TREND MICRO™

12.5 ScanMail™ for Microsoft™ Exchange

Service Pack 1

Installation and Upgrade Guide

Securing your Exchange environment

Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption.aspx

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 © 2018. Trend Micro Incorporated. All rights reserved.

Document Part No.: SMEM128278/180524

Release Date: July 2018

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that ScanMail for Microsoft Exchange collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

Preface

Preface iii

ScanMail Documentation iv

Audience iv

Document Conventions v

Chapter 1: Installing ScanMail 12.5 SP1

Upgrade Requirements 1-2

Installing Service Pack on Exchange Server 1-2

Removing the Service Pack 1-13

Chapter 2: Silent Installation

About Silent Installations 2-2

- Silent Installation Limitations 2-2

Performing a Silent Installation 2-3

- Using an Existing Pre-Configured File 2-3

Chapter 3: Technical Support

Troubleshooting Resources 3-2

- Using the Support Portal 3-2
- Threat Encyclopedia 3-2

Contacting Trend Micro 3-3

- Speeding Up the Support Call 3-4

Sending Suspicious Content to Trend Micro 3-4

- Email Reputation Services 3-4
- File Reputation Services 3-5
- Web Reputation Services 3-5

Other Resources 3-5
Download Center 3-5
Documentation Feedback 3-6

Appendix A: Glossary

Index

Index IN-1

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 manage ScanMail.

This preface discusses the following topics:

- *ScanMail Documentation on page iv*
- *Audience on page iv*
- *Document Conventions on page v*

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 latest information about all Trend Micro products. Other inquiries that were already answered area 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://docs.trendmicro.com/en-us/enterprise/scanmail-for-microsoft-exchange.aspx) 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 2016, 2013 and 2010 server role configurations
- Various message formats

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions

CONVENTION	DESCRIPTION
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Chapter 1

Installing ScanMail 12.5 SP1

Install ScanMail 12.5 SP1 locally or remotely to one or more servers using one easy-to use Setup program.

Topics in this chapter:

- *Upgrade Requirements on page 1-2*
- *Installing Service Pack on Exchange Server on page 1-2*
- *Removing the Service Pack on page 1-13*

Upgrade Requirements

The following lists the upgrade requirements for Trend Micro™ ScanMail™ *for Microsoft™ Exchange* 12.5 SP1:

- Trend Micro™ ScanMail™ *for Microsoft™ Exchange* 12.5
- Integrated Trend Micro product support as listed in table *Integrated Trend Micro Product Support on page 1-2*

TABLE 1-1. Integrated Trend Micro Product Support

TREND MICRO PRODUCT	SUPPORTED VERSIONS
Control Manager™	• 6.0 Service Pack 3 or above • 7.0
Smart Protection Server	• 3.0 or above • OfficeScan Server Integrated Smart Protection Server
Deep Discovery Advisor	2.92 or later
Deep Discovery Analyzer	5.0 or later

