate ScanMail for Microsoft Exchange servers in Temp the same way you would with ScanMail for Microsoft Exchange servers in the Product Directory. The folders and ScanMail for Microsoft Exchange servers belonging to Temp have the same folder and ScanMail for Microsoft Exchange server-level controls. However, Control Manager determines what actions you can perform on the ScanMail for Microsoft Exchange servers according to your user account's access rights.

You can use Temp for the following purposes:

- Issue commands to groups of ScanMail for Microsoft Exchange servers using folder-level access rights.
- Select a specific ScanMail for Microsoft Exchange server, and then use the available Product Directory tabs to perform an action.

Access Temp

Use Temp to collect ScanMail for Microsoft Exchange server shortcuts.

To access Temp:

1. Access Product Directory.
2. On the left most menu, click **Temp**.

Adding ScanMail for Microsoft Exchange to Temp

There are three methods to add ScanMail for Microsoft Exchange servers to Temp:

- From the Search results
- From the Product Directory
- Add ScanMail for Microsoft Exchange servers with outdated components based on the Status Summary page

Trend Micro recommends that you add several ScanMail for Microsoft Exchange servers at once to Temp using the last method. The Status Summary screen provides information as to which ScanMail for Microsoft Exchange servers use outdated components. It simplifies virus pattern and scan engine updates on groups of ScanMail for Microsoft Exchange servers belonging to different folder groups.

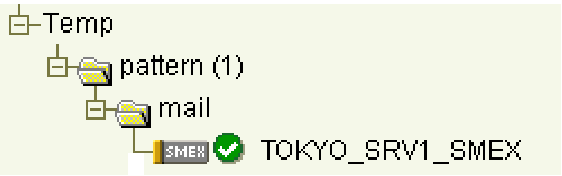
Note: Adding ScanMail for Microsoft Exchange servers to Temp only allows you to collect ScanMail for Microsoft Exchange servers with outdated components doing so does not trigger automatic deployment.

To add from the Search results

1. Click **Products** on the main menu.
2. On the left-hand menu, click **Search**.
3. On the working area, search for ScanMail for Microsoft Exchange servers or folders.

4. Specify a sub-folder name in the **Temp sub-folder for managed products** field for the Temp sub-folder that will contain the ScanMail for Microsoft Exchange server shortcuts.

Note: Step 4 is optional. If you want to create multiple folder levels belonging to Temp, specify \{folder name level1}\{sub-folder name level2} in the Temp sub-folder for entities field. For example, if you specify \pattern\mail, the following Temp structure appears:



5. Click **Add**. Control Manager adds ScanMail for Microsoft Exchange servers from the search results to Temp.

To add from the Product Directory

1. Access the Product Directory.
2. On the left-hand menu, select the ScanMail for Microsoft Exchange server you want to add to Temp.
3. Press "+" on the numeric keypad.

To add ScanMail for Microsoft Exchange servers with outdated components based on the Status Summary page:

1. Access Product Directory.
2. On the left-hand menu, select the desired Product Directory folder.
3. On the working area, click the **Product Status** tab.
4. At the Component Status table, click one of the numeric links indicating the number of ScanMail for Microsoft Exchange servers that are outdated. Depending on the link you clicked, the Virus Pattern Status (Outdated), Scan Engine Status (Outdated), Spam Rule Status (Outdated) screen opens displaying

the computer name, product name, product version, and outdated component version.

5. Click **Add to Temp** in the status page. Control Manager organizes theScanMail for Microsoft Exchange servers to Temp using folders named after the page from which they were added. For example, Control Manager places ScanMail for Microsoft Exchange servers added from the Scan Engine Status (Outdated) page under the Scan Engine Status (Outdated) folder.

Note: Clicking **Add to Temp** only adds the ScanMail for Microsoft Exchange servers shown on the status page. If the list of ScanMail for Microsoft Exchange servers spans more than one screen, click **Add to Temp** on all screens to add all products with outdated component.

6. Click **Back** to return to the Status Summary page, and then proceed to the next outdated component. Repeat the instructions until Control Manager adds all the outdated ScanMail for Microsoft Exchange servers to Temp.

Removing ScanMail for Microsoft Exchange From Temp

To remove a ScanMail for Microsoft Exchange server from Temp:

1. Access Product Directory.
2. On the left-hand menu, click **Temp**.
3. From the available ScanMail for Microsoft Exchange servers on the Temp list, select the folder or ScanMail for Microsoft Exchange server shortcut that you want to remove.
4. Press "-" in the numeric keypad.

Note: Control Manager removes ScanMail for Microsoft Exchange server shortcuts in Temp when you log off from the management console.

Removing ScanMail for Microsoft Exchange servers from Temp will neither disconnect the antivirus or content security product nor uninstall the Control Manager agent from the Control Manager server.

Download and Deploy New Components From Control Manager

Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network. Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update):

- **Pattern files/Cleanup templates** - refer to virus pattern files, Damage Cleanup templates, Vulnerability Assessment patterns, network outbreak rules, Pattern Release History, and network virus pattern files
- **Anti-spam rules** - refer to import and rule files used for anti-spam and content filtering
- **Engines** - refers to virus scan engine, damage cleanup engine, and VirusWall engine for Linux
- **Product program** - these are product specific components (for example, Service Pack releases)

Note: Only registered users are eligible for components update. For more information, see the Control Manager online help Registering and Activating your Software > Understanding product activation topic.

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

Understanding Update Manager

Update Manager provides functions that help you update the antivirus and content security components of your Control Manager network.

Updating the Control Manager network involves two steps:

- Downloading components: You can do this manually or by schedule
- Deploying components: You do this manually or by schedule

Understanding Manual Downloads

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Manually Download Components

This is the Trend Micro recommend method of configuring manual downloads. Manually downloading components requires multiple steps:

Tip: Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

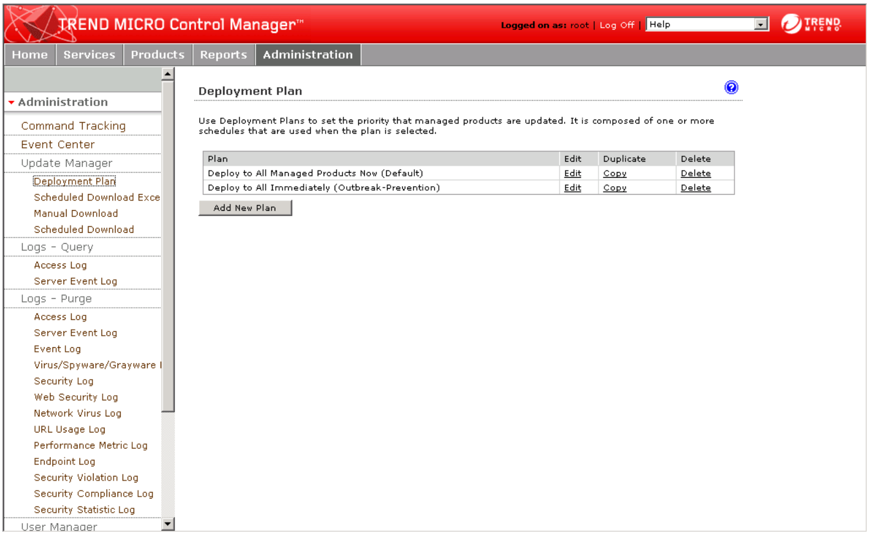
Step 6: Complete the manual download

To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.

