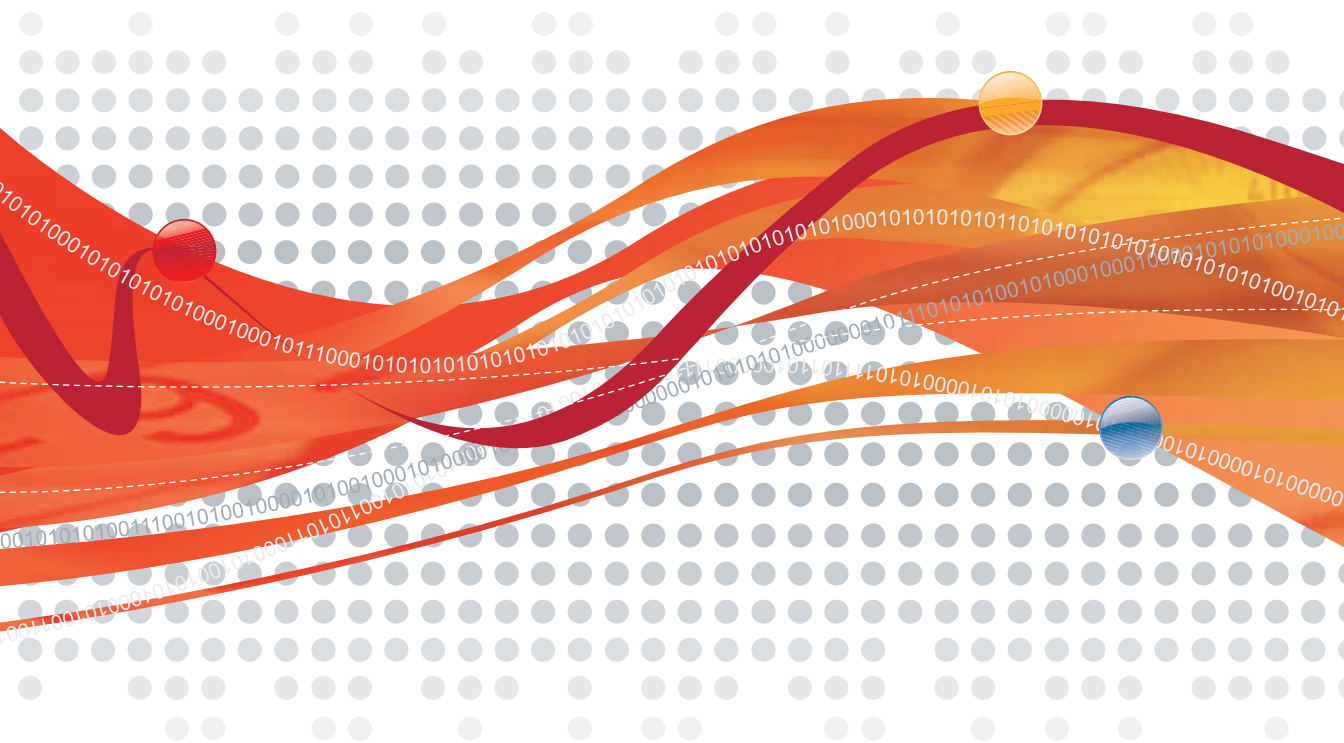
TREND MICRO™

ScanMail™ 10

Securing your Exchange environment

for Microsoft™ Exchange

Installation and Upgrade Guide



Messaging Security

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

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

Copyright© 1998-2009 Trend Micro Incorporated. All rights reserved.

Document Part No.: SSEM83030/70117

Product Name and Version No.: Trend Micro™ ScanMail™ *for Microsoft™ Exchange* 10.0

Release Date: December 2009

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

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

ScanMail Documentation viii

Audience viii

Document Conventions ix

Chapter 1: Planning ScanMail Installation and Upgrade

System Requirements 1-2
- ScanMail with Exchange Server 2010 1-2
- ScanMail with Exchange Server 2007 1-3
- ScanMail with Exchange Server 2003 1-5
- For Cluster Installation: 1-5

Before you Begin 1-6
- Pilot Installation 1-6

Deployment Strategy 1-8
- Planning for Network traffic 1-8
- Deploying ScanMail to Multiple Servers 1-9
  - Deploying ScanMail to Multiple Local Area Network (LAN) Segments 1-14

Preparing to Install 1-15
- Configuration Exceptions When You Upgrade 1-16
  - Activation Code 1-16
  - Web Server Settings 1-16
  - End User Quarantine (EUQ) and Junk E-Mail 1-17
  - Server Management Settings 1-21
  - Trend Micro Management Communication Protocol (MCP) Agent .. 1-21
- Installation with a Remote SQL Server 1-24
- Additional Requirements for Remote Installation with Windows 2008 . 1-28

Pre-Installation Checklist 1-32

Performing a Fresh Install 1-33
Installing On a Cluster 1-34
Upgrading to ScanMail 10.0 1-35
Upgrade Effect on Logs and Folders 1-35
Upgrading on Clusters 1-36
Cluster Installation 1-36

Chapter 2: Installing ScanMail with Exchange 2010/2007 Hub Transport and Mailbox Servers

Running the Setup Program 2-2
Installation with Hub Transport and Mailbox Servers 2-2

Chapter 3: Installing ScanMail with Exchange 2010/2007 Edge Transport Servers

Running the Setup Program 3-2
Installation with Edge Transport Servers 3-2

Chapter 4: Installing ScanMail with Exchange Server 2003

Running the Setup Program 4-2
Installation with Exchange Server 2003 4-2

Chapter 5: Post-Installation Tasks

Verifying a Successful Installation 5-2
Using the ScanMail Management Pack 5-3
ScanMail Management Pack Fresh Install 5-3
ScanMail Management Pack Post-Installation 5-8
Testing Your Installation 5-8
Testing Manual Scan 5-9
Testing Real-time Scan 5-9
Testing Notifications 5-10

Chapter 6: Silent Installation

About Silent Installation 6-2
Silent Installation Limitations 6-2
Performing Silent Installation 6-3
Using an Existing Pre-Configured File 6-5

Chapter 7: Removing ScanMail

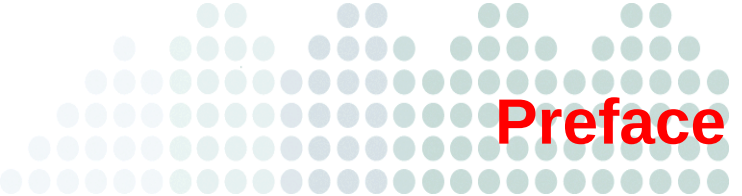
Before Removing ScanMail 7-2
Privilege Requirements 7-3
Using the Enterprise Solution DVD 7-4
Using the Windows Control Panel 7-15
Removing ScanMail from Clusters 7-16
Manually Removing from Exchange 2010/2007 Edge Transport or Hub Transport Servers 7-16
Manually Removing from Exchange 2010/2007 Mailbox Servers 7-19
Manually Removing from Exchange 2003 Servers 7-22

Chapter 8: Getting Support and Contacting Trend Micro

Contacting Technical Support 8-2
Before Contacting Technical Support 8-3
Contacting Trend Micro 8-3
TrendLabsSM 8-4
Known Issues 8-4

Appendix A: Pre-configured Files

Index



Preface

Welcome to the Trend Micro™ ScanMail™ *for Microsoft™ Exchange* Installation and Upgrade Guide. This book contains basic information about the tasks you need to perform to deploy ScanMail to protect your Exchange servers. It is intended for novice and advanced users of ScanMail who want to plan, deploy, install, and test ScanMail.

Topics in this chapter:

- *ScanMail Documentation* on page P-viii
- *Audience* on page P-viii
- *Document Conventions* on page P-ix

ScanMail Documentation

The product 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.
- **Installation and Upgrade Guide**—PDF documentation that discusses requirements and procedures for installing and upgrading the product
- **Administrator's Guide**—PDF documentation that discusses getting started information and product management
- **Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.
- **Knowledge Base**—Contains the most up-to-date information about all Trend Micro products. Answers to questions are also posted and a dynamic list of the most frequently asked question is also displayed.

  http://esupport.trendmicro.com

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

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 2010 and 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.

TABLE P-1. Conventions used in the documentation

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

Chapter 1

Planning ScanMail Installation and Upgrade

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

Topics in this chapter:

- *System Requirements* on page 1-2
- *Before you Begin* on page 1-6
- *Deployment Strategy* on page 1-8
- *Preparing to Install* on page 1-15
- *Pre-Installation Checklist* on page 1-32
- *Performing a Fresh Install* on page 1-33
- *Upgrading to ScanMail 10.0* on page 1-35
- *Cluster Installation* on page 1-36

System Requirements

The following lists the system requirements for running Trend Micro™ ScanMail™ *for Microsoft™ Exchange*.

- *ScanMail with Exchange Server 2010* on page 1-2
- *ScanMail with Exchange Server 2007* on page 1-3
- *ScanMail with Exchange Server 2003* on page 1-5

ScanMail with Exchange Server 2010

The following table lists the system requirements for running ScanMail with Exchange Server 2010.

TABLE 1-1. System requirements for installation with Exchange Server 2010

RESOURCE	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 platforms
Memory	1GB RAM (2GB RAM recommended) (Exclusively for ScanMail)
Disk space	2GB free disk space
Operating system	• Microsoft™ Windows Server™ 2008 with Service Pack 2 or above (64-bit) • Microsoft Windows Server 2008 R2 or above (64-bit)
Mail Server	Microsoft Exchange Server 2010

TABLE 1-1. System requirements for installation with Exchange Server 2010

RESOURCE	REQUIREMENTS
Web Server	• Microsoft Internet Information Services (IIS) 7.5 • Microsoft Internet information Services (IIS) 7.0
Browser	A Java-enabled Web browser that supports frames, such as • Microsoft™ Internet Explorer™ 6.0 or above • Mozilla Firefox™ 3.0 or above
Java™ software	Sun Java 2 Runtime Environment 1.6.0 U13 or above **Note:** You can download this software from http://java.sun.com/products/archive/j2se/6u13/index.html

ScanMail with Exchange Server 2007

The following table lists the system requirements for running ScanMail with Exchange Server 2007.

TABLE 1-2. System requirements for installation with Exchange Server 2007

RESOURCE	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) (Exclusively for ScanMail)
Disk space	2GB free disk space

TABLE 1-2. System requirements for installation with Exchange Server 2007

RESOURCE	REQUIREMENTS
Operating system	• Microsoft Windows Server 2008 with Service Pack 1 or above (64-bit) • Microsoft Small Business Server (SBS) 2008 **Note:** Microsoft Small Business Server (SBS) 2008 received limited compatibility testing with this version of ScanMail. The installation recommendation is to uninstall Microsoft ForeFront prior to installing ScanMail from Microsoft Small Business Server (SBS) 2008. • Microsoft Windows Server 2003 R2 with Service Pack 2 (64-bit) • Microsoft Windows Server 2003 with Service Pack 2 (64-bit)
Mail Server	Microsoft Exchange Server 2007 with Service Pack 1 or above
Web Server	• Microsoft Internet Information Services (IIS) 7.0 • Microsoft Internet information Services (IIS) 6.0
Browser	A Java-enabled Web browser that supports frames, such as • Microsoft Internet Explorer 6.0 or above • Mozilla Firefox 3.0 or above
Java software	Sun Java 2 Runtime Environment 1.6.0 U13 or above **Note:** You can download this software from http://java.sun.com/products/archive/j2se/6u13/index.html

ScanMail with Exchange Server 2003

The following table lists the system requirements for running ScanMail with Exchange Server 2003.

TABLE 1-3. System requirements for installation with Exchange Server 2003

RESOURCE	REQUIREMENT
Processor	Intel Pentium II 266 MHz or higher processor (Intel Pentium or compatible 733MHz processor recommended)
Memory	1GB RAM (2GB RAM recommended) (Exclusively for ScanMail)
Disk space	2GB free disk space
Operating system	• Microsoft Windows Server 2003 with Service Pack 2 (32-bit) • Microsoft Windows Server 2003 R2 (32-bit) with Service Pack 2 (32-bit)
Mail Server	Microsoft Exchange Server 2003 with Service Pack 2
Web Server	• Microsoft Internet Information Services (IIS) 7.0 • Microsoft Internet Information Services (IIS) 6.0
Browser	A Java-enabled Web browser that supports frames, such as • Microsoft Internet Explorer 6.0 or above • Mozilla Firefox 3.0 or above
Java software	Sun Java 2 Runtime Environment 1.6.0 U13 or above **Note:** You can download this software from http://java.sun.com/products/archive/j2se/6u13/index.html

For Cluster Installation:

The following lists support cluster environments:

- Exchange Server 2010 with Database Availability Group (DAG) model
- Exchange Server 2007 with VERITAS Cluster 5.1 and 5.0 R1
- Exchange Server 2007 with Single Copy Cluster (SCC) model
- Exchange Server 2007 with Cluster Continuous Replication (CCR) model
- Exchange Server 2007 with Standby Continuous Replication (SCR) model
- Exchange Server 2003 with VERITAS Cluster 5.1 and 5.0 R1
- Shared disk cluster model with Exchange Server 2003

Before you Begin

The following section contains 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:

Step 1 Create an appropriate test site.

Step 2 Create a rollback plan.

Step 3 Deploy and evaluate your pilot.

Step 1. 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/

Step 2. 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 2010 and 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 back up ScanMail and configurations for an Exchange 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.

Restoring ScanMail Configurations

Use the following procedures to restore ScanMail configurations if necessary.

To restore ScanMail configurations for an Exchange 2010 and 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.ldf, or Log.ldf, or Report.ldf.
4. Start SQL Server (SCANMAIL) Service and ScanMail Master Service.

To restore ScanMail configurations for an Exchange 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.

Step 3. Executing and Evaluating Your Pilot Installation

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

Deployment Strategy

The ScanMail Setup program supports installation to a single or multiple local server or remote servers.

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 ActiveUpdate 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. 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 server 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 1-4* and *Table 1-5* when you deploy ScanMail.

Another strategy is to deploy ScanMail to an Exchange server in the network demilitarized zone (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.

TABLE 1-4. Deploying ScanMail with Exchange Server 2003

SERVER ROLE	RECOMMENDATION
Front-end mail servers: • Are usually located directly behind a perimeter device and/or firewall. • Frequently communicate with 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 Active Directory to resolve email addresses and read configuration data.	• Set the Trend Micro ActiveUpdate server as the source of component updates for the front-end server, and set 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. • Configure SMTP scanning on front-end mail servers. • Configure ScanMail to screen out email messages and attachments that contain spam or undesirable content at the front-end mail servers. This reduces the burden for back-end servers that will no longer have to process these messages.

TABLE 1-4. Deploying ScanMail with Exchange Server 2003

SERVER ROLE	RECOMMENDATION
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.	• Set back-end mail servers to perform security risk scan with vigorous screening options. • Regularly schedule scans on Exchange mailboxes to prevent threats from creeping in from unexpected sources not covered in your configurations.

TABLE 1-5. Deploying ScanMail with Exchange Server 2010 or 2007

SERVER ROLE	RECOMMENDATION
Edge Transport server: • No access to Active Directory. • XML-based routing. • Port 25 SMTP relay. • Decentralized management. • 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 security risk scan. • Set Edge Transport servers to update through Trend Micro ActiveUpdate, and to regularly perform scheduled update for protection against new security risks. • Enable spam prevention features. • Enable Web reputation features.

TABLE 1-5. Deploying ScanMail with Exchange Server 2010 or 2007

SERVER ROLE	RECOMMENDATION
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 security risk scan. • If there is an Edge server, set Hub server to use the Edge server as the source of updates. Otherwise set the Trend Micro ActiveUpdate server as the source. • Enable Active Directory integrated Attachment Blocking rules and Content Filtering policies.

TABLE 1-5. Deploying ScanMail with Exchange Server 2010 or 2007

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 use the Hub Transport server as the source of updates, which decreases overall network traffic and reduces exposure to the Internet. • Set Mailbox servers to perform security risk 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. • Disable Attachment Blocking and Content Filtering scans.

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, preview the information in this section and consult the pre-installation checklist. The installation process is the same for all supported Windows server versions.

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 Setup program. The local machine is the one on which the Setup 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.

Table 1-6 displays the minimum privileges required for a ScanMail fresh install.

TABLE 1-6. Fresh Install Minimum Privileges

EXCHANGE VERSION	MINIMUM PRIVILEGES	FEATURE LIMITATION WITHOUT DOMAIN ADMINISTRATOR PRIVILEGES
Exchange Server 2010 or 2007 (Edge Transport Server Roles)	Local Administrator	N/A
Exchange Server 2010 (Hub/Mailbox)	Domain Administrator	N/A
Exchange Server 2007 (Hub/Mailbox/Cluster)	Local Administrator and Exchange Organization Administrator	Cannot activate End User Quarantine (EUQ)
Exchange Server 2003	Local Administrator and Domain User	Cannot activate End User Quarantine (EUQ) and Server Management

Configuration Exceptions When You Upgrade

When you upgrade from ScanMail 7.0 or 8.0 with Service Pack 1 to ScanMail 10, the Setup program uses your previous settings during installation. However, certain settings are not directly copied to ScanMail 10.

Activation Code

When you perform an upgrade, ScanMail always uses the new activation code. If a new activation code is not submitted, the original activation code is used.

Web Server Settings

ScanMail always uses new Web server settings. Update Web server settings to use a new Web server or keep previous settings to use the original Web server.

Note: This version of ScanMail only supports Microsoft Internet Information Services (IIS). If an Apache Web server was used previously, specify a new Web port for Internet Information Services (IIS). If a new Web port is not specified, an error message displays regarding the Web port conflict.

End User Quarantine (EUQ) and Junk E-Mail

You can switch between **Integrate with Outlook Junk E-mail** and **Integrate with End User Quarantine** during upgrade. The following table displays settings when you use an account with domain administrator privileges to perform an upgrade and the previous setting was EUQ.

TABLE 1-7. Previous setting is EUQ 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 2007 (Mailbox Server Roles)	• Removes previous EUQ mailbox and accounts • Merges EUQ related rules and forms with Junk E-mail rules and forms • Spam Maintenance menu does not appear in the product console	Retains all previous EUQ settings
Exchange Server 2003	• Removes previous EUQ mailbox and accounts • Merges EUQ related rules and forms with Junk E-mail rules and forms • Spam Maintenance menu does not appear in the product console	Retains all previous EUQ settings

The following table displays settings when you use an account with local administrator privileges to perform an upgrade and the previous setting was EUQ.

TABLE 1-8. Previous settings is EUQ with Local 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 2007 (Mailbox Server Roles)	• EUQ mailbox and accounts remain because privileges are insufficient for deletion • Merges previous EUQ approved senders list with Junk E-mail safe senders list • Spam Maintenance menu does not appear in the product console	Retains all previous EUQ settings
Exchange Server 2003	• EUQ mailbox and accounts remain because privileges are insufficient for deletion • Merges previous EUQ approved senders list with Junk E-mail safe senders list • Spam Maintenance menu does not appear in the product console	Retains all previous EUQ settings

The following table displays settings when you use an account with domain administrator privileges to perform an upgrade and the previous setting was Junk E-mail.

TABLE 1-9. Previous setting is Junk E-mail 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 2007 (Mailbox Server Roles)	Retains all previous Junk E-mail settings	• Creates EUQ mailbox • Creates EUQ account • Merge Junk E-mail Safe Sender List to EUQ Approved Sender List • Spam Maintenance menu appears in the product console • Activates EUQ
Exchange Server 2003	Retains all previous Junk E-mail settings	• Creates EUQ mailbox • Creates EUQ account • Merges Junk E-mail Safe Sender List to EUQ Approved Sender List • Spam Maintenance menu appears in the product console • Activates EUQ

The following table displays settings when you use an account with local administrator privileges to perform an upgrade and the previous setting was Junk E-mail.

TABLE 1-10. Previous settings is EUQ with Local 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 2007 (Mailbox Server Roles)	Retains all previous Junk E-mail settings	• Spam Maintenance menu appears in the product console • EUQ mailboxes, accounts, and activation cannot be completed because additional privileges are required.
Exchange Server 2003	Retains all previous Junk E-mail settings	• Spam Maintenance menu appears in the product console • EUQ mailboxes, accounts, and activation cannot be completed because additional privileges are required.

Server Management Settings

The following table displays Server Management settings that are exceptions when upgrading ScanMail.

TABLE 1-11. Server management settings when upgrading

EXCHANGE VERSION	IF YOU SELECT SPECIFY AN EXISTING ACCOUNT OR CREATE A NEW ACCOUNT	IF YOU SELECT SKIP AND REACTIVATE SERVER MANAGEMENT LATER
Exchange Server 2010 or 2007	Retains all previous management group settings	Retains all previous management group settings
Exchange Server 2003	• Removes original settings. • Applies new settings.	Removes original settings.

Trend Micro Management Communication Protocol (MCP) Agent

This version of ScanMail supports Trend Micro™ Control Manager™ 5.0 with Patch 4 and hot fix 1828 Control Manager 3.5 with Patch 7 and hot fix 1640. The communication mechanism between the Control Manager server and Trend Micro Management Communication Protocol (MCP) 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.

When upgrading from previous versions of ScanMail that use the Trend Micro Management Communications Protocol (MCP) agent, the ScanMail Setup program does not unregister from the Control Manager server. So, the original directory tree in Control Manager does not change.

TABLE 1-12. Control Manager Settings when upgrading from ScanMail 8.0 Service Pack 1

EXCHANGE VERSION	IF YOU SELECT REGISTER SCANMAIL AGENT TO CONTROL MANAGER SERVER AND REGISTER TO THE SAME CONTROL MANAGER SERVER	IF YOU SELECT REGISTER SCANMAIL AGENT TO CONTROL MANAGER AND REGISTER TO A DIFFERENT CONTROL MANAGER SERVER	IF YOU DO NOT SELECT REGISTER SCANMAIL AGENT TO CONTROL MANAGER SERVER
Exchange Server 2010, 2007, and 2003	• Retains all previous Control Manager settings. • Folder locations do not change.	• Unregister from original Control Manager server. • Removes Control Manager Agent. • Installs the latest version of the MCP agent. • Registers 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.	• Retains all previous Control Manager Settings • Folder locations do not change.

TABLE 1-13. Control Manager Settings when upgrading from ScanMail 7.0

EXCHANGE VERSION	IF YOU SELECT REGISTER SCANMAIL AGENT TO CONTROL MANAGER SERVER	IF YOU DO NOT SELECT REGISTER SCANMAIL AGENT TO CONTROL MANAGER SERVER
Exchange Server 2003	• Unregisters from original Control Manager server • Uninstalls ScanMail 7.0 Control Manager Agent • Installs the latest version of the MCP agent • Registers 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.	• Unregisters from original Control Manager server • Uninstalls ScanMail 7.0 Control Manager Agent • Removes all Control Manager Agent information from database.

Note: ScanMail 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.

Installation with a Remote SQL Server

This version of ScanMail supports storing the ScanMail database on a remote SQL server with fresh installs on Exchange Server 2010 or 2007. Prepare a remote SQL server before installing ScanMail.

Note: ScanMail cannot automatically detect the remote SQL server. Manually configure the remote SQL server settings during installation. If the settings are not configured during installation, ScanMail installs on the local SQL Server Express.