Installing Service Pack on Exchange Server

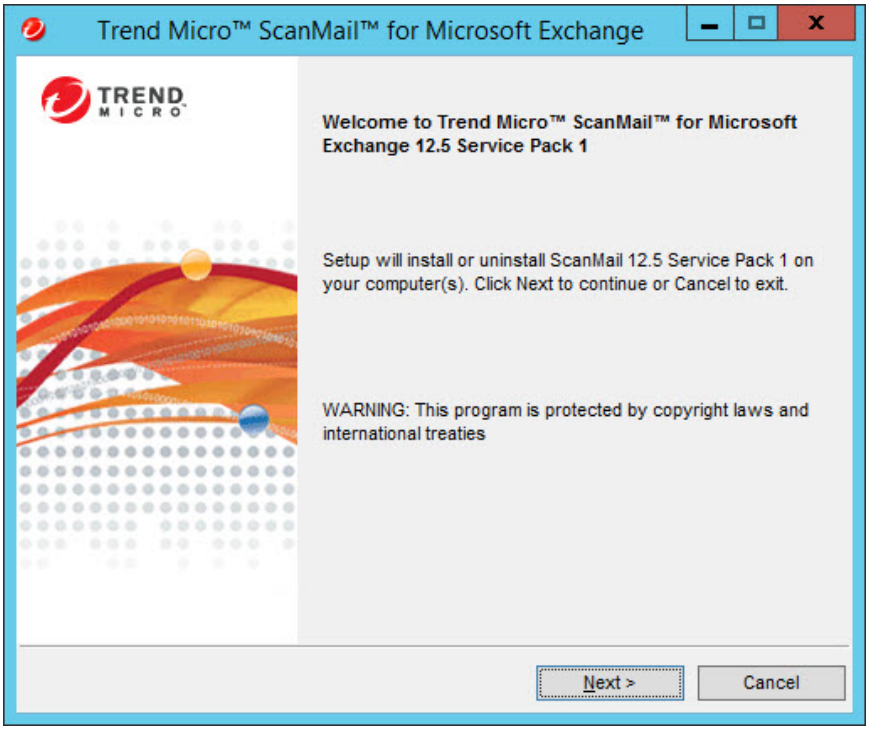
Note

Installation of this patch does not cause a disruption in email message traffic during deployment.

Procedure

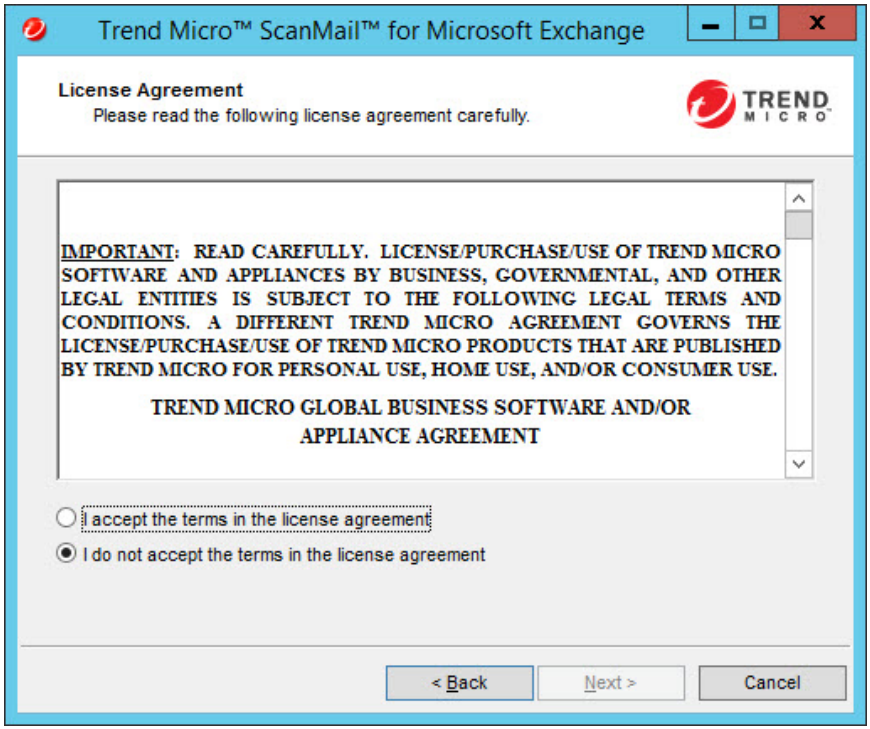
1. Click the installation program to start the installation wizard.

The **Welcome** screen appears.



2. Click **Next** to begin the installation.

The **License Agreement** screen appears.