2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

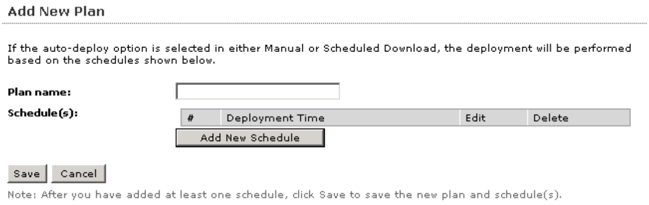


Deployment Plan

Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

Plan	Edit	Duplicate	Delete
Deploy to All Managed Products Now (Default)	Edit	Copy	Delete
Deploy to All Immediately (Outbreak-Prevention)	Edit	Copy	Delete

3. On the working area, click **Add New Plan**.



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Plan name:

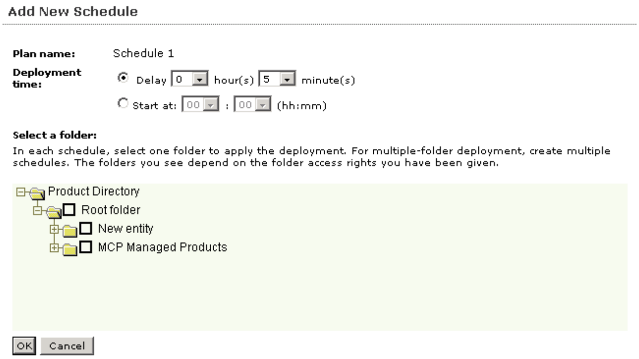
Schedule(s):

#	Deployment Time	Edit	Delete

Note: After you have added at least one schedule, click Save to save the new plan and schedule(s).

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.

5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.



Add New Schedule

Plan name: Schedule 1

Deployment time: ● Delay 0 hour(s) 5 minute(s)

○ Start at: 00 : 00 (hh:mm)

Select a folder:

In each schedule, select one folder to apply the deployment. For multiple-folder deployment, create multiple schedules. The folders you see depend on the folder access rights you have been given.

- Product Directory
  - □ Root folder
    - □ New entity
    - □ MCP Managed Products

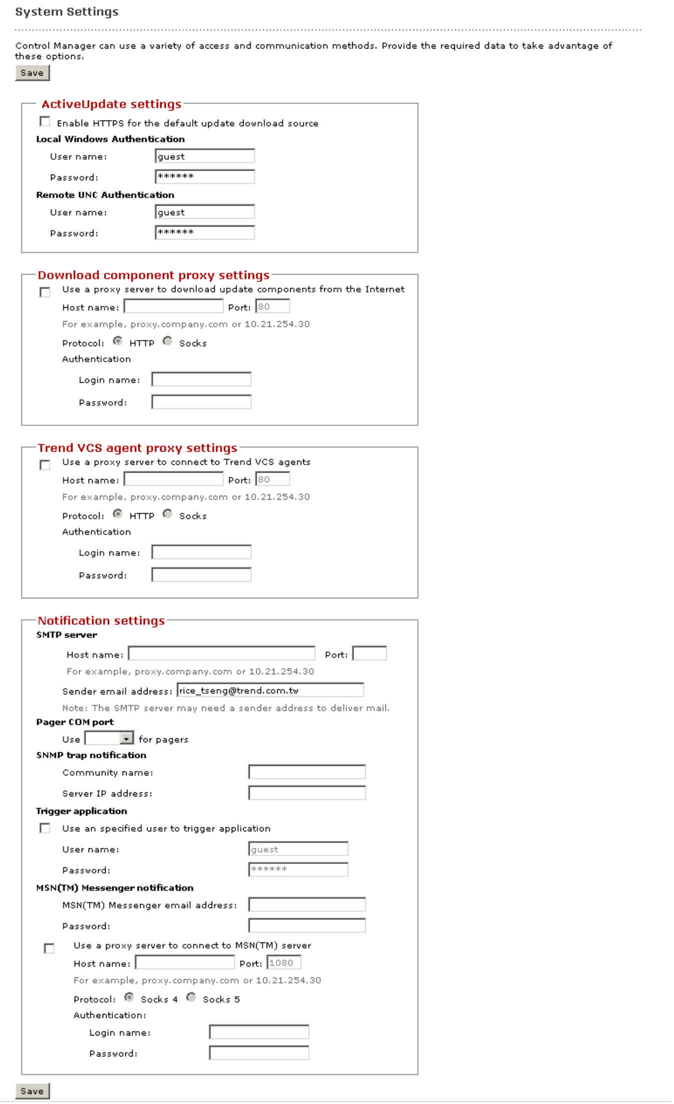
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at** - Performs the deployment at a specific time

     Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration** > **System Settings**. The System Settings screen appears.



System Settings

Control Manager can use a variety of access and communication methods. Provide the required data to take advantage of these options.

ActiveUpdate settings

□ Enable HTTPS for the default update download source

Local Windows Authentication

User name: guest

Password: ******

Remote UNC Authentication

User name: guest

Password: ******

Download component proxy settings

□ Use a proxy server to download update components from the Internet

Host name: Port: 80

For example, proxy.company.com or 10.21.254.30

Protocol: ● HTTP ○ Socks

Authentication

Login name:

Password:

Trend VCS agent proxy settings

□ Use a proxy server to connect to Trend VCS agents

Host name: Port: 80

For example, proxy.company.com or 10.21.254.30

Protocol: ● HTTP ○ Socks

Authentication

Login name:

Password:

Notification settings

SMTP server

Host name: Port:

For example, proxy.company.com or 10.21.254.30

Sender email address: rice_tseng@trend.com.tw

Note: The SMTP server may need a sender address to deliver mail.

