TREND MICRO™

12.0 ScanMail™ for Microsoft™ Exchange

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 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 website at:

http://docs.trendmicro.com/en-us/enterprise/scanmail-for-microsoft-exchange.aspx

Document Part No. SMEM127297/160113

Release Date: March 2016

Document Version No.: 1.0

Product Name and Version No.: ScanMail™ *for Microsoft*™ *Exchange* 12.0

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

The user documentation for Trend Micro ScanMail *for Microsoft Exchange* 12.0 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 Knowledge Base at Trend Micro 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

Table of Contents

Preface

Chapter 1: Planning ScanMail Installation and Upgrade

Chapter 2: Installing ScanMail with Exchange Server 2013 / 2016

Chapter 3: Upgrading ScanMail with Exchange 2010 Servers

Chapter 4: Performing Post-Installation Tasks

Chapter 5: Silent Installation

Chapter 6: Removing ScanMail

Chapter 7: Contacting Trend Micro

Appendix A: Preconfigured Files

Appendix B: Glossary

Index

Preface

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 vi*
- *Audience on page vi*
- *Document Conventions on page vii*

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

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

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

ScanMail with Exchange Server 2016

The following table lists the system requirements for running ScanMail with Exchange Server 2016.

TABLE 1-1. System Requirements for Installation with Exchange Server 2016

RESOURCE	REQUIREMENTS
Processor	• x64 architecture-based processor that supports Intel™ 64 architecture (formally known as Intel EM64T) • x64 architecture-based computer with AMD™ 64-bit processor that supports AMD64 platform
Memory	1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk space	5GB free disk space
Operating System	• Microsoft™ Windows Server™ 2012 R2 Standard or Datacenter (64-bit) • Microsoft™ Windows Server™ 2012 Standard or Datacenter (64-bit)
Mail Server	Microsoft Exchange Server 2016
Web Server	• Microsoft Internet Information Services (IIS) 8.5 • Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet Information Services (IIS) 7.5
Browser	• Microsoft™ Internet Explorer™ 6.0 or above • Mozilla Firefox™ 3.0 or above

Resource	Requirements
MSXML	4.0 Service Pack 2 or above
.NET framework	4.0 or 4.5

ScanMail with Exchange Server 2013

The following table lists the system requirements for running ScanMail with Exchange Server 2013.

Note

ScanMail v12.0 only supports fresh installation with Exchange Server 2013 SP1 or later Exchange Server versions.

Table 1-2. System Requirements for Installation with Exchange Server 2013

Resource	Requirements
Processor	• x64 architecture-based processor that supports Intel™ 64 architecture (formally known as Intel EM64T) • x64 architecture-based computer with AMD™ 64-bit processor that supports AMD64 platform
Memory	1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk space	5GB free disk space

Resource	Requirements
Operating System	• Microsoft™ Windows Server™ 2012 R2 Standard or Datacenter (64-bit) • Microsoft™ Windows Server™ 2012 Standard or Datacenter (64-bit) • Microsoft™ Windows Server™ 2008 R2 Standard with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 Enterprise with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 Datacenter RTM or above (64-bit)
Mail Server	Microsoft Exchange Server 2013 SP1 or above
Web Server	• Microsoft Internet Information Services (IIS) 8.5 • Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet Information Services (IIS) 7.5
Browser	• Microsoft™ Internet Explorer™ 6.0 or above • Mozilla Firefox™ 3.0 or above
MSXML	4.0 Service Pack 2 or above
.NET framework	4.0 or 4.5

ScanMail with Exchange Server 2010

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

Important

ScanMail only supports upgrade installations from ScanMail 11.0 SP1 for customers using Exchange Server 2010 SP3 or above.

Table 1-3. System Requirements for Installation with Exchange Server 2010

Resource	Requirements
Processor	• x64 architecture-based processor that supports Intel™ 64 architecture (formally known as Intel EM64T) • x64 architecture-based computer with AMD™ 64-bit processor that supports AMD64 platform
Memory	1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk space	5GB free disk space
Operating System	• Microsoft™ Windows Server™ 2012 R2 Standard or Datacenter (64-bit) • Microsoft™ Windows Server™ 2012 Standard or Datacenter (64-bit) • Microsoft Windows Server 2008 R2 or above (64-bit) • Microsoft Windows Server 2008 with Service Pack 2 or above (64-bit) • Microsoft Small Business Server (SBS) 2011 **Note** Microsoft Small Business Server (SBS) 2011 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) 2011.
Mail Server	Microsoft Exchange Server 2010 SP3 or above
Web Server	• Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet Information Services (IIS) 7.5 • Microsoft Internet Information Services (IIS) 7.0