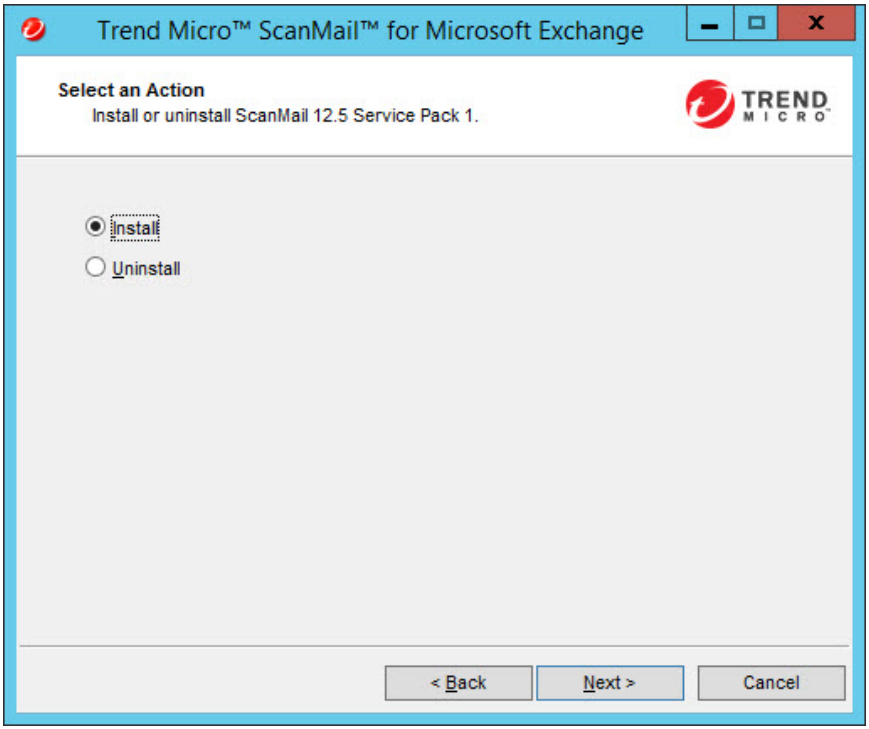


3. Click **I accept the terms in the license agreement** to agree to the terms of the agreement and continue installation. Click **Next** to continue.

Note

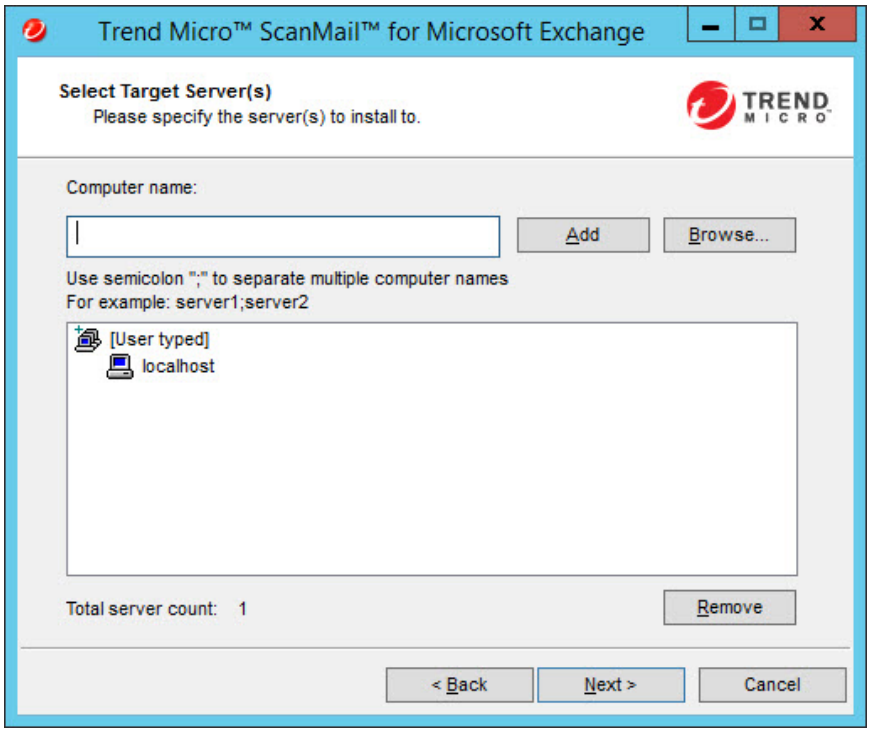
If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the installation without modifying your operating system.

The **Select an Action** screen appears.



4. Select **Install** and click **Next** to continue.

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



5. 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.