Pager COM port

Use for pagers

SNMP trap notification

Community name:

Server IP address:

Trigger application

□ Use an specified user to trigger application

User name: guest

Password: ******

MSN(TM) Messenger notification

MSN(TM) Messenger email address:

Password:

□ Use a proxy server to connect to MSN(TM) server

Host name: Port: 1080

For example, proxy.company.com or 10.21.254.30

Protocol: ● Socks 4 ○ Socks 5

Authentication:

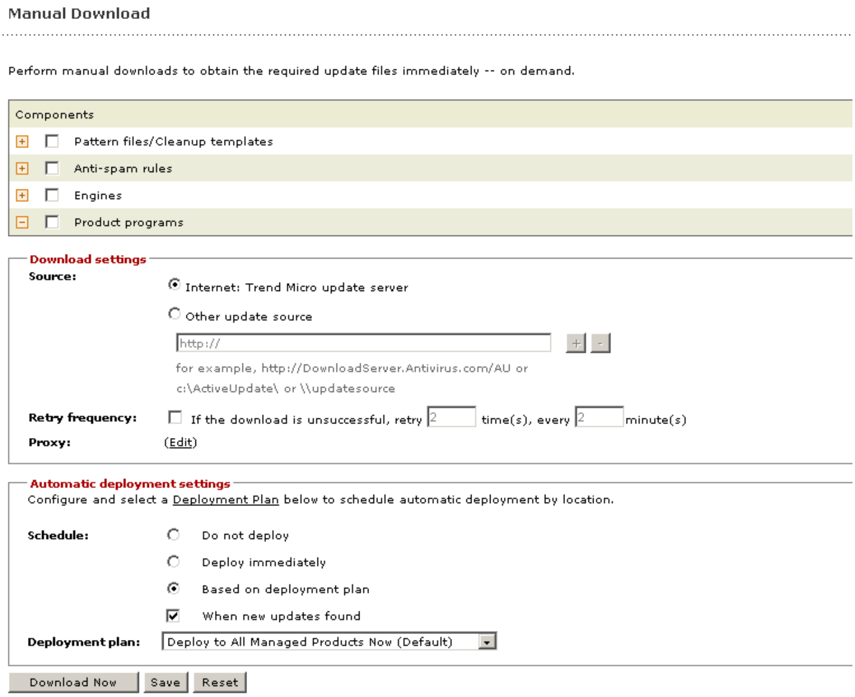
Login name:

Password:

2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:
    - **HTTP**
    - **SOCKS**
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration** > **Update Manager** > **Manual Download**. The Manual Download screen appears.



Manual Download

Perform manual downloads to obtain the required update files immediately -- on demand.

Components

- ⊞ □ Pattern files/Cleanup templates
- ⊞ □ Anti-spam rules
- ⊞ □ Engines
- ⊟ □ Product programs

Download settings

Source: ● Internet: Trend Micro update server ○ Other update source

http://

for example, http://DownloadServer.Antivirus.com/AU or c:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

Schedule:
- ○ Do not deploy
- ○ Deploy immediately
- ● Based on deployment plan
- ☑ When new updates found

Deployment plan: Deploy to All Managed Products Now (Default)

2. From the Components area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the following components to download:

   From Pattern files/Cleanup templates:

   - Anti-spam rules

   From Engines:

   - Product Programs

Step 4: Configure the download settings

1. Select the update source:
   - **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source:** Type the URL of the update source in the accompanying field.

     After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select Retry frequency and specify the number or retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 5: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy immediately:** Components download to Control Manager, then deploy to managed products
   - **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Note: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.
3. Click **Save**.

Step 6: Complete the manual download

1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.
2. Click the **Command Details** to view details from the Command Details screen.
3. Click **OK** to return to the Manual Download screen.

Configure Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

To configure scheduled download exceptions:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Update Manager, click **Scheduled Download Exceptions**.
3. Do the following:
   - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, all downloads for the selected day(s) are blocked.
   - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, all downloads for the selected hours are blocked.

4. Click **Save**.

Understanding Scheduled Downloads

Configure scheduled downloading of components to keep your components up-to-date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules. All schedules are autonomous of each other. Scheduling downloads for a component group, downloads all components in the group.

Use the Scheduled Download screen to obtain the following information for components currently in your Control Manager system:

- **Frequency:** Shows how often the component is updated
- **Enabled:** Indicates if the schedule for the component is either enabled or disabled
- **Update Source:** Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

Step 2: Configure your proxy settings, if you use a proxy server

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

Step 6: Configure the automatic deployment settings

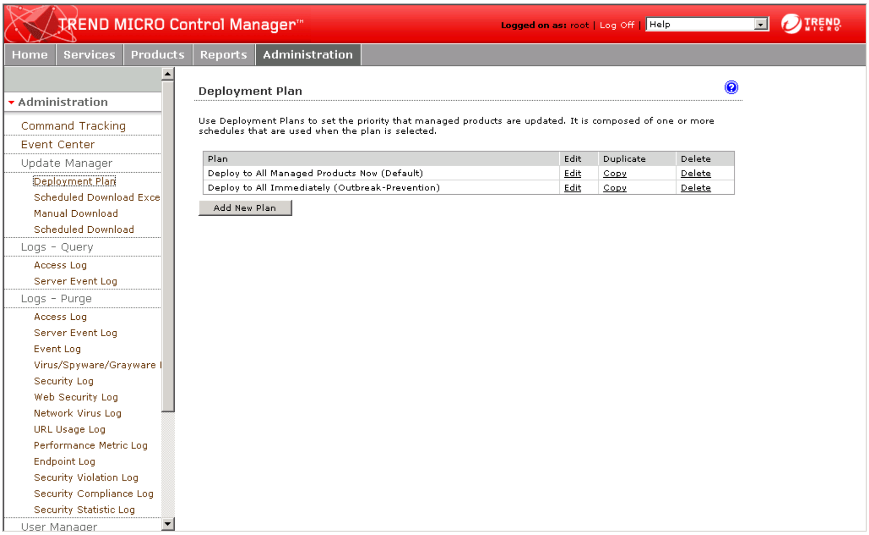
Step 7: Enable the schedule and save settings

Configure Scheduled Downloads and Enable Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.

2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

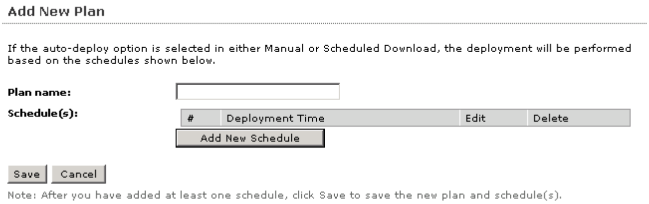


Deployment Plan

Use Deployment Plans to set the priority that managed products are updated. It is composed of one or more schedules that are used when the plan is selected.

Plan	Edit	Duplicate	Delete
Deploy to All Managed Products Now (Default)	Edit	Copy	Delete
Deploy to All Immediately (Outbreak-Prevention)	Edit	Copy	Delete

3. On the working area, click **Add New Plan**.



Add New Plan

If the auto-deploy option is selected in either Manual or Scheduled Download, the deployment will be performed based on the schedules shown below.

Plan name:

Schedule(s):

#	Deployment Time	Edit	Delete

Note: After you have added at least one schedule, click Save to save the new plan and schedule(s).

4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.

5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:

- **Delay** - After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

  Use the menus to indicate the duration, in terms of hours and minutes.