To install ScanMail with a remote SQL server:

1. Prepare a remote SQL server.
2. Create an account as a dbcreator role in the SQL instance where you want to install ScanMail.

   Note: ScanMail supports SQL server accounts, Windows accounts are not supported.

3. During installation specify the remote SQL server on the following screens:

   Note: When ScanMail is installed with a remote SQL server and connection to the server is unavailable, ScanMail will perform a database reconnect. ScanMail logs the error to Windows Event Log and adds an entry every hour the server is unavailable. When the server is unavailable, ScanMail does not scan messages. All messages are sent to the mail database. ScanMail tries to reconnect to the database server every minute, by default. When connection to the database is recovered, another windows event log entry is added and ScanMail will continue message scans.

a. On the **Select Target Server(s)** screen of the ScanMail Setup program, click the link to configure remote SQL server settings. The remote SQL configuration screen appears.

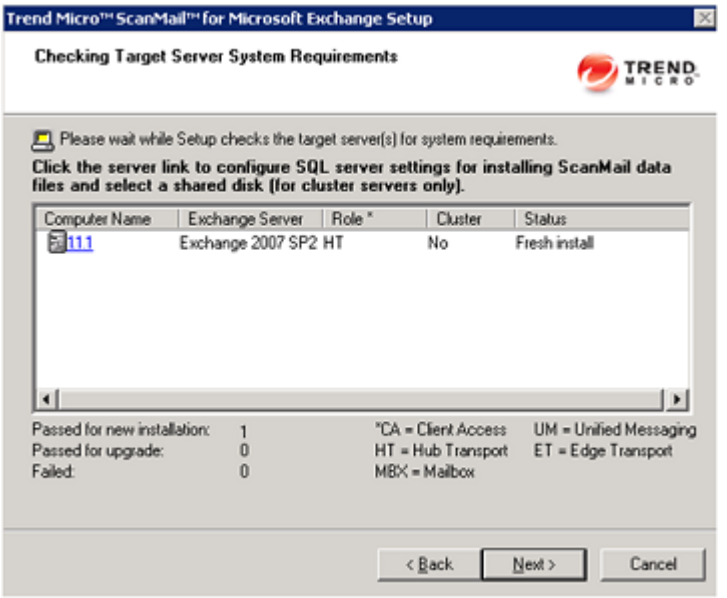


FIGURE 1-1 Installing remotely - Select Target Servers

b. Type the SQL instance name and SQL account prepared in Step 2. Then, click OK. The Target Server Requirements screen appears.

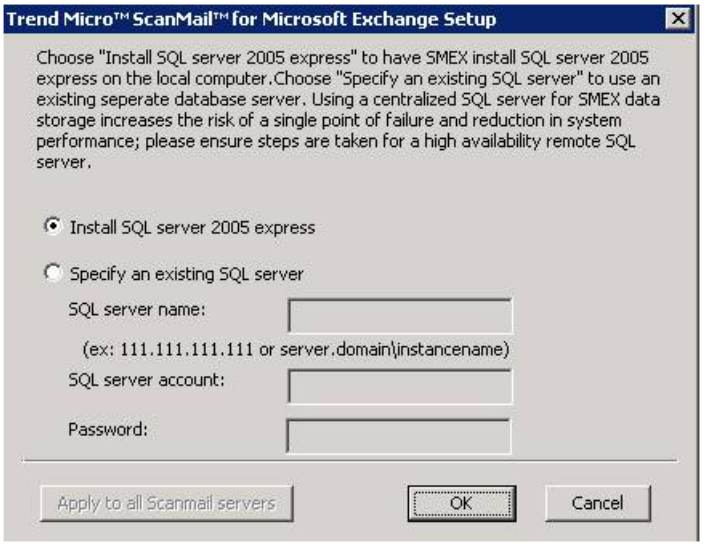


FIGURE 1-2 Installing remotely - SQL settings

c. Click **Next** to continue with the installation process if the status check was successful. The Check SQL Server Database screen appears.

   Otherwise, click **Back** to navigate to the Target Server Requirements screen to configure remote SQL server settings.

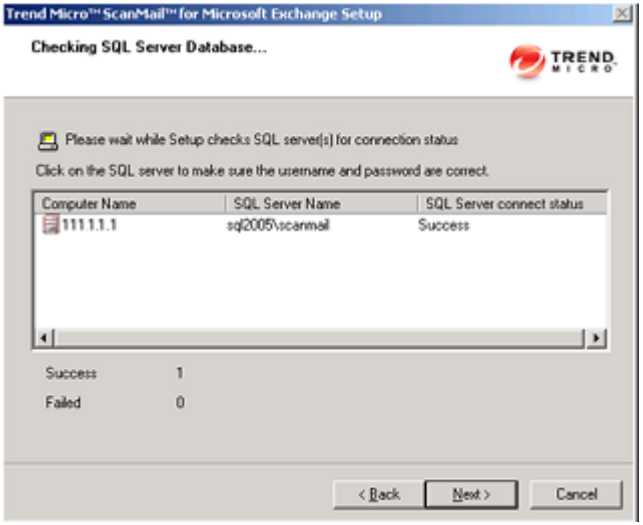


FIGURE 1-3 Installing remotely - Check SQL server database

4. Complete the rest of the installation process.

Additional Requirements for Remote Installation with Windows 2008

This only applies to Windows 2008 operating systems when remotely installing multiple Exchange servers.

Prepare the following:

- An account with domain administrator privileges or domain user privileges. If it is an account with domain user privileges, this account must have local administrator privileges on each Exchange server.
- Enable file sharing on Windows Firewall or disable Windows Firewall on each Exchange server.
- Ensure that administrative shares are available on each Exchange server.

To install to multiple remote Exchange servers:

1. Log on to the operating system with an account that has domain administrator privileges and launch the ScanMail Setup program.
2. Specify the options on the following screens:

a. At the **Select Target Server(s)** screen of the installation process, **Add** or **Browse** to add multiple target ScanMail servers that belong to the same domain.

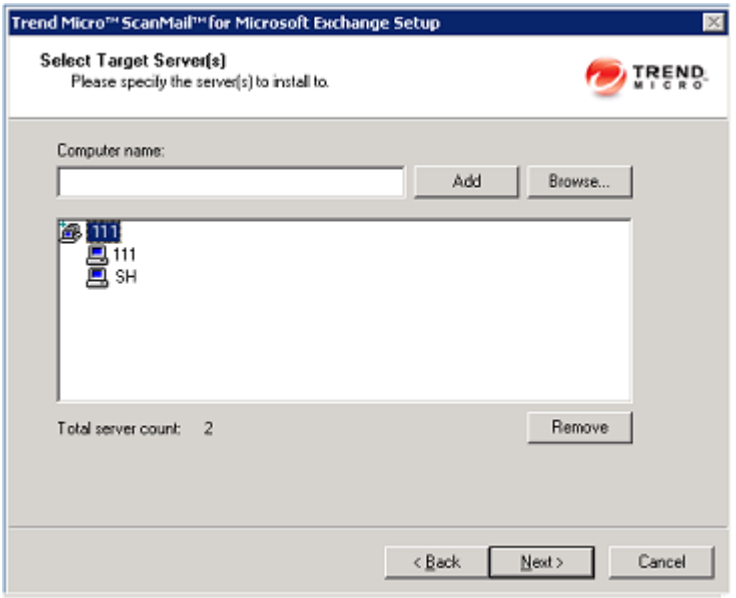


FIGURE 1-4 Installing remote servers - Select Target Server(s)

b. At the **Log on** screen of the installation process, type the same account that was used to log on to the operating system in Step 1.

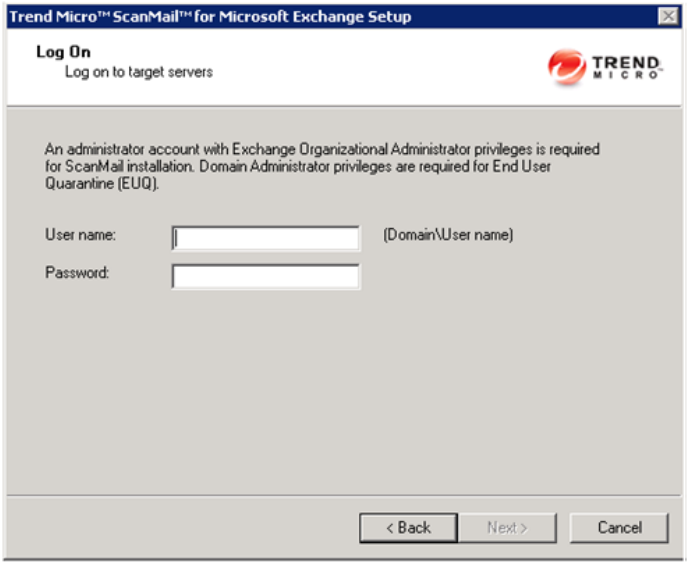


FIGURE 1-5 Installing remote servers - Log on

c. At the **Configure Shared/Target Directory** screen of the installation process, type the administrative shares such as ADMIN$, C$, and D$.

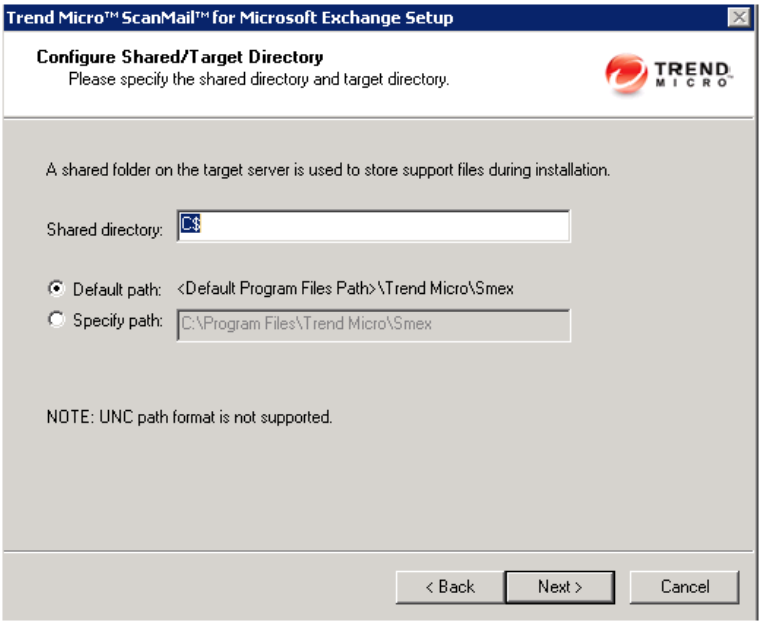


FIGURE 1-6 Installing remote servers - Configure Shared/Target Directory

3. Complete the rest of the installation process.

Pre-Installation Checklist

TABLE 1-14. Pre-installation checklist

ITEM	NOTES
Minimum Account privileges	• For Exchange Server 2010 and 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 2010 and Exchange Server 2007 Edge Transport you need Local Administrator privileges. • For Exchange Server 2003 you need Local Administrator and Domain User privileges. Activate End User Quarantine and Server Management with an account with Domain Administrator privileges.
Restart	You do not need to stop Exchange services before installing or restart them after a successful installation.

TABLE 1-14. Pre-installation checklist

ITEM	NOTES
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 specify 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.
CGI component	On Windows 2008, install CGI role service before installing ScanMail. Add CGI role service from Windows Server Manager > Add Roles > Web Server (IIS) > Add Role services > Application development > CGI.

Performing a Fresh Install

If you do not have a previous version of ScanMail installed on your Exchange server, perform a fresh installation. Before beginning your installation, consult the pre-installation checklist, *Table 1-14*.

Note: The installation procedure is the same for all supported Windows versions.

Installing On a Cluster

You can install ScanMail on the following:

- Windows 2008 cluster (Node and Disk Majority Cluster) with Exchange Server 2007 SCC model
- Windows 2008 cluster (Node and Disk Majority Cluster, Node and File Share Majority Cluster) with Exchange Server 2007 CCR model
- Windows 2003 cluster (Single Quorum Device Cluster) with Exchange Server 2003 or Exchange Server 2007 SCC model
- Windows 2003 cluster (Majority Node Set Cluster, Standard Quorum Cluster) with Exchange Server 2007 CCR model.
- Exchange Server 2010 with Database Availability Group (DAG) model
- Exchange Server 2007 with VERITAS Cluster 5.1 or VERITAS Cluster 5.0 R1
- Exchange Server 2003 with VERITAS Cluster 5.1 or VERITAS Cluster 5.0 R1

For cluster installation, ScanMail adds resources for each virtual server and installs to 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, this means 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 10.0

Before beginning your installation, consult the pre-installation checklist, *Table 1-14*. To upgrade ScanMail, run the Setup program.

ScanMail 10.0 supports upgrading from the following previous versions:

- ScanMail 10.0 Beta
- ScanMail 8.0 with Service Pack 1
- ScanMail 7.0.

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

When upgrading, if ScanMail 10.0 has configuration settings similar to the previous version, then the upgraded version maintains these customized configurations. However, when there is no equivalent configuration setting, ScanMail installs and uses the Trend Micro default configurations.

Upgrade Effect on Logs and Folders

Upgrading to this version of ScanMail 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.

Upgrading on Clusters

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

WARNING! Never upgrade a cluster during failover.

ScanMail does not stop the Exchange System Attendant service and IIS admin when you perform a version or build upgrade on cluster servers.

Cluster Installation

You can use the regular ScanMail Setup program to install ScanMail on all virtual servers on Exchange 2007 and Exchange 2003 clusters. For cluster installation, you can select virtual servers just like selecting 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. Refer to the installation chapter that corresponds to your Exchange version for instructions for installing ScanMail to a cluster server environment.

Note: For Microsoft clusters, type the node name, Exchange Virtual Server (EVS) name, or cluster name on the Select Target Servers screen. For VERITAS clusters, type the node name or Exchange Virtual Server (EVS) name on the Select Target Servers screen and ScanMail can detect and install on each Exchange Virtual Server (EVS) in the cluster.

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 the Administrator's Guide topic on manually creating a ScanMail resource for virtual servers.

Chapter 2

Installing ScanMail with Exchange 2010/2007 Hub Transport and Mailbox Servers

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

Topics in this chapter:

- *Running the Setup Program* on page 2-2
- *Installation with Hub Transport and Mailbox Servers* on page 2-2

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 with Hub Transport and Mailbox Servers

The following lists the steps to install ScanMail with Exchange Server 2010 or 2007 Hub Transport and Mailbox server roles.

To install ScanMail:

1. Select a source for the Setup program:

   Trend Micro Web site.

   a. Download ScanMail from the Trend Micro Web site.

   b. Unzip the file to a temporary directory

   c. Run setup.exe to install ScanMail

   The Trend Micro Enterprise Solution DVD.

   a. Insert the DVD 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.

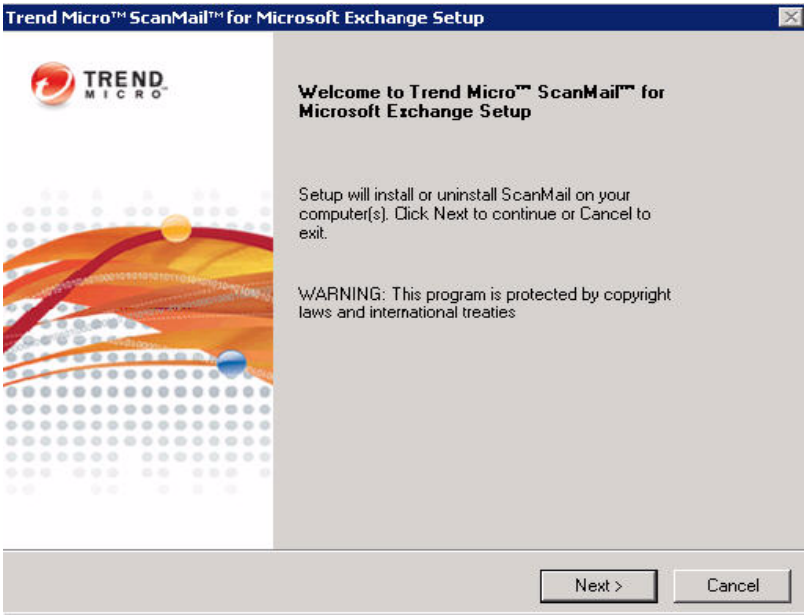


FIGURE 2-1. Welcome screen

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 installation without modifying your operating system.

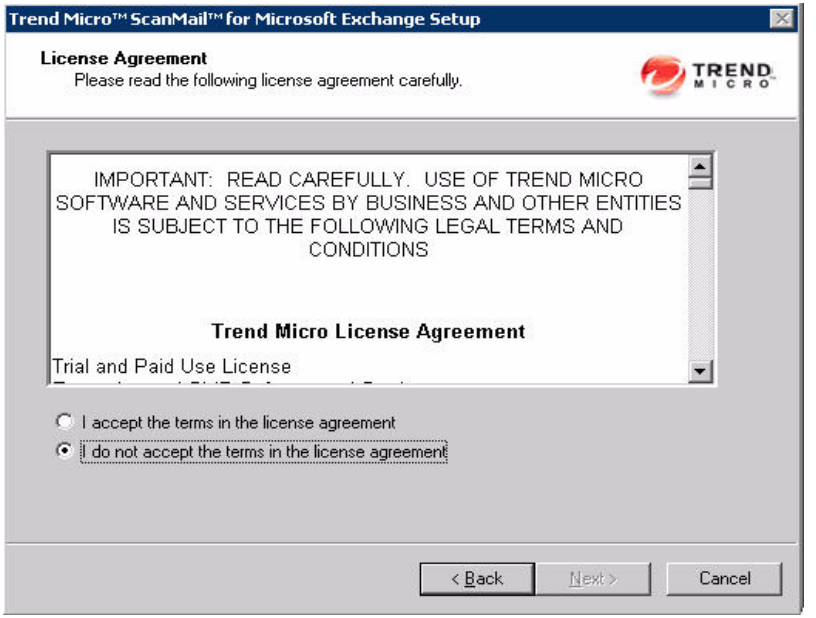


FIGURE 2-2. License Agreement screen

4. Select an action.
   a. Select **Install/Upgrade** to:
      - Perform a fresh install
      - Upgrade a previous ScanMail version. For more information about upgrading, see Upgrading to ScanMail 10.0 on page 1-35.
   b. Click **Next** to continue. The Server Version Selection screen appears.

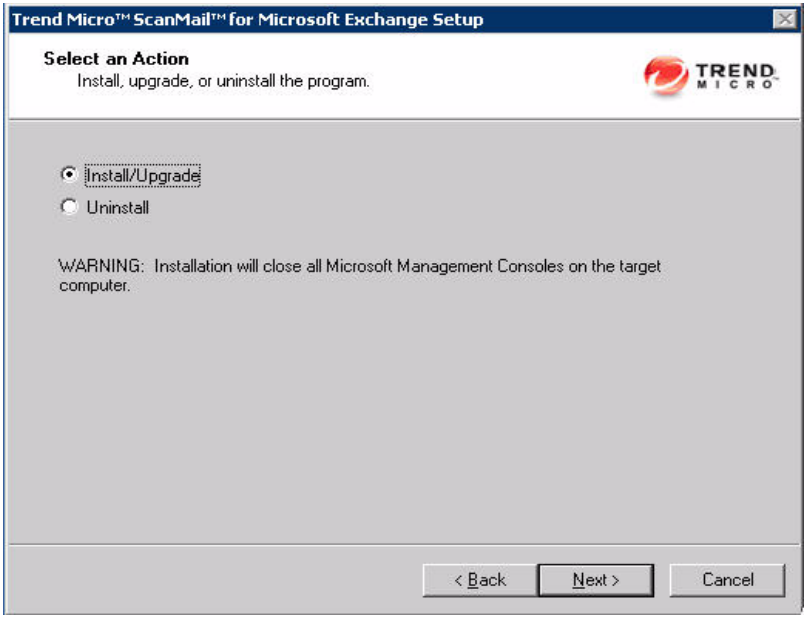


FIGURE 2-3. Select an installation action screen

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.

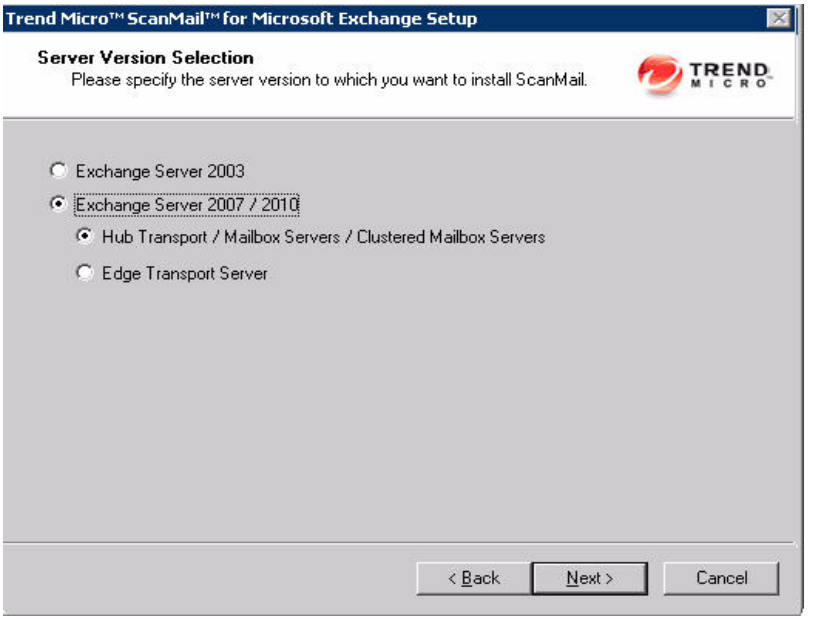


FIGURE 2-4. Server Version Selection screen

6. Select the computers to which you want to install ScanMail
   a. Perform 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, then double-click the domain or computers you want to add to the list.
      - 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.

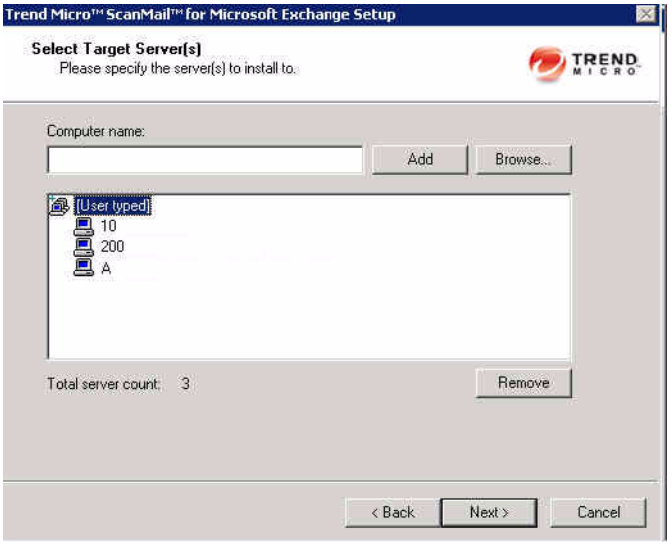


FIGURE 2-5. Select Target Server(s) screen

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. This version of ScanMail supports IPv6.

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.