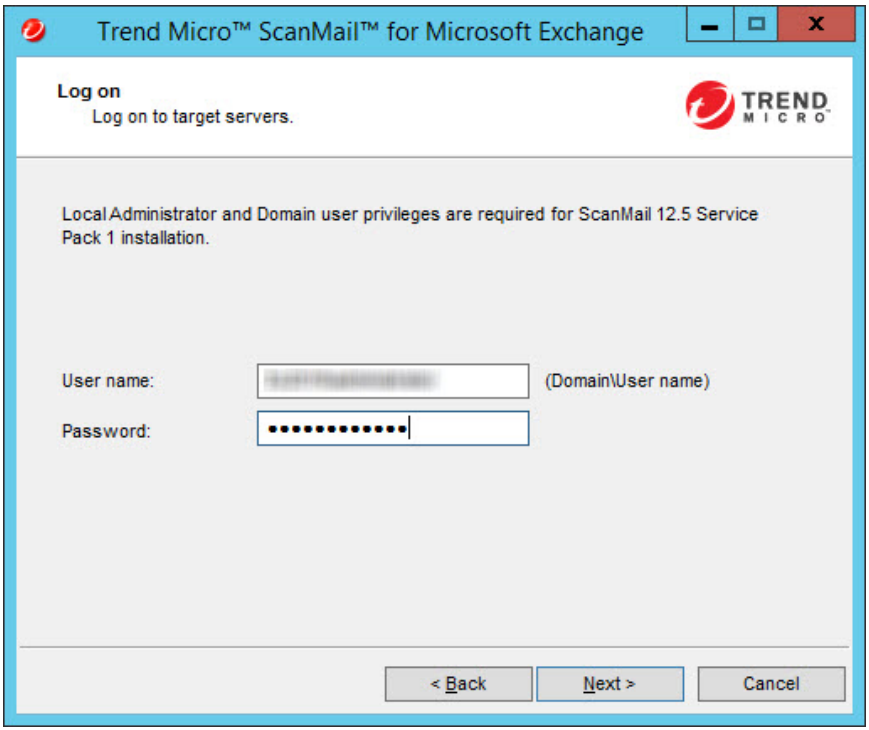
      - Click **Remove** to remove a server from the list.

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

Note

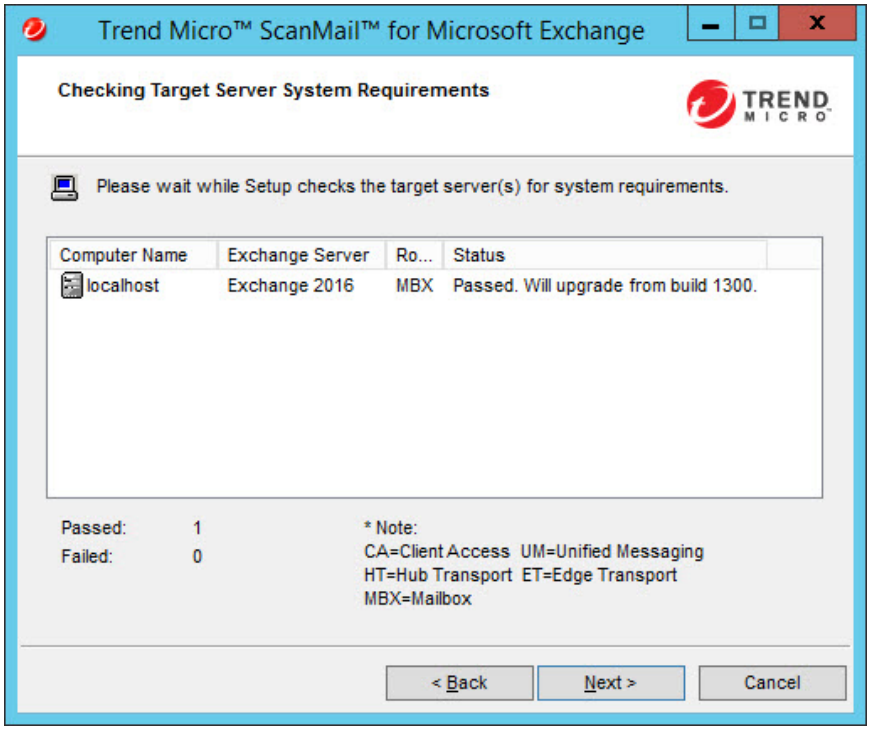
The Setup program can install ScanMail to a number of single servers or to all the computers in a domain. Use an account with the appropriate privileges to access every target server.

The **Log on** screen appears.