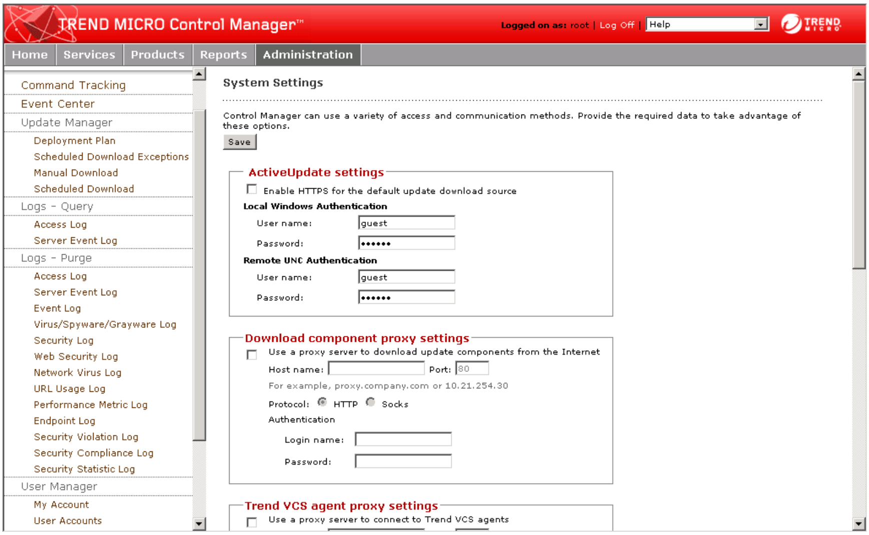
- **Start at** - Performs the deployment at a specific time

  Use the menus to designate the time in hours and minutes.

7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

Step 2: Configure your proxy settings, if you use a proxy server

1. Click **Administration** > **System Settings**. The System Settings screen appears.



System Settings

Control Manager can use a variety of access and communication methods. Provide the required data to take advantage of these options.

Save

ActiveUpdate settings

□ Enable HTTPS for the default update download source

Local Windows Authentication

User name: guest

Password: ••••••

Remote UNC Authentication

User name: guest

Password: ••••••

Download component proxy settings

□ Use a proxy server to download update components from the Internet

Host name: Port: 80

For example, proxy.company.com or 10.21.254.30

Protocol: ● HTTP ○ Socks

Authentication

Login name:

Password:

Trend VCS agent proxy settings

□ Use a proxy server to connect to Trend VCS agents

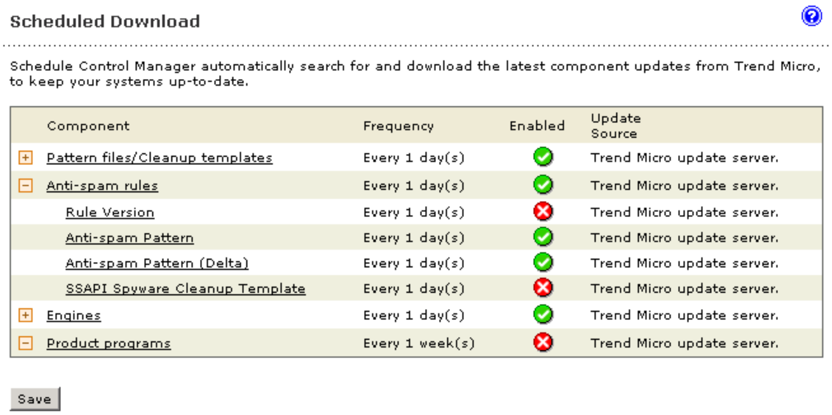
2. Select the **Use a proxy server to download update components from the Internet** check box in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:

- HTTP
- SOCKS

6. Type a login name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the components to update

1. Click **Administration** > **Update Manager** > **Scheduled Download**. The Scheduled Download screen appears.



Scheduled Download

Schedule Control Manager automatically search for and download the latest component updates from Trend Micro, to keep your systems up-to-date.

	Component	Frequency	Enabled	Update Source
⊞	Pattern files/Cleanup templates	Every 1 day(s)	✓	Trend Micro update server.
⊟	Anti-spam rules	Every 1 day(s)	✓	Trend Micro update server.
	Rule Version	Every 1 day(s)	✗	Trend Micro update server.
	Anti-spam Pattern	Every 1 day(s)	✓	Trend Micro update server.
	Anti-spam Pattern (Delta)	Every 1 day(s)	✓	Trend Micro update server.
	SSAPI Spyware Cleanup Template	Every 1 day(s)	✗	Trend Micro update server.
⊞	Engines	Every 1 day(s)	✓	Trend Micro update server.
⊟	Product programs	Every 1 week(s)	✗	Trend Micro update server.

2. From the Components area select the components to download.
   a. Click the + icon to expand the component list for each component group.
   b. Select the following components to download:

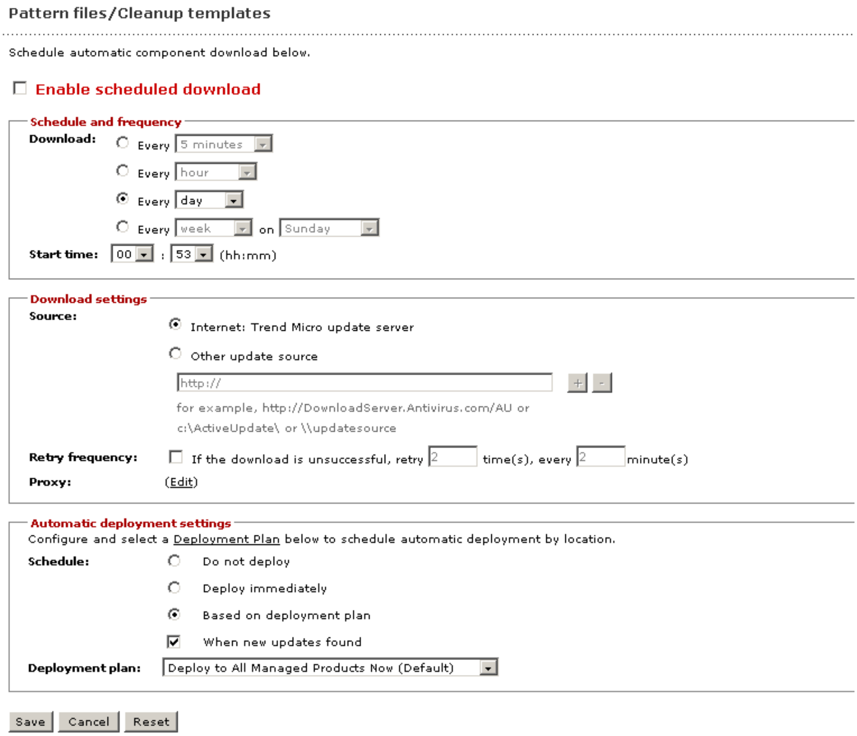
From Pattern files/Cleanup templates:

- Anti-spam rules

From Engines:

- Product Programs

The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.