RESOURCE	REQUIREMENTS
Browser	• Microsoft™ Internet Explorer™ 6.0 or above • Mozilla Firefox™ 3.0 or above
MSXML	4.0 Service Pack 2 or above
.NET framework	3.5 Service Pack 1

SQL Server Express Requirements

During an upgrade installation, ensure that you upgrade your current SQL Server Express version as follows before running the setup program:

- SQL Server Express 2005: Upgrade to SQL Server Express 2014 32-bit
- SQL Server Express 2008: Upgrade to SQL Server Express 2014 64-bit

Cluster Installations

The following lists supported cluster environments:

- Exchange Server 2016 with Database Availability Group (DAG) model
- Exchange Server 2013 with Database Availability Group (DAG) model
- Exchange Server 2010 with VERITAS Cluster 5.1 SP2
- Exchange Server 2010 with Database Availability Group (DAG) model

ScanMail Integration with Trend Micro Products

You can optionally integrate ScanMail with other Trend Micro products. The following table outlines the supported products and versions.

TABLE 1-4. Integrated Trend Micro Product Support

TREND MICRO PRODUCT	SUPPORTED VERSIONS
Control Manager™	• 6.0 or above • 5.5 with Service Pack 1 • 5.0 with Patch 7 and Hotfix 2108
Smart Protection Server	• 3.0 • 2.5 • 2.1 • 2.0 • OfficeScan Server Integrated Smart Protection Server
Deep Discovery Advisor	2.92 or later
Deep Discovery Analyzer	5.0

Conducting a Pilot Installation

The following section contains Trend Micro recommendations for installing ScanMail. Read this section before you begin your 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, refer to the following:

- *Step 1: Creating an Appropriate Test Site on page 1-8*
- *Step 2: Preparing a Rollback Plan on page 1-8*
- *Step 3: Executing and Evaluating Your Pilot Installation on page 1-9*

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 website:

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 setup process. This process should take into account local corporate policies, as well as technical specifics.

Backing Up ScanMail Configurations

Before making any changes, back up ScanMail configurations.

Procedure

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.

Restoring ScanMail Configurations

Use the following procedures to restore ScanMail configurations if necessary.

Procedure

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.mdf`, or `Log.mdf`, or `Report.mdf`.
3. Replace the `Conf.mdf`, or `Log.mdf`, or `Report.mdf`.
4. Start SQL Server (SCANMAIL) Service and ScanMail Master Service.

Step 3: Executing and Evaluating Your Pilot Installation

Install and evaluate the pilot based on expectations regarding 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. 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 1-5: Deploying ScanMail with Exchange Server on page 1-11* 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 1-5. Deploying ScanMail with Exchange Server

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.

Server Role	Recommendation
Hub Transport server 2010: • 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.
Mailbox server 2010: • 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.

Server Role	Recommendation
Mailbox server 2013 or 2016: • 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 • 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 the servers to perform real-time security risk scan. • If there is an Edge server, set this 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. • Regularly perform scheduled scans on Exchange mailboxes to prevent security risks from creeping in from unexpected sources not covered in your configurations.

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.

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

TABLE 1-6. Fresh Installation Minimum Privileges

EXCHANGE ROLE	MINIMUM PRIVILEGES
Exchange Server 2013/2016 (Mailbox Server Roles)	Local Administrator and Domain User Exchange Organization Management group
Exchange Server 2010/2013/2016 (Edge Transport Server Roles)	Local Administrator

Exchange Role	Minimum Privileges
Exchange Server 2010 (Hub/Mailbox/ Cluster Roles)	Local Administrator and Domain User Exchange Organization Management group

Configuration Exceptions When You Upgrade

When you upgrade from ScanMail 11.0 with Service Pack 1 to ScanMail 12.0, the Setup program uses your previous settings during installation. However, certain settings are not directly copied to ScanMail 12.0.

Table 1-7. Configuration Exception Settings

Setting	Description
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	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.

Installing without Internet Information Services

ScanMail does not require the installation of Internet Information Services (IIS) on your server. If you do not require the ScanMail management console on your server, you can install ScanMail without the normal IIS requirement.

Procedure

1. Run `cmd.exe`.

2. Navigate to the `Smex` folder and type the following after the command prompt:

   ```
   setup /skipwebconsole
   ```

3. Setup continues to the **Welcome** screen and the installation process proceeds like a normal install. ScanMail does not check for IIS and does not install the management console on this server.

Installing with a Remote SQL Server

ScanMail supports storing the ScanMail database on a remote SQL server with fresh installs on supported versions of Exchange Server. 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 the database on the local SQL Server Express.