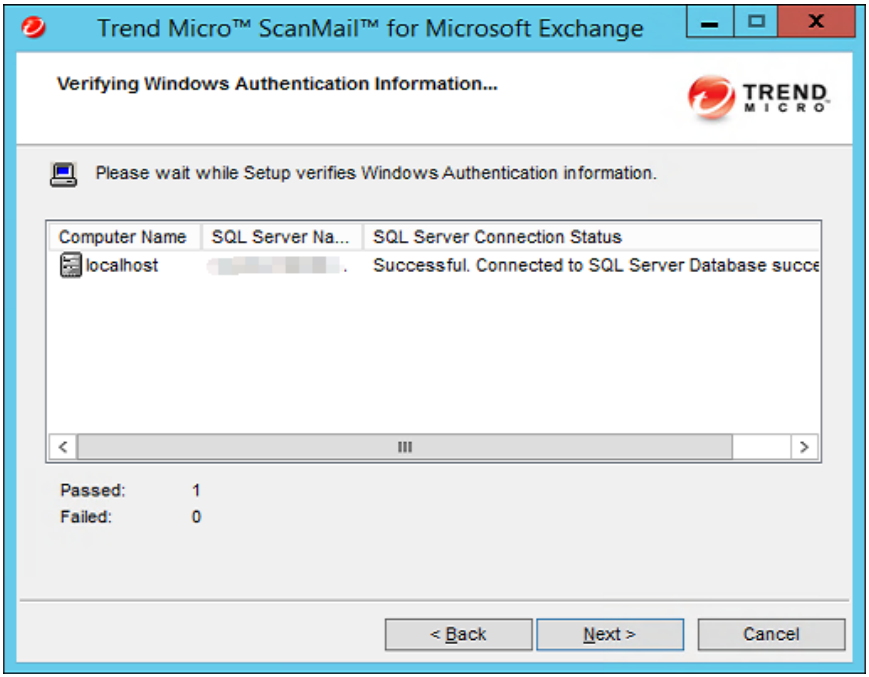
6. Log on to the where you want to install ScanMail. Click **Next** to continue.

The **Checking Target Server System Requirements** screen appears.



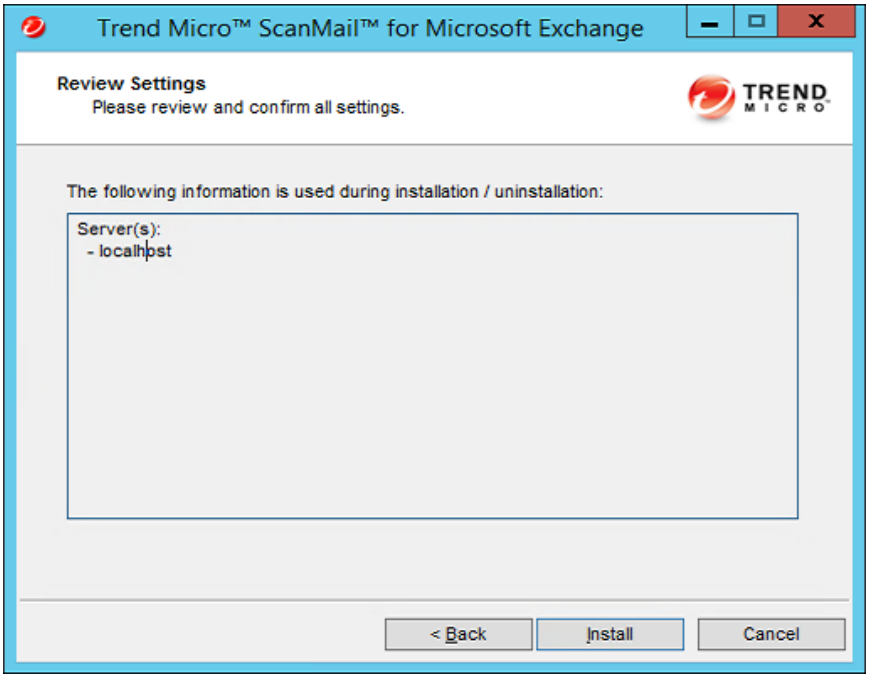
7. If the SQL Server Windows Authentication Information screen appears, type the logon account credentials for ScanMail installation, and then click **Next** to continue.

The **Verifying Windows Authentication Information** screen appears.