Pattern files/Cleanup templates

Schedule automatic component download below.

□ Enable scheduled download

Schedule and frequency

Download:
○ Every 5 minutes
○ Every hour
● Every day
○ Every week on Sunday

Start time: 00 : 53 (hh:mm)

Download settings

Source:
● Internet: Trend Micro update server
○ Other update source
http://
for example, http://DownloadServer.Antivirus.com/AU or c:\ActiveUpdate\ or \\updatesource

Retry frequency: □ If the download is unsuccessful, retry 2 time(s), every 2 minute(s)

Proxy: (Edit)

Automatic deployment settings

Configure and select a Deployment Plan below to schedule automatic deployment by location.

Schedule:
○ Do not deploy
○ Deploy immediately
● Based on deployment plan
☑ When new updates found

Deployment plan: Deploy to All Managed Products Now (Default)

Step 4: Configure the download schedule

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.
3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the download settings

1. Select the update source:
   - **Internet: Trend Micro update server:** Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source:** Type the URL of the update source in the accompanying field.

     After selecting Other update source, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number or retries and duration between retries for downloading components.

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

---

3. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the System Settings screen.

Step 6: Configure the automatic deployment settings

1. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy immediately:** Components download to Control Manager, then deploy to managed products
   - **Based on deployment plan:** Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found:** Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Tip: Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the **Deployment plan** list.
3. Click **Save**.

Step 7: Enable the schedule and save settings

1. Click the status button in the Enabled column.
2. Click **Save**.

Use Reports

A Control Manager **report** is an online collection of figures about virus, spyware/grayware, and content security events that occur on the Control Manager network. The Enterprise edition provides the Control Manager reports.

Control Manager 3.5 categorizes reports according to the following types:

- *Local reports*
- *Global reports*

Note: You can only configure the **Global Report Profile** option through the *parent Server Management console*.

Local Reports

Local reports are reports about managed products administered by the parent server. Local reports do not include reports generated by child servers. Use the Global Report options to view reports about managed products administered by child servers registered to the parent server.

Use Local Reports screen to view available one-time-only and scheduled local report profiles.

To access Local Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Local Report Profile**.

Note: When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Global Reports

Global reports are reports about managed products administered by child servers as well as the parent server.

Use Global Reports screen to view available one-time-only and scheduled global report profiles.

To access Global Reports:

1. Click **Reports** on the main menu.
2. On the left most menu under Reports, click **Global Report Profile**.
3. When multiple reports are available, sort reports according to Report Profile or Last Created date.

Note: Only the parent server can display the global report profiles.

When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Understanding Report Templates

A report template outlines the look and feel of Control Manager reports. In particular, a template defines which sections appear in a report:

- Headers
- Report body
- Footers

Trend Micro Control Manager 3.5 adds 3 new report templates to the 77 previously available since Control Manager 3.0 Service Pack 3. The reports added in Control Manager 3.0 Service Pack 3 fall into five categories: Desktop, Fileserver, Gateway, MailServer and Executive Summary. The new reports in Control Manager 3.5 fall into a new 6th category: Network Products. This category offers reports related to Network VirusWall.

Note: In Control Manager 3.5 spyware/grayware are no longer considered viruses/malware. This change effects the virus count in all original virus related reports.

To generate these reports, click **Reports** on the main menu, then click **Create Report Profile** under Local Report Profile on the navigation menu. In the Contents tab that appears in the working area, you can enter a report name, an optional report title and an optional report description. Use the **Report Category** list to peruse the six categories of reports listed below. Clicking a mark into a check box includes the associated report in the final exported report file.

Control Manager 3.5 also provides 18 templates stored in `<root>\Program Files\Trend Micro\Control Manager\Reports` as Crystal Report version 9 files (*.rpt). These templates also apply to Local and Global reports..

Understanding Report Profiles

A **profile** lays out the content (template and format), target, frequency, and recipient of a report. You can view reports in the following file formats:

- **RTF:** Rich text format; use a word processor (for example, Microsoft Word™) to view *.RTF reports
- **PDF:** Portable document format; use Adobe Reader to view *.PDF reports
- **ActiveX™:** ActiveX documents; use a Web browser to view reports in ActiveX format

Note: Control Manager cannot send reports in ActiveX format as email attachments.

- **RPT:** Crystal Report format; use Crystal Smart Viewer to view *.RPT reports

After generating the report, Report Server launches the default viewer for that report file format. For RPT reports, you must have the Crystal Smart Viewer installed.

Create Report Profiles

Creating a report profile is a five-step process. Creating local or global reports, the process stays very similar. The process to create a report profile is as follows:

Step 1: Select whether to create a local or global report

Step 2: Configure the Contents tab settings

Step 3: Configure the Targets tab settings

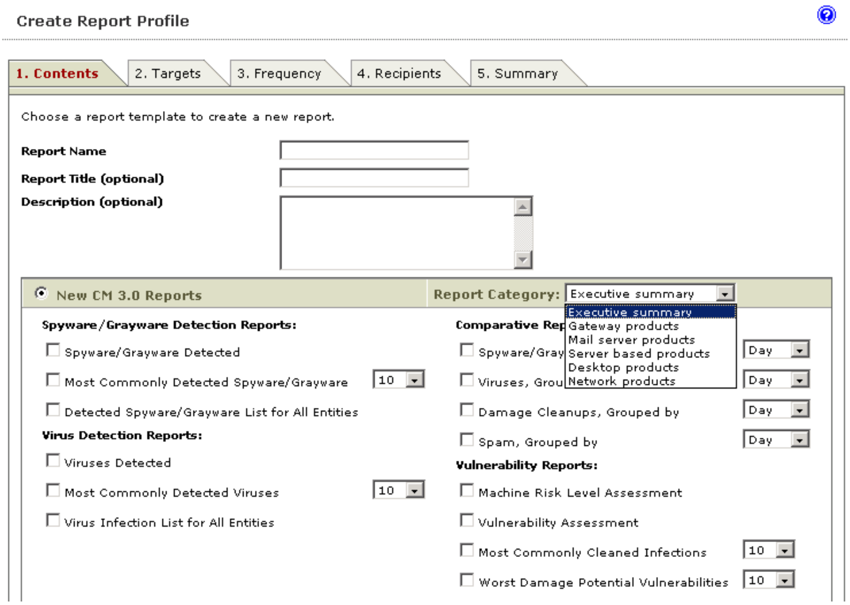
Step 4: Configure the Frequency tab settings

Step 5: Configure the Recipient tab settings

To create local or global report profile:

Step 1: Select whether to create a local or global report

1. Click **Reports** on the main menu.
2. Take one of the following actions:
   - To create a local report profile, click **Local Report Profile** under Reports.
   - To create a global report profile, click **Global Report Profile** under Reports.
3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.