Procedure

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 both SQL server accounts and Windows accounts. If you use a Windows account, the account requires the following privileges:

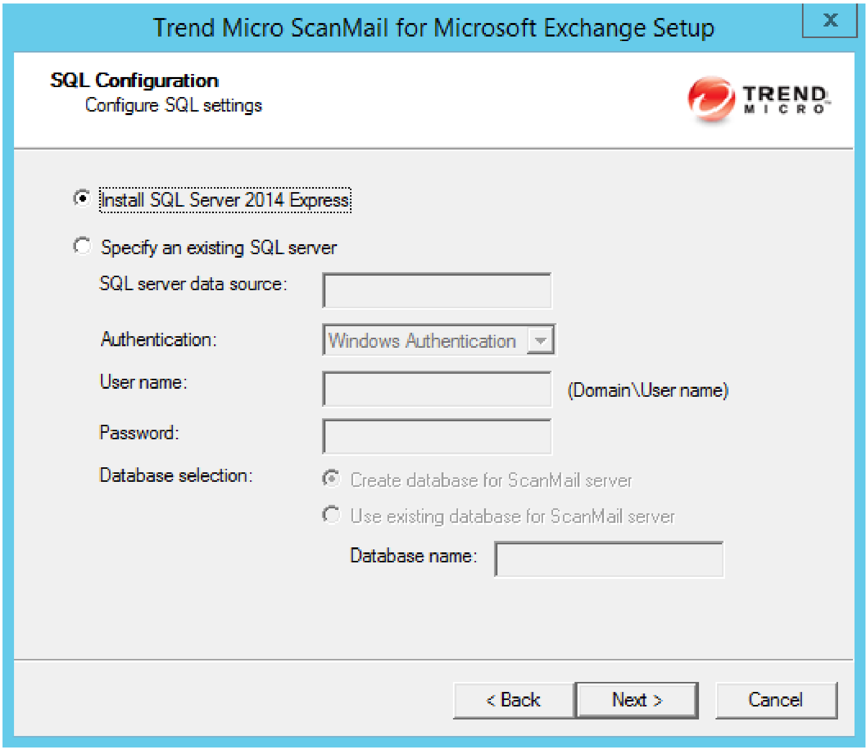
- Local Administrator
- Exchange ApplicationImpersonation role
- Exchange Organization Management group

To activate EUQ during installation, you must enable the domain administrator privileges for the user account. You can disable the domain administrator privileges for the account after completing the installation.

3. During installation type the SQL server data source and SQL or Windows account prepared in Step 2, on **SQL Configuration screen**.

Note

When ScanMail is installed with a remote SQL server and connection to the server is unavailable, ScanMail performs 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 continues to scan messages and stores the log data on the local server. 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 updates the database with the locally stored data.



Trend Micro ScanMail for Microsoft Exchange Setup

SQL Configuration

Configure SQL settings

● Install SQL Server 2014 Express

○ Specify an existing SQL server

SQL server data source:

Authentication: Windows Authentication

User name: (Domain\User name)

Password:

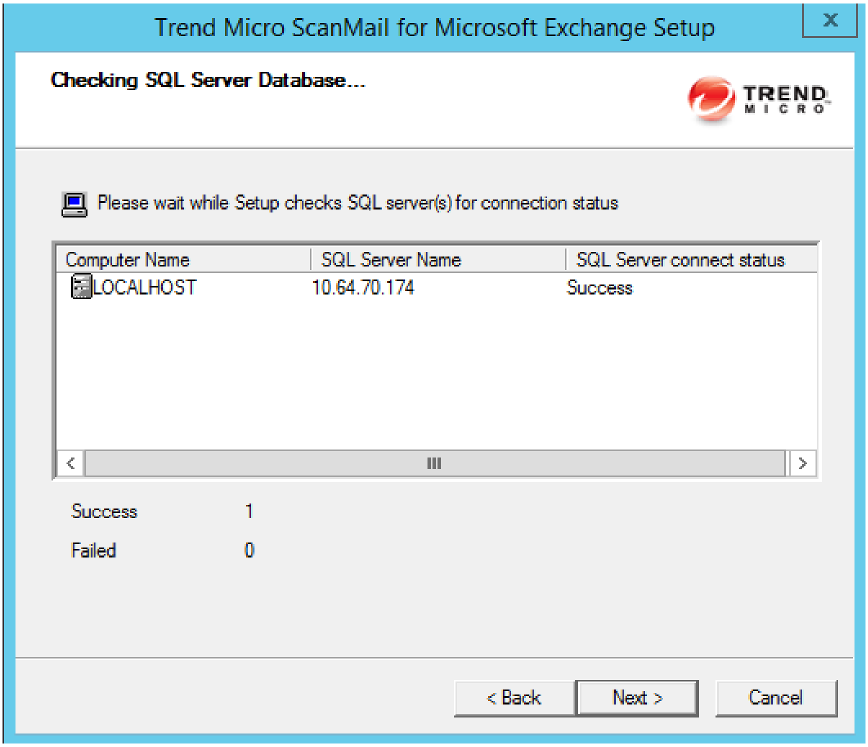
Database selection: ● Create database for ScanMail server

○ Use existing database for ScanMail server

Database name:

4. Click **Next**

The **Check SQL Server Database** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Checking SQL Server Database...