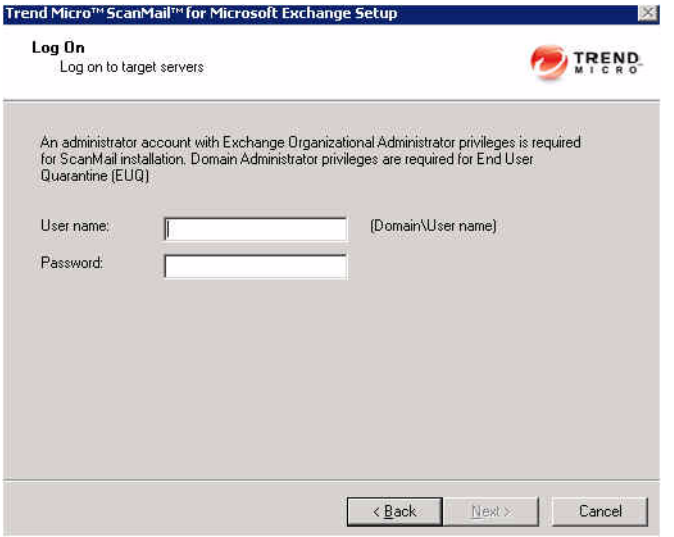


FIGURE 2-6. Log On screen

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 to where you will install ScanMail on the target server. Click **Next** to continue. The Web Server Information screen appears.

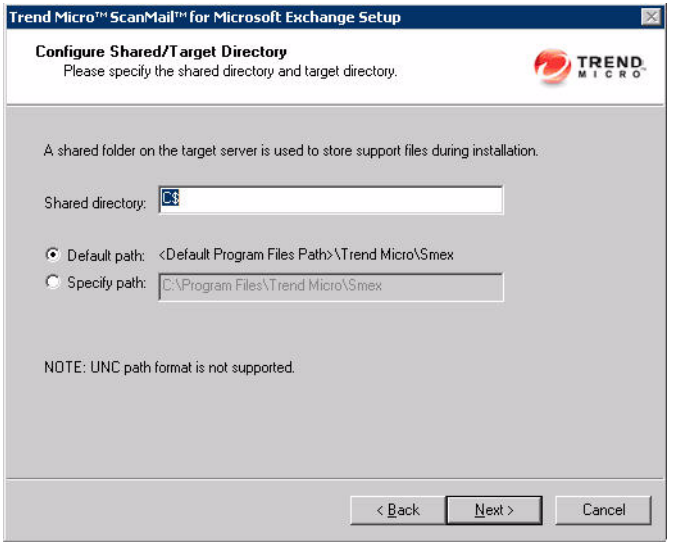


FIGURE 2-7. Configure Shared / Target Directory

9. Select **IIS Default Web Site** or **IIS Virtual Web Site**. 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 Checking Target Server System Requirements screen appears.

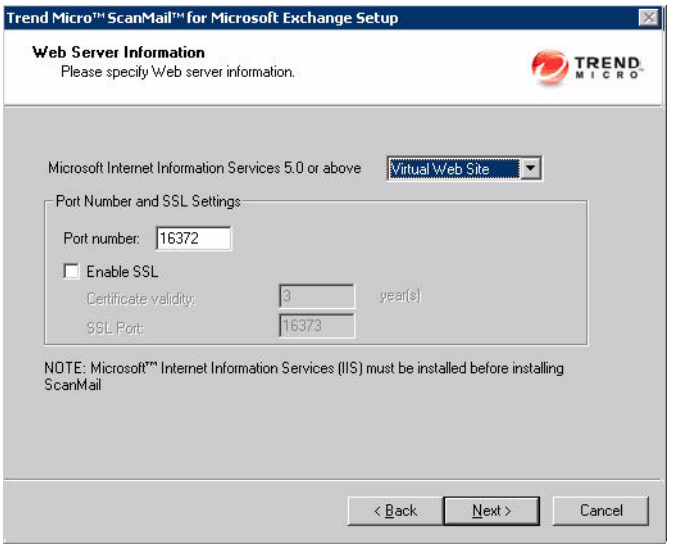


FIGURE 2-8. Select Web Server Type screen

10. Review the settings and click **Next** to continue. The Connection Settings screen appears.

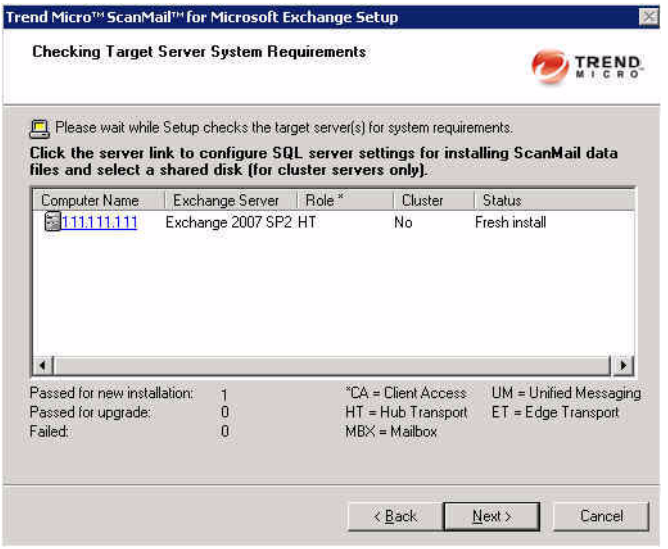


FIGURE 2-9. Checking Target Server System Requirements screen

a. If this is an SCC or VERITAS cluster, click the virtual server to configure the data files path. To install ScanMail on a remote SQL server, click the server on which to configure remote SQL server settings.

b. Click the computer name and refer to one of the following:

- **For SCC and VERITAS clusters**: Specify the shared disk for ScanMail to store data files. Then, specify SQL settings. Select **Install SQL server 2005 express** to install SQL server 2005 express on the local computer. Select **Specify an existing SQL server** to use an existing separate database server.

Note: Using a centralized SQL server for ScanMail data storage increases the risk of a single point of failure and reduction in performance. Ensure that steps are taken for a high availability remote SQL server.

---

c. Click **OK**. The Checking SQL Server Database screen appears.

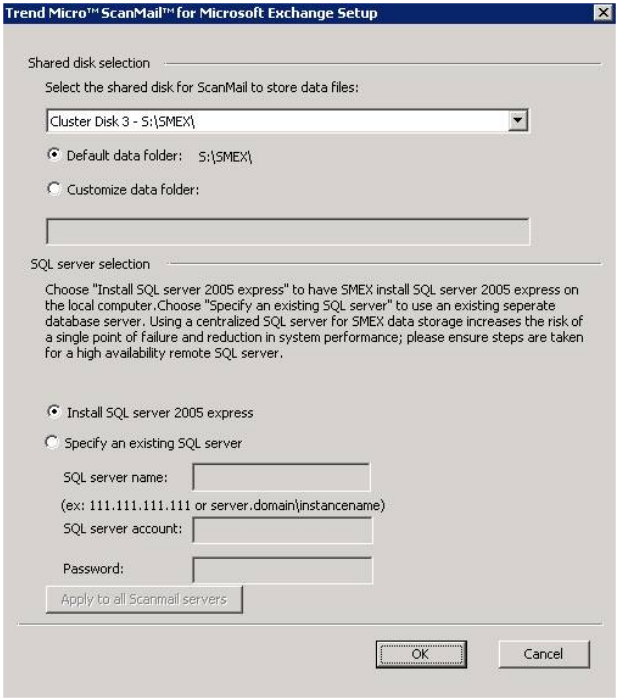


FIGURE 2-10. Shared disk configuration and SQL server selection screen

- **For CCR clusters and single servers**: Select one of the following:
  - Select **Install SQL server 2005 express** to install an SQL server on the local computer.
  - Otherwise, select **Specify an existing SQL server** to use an existing database server. Type the SQL server name, SQL server account, and password.

Note: Using a centralized SQL server for ScanMail data storage increases the risk of a single point of failure and reduction in performance. Ensure that steps are taken for a high availability remote SQL server.

a. Click **OK**. The Checking SQL Server Database screen appears.

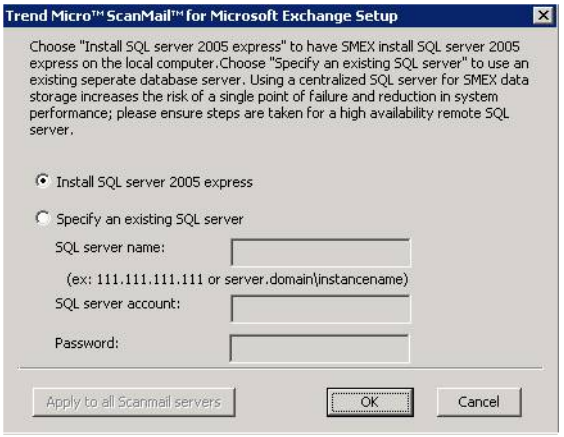


FIGURE 2-11. SQL Settings screen

b. Check that the user name and password are correct. Click **Next**, the Connection Settings screen appears.

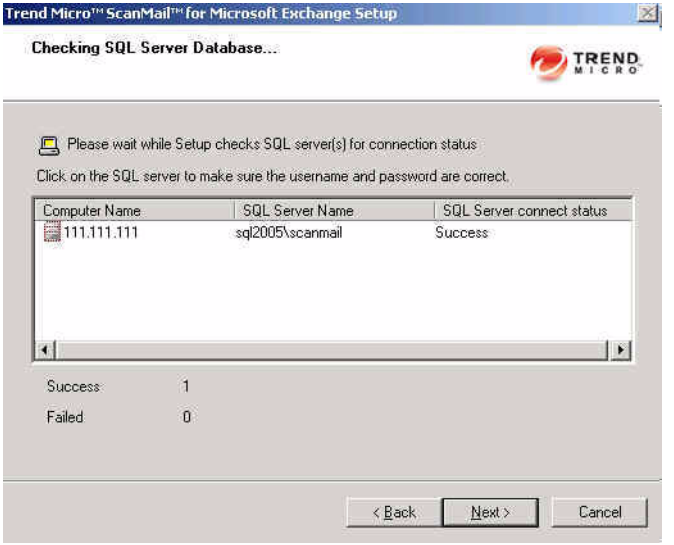


FIGURE 2-12. Check SQL Server Database

11. If a proxy server handles Internet traffic on your network, select **Use a proxy server to connect to Internet** and then type the proxy hostname or address and port number that your proxy uses. By default, the proxy server is disabled. If you want to use SOCKS 5 for secure communication behind the proxy, select **Use SOCKS 5**. If your proxy requires authentication, type the user name and password used for authentication. Click **Next** to continue. The Product Activation screen appears.

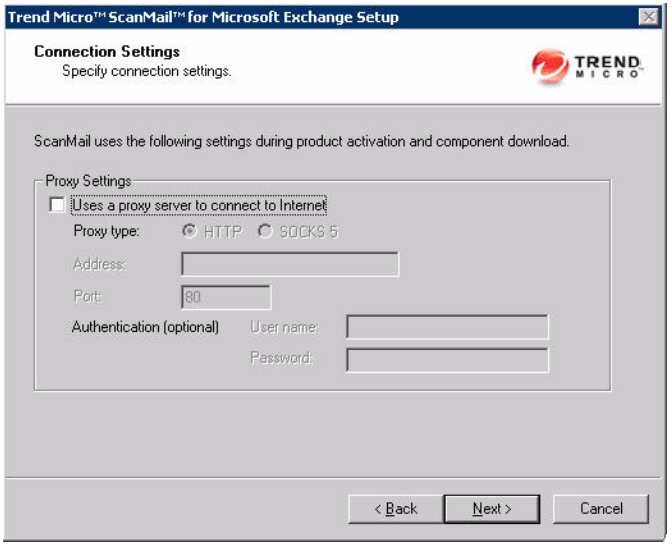


FIGURE 2-13. Connection Settings screen

12. In the **Product Activation** screen, type the activation code. Click **Next** to continue. The World Virus Tracking Program screen appears.

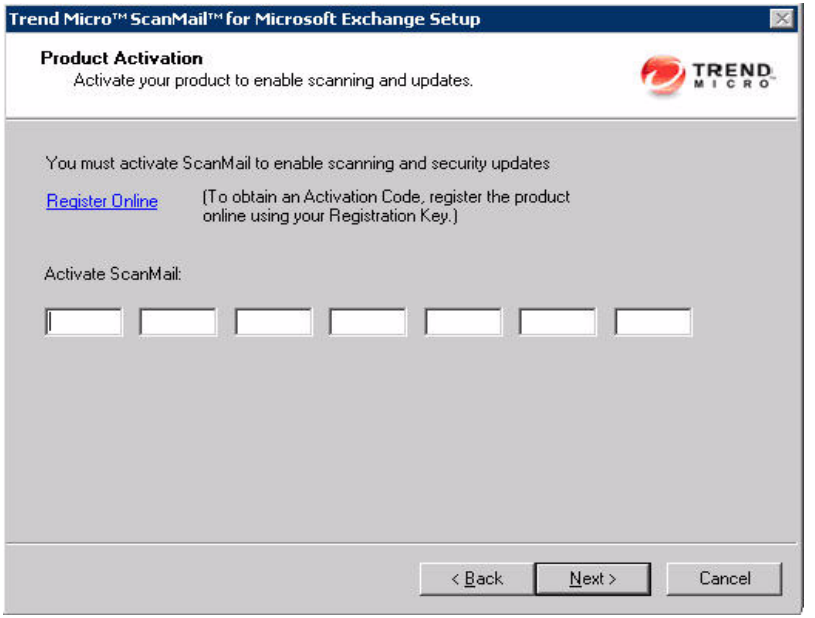


FIGURE 2-14. Product Activation screen

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.

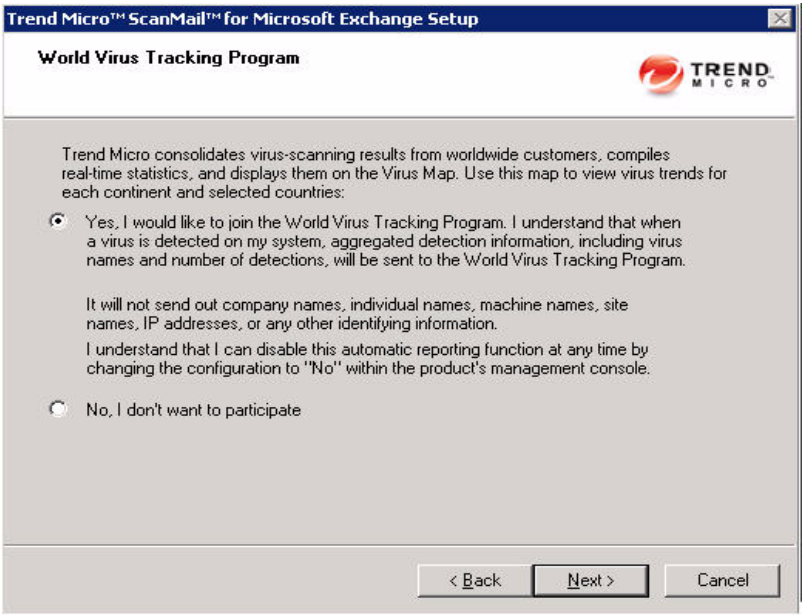


FIGURE 2-15. World Virus Tracking Program screen

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 **Integrate with End User Quarantine** 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.

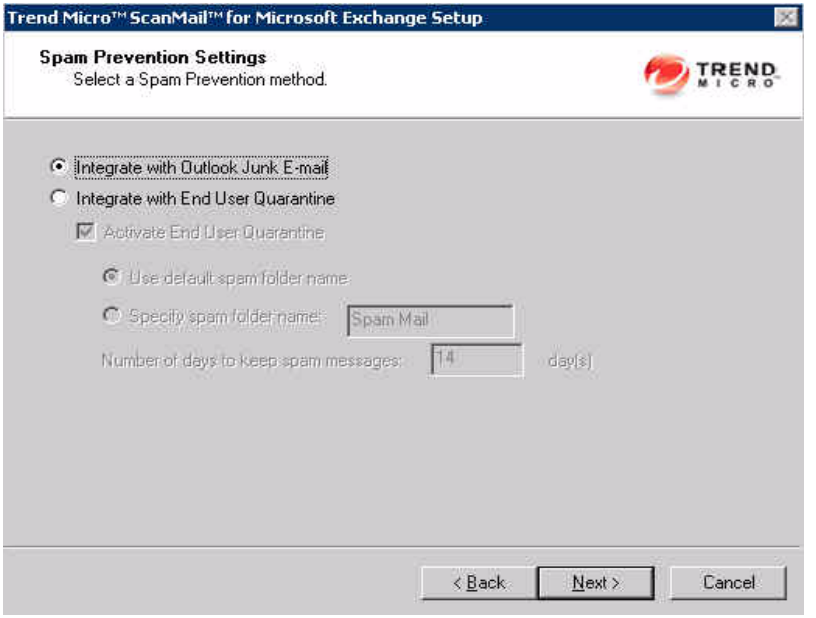


FIGURE 2-16. End User Quarantine Settings screen

Note: End User Quarantine (EUQ) is not supported with Microsoft Outlook on Exchange Mailbox Server or Combo Server roles for Exchange Server 2010 or 2007.

15. 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.

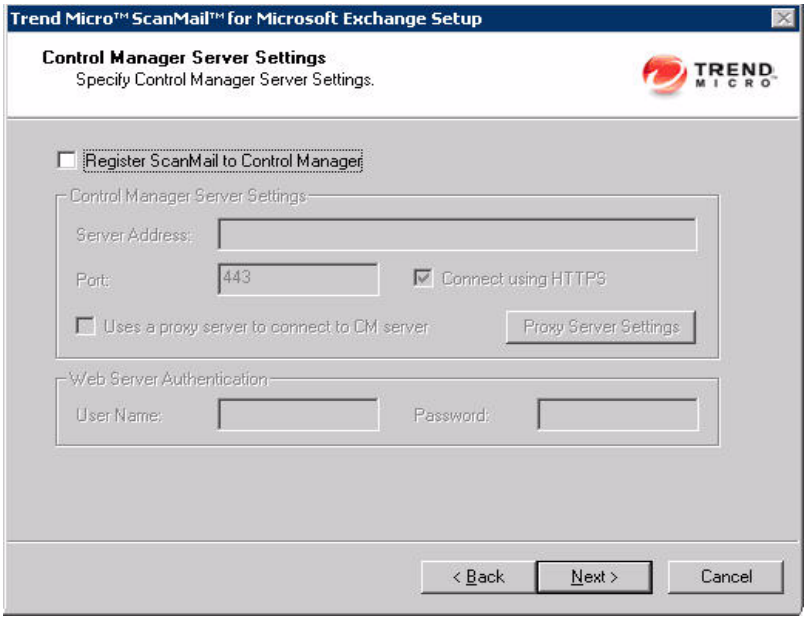


FIGURE 2-17. Control Manager Server Settings screen

16. 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.

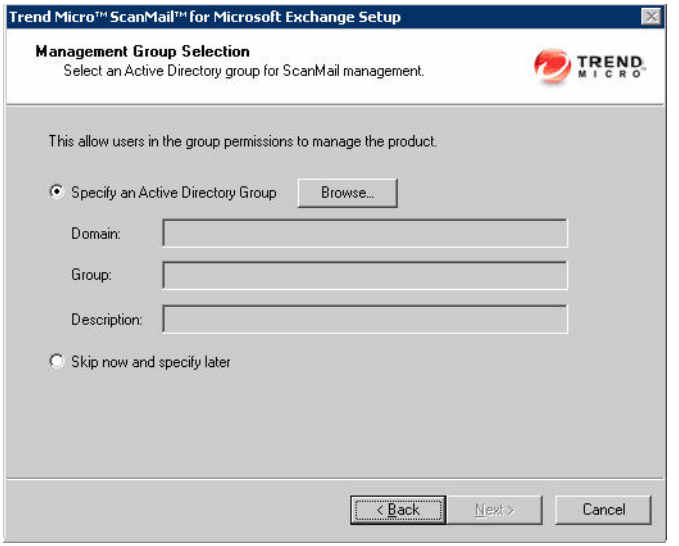


FIGURE 2-18. Management Group Selection screen

17. Review your settings and select the **Update pattern files when installation is complete** check box if you want to update pattern files immediately after installation. Click **Next** to continue. The Installation Progress screen appears.

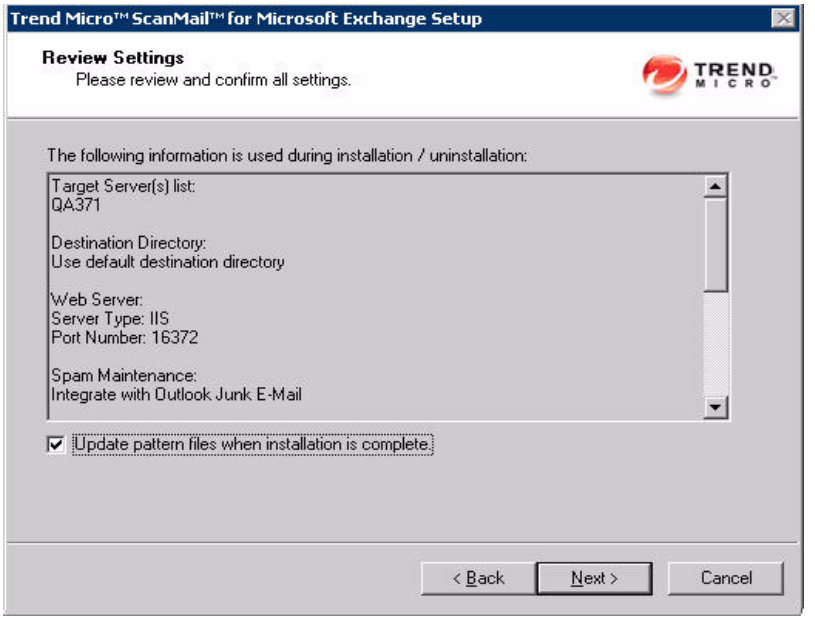


FIGURE 2-19. Review Settings screen

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 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.