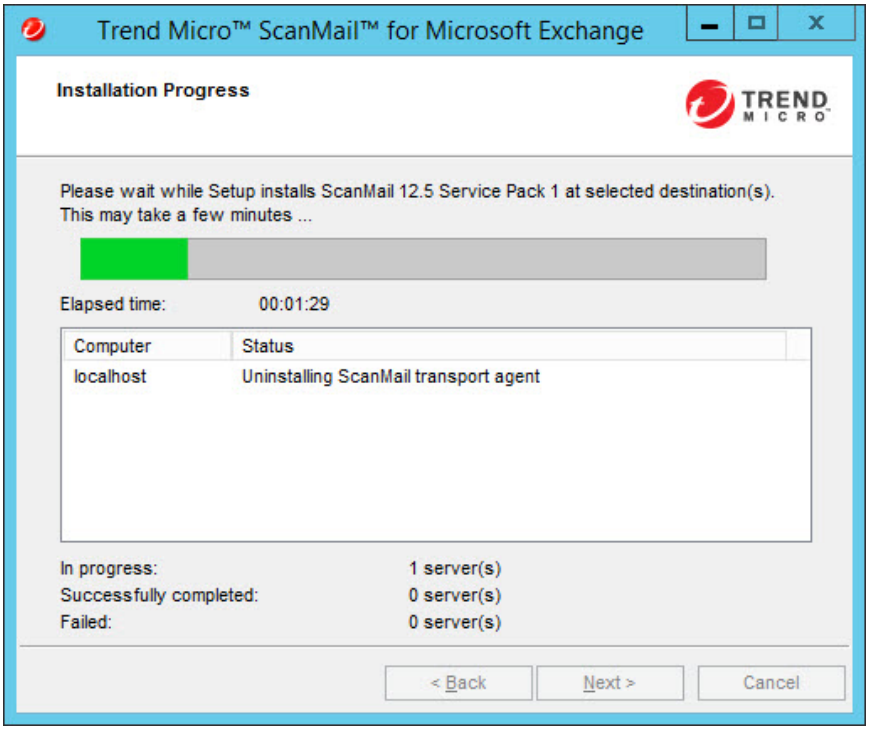
8. Review the results of each target server and click **Next** to continue.

The **Review Settings** screen appears.



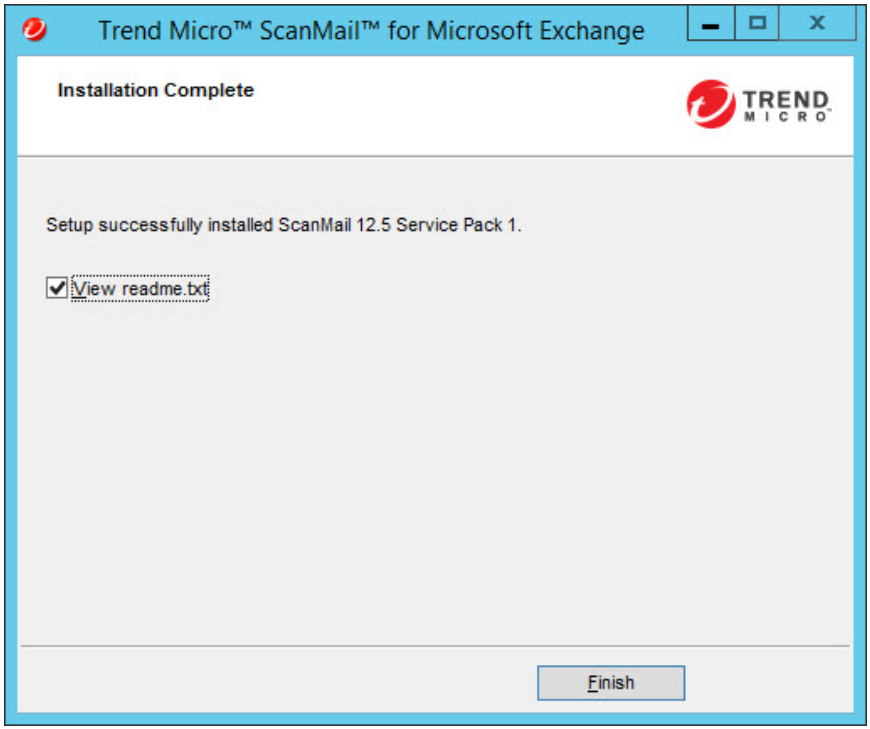
9. Review settings and click **Install** to continue.

The **Installation Progress** screen appears.