Please wait while Setup checks SQL server(s) for connection status

Computer Name	SQL Server Name	SQL Server connect status
LOCALHOST	10.64.70.174	Success

Success	1
Failed	0

5. Complete the rest of the installation process.

Additional Requirements for Installing Remotely with Windows 2008 and 2012

This only applies to Windows 2008, Windows 2012, and Windows 2012 R2 operating systems when remotely installing multiple Exchange servers.

Prepare the following:

- An account with the following privileges:
  - For Exchange Server 2013 / 2016 Mailbox or Exchange Server 2010 Hub/ Mailbox:
    - Local Administrator
    - Domain User
    - Exchange Organization Management Group
  - Exchange Server 2013, 2016, or 2010 Edge Transport:
    - Local Administrator

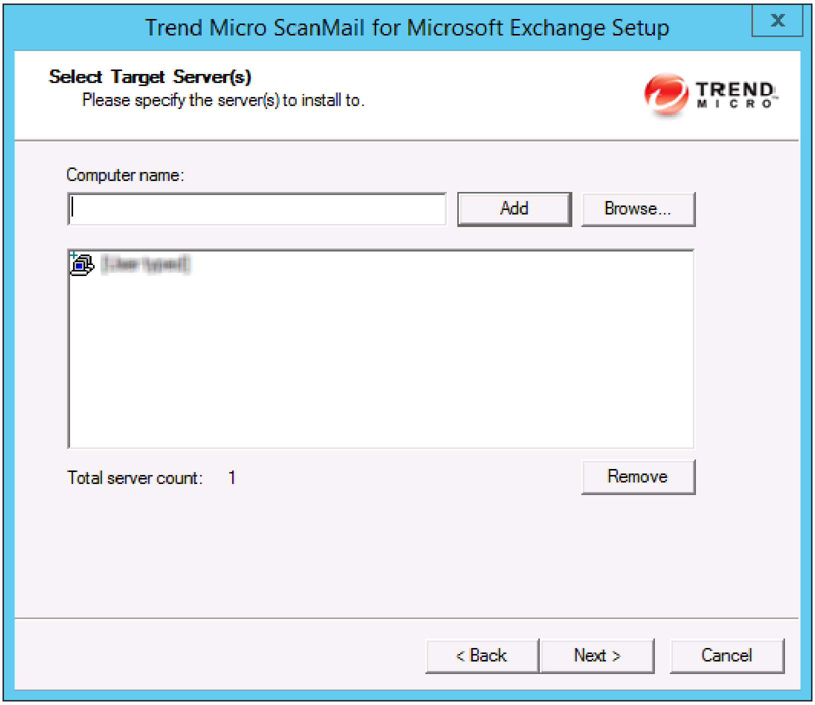
> **Note**
>
> If it is an account with domain user privileges, this account must have local administrator privileges on each Exchange server.

- Enable file sharing on Windows Firewall or disable Windows Firewall on each Exchange server.
- Ensure that administrative shares are available on each Exchange server.

Procedure

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. On 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.



Trend Micro ScanMail for Microsoft Exchange Setup

Select Target Server(s)

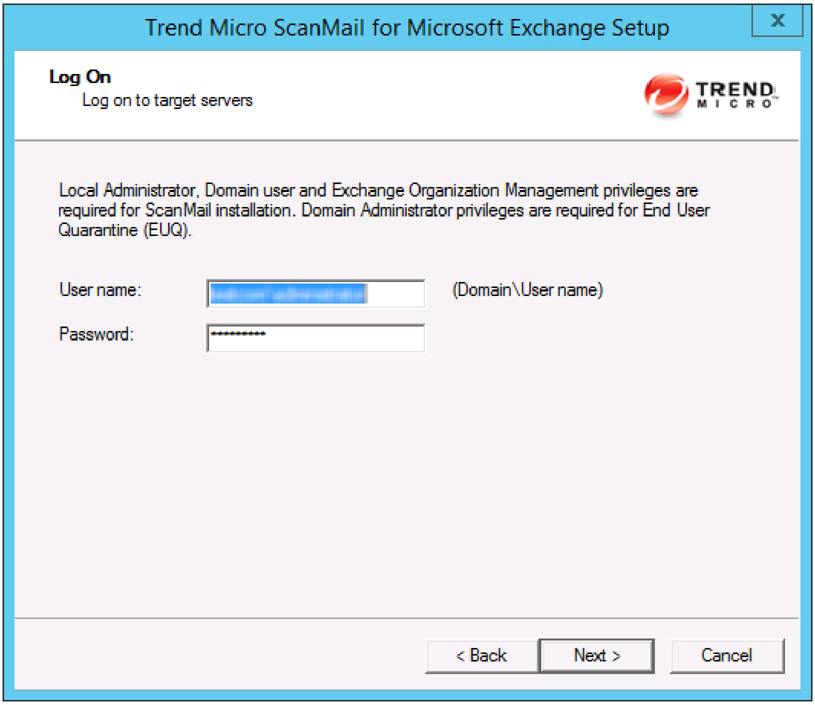
Please specify the server(s) to install to.