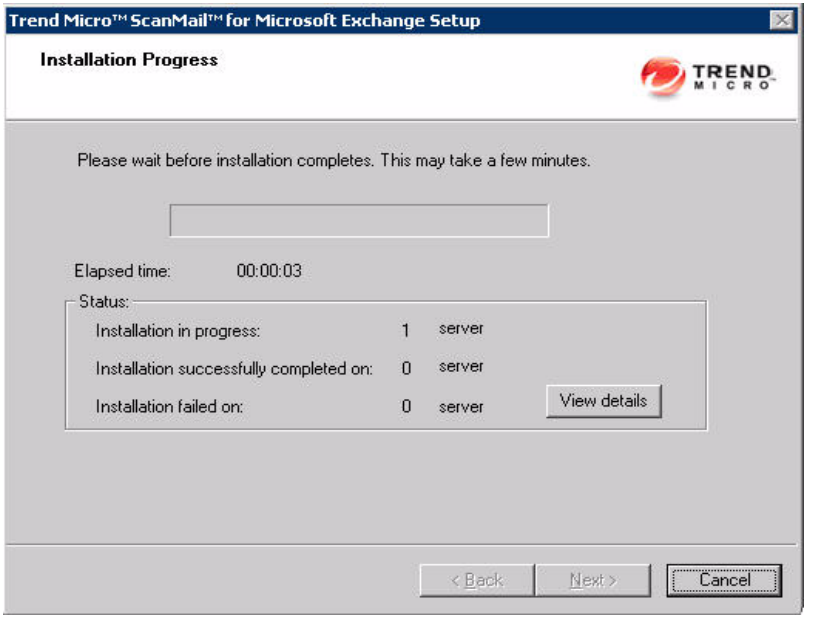


FIGURE 2-20. Installation Progress screen

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

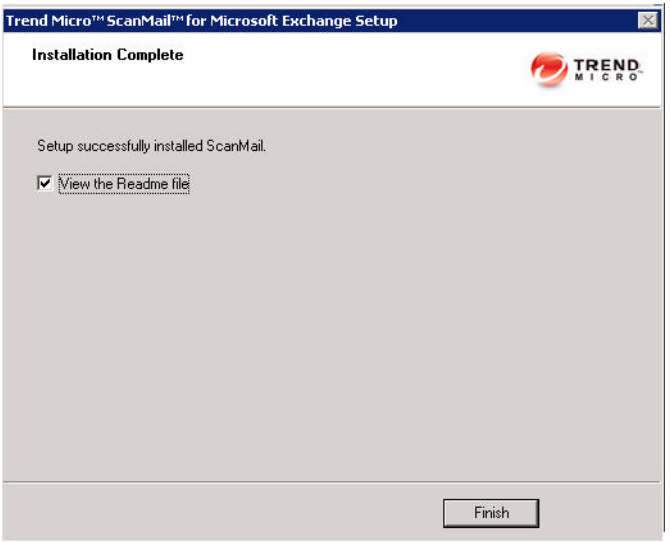


FIGURE 2-21. Installation Complete screen

Chapter 3

Installing ScanMail with Exchange 2010/2007 Edge Transport Servers

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

Topics in this chapter:

- *Running the Setup Program* on page 3-2
- *Installation with Edge Transport Servers* on page 3-2

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 with Edge Transport Servers

The following lists the steps to install ScanMail with Exchange Server 2010 or 2007 Edge Transport server roles.

To install ScanMail:

1. Select a source for the Setup program:

   Trend Micro Web site.

   a. Download ScanMail from the Trend Micro Web site.

   b. Unzip the file to a temporary directory

   c. Run setup.exe to install ScanMail

   The Trend Micro Enterprise Solution DVD.

   a. Insert the DVD 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.

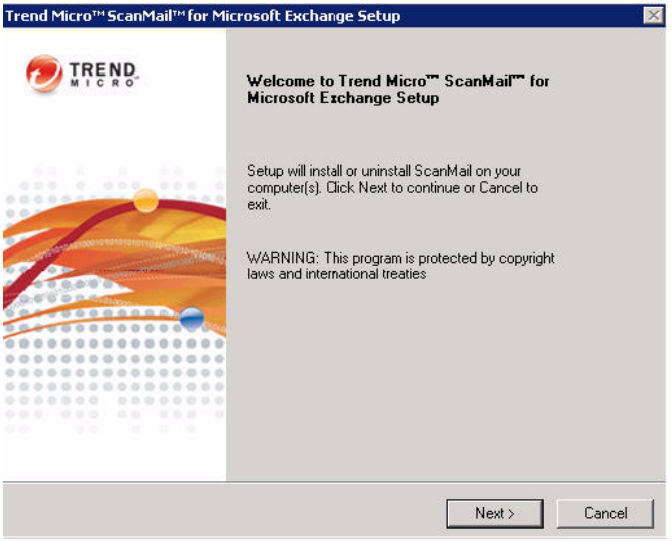


FIGURE 3-1. Welcome screen

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 installation without modifying your operating system.

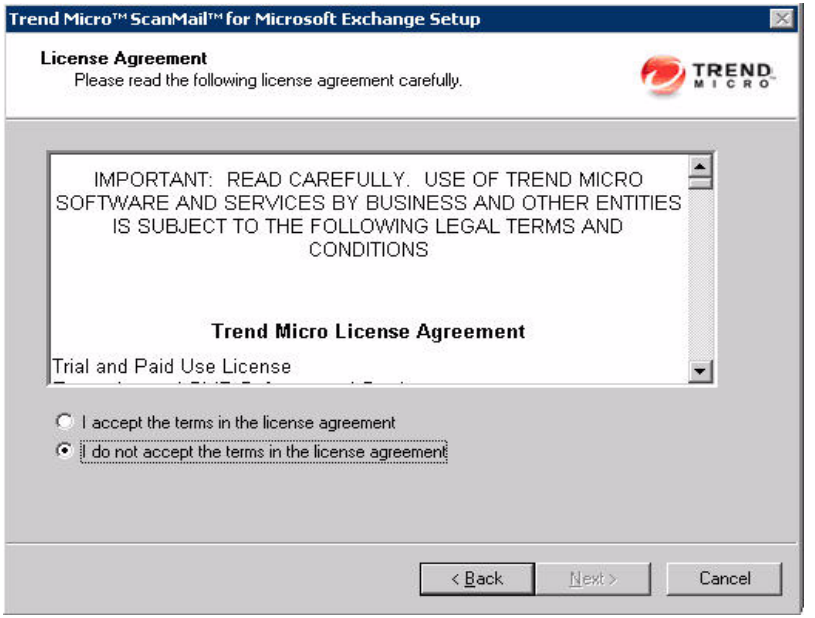


FIGURE 3-2. License Agreement screen

4. Select an action.
   a. Select **Install/Upgrade** to:
      - Perform a fresh install
      - Upgrade a previous ScanMail version. For more information about upgrading, see Upgrading to ScanMail 10.0 on page 1-35.
   b. Click **Next** to continue. The Server Version Selection screen appears.

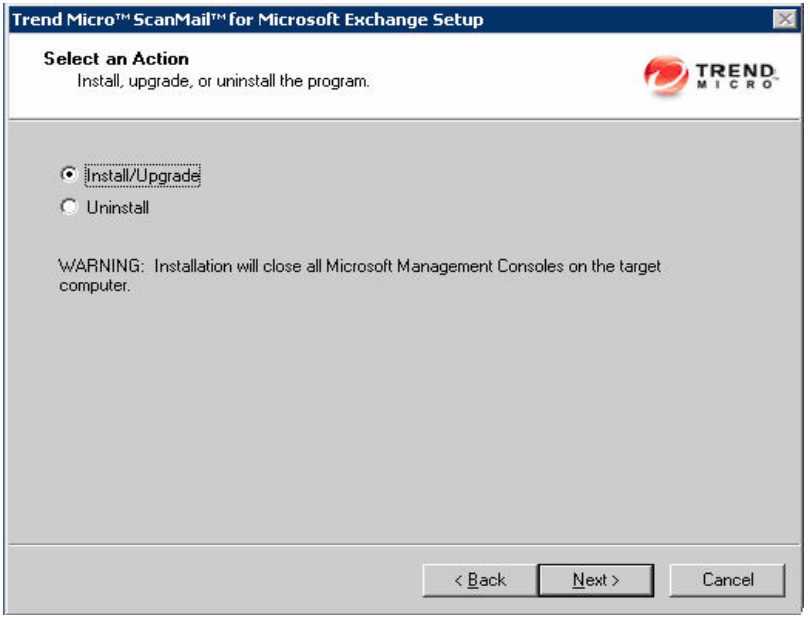


FIGURE 3-3. Select an installation action screen

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.

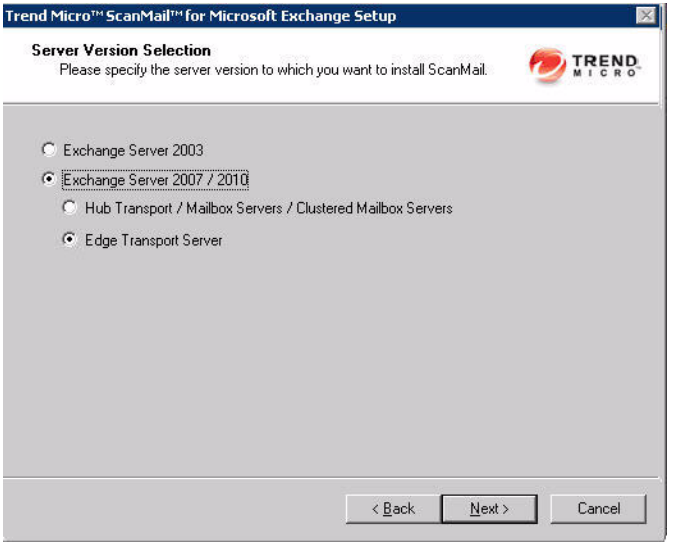


FIGURE 3-4. Server Version Selection screen

6. Select the computers to which you want to install ScanMail
   a. Perform 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, then double-click the domain or computers you want to add to the list.
      - 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.

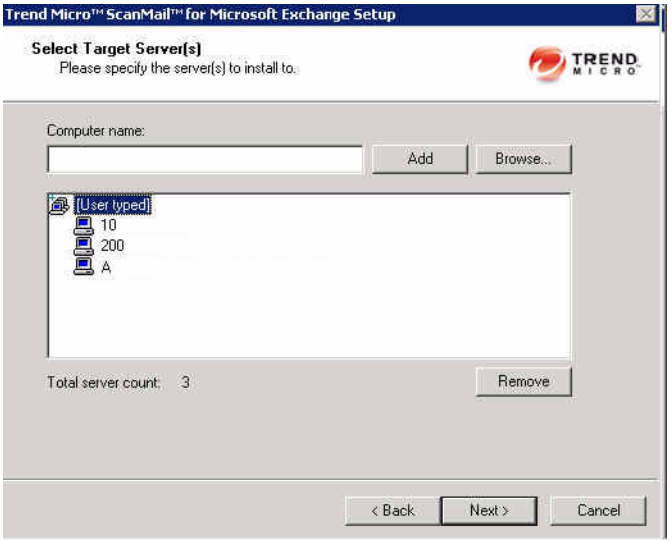


FIGURE 3-5. Select Target Server(s)

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.

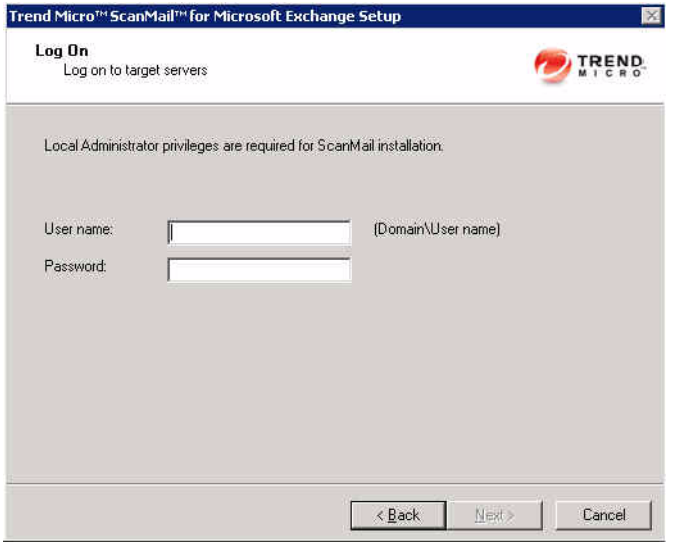


FIGURE 3-6. Log On screen

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 to where you will install ScanMail on the target server. Click **Next** to continue. The Select Web Server Type screen appears.

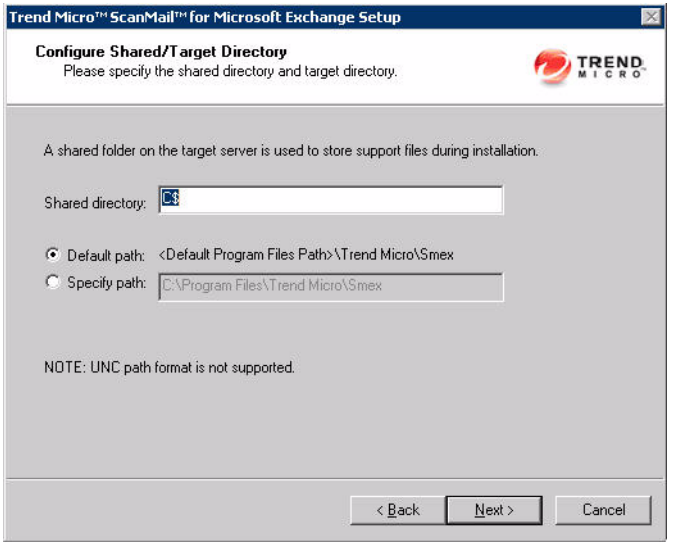


FIGURE 3-7. Configure Shared / Target Directory

9. Select **IIS Default Web Site** or **IIS Virtual Web Site**. 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 Checking Target Server System Requirements screen appears.

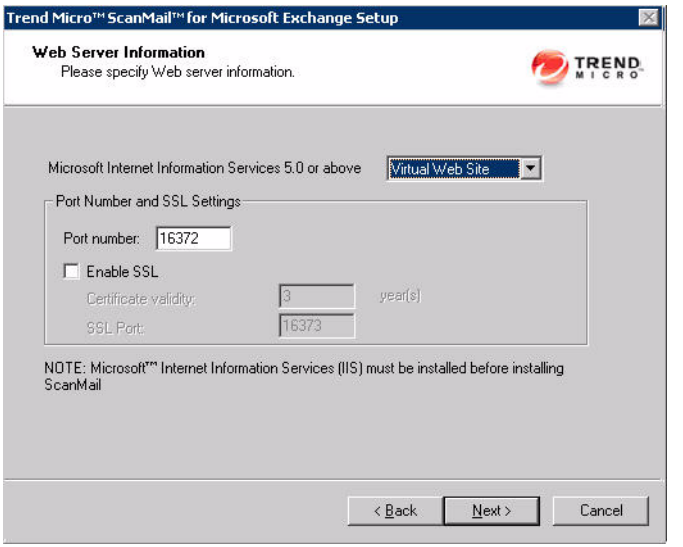


FIGURE 3-8. Select Web Server Type screen

10. Review the settings and click **Next** to continue. The Connection Settings screen appears.

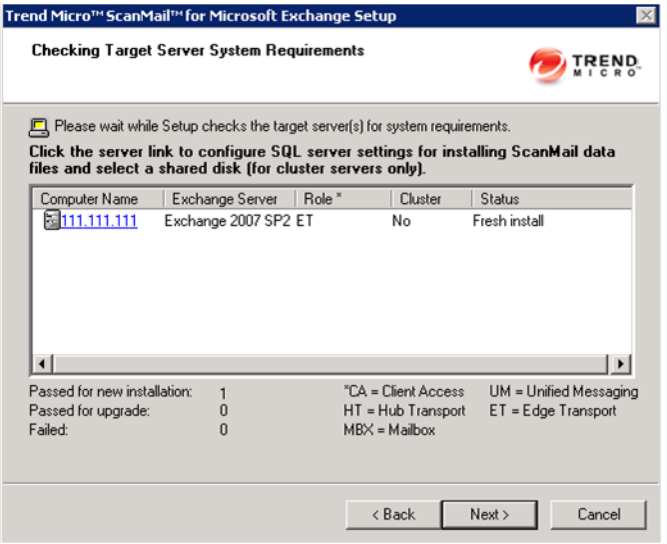


FIGURE 3-9. Checking Target Server System Requirements screen

a. To install ScanMail on a remote SQL server, double-click the virtual server on which to install ScanMail data files. The SQL Server Selection screen appears.

b. Select one of the following:

- Select **Install SQL server 2005 express** to install an SQL server on the local computer.
- Otherwise, select **Specify an existing SQL server** to use an existing database server. Type the SQL server name, SQL server account, and password.

Note: Using a centralized SQL server for ScanMail data storage increases the risk of a single point of failure and reduction in performance. Ensure that steps are taken for a high availability remote SQL server.

c. Click **OK**. The Checking SQL Server Database screen appears.

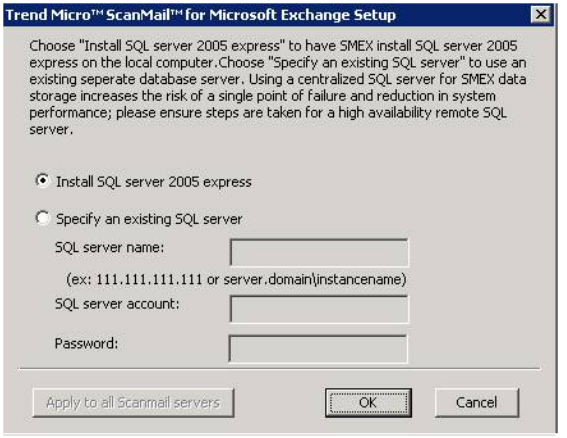


FIGURE 3-10.SQL Settings screen

d. Check that the user name and password are correct. Click **Next**, the Connection Settings screen appears.

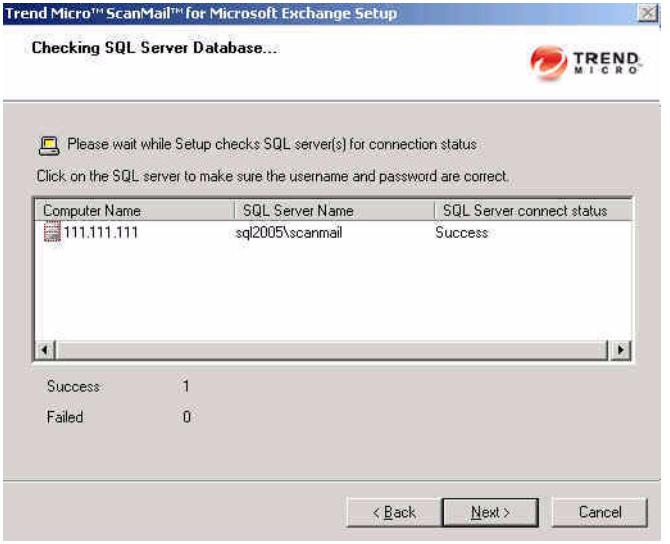


FIGURE 3-11. Checking SQL Server Database

11. If a proxy server handles Internet traffic on your network, select **Use a proxy server to connect to Internet** and then type the proxy hostname or address and port number that your proxy uses. By default, the proxy server is disabled. If you want to use SOCKS 5 for secure communication behind the proxy, select **Use SOCKS 5**. If your proxy requires authentication, type the user name and password used for authentication. Click **Next** to continue. The Product Activation screen appears.

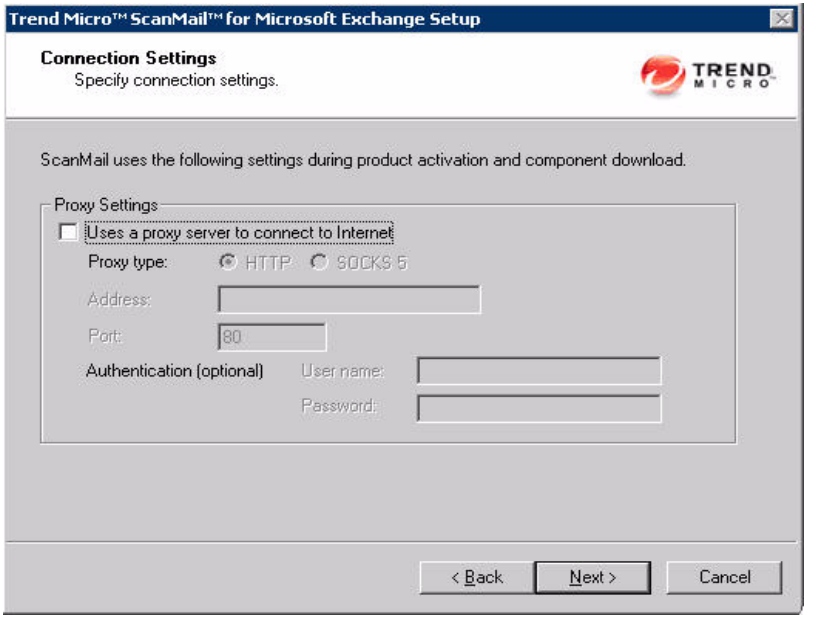


FIGURE 3-12. Connection Settings screen

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.

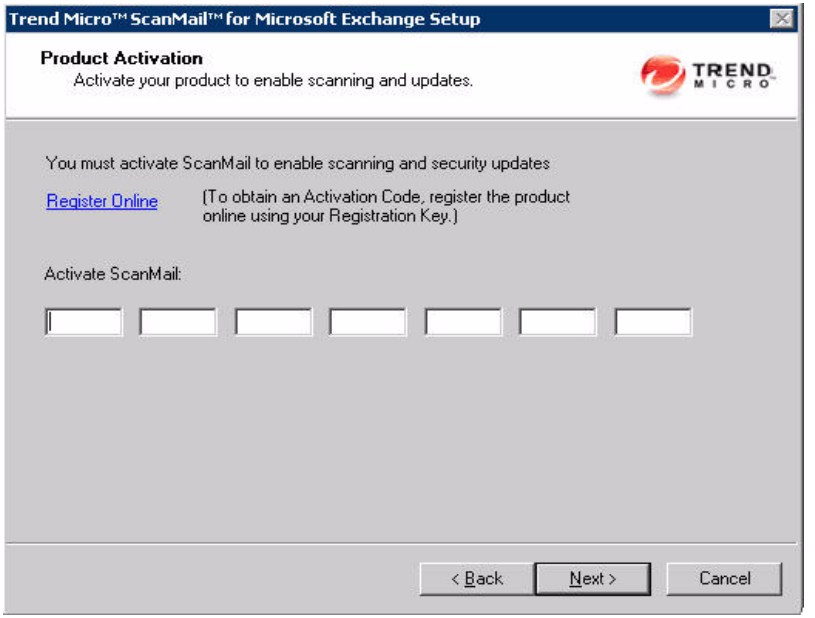


FIGURE 3-13. Product Activation screen

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 End User Quarantine Settings screen appears.

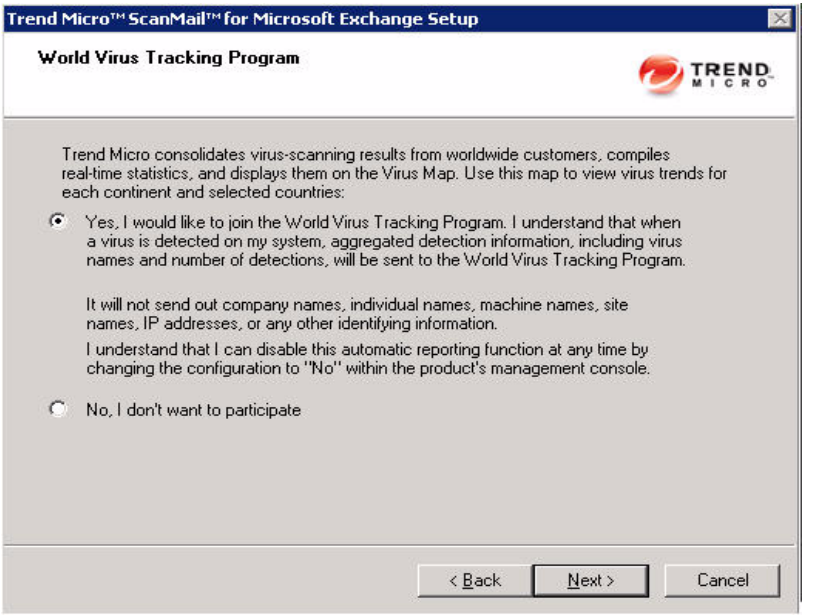


FIGURE 3-14. World Virus Tracking Program screen

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 **Integrate with End User Quarantine** 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.