10. View the progress of the installation and click **Next** when the installation completes.

The **Installation Complete** screen appears.



11. Click **Finish** to exit the Setup program.

    The Readme file displays.

What to do next

For the Writing Style Analysis feature to work properly, make sure that the Exchange server can access the Trend Micro Anti-Spam Engine (TMASE) server directly or through ScanMail proxy (**Administrator** > **Proxy setting**).

Removing the Service Pack

Removing the Service Pack reverts ScanMail to the previously installed version.

Procedure

1. Run the Service Pack `setup.exe` program and select **Uninstall** on the **Select an Action** screen.

Chapter 2

Silent Installation

Install ScanMail to one or more servers using silent installation.

Topics in this chapter:

- *About Silent Installations on page 2-2*
- *Performing a Silent Installation on page 2-3*

About Silent Installations

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

The differences 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).
- If the ScanMail connects to SQL server using Windows authentication you need to provide the password for recording script.
- If the ScanMail server connects with SQL database using Windows domain account, you need to provide Windows credential when recording script.
- Once the recording completes, the file name and location information is listed on the setup screen.
- **Checking Target Server System Requirements** and **Select 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.
- Record settings separately for target servers with different languages. For example, do not apply pre-configured files recorded on an English operating system to a target server with a German operating system.

Performing a Silent Installation

Procedure

1. Launch the Windows command prompt.
2. Locate the ScanMail *for Microsoft Exchange* 12.5 SP1 installation package directory.
3. Type `Setup /R <config_file_path>` to start recording mode.
4. Type `Setup /S <config_file> /output <result_file>]` to begin silent installation.

Using an Existing Pre-Configured File

The following table displays the parameters you can use to configure silent installation settings.

TABLE 2-1. Silent Installation Setting Parameters

PARAMETER	DESCRIPTION
`Setup /H |Help| ?`	Displays the **Help** screen.
`Setup /R <config_file path>`	Starts recording mode. If the path is empty, the default path is the Windows directory `C:\Windows\temp\setup-silent-config.dat`
`Setup /S <config_file>`	Performs a silent installation with the file name you specify.
`Setup /output <result_file>`	Specifies the result file and name. The default path is the Windows directory `C:\Windows\temp\ScanMail_SilentOutput.txt`

Chapter 3

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 3-2*
- *Contacting Trend Micro on page 3-3*
- *Sending Suspicious Content to Trend Micro on page 3-4*
- *Other Resources on page 3-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

Tip

To submit a support case online, visit the following URL:

http://esupport.trendmicro.com/srf/SRFMain.aspx

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

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

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

Appendix A

Glossary

The following is a list of terms in this document:

TERM	DESCRIPTION
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.
Configuration	Selecting options for how ScanMail will function, for example, selecting whether to quarantine or delete a virus-infected email message.
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
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 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.

TERM	DESCRIPTION
Executable file	A binary file containing a program in machine language which is ready to be executed (run).
Hostname	The unique name composed of ASCII characters, by which a computer is known on a network.
Hot Fixes and Patches	Workaround solutions to customer related problems or newly discovered security vulnerabilities that you can download from the Trend Micro website and deploy to the ScanMail server and/or client program.
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.
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.
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.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application.
Registration key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database.
Remote access tools	Tools used to help hackers remotely access and control a computer.

TERM	DESCRIPTION
Standard maintenance	See Maintenance Agreement
Traffic	Data flowing between the Internet and your network, both incoming and outgoing.
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.

Index

D

documentation feedback, 3-6

I

installations
- silent, 2-2

installation steps, 1-2

installing
- silent installation, 2-3

installing the Patch, 1-2

P

patch
- uninstalling, 1-13

R

removing patch, 1-13

S

screens
- Checking Target Server System Requirements, 1-8
- Installation Complete, 1-12
- Installation Progress, 1-11
- License Agreement, 1-4
- Log on, 1-7
- Review Settings, 1-10
- Select an Action, 1-5
- Select Target Servers, 1-6
- Verifying Windows Authentication Information, 1-9
- Welcome, 1-3

silent installations, 2-2
- limitations, 2-2
- performing, 2-3
- pre-configured files, 2-3
- setting parameters, 2-3

support
- resolve issues faster, 3-4

T

target servers
- servers, 1-7

U

uninstalling patch, 1-13

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: SMEM128278/180524