Computer name:

[redacted]

Total server count: 1

b. On 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.



Trend Micro ScanMail for Microsoft Exchange Setup

Log On

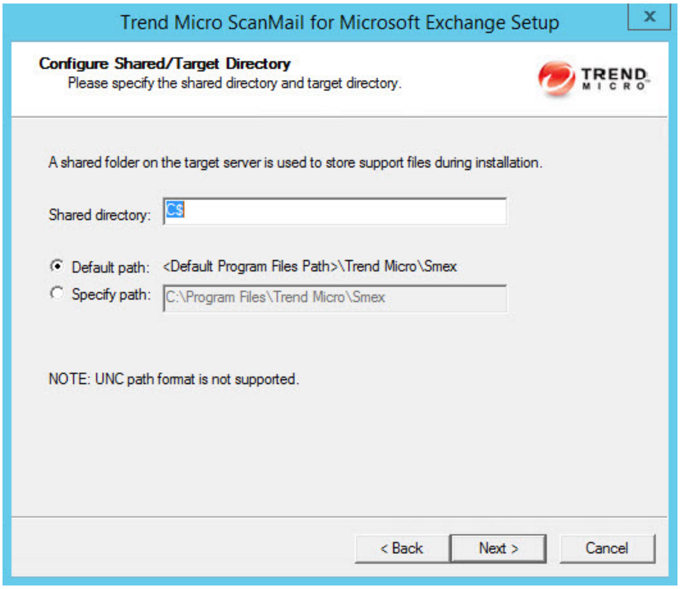
Log on to target servers

Local Administrator, Domain user and Exchange Organization Management privileges are required for ScanMail installation. Domain Administrator privileges are required for End User Quarantine (EUQ).

User name: [redacted] (Domain\User name)

Password: **********

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



Trend Micro ScanMail for Microsoft Exchange Setup

Configure Shared/Target Directory

Please specify the shared directory and target directory.

A shared folder on the target server is used to store support files during installation.

Shared directory: C$

● Default path: <Default Program Files Path>\Trend Micro\Smex

○ Specify path: C:\Program Files\Trend Micro\Smex

NOTE: UNC path format is not supported.

3. Complete the rest of the installation process.

Pre-installation Checklist

The following table outlines important items to note before proceeding with a ScanMail installation.

TABLE 1-8. Pre-installation Checklist

ITEM	NOTES
Minimum account privileges	• For Exchange Hub / Mailbox you need Local Administrator and Exchange Organization Management Group privileges. However, you need to activate End User Quarantine later with an account with Domain Administrator privileges • For Exchange Server Edge Transport you need Local Administrator privileges.
Restart	You do not need to stop Exchange services before installing or restart them after a successful installation.
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 website. The Setup program provides a link to the Trend Micro website. 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, 2012, and 2012 R2, 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**.
SQL Server Express	During an upgrade installation, ensure that you upgrade your current SQL Server Express version to 2014 or later.

About Fresh Installations

Perform a fresh installation to install ScanMail for the first time. Before beginning your installation, consult the pre-installation checklist (*Pre-installation Checklist on page 1-23*).

Note

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

About Upgrading to ScanMail 12.0

Before beginning your installation, consult the pre-installation checklist (*Table 1-8: Pre-installation Checklist on page 1-24*). To upgrade ScanMail, run the Setup program.

ScanMail 12.0 supports upgrading from the following previous versions:

- ScanMail 11.0 with Service Pack 1

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 12.0 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.

About Cluster Installations

Cluster Installation for Exchange Server 2010, 2013, and 2016

Installing ScanMail on Exchange 2010, 2013, or 2016 clusters with DAG is the same as installing on a normal server. ScanMail does not automatically install on all the DAG or VERITAS cluster nodes. ScanMail will only install on the nodes that you configure on the **Select Target Servers** screen. Manually add all the nodes of the DAG cluster to the target server on the **Select Target Server** screen during installation.