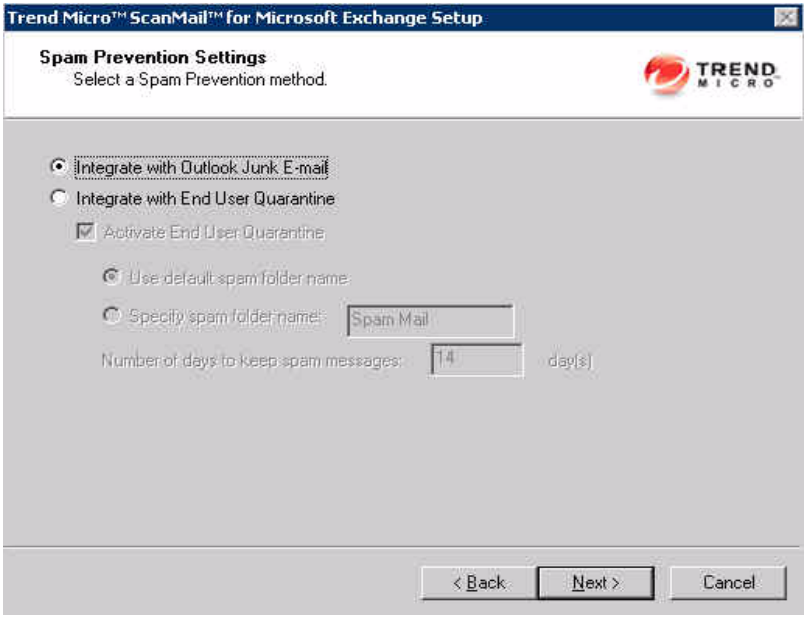


FIGURE 3-15. End User Quarantine Settings screen

15. 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.

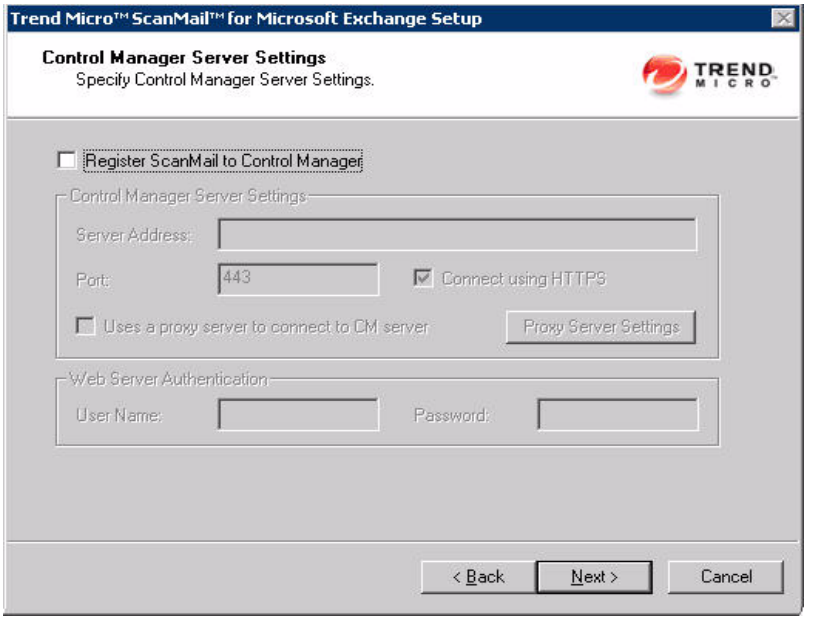


FIGURE 3-16. Control Manager Server Settings screen

16. Review your settings and select the **Update pattern files when installation is complete** check box if you want to update pattern files immediately after installation. Click **Next** to continue. The Installation Progress screen appears.

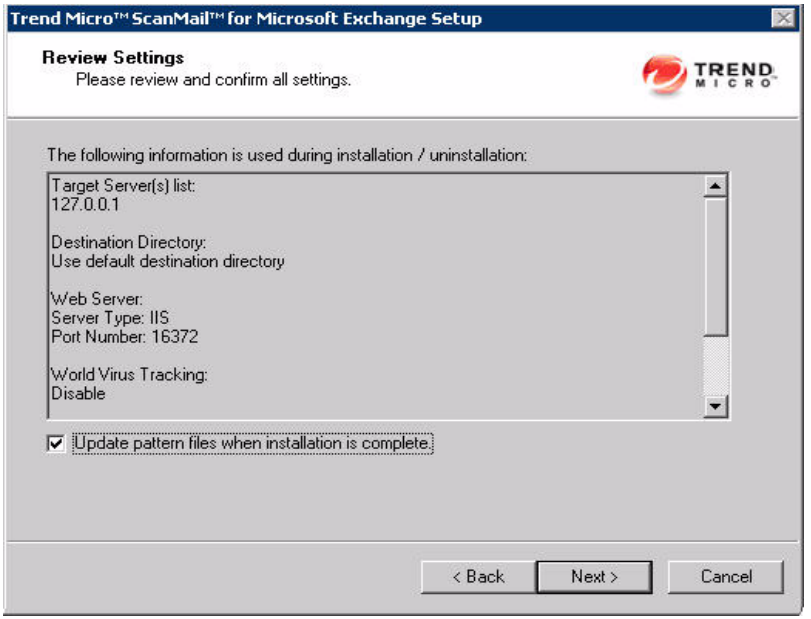


FIGURE 3-17. Review Settings screen

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 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.

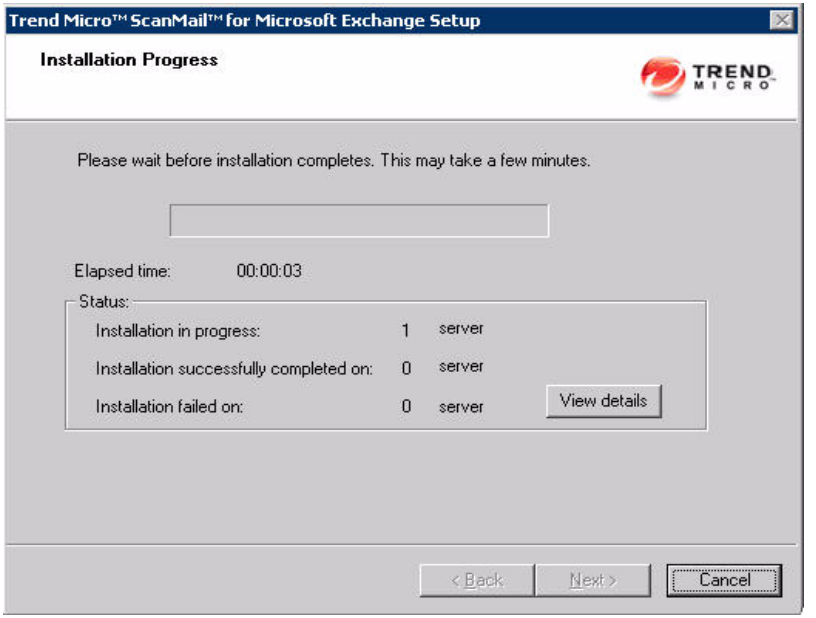


FIGURE 3-18. Installation Progress screen

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

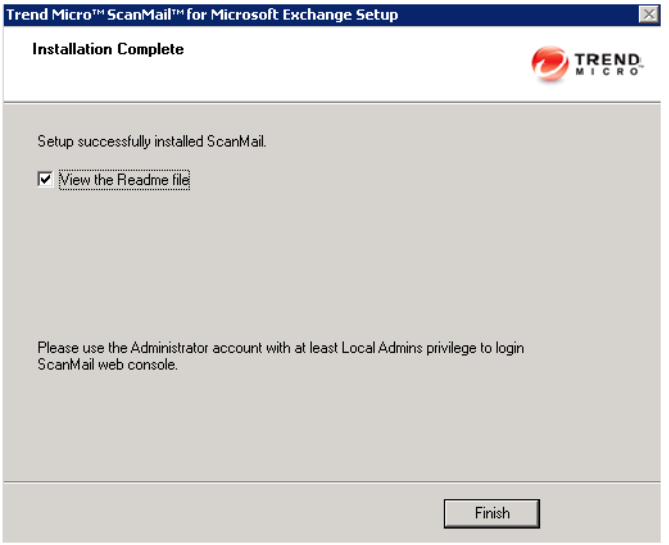


FIGURE 3-19. Installation Complete screen

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

Chapter 4

Installing ScanMail with Exchange Server 2003

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

Topics in this chapter:

- *Running the Setup Program* on page 4-2
- *Installation with Exchange Server 2003* on page 4-2

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 with Exchange Server 2003

The following lists the steps to install ScanMail with Exchange Server 2003.

To install ScanMail with Exchange Server 2003:

1. Select a source for the Setup program:

   Trend Micro Web site.

   a. Download ScanMail from the Trend Micro Web site.

   b. Unzip the file to a temporary directory.

   c. Run setup.exe to install ScanMail.

   The Trend Micro Enterprise Solution DVD.

   a. Insert the DVD 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.

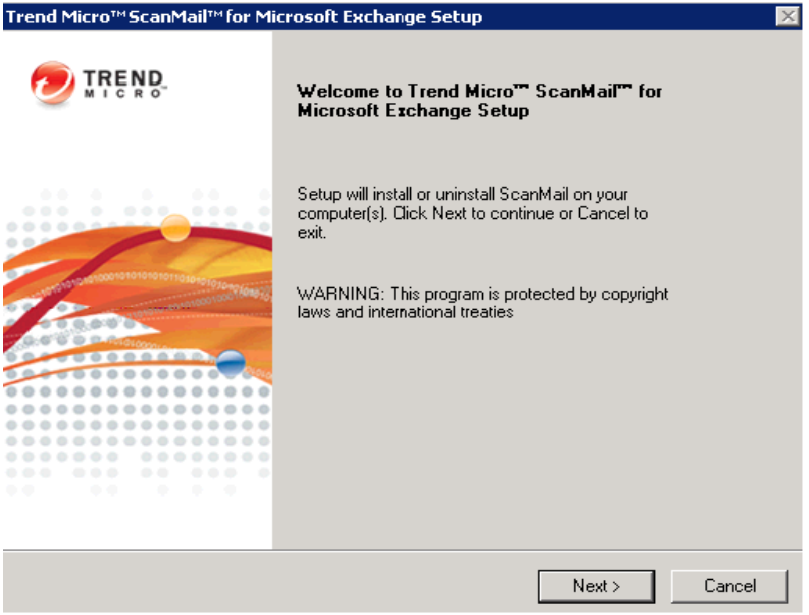


FIGURE 4-1. Welcome screen

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 installation without modifying your operating system.

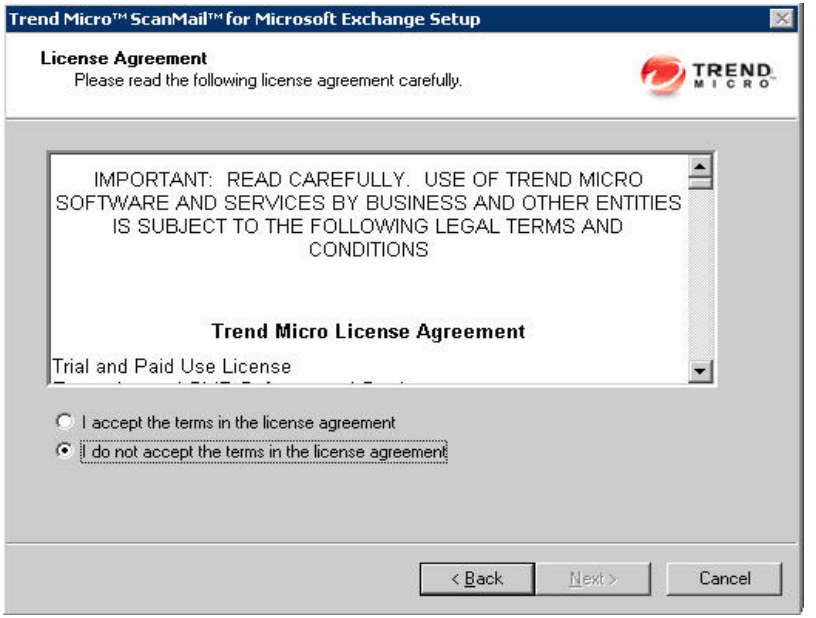


FIGURE 4-2. License Agreement screen

4. Select an action.
   a. Select **Install/Upgrade** to:
      - Perform a fresh install
      - Upgrade a previous ScanMail version. For more information about upgrading, see Upgrading to ScanMail 10.0 on page 1-35.
   b. Click **Next** to continue. The Server Version Selection screen appears.

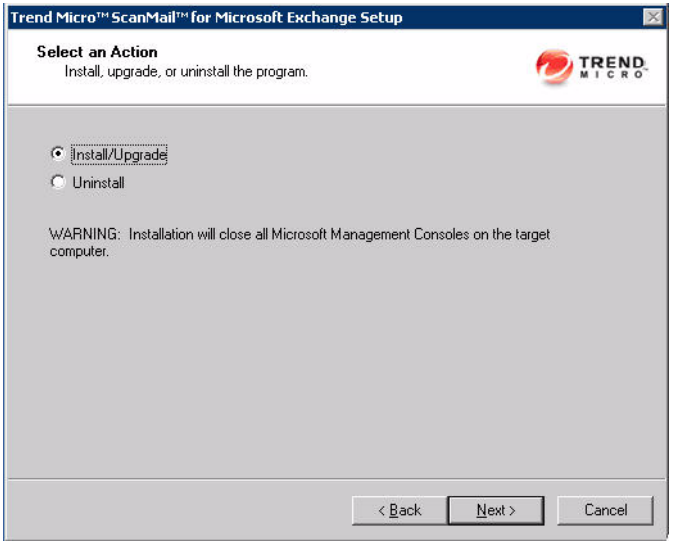


FIGURE 4-3. Select an installation action screen

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

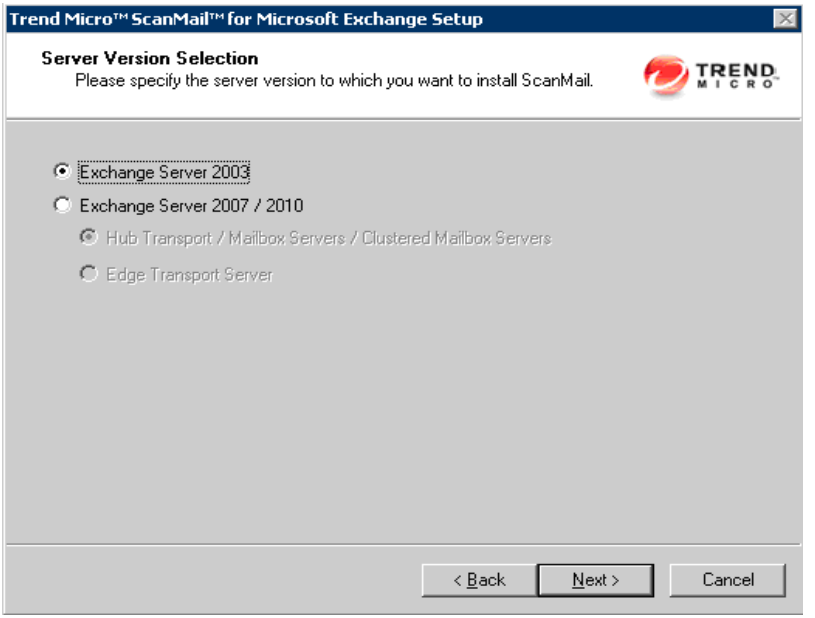


FIGURE 4-4. Server Version Selection for Exchange Server 2003 screen

6. Select the computers to which you want to install ScanMail
   a. Perform 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, then double-click the domain or computers you want to add to the list.
      - 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.

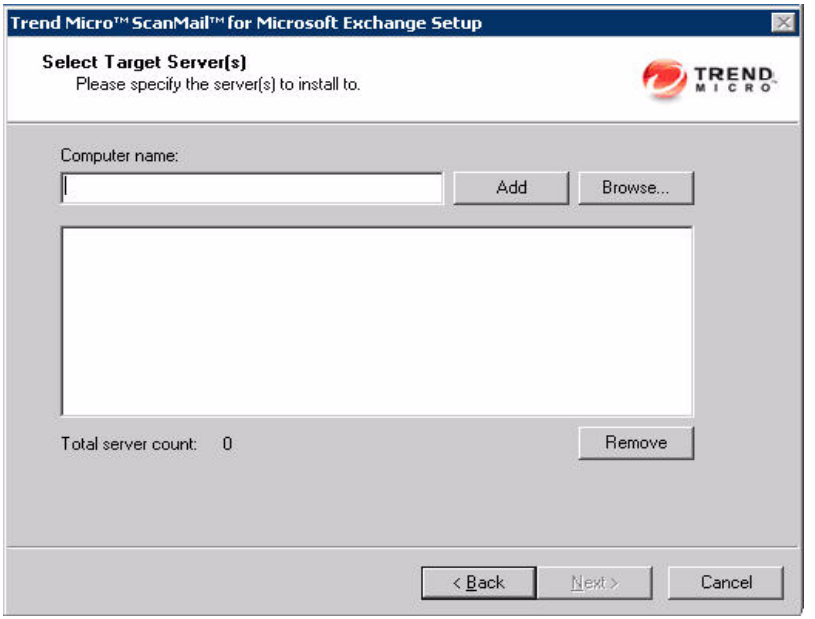


FIGURE 4-5. Select Target Server(s) screen

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.

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.

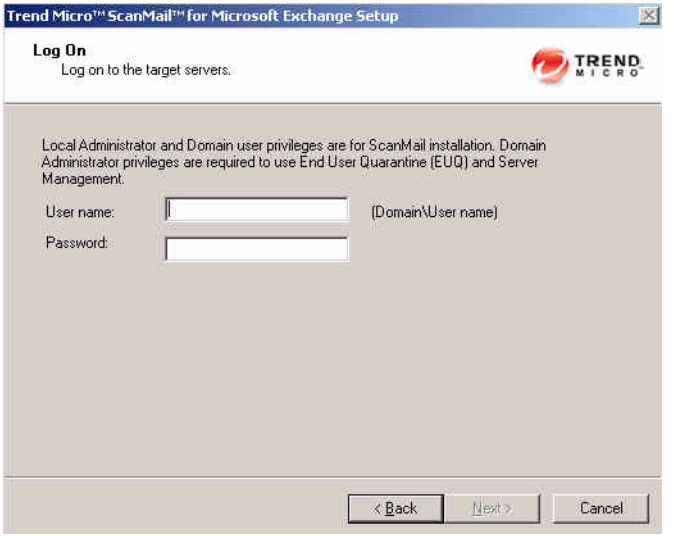


FIGURE 4-6. Log On screen

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 shared directory to copy temporary files during installation and is only accessible to the administrator. Select **Default path** or **Specific path** and type the directory path on the target server where you will install ScanMail. Click **Next** to continue. The Select Web Server Information screen appears.

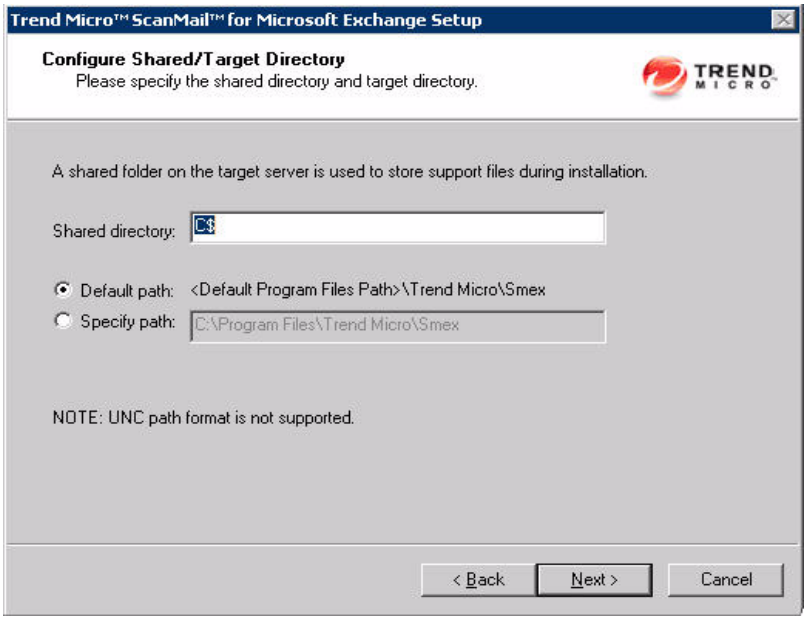


FIGURE 4-7. Configure Shared/Target Directory screen

9. Select **IIS Default Web Site** or **IIS Virtual Web Site**. 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 Checking Target Server System Requirements screen appears.

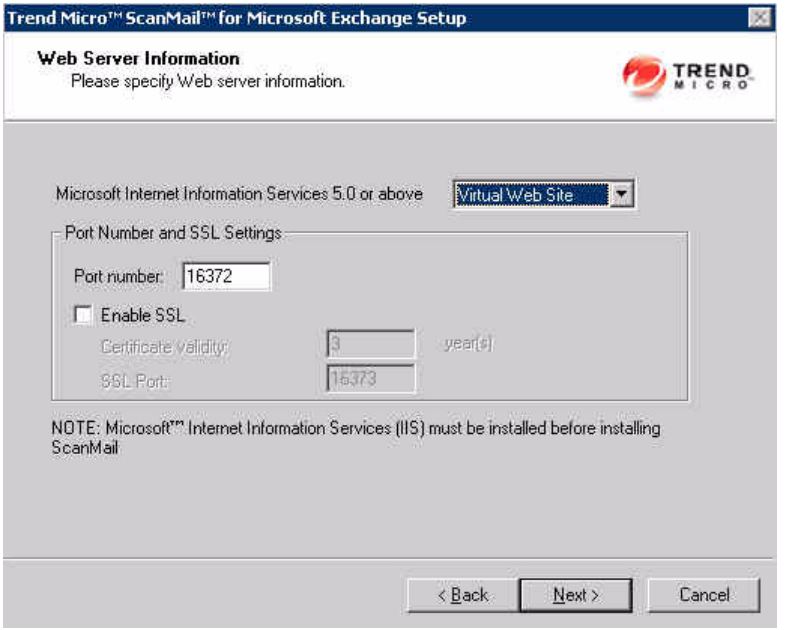


FIGURE 4-8. Select a Web server screen

WARNING! If SSL is used in a cluster environment, SMTP services may stay in pending for an extended period and cause SMTP resources to encounter issues. If using SSL on clusters is necessary, extend the pending time-out of SMTP resources in each Exchange virtual server group.