Create Report Profile

1. Contents | 2. Targets | 3. Frequency | 4. Recipients | 5. Summary

Choose a report template to create a new report.

Report Name

Report Title (optional)

Description (optional)

● New CM 3.0 Reports

Report Category: Executive summary

Executive summary
Gateway products
Mail server products
Server based products
Desktop products
Network products

Spyware/Grayware Detection Reports:

□ Spyware/Grayware Detected

□ Most Commonly Detected Spyware/Grayware 10

□ Detected Spyware/Grayware List for All Entities

Virus Detection Reports:

□ Viruses Detected

□ Most Commonly Detected Viruses 10

□ Virus Infection List for All Entities

Comparative Rep

□ Spyware/Gray Day

□ Viruses, Grou Day

□ Damage Cleanups, Grouped by Day

□ Spam, Grouped by Day

Vulnerability Reports:

□ Machine Risk Level Assessment

□ Vulnerability Assessment

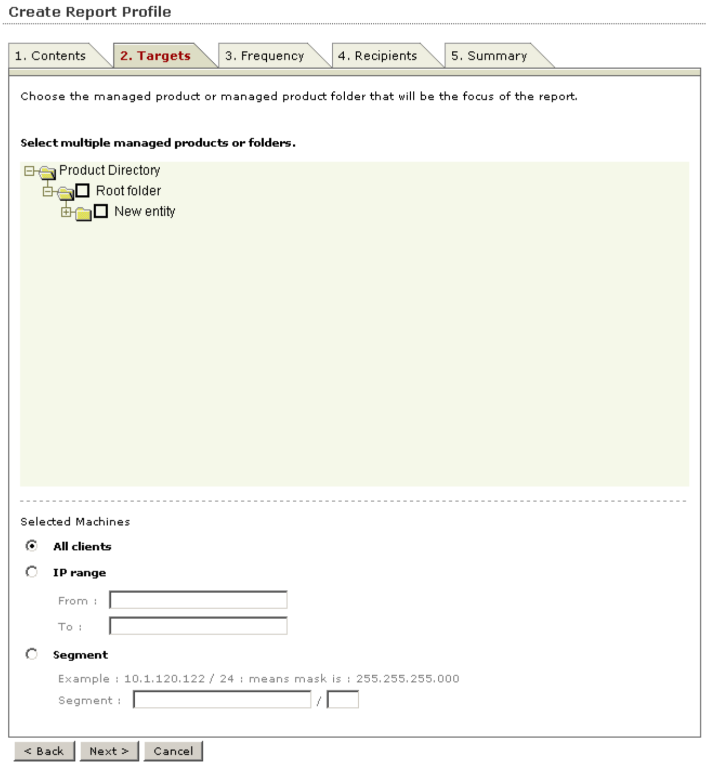
□ Most Commonly Cleaned Infections 10

□ Worst Damage Potential Vulnerabilities 10

Step 2: Configure the Contents tab settings

1. In the working area under the Contents tab, type a name for the report in the **Report name** field to identify the profile on the Local Reports screen.
2. Type a title for the report in the **Report Title** field (optional).
3. Type a description of the report profile in the **Description** field (optional).
4. Select **Network Products** from the **Select report template** list.

5. Select the report format.
6. Click **Next** > to proceed to the Targets tab.



Create Report Profile

Choose the managed product or managed product folder that will be the focus of the report.

Select multiple managed products or folders.

- Product Directory
  - □ Root folder
    - □ New entity

Selected Machines

● **All clients**

○ **IP range**

From :

To :

○ **Segment**

Example : 10.1.120.122 / 24 : means mask is : 255.255.255.000

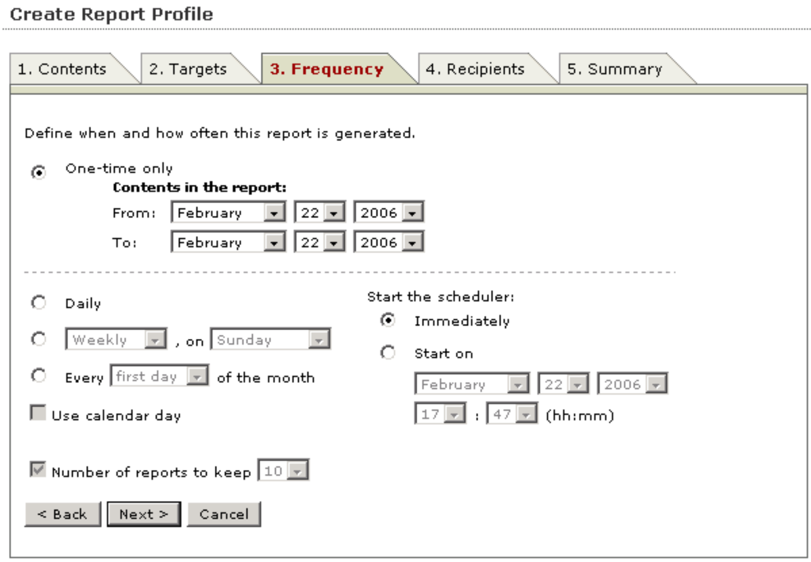
Segment : /

Step 2: Configure the Contents tab settings

1. On the working area under the Targets tab, select the target of the local or global report profile:
   - Select the ScanMail for Microsoft Exchange servers or folders. The profile only contains information about the ScanMail for Microsoft Exchange servers or folders selected.

- Select the child servers. The profile only contains information about the child servers selected. Select the parent server to include all child servers' managed products in the profile.

2. Select the machines that the report will include:
   - **All clients:** All clients the selected ScanMail for Microsoft Exchange server protects
   - **IP range:** Select the IP range of the clients you want to include in the report
   - **Segment:** Select the IP range and segment of the clients you want to include in the report
3. Click **Next >** to proceed to the Frequency tab.



Define when and how often this report is generated.