Chapter 2

Installing ScanMail with Exchange Server 2013 / 2016

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

Topics in this chapter:

Privileges Requirements

The following table displays the privileges required for installing ScanMail on Exchange 2013/2016 with mailbox role.

TABLE 2-1. Privileges Required for Installing ScanMail on Exchange 2013/2016 with Mailbox Role

SCANMAIL DATABASE OPTION	SETUP ACCOUNT PRIVILEGES	DATABASE ACCESS ACCOUNT PRIVILEGES
Local database	• Local Administrator • Domain User • Exchange Organization Management group Activate End User Quarantine setup account should be the Domain Administrator account.	N/A
Remote SQL Server with SQL Windows Authentication	• Local Administrator • Domain User • Exchange Organization Management Group Activate End User Quarantine setup account should be promoted as Domain Administrator temporarily during installation.	dbcreator role plus the following privileges: • Local Admin • Exchange Organization Management Group • Exchange Application Impersonation role Activate End User Quarantine database access account should be promoted as Domain Administrator temporarily during installation.

ScanMail Database Option	Setup Account Privileges	Database Access Account Privileges
Remote SQL Server with SQL Server Authentication	• Local Administrator • Domain User • Exchange Organization Management Group Activate End User Quarantine setup account should be the Domain Administrator.	dbcreator role

Note

If you use Remote SQL Server with SQL Windows Authentication option, it is a best practice to use the same domain account for Setup Account and Database Access Account.

Installing with Exchange Server 2013/2016

The following lists the steps to install ScanMail with Exchange Server 2013/2016 Mailbox and Edge Servers.

Procedure

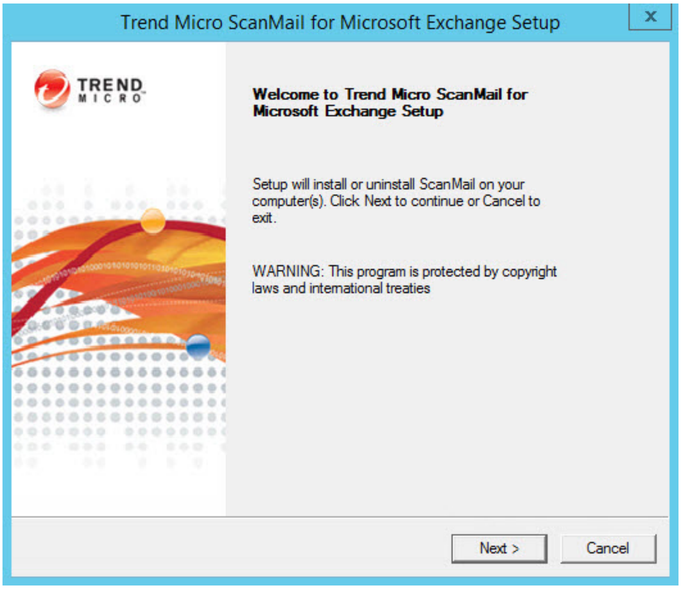
1. Obtain the Setup program:

    a. Download ScanMail from the Trend Micro website.

    b. Unzip the file to a temporary directory.

    c. Run `setup.exe` to install ScanMail.

The **Welcome to Trend Micro ScanMail for Microsoft Exchange Setup** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

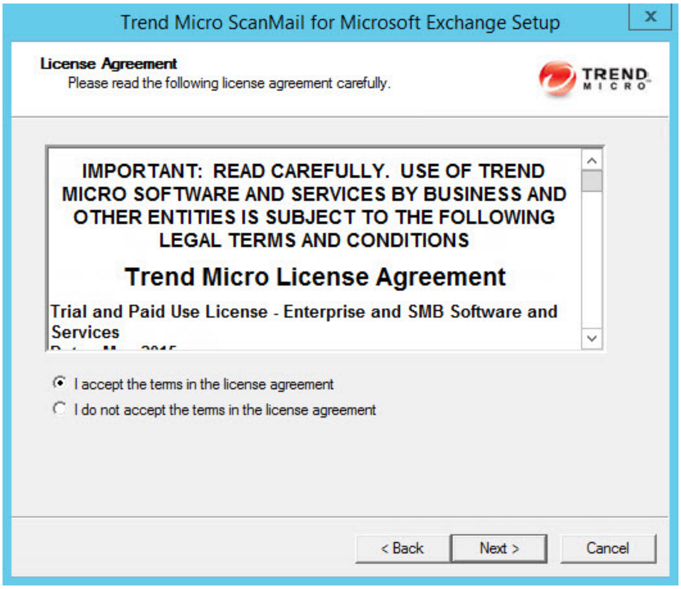
Welcome to Trend Micro ScanMail for Microsoft Exchange Setup

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

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

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

The **License Agreement** screen appears.