10. Review the settings and click **Next** to continue. The Connection Settings screen appears.

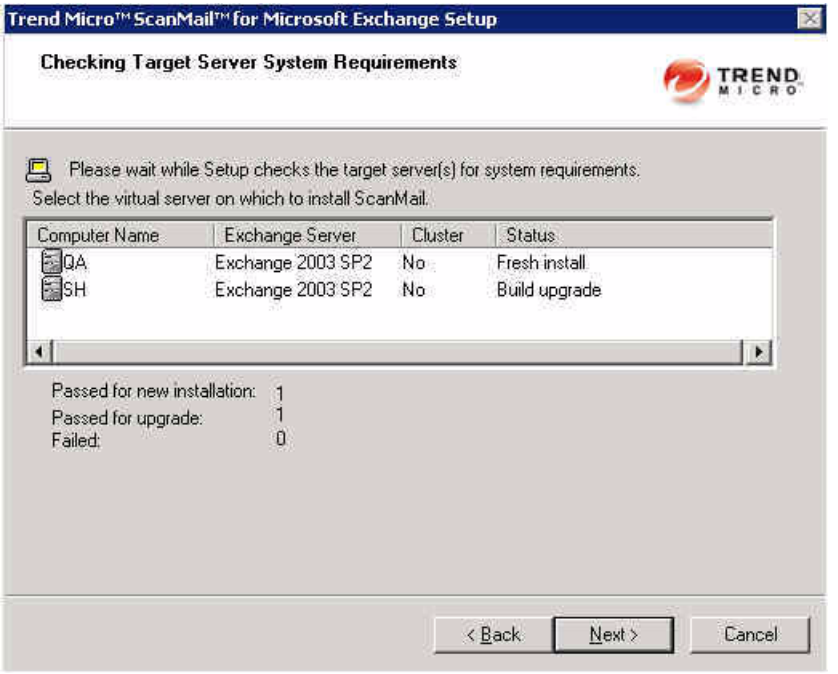


FIGURE 4-9. Checking Target Server System Requirements screen

Note: For cluster servers, double-click the virtual server on which to install ScanMail data files.

11. If a proxy server handles Internet traffic on your network, select **Use a proxy server to connect to Internet** and then type the proxy hostname or address and port number that your proxy uses. By default, the proxy server is disabled. If you want to use SOCKS 5 for secure communication behind the proxy, select **Use SOCKS 5**. If your proxy requires authentication, type the user name and password used for authentication. Click **Next** to continue. The Product Activation screen appears.

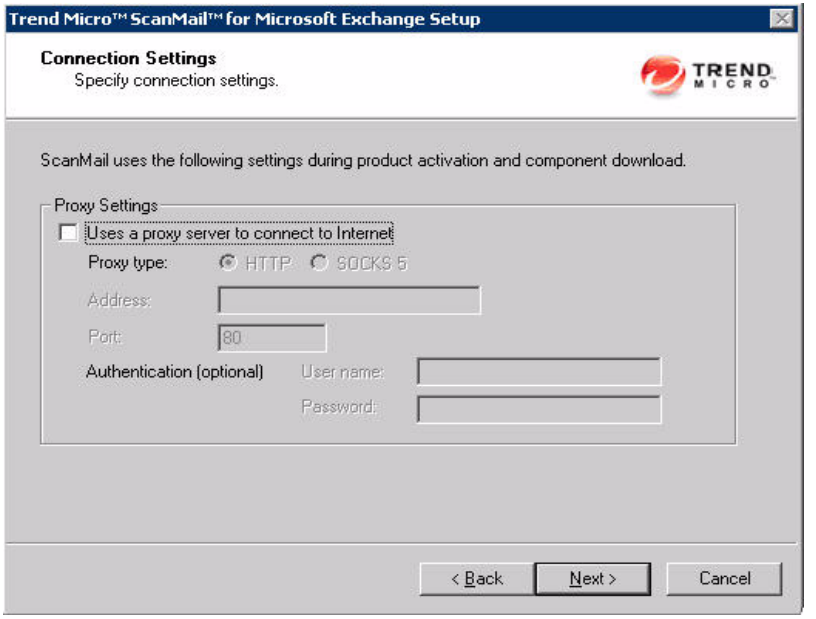


FIGURE 4-10. Connection settings screen

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.

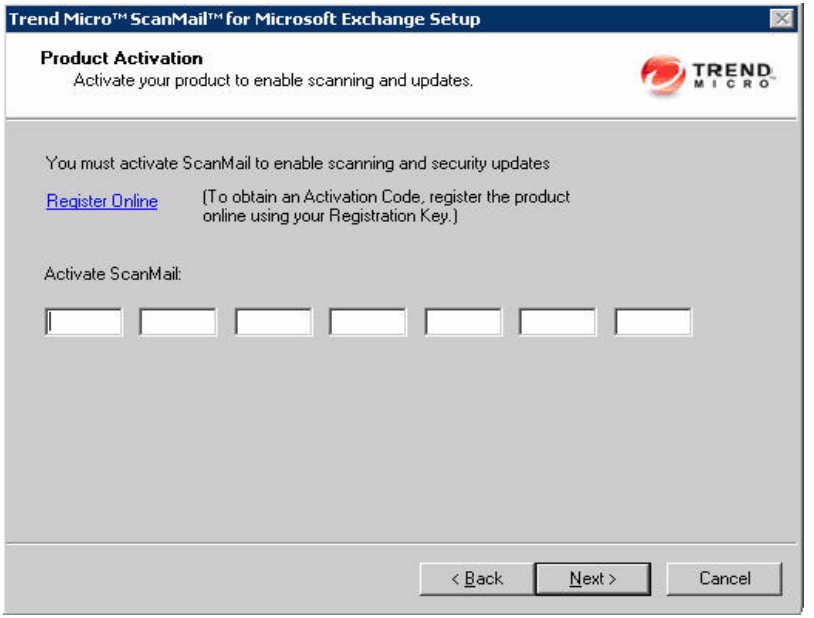


FIGURE 4-11. Product Activation screen

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.

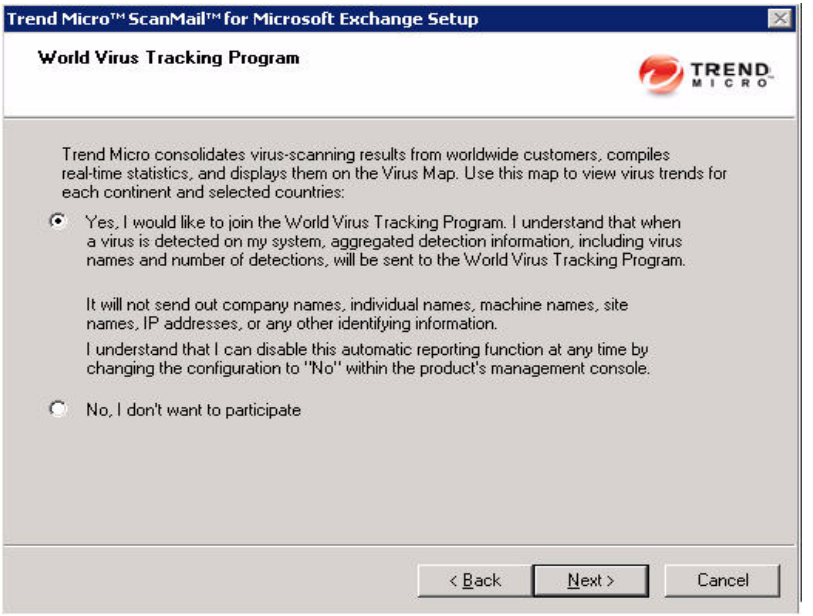


FIGURE 4-12. World Virus Tracking Program screen

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 **Integrate with End User Quarantine** 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.

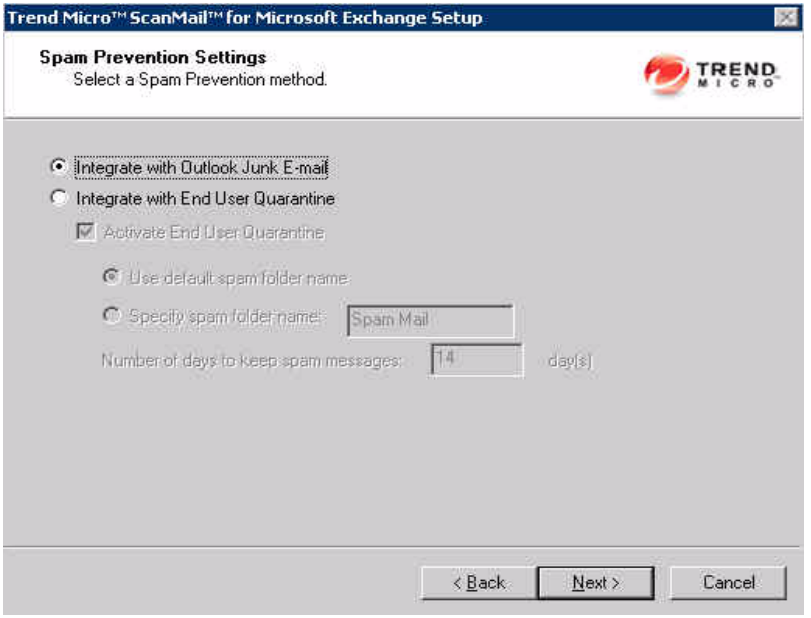


FIGURE 4-13. End User Quarantine Settings screen

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 Product Console Administrator Account screen appears.

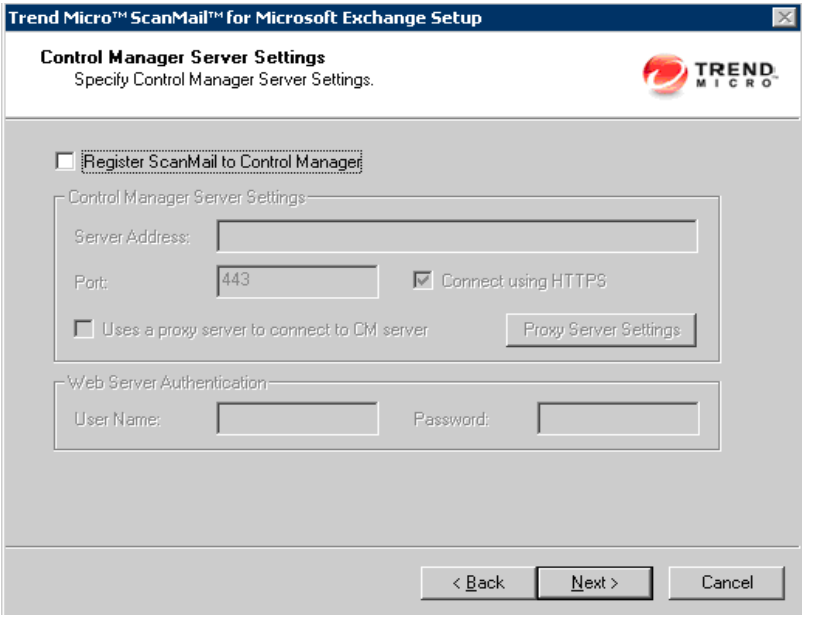


FIGURE 4-14. Control Manager Server Settings screen

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**.

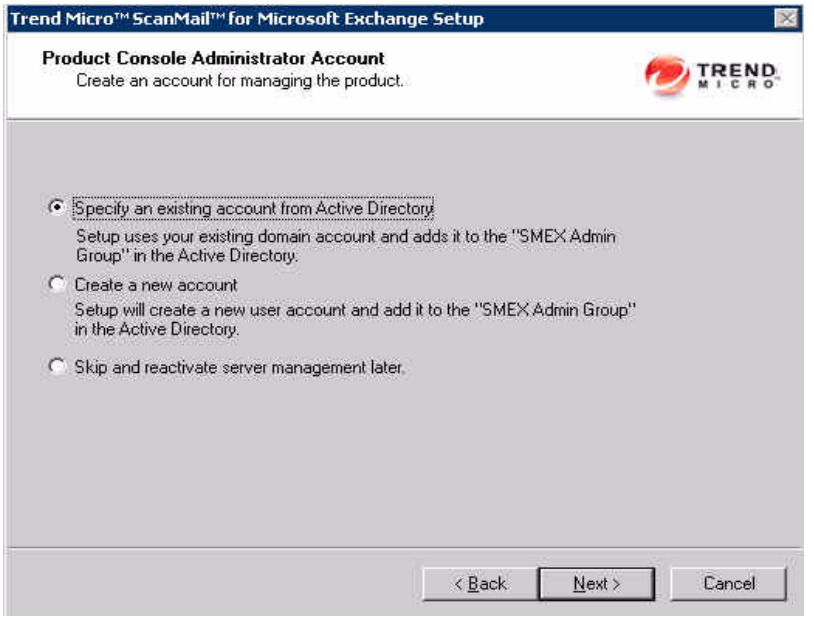


FIGURE 4-15. Product Console Administrator Account screen

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.

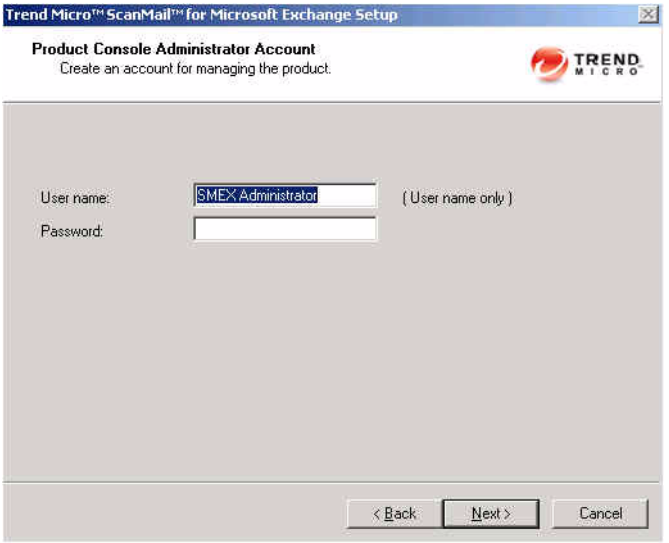


FIGURE 4-16. Product Console Administrator Account screen

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.

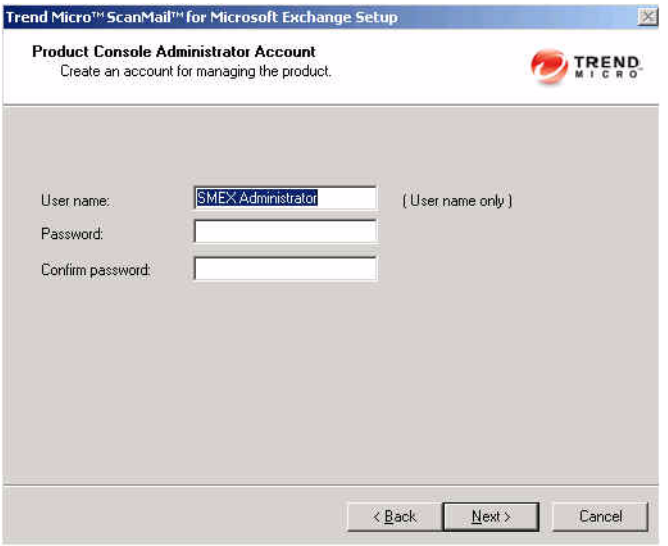


FIGURE 4-17. Product Console Administrator Account screen

- 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 select the **Update pattern files when installation is complete** check box if you want to update pattern files immediately after installation. Click **Next**. The Installation Progress screen appears.

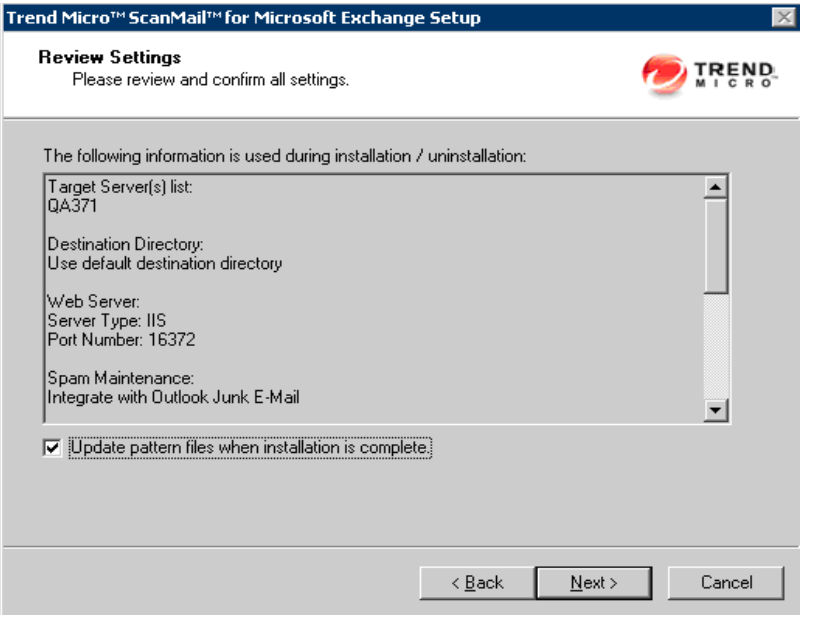


FIGURE 4-18. Review Settings screen

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.

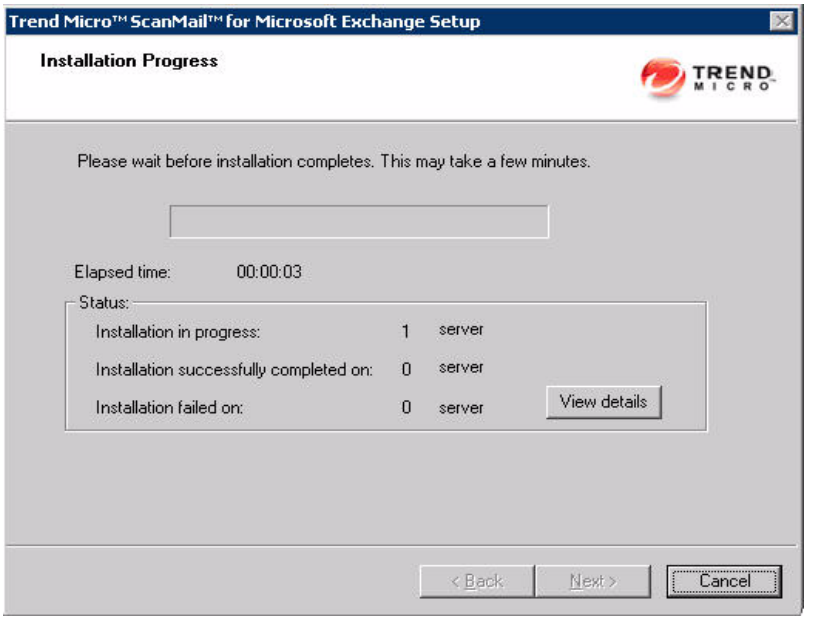


FIGURE 4-19. Installation progress screen

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

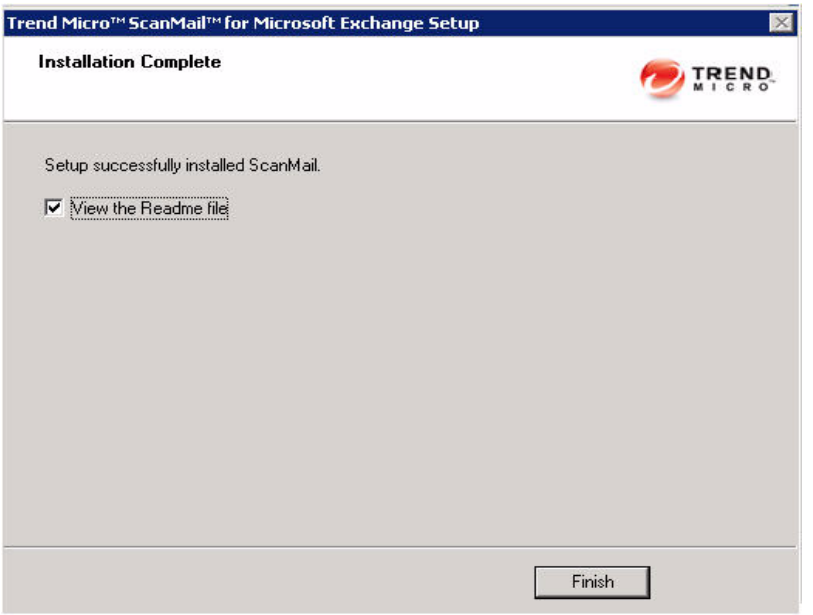


FIGURE 4-20. Installation Complete screen

Chapter 5

Post-Installation Tasks

Perform post-installation tasks to ensure that ScanMail was successfully installed.

Topics in this chapter:

- *Verifying a Successful Installation* on page 5-2
- *Using the ScanMail Management Pack* on page 5-3
- *Testing Your Installation* on page 5-8

Verifying a Successful Installation

Check for ScanMail folders, services, and registry keys to verify a successful installation.

TABLE 5-1. Verifying a successful installation

Installation folder	`C:\Program Files\Trend Micro\SMEX\`
Services	• ScanMail for Microsoft Exchange Master Service • ScanMail EUQ Monitor Service • ScanMail for Microsoft Exchange Remote Configuration Server **Note:** This service is not added to Exchange Server 2010 or 2007 Edge Transport server roles. • ScanMail for Microsoft Exchange System Watcher
Registry keys (All versions)	• HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange
Registry keys • Hub Transport with Mailbox Servers • Mailbox Servers • Exchange Server 2003	• 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 **Note:** These keys are not added to Edge Transport Servers or Hub Transport Servers.

Using the ScanMail Management Pack

Install the ScanMail management package to your operating system. Then import the ScanMail management package to System Center Operations Manager (SCOM) or Microsoft Operations Manager (MOM) from the following path in the ScanMail Package to use ScanMail with Systems Center Operations Manager (SCOM) or Microsoft Operations Manager (MOM):

```
\Management Pack\Trend Micro ScanMail for Microsoft Exchange
Management Pack.msi
```

ScanMail Management Pack Fresh Install

This section includes the steps to perform a fresh installation of the ScanMail management pack.

To install the ScanMail management pack:

1. Run Trend Micro ScanMail for Microsoft Exchange Management Pack.msi. The Welcome screen appears.

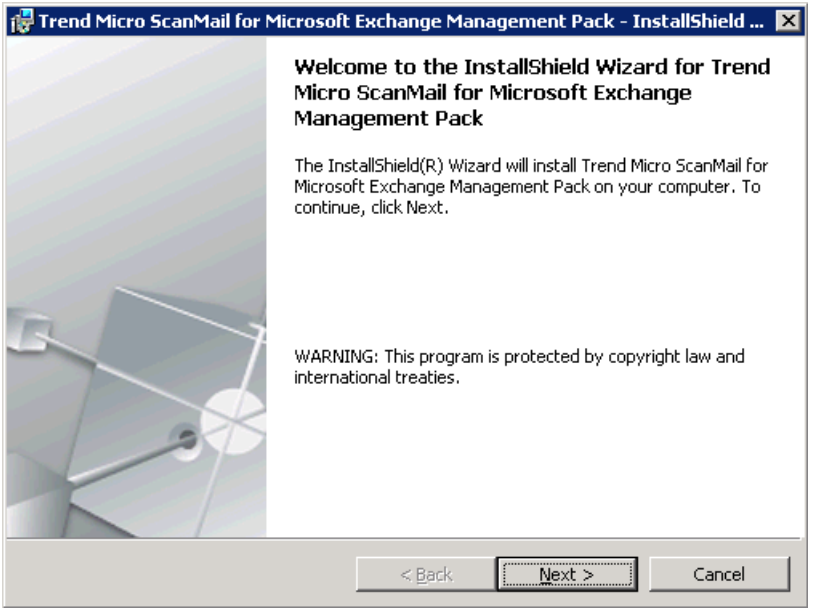


FIGURE 5-1. Management package Welcome screen

2. Click **Next**. The Destination folder screen appears.

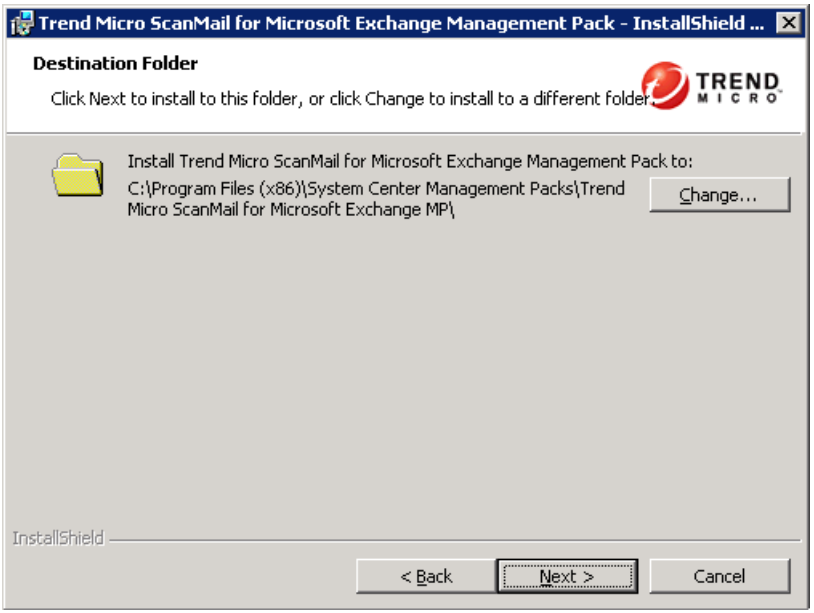


FIGURE 5-2. Management package Destination folder screen

3. Click **Change** to select a folder to install to, or click **Next** to install to the default folder. The **Ready to Install the Program** appears.