● One-time only

Contents in the report:

From: February 22 2006

To: February 22 2006

○ Daily

○ Weekly , on Sunday

○ Every first day of the month

□ Use calendar day

Start the scheduler:

● Immediately

○ Start on

February 22 2006

17 : 47 (hh:mm)

☑ Number of reports to keep 10

Step 4: Configure the Frequency tab settings

1. On the working area under the Frequency tab, specify how often Control Manager generates this report. You have the following options:
   - **One-time only:** Provides information you specified in the From and To dates

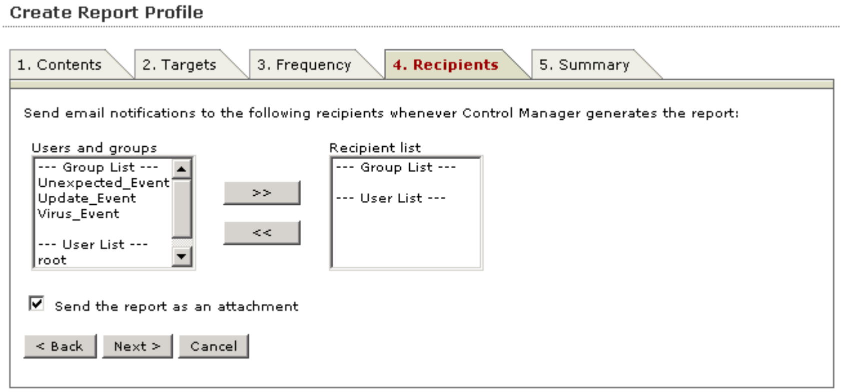
- **Daily:** Contains information from the creation time (12:00 AM yesterday) up to the current time
- **Weekly or Bi-weekly:** Contains 7 or 14 days worth of information; select the day of the week that will trigger the report server to generate a report
- **Monthly:** Contains 30 days worth of information; select the day of the month (first, 15th, or last day) that will trigger the report server to generate a report
- **Use calendar day:** If checked, the start time is 00:00:00 of the first day and the end time is 00:00:00 of the day before generation

  If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs

2. Under Start the scheduler, specify when the Report Server starts collecting information for this report. Select one of the following:
   - **Immediately:** The report server collects information as soon as you save the report profile
   - **Start at:** The report server collects information at the specified date and time
3. For scheduled reports, click **Number of reports to keep** and then specify the instance Control Manager will maintain on the server.

Note: Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

4. Click **Next** > to proceed to the Recipient tab.



Create Report Profile

Send email notifications to the following recipients whenever Control Manager generates the report:

Users and groups
--- Group List ---
Unexpected_Event
Update_Event
Virus_Event

--- User List ---
root

Recipient list
--- Group List ---

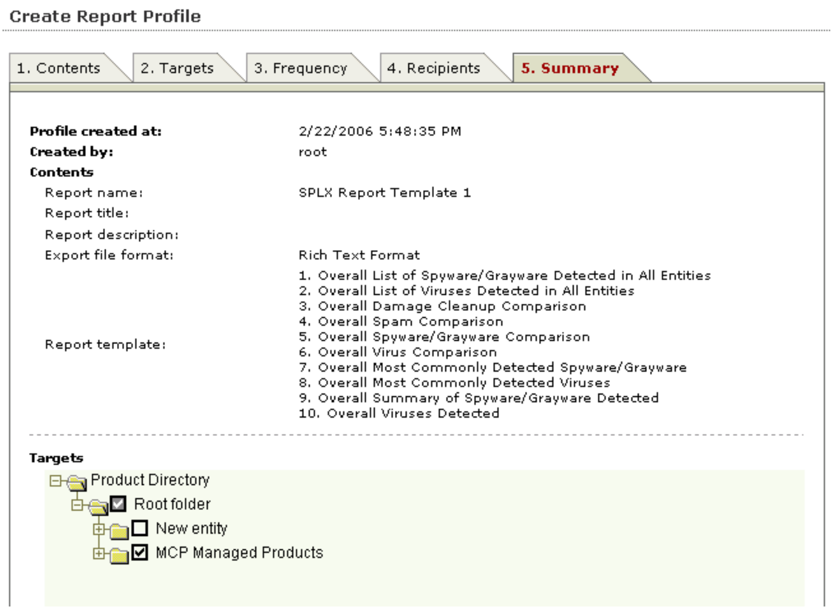
--- User List ---

☑ Send the report as an attachment

Step 5: Configure the Recipient tab settings

1. On the working area under the Recipients tab, select recipients from the existing Control Manager users and groups.
   - Use >> to add recipients from the **Users and groups** list to the Recipient list
   - Use << to remove recipients from the **Recipient** list
2. Click **Send the report as an attachment** to send the report as an attachment. Otherwise, recipients will only receive an email notification about the report being generated.

3. Click **Next** > to proceed to the Summary tab.



Create Report Profile

Profile created at:	2/22/2006 5:48:35 PM
Created by:	root
Contents	
Report name:	SPLX Report Template 1
Report title:	
Report description:	
Export file format:	Rich Text Format
Report template:	1. Overall List of Spyware/Grayware Detected in All Entities 2. Overall List of Viruses Detected in All Entities 3. Overall Damage Cleanup Comparison 4. Overall Spam Comparison 5. Overall Spyware/Grayware Comparison 6. Overall Virus Comparison 7. Overall Most Commonly Detected Spyware/Grayware 8. Overall Most Commonly Detected Viruses 9. Overall Summary of Spyware/Grayware Detected 10. Overall Viruses Detected

Targets

- Product Directory
  - ☑ Root folder
    - □ New entity
    - ☑ MCP Managed Products

4. On the working area under the Summary tab, review the profile settings and then click **Finish** to save the profile.

Review Report Profile Settings

Use the Profile Summary screen to review profile settings.

To access Profile Summary and review report profiles:

- Access Local or Global Reports

  On the working area under the Profile Summary column, click **View Profile**.

- Access Local or Global Scheduled Reports

  On the working area under the Profile Summary column, click **View Profile**.

Enable Scheduled Report Profiles

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it via the Scheduled Local Reports or Scheduled Global Reports screen.

To enable scheduled report profiles:

1. Access Local or Global Scheduled Reports.
2. On the working area under Report Profiles column, click the profile check box.

   Click the check box adjacent to Report Profiles to select or deselect all profiles.
3. Click **Enable**.

Note: The options to enable, disable, and edit one-time-only profiles are not available because Control Manager generates these reports only once.

Generate On-demand Scheduled Reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **Run Now** to create scheduled reports on demand.

To generate on-demand scheduled reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
   - To create a local report profile, click **Local Report Profile** on the left menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.
4. On the Available Reports for {profile name} under **Generate a {Frequency} report starting from**, specify the starting month, day, and year.
5. Click **Run Now**.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

View Generated Reports

Aside from sending and then viewing reports as email attachments, you can also use the Local Report Profile or Global Report Profile screen to view the available local or global reports.

To view reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
   - To create a local report profile, click **Local Report Profile** on the left menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the Available Reports column, click the corresponding **View** link.

   On the Available Reports for {profile name}, you can sort reports according to **Submission Time** or **Stage Completion Time.**
4. Under the Status column, click **View Report**. The default program used to open the file format opens.

Appendix D

Glossary of Terms

The following is a list of terms in this document:

Term	Description
Activation code	A 37-character code, including hyphens, that is used to activate ScanMail. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 Also, see Registration Key.
ActiveUpdate	A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine.
Adware	Similar to spyware, adware gathers user data, such as Web surfing preferences, that could be used for advertising purposes.
Anti-spam	Refers to a filtering mechanism, designed to identify and prevent delivery of unsolicited advertisements, pornography, and other “nuisance” mail.
Approved sender	A sender whose messages are not processed by spam filters.
Attachment	A file attached to (sent with) an email message.
Blocked sender	A sender whose messages are always deleted.
Body (email body)	The content of an email message.
Boot sector viruses	A type of virus that infects the boot sector of a partition or a disk.
Clean	To remove virus code from a file or message.