License Agreement

Please read the following license agreement carefully.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

● I accept the terms in the license agreement

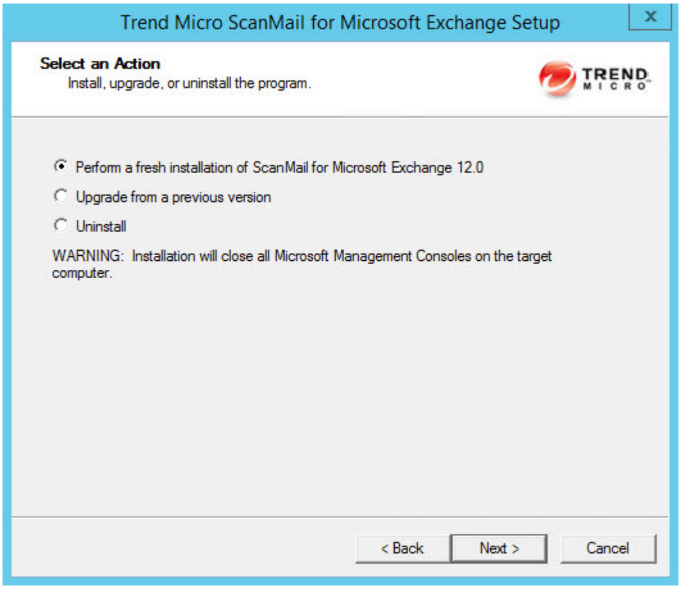
○ I do not accept the terms in the license agreement

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.



Trend Micro ScanMail for Microsoft Exchange Setup

Select an Action

Install, upgrade, or uninstall the program.

● Perform a fresh installation of ScanMail for Microsoft Exchange 12.0

○ Upgrade from a previous version

○ Uninstall

WARNING: Installation will close all Microsoft Management Consoles on the target computer.

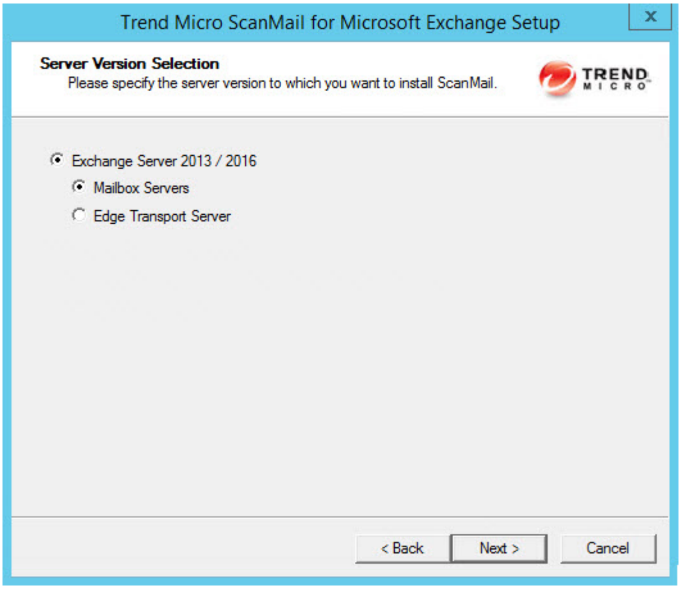
4. Select an action.

   a. Select **Perform a fresh installation of ScanMail for Microsoft Exchange 12.0** to perform a fresh install.

   b. Select **Upgrade from a previous version** to upgrade an existing version of ScanMail. For more information about upgrading, see *About Upgrading to ScanMail 12.0 on page 1-25*.

   c. Click **Next** to continue.

The **Server Version Selection** screen appears.


Trend Micro ScanMail for Microsoft Exchange Setup

Server Version Selection

Please specify the server version to which you want to install ScanMail.