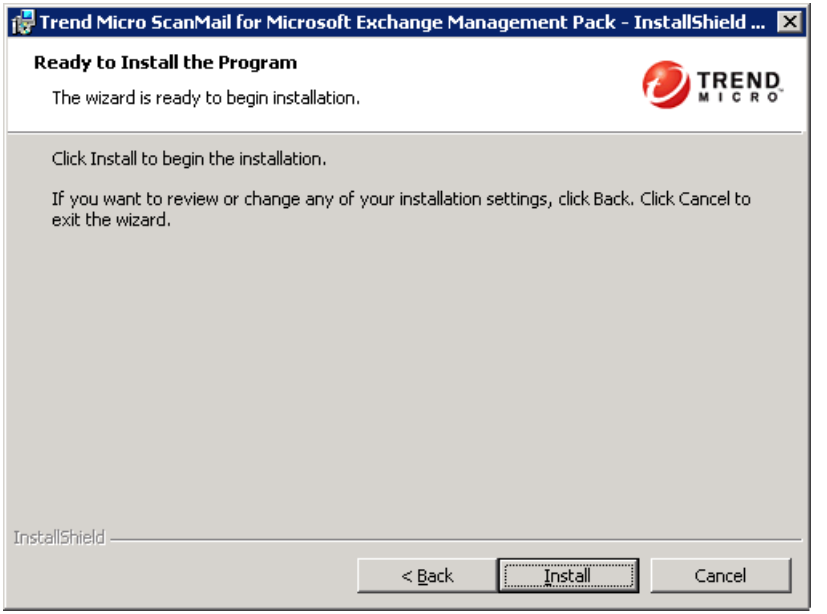


FIGURE 5-3. Management package Ready to Install the Program screen

4. Click **Install** to continue start the installation process. The InstallShield Wizard Completed screen appears.

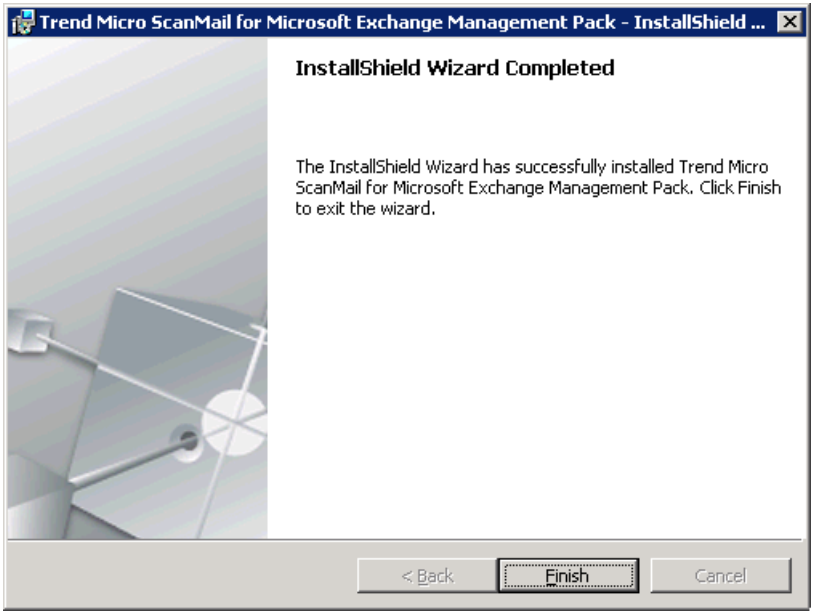


FIGURE 5-4. Management package Installshield Wizard Completed screen

5. Click **Finish**.
6. Navigate to the installation folder that was specified.
7. Get the package from:

```
\System Center Management Packs\Trend Micro ScanMail for
Microsoft Exchange MP\Microsoft Operations Manager 2005
```

```
\System Center Management Packs\Trend Micro ScanMail for
Microsoft Exchange MP\System Center Operations Manager
2007\Trend.Micro.ScanMail.for.Microsoft.Exchange.xml
```

ScanMail Management Pack Post-Installation

After the installation process, perform the following:

- Import the management pack to Microsoft Operations Manager (MOM) or Microsoft Systems Center Operations Manager (SCOM).
- Check for the Trend Micro folder under Monitoring and Reporting from MOM or SCOM.

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.

Testing Manual Scan

The following lists the steps to test manual scan.

To test manual scan:

1. Make sure you have a valid mail client connected to the Exchange2010, 2007, 2003 you are testing.
2. Change the Real-time virus scan action to Pass or so that all the messages and text file attachments can be delivered to the database you selected for the Manual Scan.
3. 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 mailbox
4. Configure your manual scan or accept the Trend Micro default configurations. The default virus scanning configuration scans all files and cleans viruses.
5. Perform a manual scan. ScanMail will detect the EICAR virus and take the action that you have configured against it.
6. View the results in the Virus Summary screen or a ScanMail log.

Testing Real-time Scan

The following lists the steps to test real-time scan.

To test real-time scan:

1. Ensure you have a valid email client connected to the Exchange 2010, 2007, or 2003 you are testing.
2. 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 security risk detection result in the Virus Log from the ScanMail product console.

Testing Notifications

The following lists the steps to test notifications.

To test notifications:

1. Configure security risk scan to detect the virus/malware and notify the administrator.
   a. Click **Security Risk Scan > 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.

Chapter 6

Silent Installation

Install ScanMail locally or remotely to one or more servers using silent installation.

Topics in this chapter:

- *About Silent Installation* on page 6-2
- *Performing Silent Installation* on page 6-3

About Silent Installation

This version of ScanMail supports silent installation. The steps in silent installation follow the same steps as regular installation. Refer to corresponding installation sections for the different server roles.

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.

Silent Installation Limitations

The following lists the limitations for silent installation:

- Silent installations are only supported on local computers.
- 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.
- For version/build upgrades, record settings using the new package. Silent installation will keep the previous settings when an upgrade is performed.
- 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 following lists the steps required to perform silent installation.

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.
   - This version of ScanMail supports installations on remote SQL servers. After the recording completes, type the SQL server information in the pre-configured file. The password is not encrypted in the pre-configured file. If the SQL server information is not specified, SMEX is installs on the local SQL server. If the SQL server information is incorrect, ScanMail displays an error message and installation stops.

     For example:

     ```
     [RemoteSQL]
     RemoteSQLServerName=mysql/instance1
     RemoteSQLUserName=sqluser
     RemoteSQLPassword=userpwd
     ```

Note: The password cannot be encrypted in the file.

- This version of ScanMail supports silent install on cluster servers. For Cluster Continuous Replication (CCR) clusters, there is no need to edit the pre-configure file. For Microsoft cluster for Exchange 2003, Single Copy Cluster (SCC) and VERITAS cluster silent installations, type the shared disk and data folder path in the pre-configured file. If the shared disk and data folder path is not specified, ScanMail installs to the default shared disk and data folder path.

  For example, the following is a record file after an edit:

```
[Cluster]
VirtualServers=EVS1, EVS2
[EVS1]
DiskResourceName=Disk Q:
SMEXFolderPath=Q:\Data\SMEX
RemoteSQLServerName=mysql2\instance2
RemoteSQLUserName=sqluser2
RemoteSQLPassword=userpwd
[EVS2]
DiskResourceName=Disk R:
SMEXFolderPath=R:\SMEX
RemoteSQLServerName=
RemoteSQLUserName=
RemoteSQLPassword=
[RemoteSQL]
RemoteSQLServerName=mysql/instance1
RemoteSQLUserName=sqluser
RemoteSQLPassword=userpwd
```

Note: Separate multiple Exchange Virtual Servers with a comma, semicolon, or space. If the Exchange Virtual Server information is incorrect, ScanMail installs using default settings.

5. Type `Setup /S <pre-configured filename>` to perform silent installation.

Using an Existing Pre-Configured File

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.

TABLE 6-1. Silent Installation setting parameters

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 file-name>	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 6-1. 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 %temp% folder.

Chapter 7

Removing ScanMail

This chapter describes how to remove ScanMail.

Topics in this chapter:

- *Before Removing ScanMail* on page 7-2
- *Using the Enterprise Solution DVD* on page 7-4
- *Using the Windows Control Panel* on page 7-15
- *Removing ScanMail from Clusters* on page 7-16
- *Manually Removing from Exchange 2010/2007 Edge Transport or Hub Transport Servers* on page 7-16
- *Manually Removing from Exchange 2010/2007 Mailbox Servers* on page 7-19
- *Manually Removing from Exchange 2003 Servers* on page 7-22

Before Removing ScanMail

Uninstallation removes the following components:

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

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

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

WARNING! **For single servers, uninstall ScanMail from the Windows Control Panel or the Uninstall program. For cluster servers, uninstall ScanMail from the Uninstall program. Do not manually uninstall ScanMail.**

Privilege Requirements

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

TABLE 7-1. Minimum privileges required for uninstalling ScanMail

EXCHANGE VERSION	MINIMUM PRIVILEGES	FEATURE LIMITATION WITHOUT DOMAIN ADMINISTRATOR PRIVILEGES
Exchange Server 2010 or 2007 Edge Transport	Local Administrator	N/A
Exchange Server 2010 or 2007 Hub/Mailbox/Cluster	Local Administrator and Exchange Organization Administrator	Manual removal of EUQ mailbox required.
Exchange Server 2003	Local Administrator and Domain User	Manual removal of EUQ mailbox required.

Using the Enterprise Solution DVD

You can use the Trend Micro™ Enterprise Solution DVD to uninstall ScanMail.

To uninstall ScanMail:

1. To remove ScanMail, run setup.exe from the Trend Micro Enterprise Solution DVD. Select uninstall when prompted. The Welcome to Trend Micro ScanMail Setup screen appears.

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. Click **Next** to continue with the uninstallation. The License Agreement screen appears.

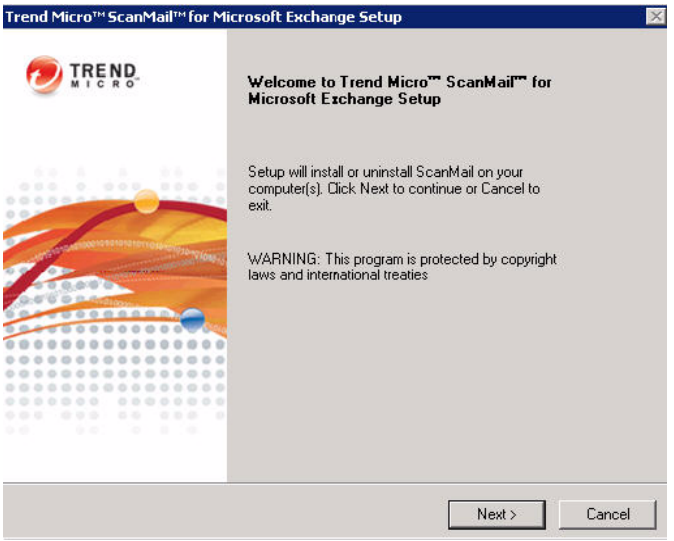


FIGURE 7-1. Welcome screen

3. 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.

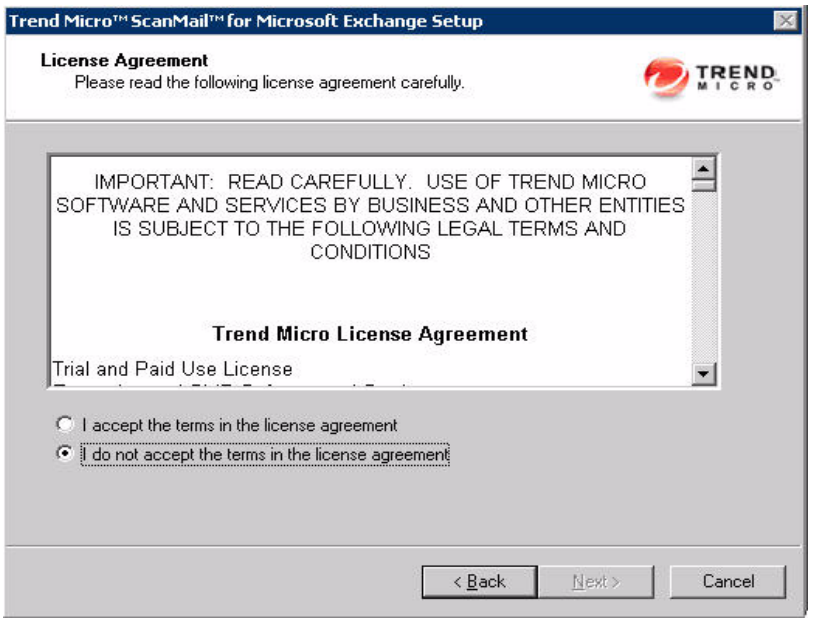


FIGURE 7-2. License Agreement screen

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

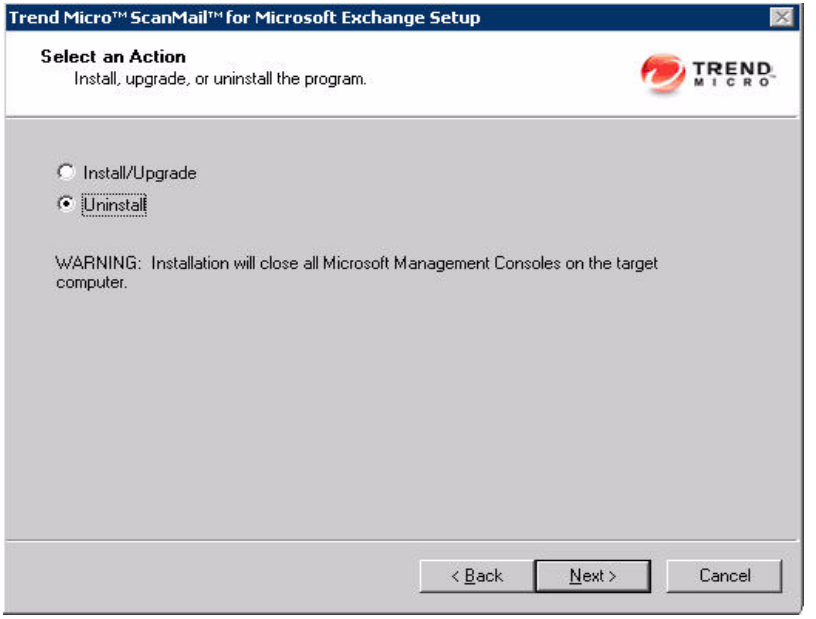


FIGURE 7-3. Select an Action screen

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, then double-click the domain or computers you want to add to the list
      - Click **Remove** to remove a server from the list.

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

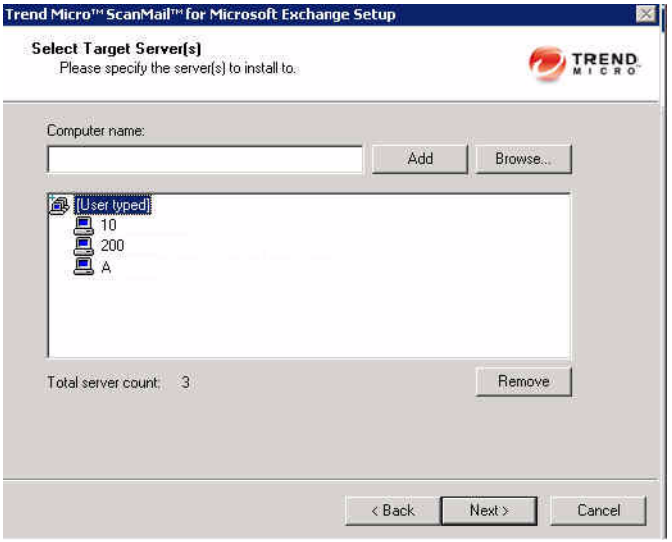


FIGURE 7-4. Select Target Server(s) screen

6. 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.

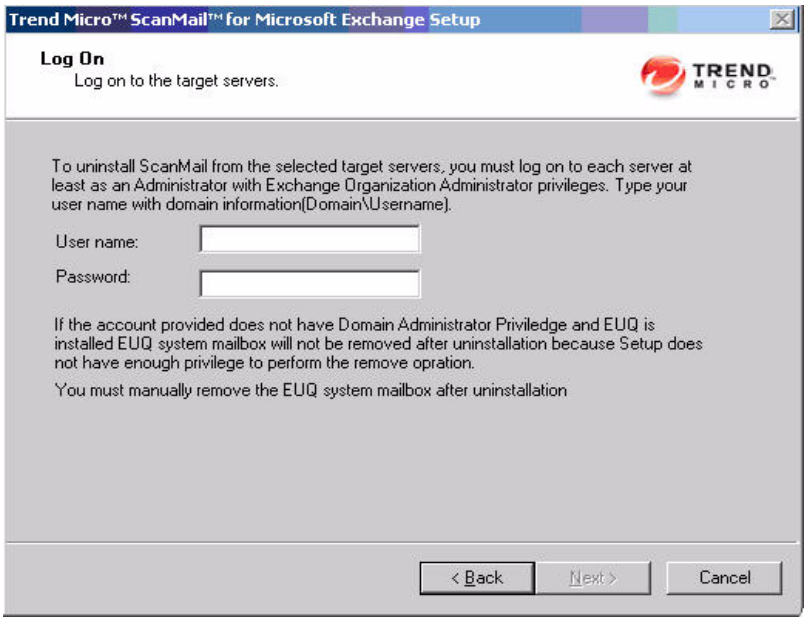


FIGURE 7-5. Log On screen

7. Use this screen to specify the shared directory for the target servers from where you will uninstall ScanMail.

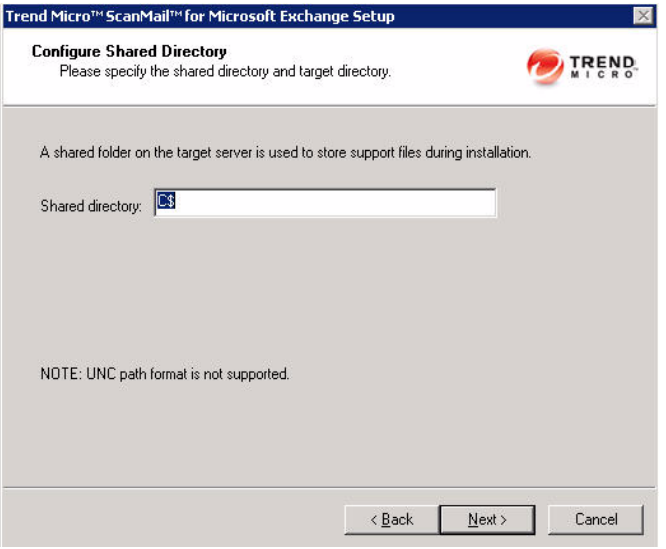


FIGURE 7-6. Configured Shared Directory screen

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

b. Click **Next**. The Checking Target System Requirements screen appears.

8. View the screen and ensure the settings for the uninstallation are correct and click **Next** to continue. The Removal Option screen appears.

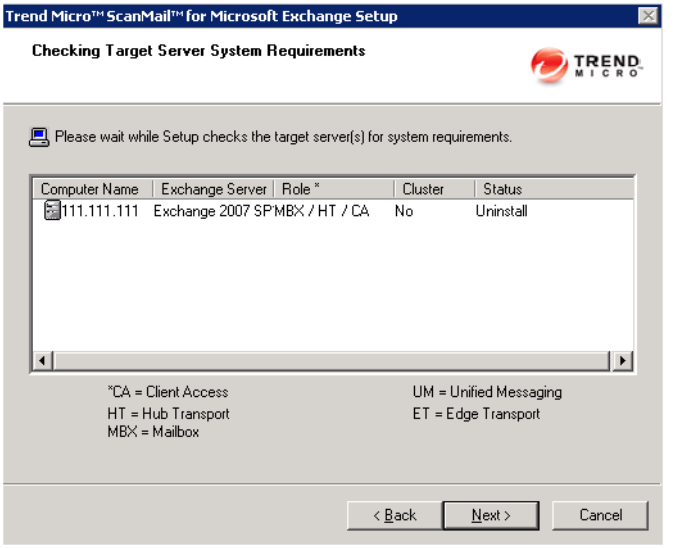


FIGURE 7-7. Checking Target Server System Requirements screen

9. Select the components to remove and click **Next**. The Review Settings screen appears.

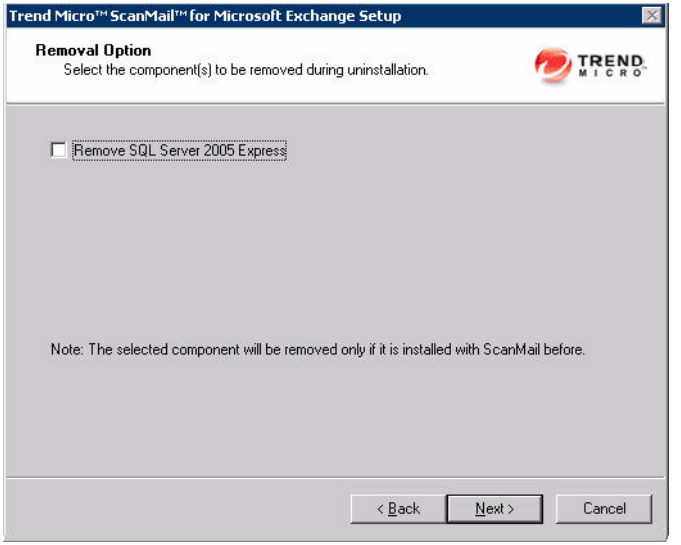


FIGURE 7-8. Removal Option screen

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

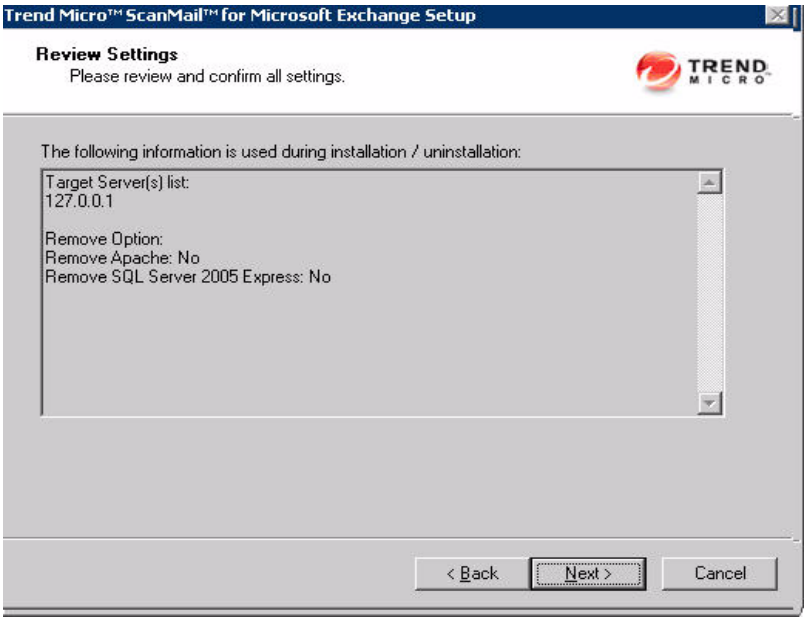


FIGURE 7-9. Review Settings screen

11. When the uninstallation is complete, click **Next** to proceed. The Uninstallation Complete screen appears to inform you that the servers successfully uninstalled.