Term	Description
Compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
Configuration	Selecting options for how ScanMail will function, for example, selecting whether to quarantine or delete a virus-infected email message.
Content filtering	Scanning email messages for content (words or phrases) prohibited by your organization’s Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
Default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
Denial of Service Attack (DoS Attack)	An attack on a computer or network that causes a loss of 'service', namely a network connection. Typically, DoS attacks negatively affect network bandwidth or overload computer resources such as memory.
Dialers	Software that changes client Internet settings and can force the client to dial pre-configured phone numbers through a modem.
Domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
Dynamic Host Control Protocol (DHCP)	A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static. A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.
Dynamic IP Address (DIP)	A Dynamic IP address is an IP address that is assigned by a DHCP server. The MAC address of a computer will remain the same, however, the computer may be assigned a new IP address by the DHCP server depending on availability.

Term	Description
End-User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and other types of grayware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
End User Quarantine	The End User Quarantine is a tool that adds extra spam management features to ScanMail. During installation, ScanMail adds a folder to the server-side mailbox of each end user. When spam messages arrive, the system quarantines them in this folder according to spam filter rules predefined by ScanMail. End users can view this spam folder to open, read, or delete the suspect email messages.
Executable file	A binary file containing a program in machine language which is ready to be executed (run).
False positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
File Transfer Protocol (FTP)	FTP is a standard protocol used for transporting files from a server to a client over the Internet. Refer to Network Working Group RFC 959 for more information.
File type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
Gateway	A device that enables data to flow between different networks.
Spyware/ Grayware	Files and programs, other than viruses, that can negatively affect the performance of the computers on your network. These include spyware, adware, dialers, joke programs, hacking tools, remote access tools, password cracking applications, and others. The ScanMail scan engine scans for grayware as well as viruses.
Hacker	See virus writer.
Hacking tools	Tools used to help hackers enter computers, often through empty ports.
Hostname	The unique name composed of ASCII characters, by which a computer is known on a network.
Hot Fixes and Patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the ScanMail server and/or client program.
HTTP (Hypertext Transfer Protocol)	The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.

Term	Description
HTML, VBScript, or JavaScript viruses	Viruses that reside in Web pages and are downloaded through a browser.
HTTPS (Hypertext Transfer Protocol Secure)	A variant of HTTP used for handling secure transactions.
Incoming	Email messages routed into your network.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet Protocol (IP)	"The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses." (RFC 791)
Java malicious code	Operating system-independent virus code written or embedded in Java.
Joke program	Software that causes a computer to behave abnormally, such as forcing the screen to shake.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.
License	Authorization by law to use ScanMail for Microsoft Exchange.
Macro viruses	Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
Mass-mailing behavior	A malicious program that has high damage potential, because it causes large amounts of network traffic.
Message size	The number of bytes occupied by a message and all its attachments.
Maintenance Agreement	A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Term	Description
Notification	A message that is forwarded to one or more of the following: • System administrator • Sender of a message • Recipient of a message, • Other email address • SNMP and Windows event log The purpose of the notification is to communicate that an event has occurred, such as a virus being detected in a message
Offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
Outgoing	Email messages or other data leaving your network, routed out.
Password cracking applications	Software that can help hackers decipher user names and passwords.
Pattern file	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
Phish sites	A Web site that lures users into providing personal details, such as credit card information. Links to phish sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses.
Ping	A utility that sends an ICMP echo request to an IP address and waits for a response. The Ping utility can determine if the machine with the specified IP address is online or not.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computer’s buffer to overflow, which can freeze or reboot the machine.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.
Quarantine entire message	To place email messages in an isolated directory (the Quarantine Directory) on the ScanMail scanner. Items placed in the quarantine directory are indexed in the ScanMail database.
Quarantine message part	To move the email message body or attachment to a restricted access folder, removing it as a security risk to the Exchange environment. ScanMail replaces the message part with the text/file you specify.

Term	Description
Registration key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8. Also see Activation Code
Remote access tools	Tools used to help hackers remotely access and control a computer.
Scan	To examine items in a file in sequence to find those that meet a particular criteria.
Scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
Secure Socket Layer (SSL)	SSL is a scheme proposed by Netscape Communications Corporation to use RSA public-key cryptography to encrypt and authenticate content transferred on higher-level protocols such as HTTP, NNTP, and FTP.
SSL certificate	A digital certificate that establishes secure HTTPS communication between the Policy Server and the ACS server.
Simple Mail Transport Protocol (SMTP)	SMTP is a standard protocol used to transport email messages from server to server, and client to server, over the internet.
SOCKS 4	A TCP protocol used by proxy servers to establish a connection between clients on the internal network or LAN and computers or servers outside the LAN. The SOCKS 4 protocol makes connection requests, sets up proxy circuits and relays data at the Application layer of the OSI model.
Spam	Unsolicited email messages meant to promote a product or service.
Spyware/ Grayware	A type of grayware that installs components on a computer for the purpose of recording Web surfing habits (primarily for marketing purposes). Spyware sends this information to its author or to other interested parties when the computer is online. Spyware often downloads with items identified as 'free downloads' and does not notify the user of its existence or ask for permission to install the components. The information spyware components gather can include user keystrokes, which means that private information such as login names, passwords, and credit card numbers are vulnerable to theft.
Standard maintenance	See Maintenance Agreement
Subject (message subject)	The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.” ScanMail uses the subject from the message header to determine the message subject.
Tag	To place an identifier, such as “Spam:” in the subject field of an email message.

Term	Description
Telnet	Telnet is a standard method of interfacing terminal devices over TCP by creating a "Network Virtual Terminal". Refer to Network Working Group RFC 854 for more information.
Test virus	An inert file that acts like a real virus and is detectable by virus-scanning software. Use test files, such as the EICAR test script, to verify that your antivirus installation is scanning properly.
Traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol (TCP)	A connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. TCP relies on IP datagrams for address resolution. Refer to DARPA Internet Program RFC 793 for information.
TrendLabs	TrendLabs is Trend Micro's global network of antivirus research and product support centers that provide 24 x 7 coverage to Trend Micro customers around the world.
Trojan horses	Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter.
True file type	A virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
Undesirable content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
Unsolicited email	See spam
User Datagram Protocol (UDP)	A connectionless communication protocol used with IP for application programs to send messages to other programs. Refer to DARPA Internet Program RFC 768 for information.
Virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
Virus writer	Another name for a computer hacker. Someone who writes virus code.
Wildcard	For ScanMail, an asterisk (*) represents any character. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on.

Term	Description
Worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email. A worm can also be called a network virus.
Zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.

Index