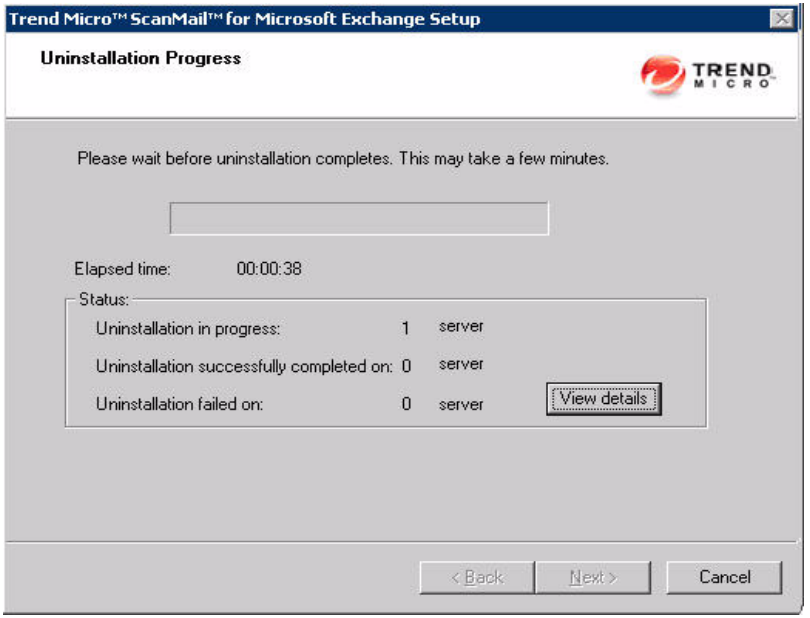


FIGURE 7-10. Uninstallation Progress

12. Click **Finish** to exit the Setup program. The Setup program removes ScanMail from the selected servers.

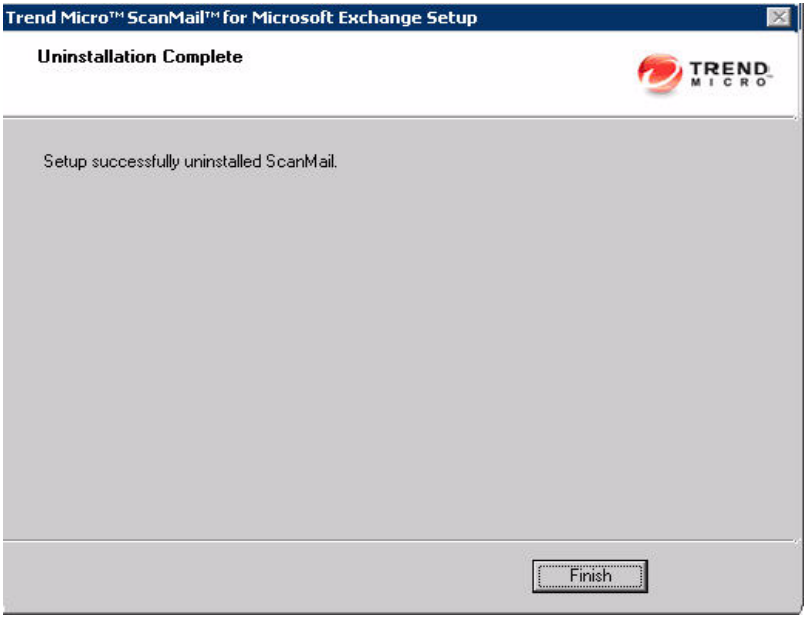


FIGURE 7-11. Uninstallation Complete screen

Using the Windows Control Panel

You can remove ScanMail using the Microsoft™ Windows™ Control Panel, but you must remove Microsoft SQL Server 2005 Express separately after uninstallation. 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: ScanMail 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 *Using the Enterprise Solution DVD* on page 7-4.

Note: For Microsoft clusters, type the node name, Exchange Virtual Server (EVS) name, or cluster name on the Select Target Servers screen. For VERITAS clusters, type the node name or Exchange Virtual Server (EVS) name on the Select Target Servers screen and ScanMail can detect and install on each Exchange Virtual Server (EVS) in the cluster.

To remove ScanMail from clusters:

1. Run `setup.exe` again and uninstall ScanMail.
2. Remove ScanMail together from each cluster node belonging to the same cluster and remove the resources on each online virtual server.
3. Remove all the changes from each Exchange virtual server accordingly.

Note: ScanMail installs Microsoft Visual C++ 2005 Redistributable and Microsoft Visual C++ 2005 Redistributable (X64) and they are not uninstalled when you uninstall ScanMail.

Manually Removing from Exchange 2010/2007 Edge Transport or Hub Transport Servers

Manually remove ScanMail from Exchange 2010 or 2007 Edge Transport or Hub Transport servers by following the instructions below.

To manually remove ScanMail:

1. Stop ScanMail related services:
   - ScanMail for Microsoft Exchange Master Service
   - ScanMail for Microsoft Exchange Remote Configuration Server
   - ScanMail for Microsoft Exchange System Watcher
   - Microsoft Exchange Transport Service

2. Remove ScanMail transport agent from Exchange 2010 or 2007.
   a. Type the following command:
      Uninstall-TransportAgent –Identity "ScanMail Routing Agent"
      Uninstall-TransportAgent –Identity "ScanMail SMTP Receive Agent"
   b. Type Y.
   c. Type the following to ensure that ScanMail transport agent has been removed.
      get-transportagent
3. Delete related registry keys:
   - Product registry keys:
     - HKLM\SOFTWARE\ Trend Micro\ScanMail for Exchange
     - HKLM\SOFTWARE\Wow6432Node\Trend Micro\ScanMail for Exchange (This key only exists in 64-bit environments)
   - Service registry keys:
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_Master
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_RemoteConfig
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_SystemWatcher
     - HKLM\SYSTEM\CurrentControlSet\Services\RIFRemoteInstallAgent (This key only exists if installation stopped unexpectedly.)
4. Delete Web Server Configurations
   a. Launch the Internet Information Services (IIS) Manager console.
   b. Extend **Web Sites**.
   c. Right click **SMEX Web Site**.
   d. Select **Delete**.
5. Delete ScanMail from the Start menu. For example:
   C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro ScanMail for Microsoft Exchange.
6. Delete all files and subfolders in the folder that ScanMail installed to. For example: C:\Program Files\Trend Micro\SMEX\.

7. Delete all files and sub folders in "Shared Directory"\SMEXtemp\. This is the shared directory that was specified during installation. The default is C$.
8. Remove Microsoft SQL Server 2005 on local servers:
   a. Launch the **Add or Remove Programs** console.
   b. Next to Microsoft SQL Server, click **Remove**.
   c. Select **SCANMAIL: Database Engine**.
   d. Click **Next**.
   e. Click **Finish**.
9. Remove Microsoft SQL Server 2005 on remote servers:
   a. Use SQL Server Management Studio Express to connect to the remote SQL server which has the ScanMail installation.
   b. Delete ScanMail databases:
      - Conf_HostName_UUID
      - Log_HostName_UUID
      - Report_HostName_UUID
10. Install Microsoft Windows Installer Cleanup utility on the target server(s) that you want to manually remove ScanMail from.
    a. Launch Windows Install Cleanup
    b. Select **Trend Micro ScanMail for Microsoft Exchange**.
    c. Click **Remove**.

Manually Removing from Exchange 2010/2007 Mailbox Servers

Manually remove ScanMail from Exchange 2010 or 2007 Mailbox servers, including cluster servers, by following the instructions below.

To manually remove ScanMail:

1. Stop ScanMail related services:
   - ScanMail for Microsoft Exchange Master Service
   - ScanMail for Microsoft Exchange Remote Configuration Server
   - ScanMail EUQ Monitor

     Note: This service only exists if End User Quarantine (EUQ) was installed.

   - ScanMail EUQ Migrator service

     Note: This service only exists if upgrades included End User Quarantine (EUQ) settings.

2. For non-cluster removal, skip this step.
   - If removing ScanMail from Microsoft cluster servers:
     - Delete ScanMail resources from the Cluster Administrator console.
     - Delete the following ScanMail resource type on each node for Cluster Continuous Replication (CCR):

       HKLM\Cluster\ResourceTypes\clusRDLLCCR
     - Delete the following ScanMail resource type on each node for Single Copy Clusters (SCC):

       HKLM\Cluster\ResourceTypes\clusRDLL
     - Delete the following ScanMail resource type on each node for Standby Continuous Replication (SCR):

       HKLM\Cluster\ResourceTypes\clusRDLL
   - If removing ScanMail from VERITAS cluster servers, delete ScanMail resources from the Cluster Explorer console:

- EVS name-ScanMail_RegRep
- EVS name-ScanMail_Master
- EVS name-ScanMail_SystemWatcher
- EVS name-ScanMail_RemoteConfig
- EVS name-EUQ_Monitor (Only if End User Quarantine was installed.)

3. Delete related registry keys:
   - Product registry keys:
     - HKLM\SOFTWARE\ Trend Micro\ScanMail for Exchange
     - HKLM\SOFTWARE\Wow6432Node\Trend Micro\ScanMail for Exchange (This key only exists in 64-bit environments.)
   - Service registry keys:
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_Master
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_RemoteConfig
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_SystemWatcher
     - HKLM\SYSTEM\CurrentControlSet\Services\RIFRemoteInstallAgent
     - HKLM\SYSTEM\CurrentControlSet\Services\EUQ_Monitor

     Note: This exists only if End User Quarantine (EUQ) was installed.

     - HKLM\SYSTEM\CurrentControlSet\Services\EUQ_Migrator

     Note: This exists only if upgrades included End User Quarantine (EUQ) settings.

   - The security risk scan registry key:
     HKLM\SYSTEM\CurrentControlSet\Serices\MSExchangeIS\VirusScan

- The security risk scan registry key for each mailbox store. There are three REG_DWORD items for each mailbox store:

  HKLM\SYSTEM\CurrentControlSet\Serices\MSExchangeIS\<computer name>\<storename>\

  - VirusScanBackgroundScanning
  - VirusScanEnabled
  - VirusScanProactiveScanning

4. Delete Web Server Configurations.
   a. Launch the Internet Information Services (IIS) Manager console.
   b. Extend **Web Sites**.
   c. Right click **SMEX Web Site**.
   d. Select **Delete**.
5. If End User Quarantine (EUQ) was installed, delete End User Quarantine Accounts and Mailboxes.
   a. Launch **Active Users and Computers**.
   b. Remove the End User Quarantine (EUQ) accounts and mailboxes for the Exchange Server.
6. Delete ScanMail from the Start menu. For example:

   C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro ScanMail for Microsoft Exchange.
7. Delete all files and sub folders in the folder that ScanMail installed to. For example: C:\Program Files\Trend Micro\SMEX\.
8. Delete all files and subfolders in "Shared Directory"\SMEXtemp\. This is the shared directory that was specified during installation. The default is C$.
9. Remove Microsoft SQL Server 2005 on local servers:
   a. Launch the **Add or Remove Programs** console.
   b. Next to Microsoft SQL Server, click **Remove**.
   c. Select **SCANMAIL: Database Engine**.
   d. Click **Next**.
   e. Click **Finish**.

10. Remove Microsoft SQL Server 2005 on remote servers:
    a. Use SQL Server Management Studio Express to connect to the remote SQL server which has the ScanMail installation.
    b. Delete ScanMail databases:
        - Conf_HostName_UUID
        - Log_HostName_UUID
        - Report_HostName_UUID
11. Install Microsoft Windows Installer Cleanup utility on the target server(s) that you want to manually remove ScanMail from.
    a. Launch Windows Install Cleanup
    b. Select **Trend Micro ScanMail for Microsoft Exchange**.
    c. Click **Remove**.

Manually Removing from Exchange 2003 Servers

Manually remove ScanMail from Exchange 2003 server, including cluster servers, by following the instructions below.

To manually remove ScanMail:

1. Stop ScanMail related services:
    - ScanMail for Microsoft Exchange Master Service
    - ScanMail for Microsoft Exchange Remote Configuration Server
    - ScanMail System Watcher Service
    - ScanMail EUQ Monitor

    Note: This service only exists if End User Quarantine (EUQ) was installed.

    - ScanMail EUQ Migrator service

    Note: This service only exists if upgrades included End User Quarantine (EUQ) settings.

2. For non-cluster removal, skip this step.
   - If removing ScanMail from Microsoft cluster servers:
     - Delete ScanMail resources from the Cluster Administrator console.
     - Delete the following ScanMail resource type on each node: HKLM\Cluster\ResourceTypes\clusRDLL
   - If removing ScanMail from VERITAS cluster servers, delete ScanMail resources from the Cluster Explorer console:
     - EVS name-ScanMail_RegRep
     - EVS name-ScanMail_Master
     - EVS name-ScanMail_SystemWatcher
     - EVS name-ScanMail_RemoteConfig
     - EVS name-EUQ_Monitor (Only if EUQ was installed.)
3. Delete related registry keys:
   - Product registry key:

     HKLM\SOFTWARE\ Trend Micro\ScanMail for Exchange
   - Service registry keys:
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_Master
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_RemoteConfig
     - HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_SystemWatcher
     - HKLM\SYSTEM\CurrentControlSet\Services\RIFRemoteInstallAgent
     - HKLM\SYSTEM\CurrentControlSet\Services\EUQ_Monitor

     Note: This exists only if End User Quarantine (EUQ) was installed.

     - HKLM\SYSTEM\CurrentControlSet\Services\EUQ_Migrator

     Note: This exists only if upgrades included End User Quarantine (EUQ) settings.

   - The security risk scan registry key:

     HKLM\SYSTEM\CurrentControlSet\Serices\MSExchangeIS\VirusScan

- The virus/malware scan registry key for each mailbox store. There are three REG_DWORD items for each mailbox store:

  HKLM\SYSTEM\CurrentControlSet\Serices\MSExchangeIS\<computer name>\<storename>\

  - VirusScanBackgroundScanning
  - VirusScanEnabled
  - VirusScanProactiveScanning

4. Delete Web Server Configurations:
   a. Launch the Internet Information Services (IIS) Manager console.
   b. Extend **Web Sites**.
   c. Right click **SMEX Web Site**.
   d. Select **Delete**.
5. If End User Quarantine (EUQ) was installed, delete End User Quarantine Accounts and Mailboxes.
   a. Launch **Active Users and Computers**.
   b. Remove the End User Quarantine (EUQ) accounts and mailboxes for the Exchange Server.
6. Delete ScanMail from the Start menu.

   C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro ScanMail for Microsoft Exchange.
7. Delete all files and sub folders in the folder that ScanMail installed to. For example: C:\Program Files\Trend Micro\SMEX\.
8. Delete all files and sub folders in "Shared Directory"\SMEXtemp\. This is the shared directory that was specified during installation. The default is C$.
9. Install Microsoft Windows Installer Cleanup utility on the target server(s) that you want to manually remove ScanMail from.
   a. Launch Windows Install Cleanup
   b. Select **Trend Micro ScanMail for Microsoft Exchange**.
   c. Click **Remove**.

Chapter 8

Getting Support and Contacting Trend Micro

This chapter discusses how to get technical support.

Topics in this chapter:

- *Contacting Technical Support* on page 8-2
- *Before Contacting Technical Support* on page 8-3
- *Contacting Trend Micro* on page 8-3
- *Known Issues* on page 8-4

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 security risk scans, web feeds, and security testing

To contact Trend Micro technical support:

1. Visit the following URL:

   http://esupport.trendmicro.com/

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 inquiries, there are a few additional resources for quickly finding answers.

- Check the documentation: the manual and online help provide comprehensive information about ScanMail. Search both documents to see if they contain your solution.
- To speed up your problem resolution, when you contact Trend Micro technical support, please provide as much of the following information as you can:
  - Product serial number
  - ScanMail program, scan engine, pattern file, version number
  - Operating system 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:

Kinkajou 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://us.trendmicro.com/us/about/contact/index.html

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℠

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 work around. 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

Appendix A

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.

TABLE A-1. Pre-configured files

SECTION	CONTENTS
Log on	• LogonUserDomain=User's configuration • LogonUserName= User's configuration
Directory	• TempDir=smex80temp • ShareName=C$ Default is C$ and can be changed. • TargetDir=C:\Program Files\Trend Micro\Smex This is the default setting and can be changed. • UseDefaultProgPath=0 or 1 0 uses your configuration and 1 uses the default
Activation	MasterACCode=User's configuration

TABLE A-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=Your configuration • ProxyPort=Your configuration The range is 1 to 65535 • ProxyUsername=Your 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 applicable when IIS is selected. • WebPort=Your configuration The range is 1 to 65535 • EnableSSL=0 or 1 0 is disable, 1 is enable • SSLPort=Your configuration The range is 1 to 65535 • SSLValidPeriodCertificate=Your configuration
WTC	WTCEnable=0 or 1 0 is disable, 1 is enable
ServerManage-ment	• CreateNewConsoleAccount=0 or 1 0 uses the current or skip, 1 creates a new account • ConsoleUsername= Your configuration • ActivateServerManagement=0 or 1 0 is deactivate, 1 is activate
SMTP	EnableSMTPScanning=1 0 is disable, 1 is enable

TABLE A-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 and can be changed. • SpamMsgRetainDay=14 This is default setting and can be changed. The range is 0 to 30.
CMAgent	• RegisterCMAgent=0 or 1 0 is disable, 1 is enable • CMServerAddress=Your configuration • CMServerPortNumber=443 This is the default setting and can be changed. 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=Your configuration • ConnectCMServerUseSOCKS5=0 or 1 0 is disable, 1 is enable • ConnectCMServerProxyUserName=Your configuration • CMServerWebUserName= Your configuration • ConnectCMServerProxyPortNumber=80 This is the default setting and can be changed. The range is 1 to 65535.

TABLE A-1. Pre-configured files

SECTION	CONTENTS
Do NOT edit these settings	• LogonPassword= Your configuration Password does not display. • ExchangeType=1, 2 or 3 • 1 is “Exchange 2007 Edge Transport Server” • 2 is “Exchange 2007 Hub Transport Server / Mailbox Server” • 3 is “Exchange 2003 Server” • ProxyPassword= Your configuration Password does not display. • ConsolePassword= Your configuration Password does not display. • EUQInstallLangID=1033 Do not change this setting. • EUQDefaultLangID=9 Do not change the setting. • ConnectCMServerProxyPassword= Your configuration Password does not display. • CMServerWebPassword= Your configuration Password does not display. • ConsoleGroup= “SMEX Admin Group” for 2003 (Do not modify the group name) “User’s configuration” for 2007 (For example: DomainName\Group, do not modify the group name) • ServerManagementGroupSid= (Do not modify the SID)

TABLE A-1. Pre-configured files

SECTION	CONTENTS
Cluster	• VirtualServers= Your configuration • [VirtualServerName] (type the virtual server name here) • DiskResourceName= Your configuration • SMEXFolderPath= Your configuration • RemoteSQLServerName= Your configuration • RemoteSQLUserName= Your configuration • RemoteSQLPassword= Your configuration
RemoteSQL	• RemoteSQLServerName= Your configuration • RemoteSQLUserName= Your configuration (A dbcreator role is required.) • RemoteSQLPassword= Your configuration
InstallOption	WaitIISAdminToUnloadSMTPHook=-1 • This setting is applicable only when migrating. • -1: The default setting. ScanMail Setup program restarts the IIS service during upgrades to regular server(s) and waits 20 minutes for cluster server(s). Migration includes build and version upgrades. • 0: Restart the IIS service without waiting 20 minutes for regular or cluster server(s). • 1: Wait 20 minutes for regular and cluster server(s) before restarting the IIS service.

Glossary

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. 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.
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.

TERM	DESCRIPTION
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.

TERM	DESCRIPTION
Hot Fixes and Patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro Web site and deploy to the ScanMail server and/or client program.
HTTP (Hypertext Transfer Protocol)	The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTML, VBScript, or JavaScript viruses	Viruses that reside in Web pages and are downloaded through a browser.
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.

TERM	DESCRIPTION
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.
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.

TERM	DESCRIPTION
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.
Registration key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. 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.

TERM	DESCRIPTION
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.
Test virus	An inert file that acts like a real virus and is detectable by security risk-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.

TERM	DESCRIPTION
Unsolicited email	See spam
Virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
Virus writer	Another name for a computer hacker. Someone who writes virus code.
Wildcard	For ScanMail, an asterisk (*) represents any character. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on.
Worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email. A worm can also be called a network virus.
Zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.

Index

A

account privileges, required to install 1-32

C

contacting Technical Support 8-2

D

deploying ScanMail
  network traffic, ScanMail effect 1-8

F

FAQ, frequently asked questions 8-4
frequently asked questions (FAQ) 8-4

I

installing ScanMail
  activation code, entering 1-33
  pre-installation tasks 1-32
  registration key required 1-33
  setting proxy server 1-33
  stopping and restarting services unnecessary 1-32
  verifying success 5-2
ISO 9002 certification-see TrendLabs 8-4

J

Java
  malicious code
    definition 1-4

K

Knowledge base
  url 8-4
known issues 8-4

N

network traffic, ScanMail generating 1-8

P

pilot installation
  testing 1-15

R

removing ScanMail 6-5, 7-2
  components removed 7-2
  from cluster server 7-16

T

Technical Support
  contacting 8-2
  URL 8-2
testing your installation 1-15
Trend Micro
  contacting corporate offices 8-2
  headquarters 8-2

U

uninstalling ScanMail 6-5, 7-2
upgrading ScanMail
  on cluster servers 1-36
  supported versions 1-35
URLs
  Knowledge base 8-4
  Technical Support 8-2

V

Virus Doctors - See TrendLabs 8-4