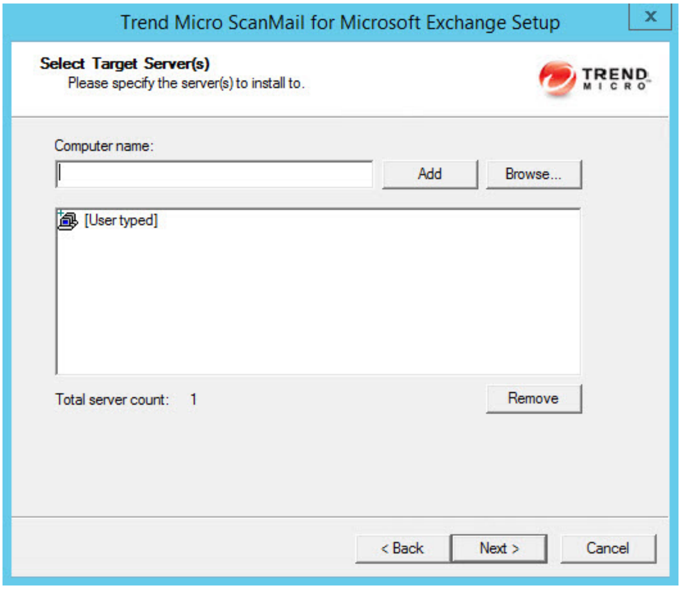
● Exchange Server 2013 / 2016

● Mailbox Servers

○ Edge Transport Server

5. Select the type of **Exchange Server 2013 / 2016** you want to install ScanMail on (**Mailbox Servers** or **Edge Transport Server**) and click **Next** to continue.

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



Trend Micro ScanMail for Microsoft Exchange Setup

Select Target Server(s)

Please specify the server(s) to install to.

Computer name:

[User typed]

Total server count: 1

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

   a. Perform one of the following:

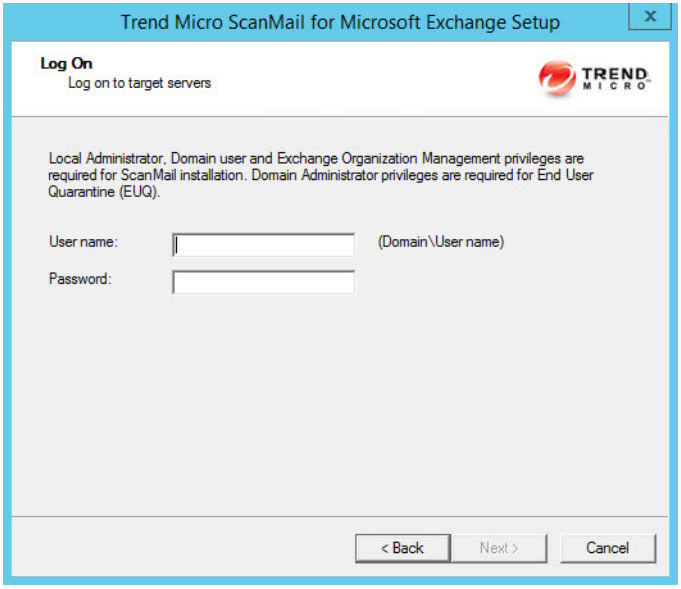
      - Type the name of the server to which you want to install in the **Computer name** field and click **Add** to add the computers to the list of servers.

      - 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.



Trend Micro ScanMail for Microsoft Exchange Setup

Log On

Log on to target servers

Local Administrator, Domain user and Exchange Organization Management privileges are required for ScanMail installation. Domain Administrator privileges are required for End User Quarantine (EUQ).

User name: (Domain\User name)

Password:

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.

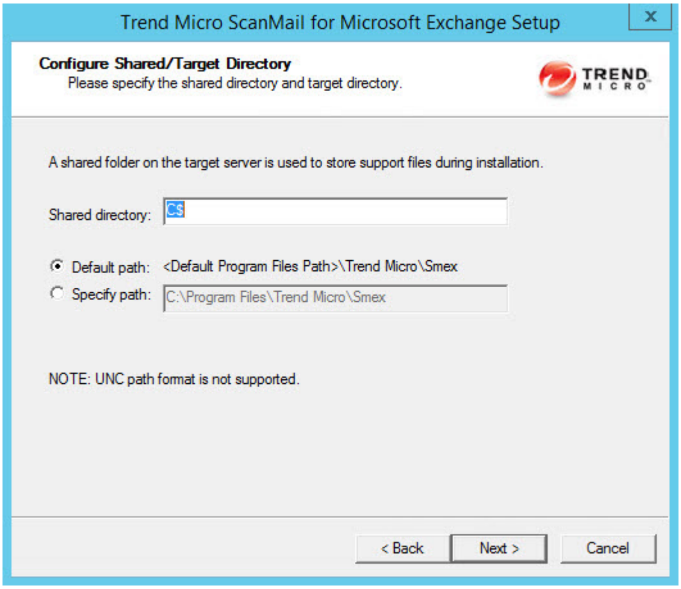
7. Log on to the target servers where you want to install ScanMail. Type the user name and password to log on to the target server to install ScanMail. Click **Next** to continue.

Note

Depending on the Exchange server role, ScanMail requires the following privileges:

- Mailbox Server: Local Administrator, Domain end user and Exchange Organization Management
- Edge Transport Server: Local Administrator

The **Configure Shared/Target Directory** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Configure Shared/Target Directory

Please specify the shared directory and target directory.

A shared folder on the target server is used to store support files during installation.

Shared directory: C$

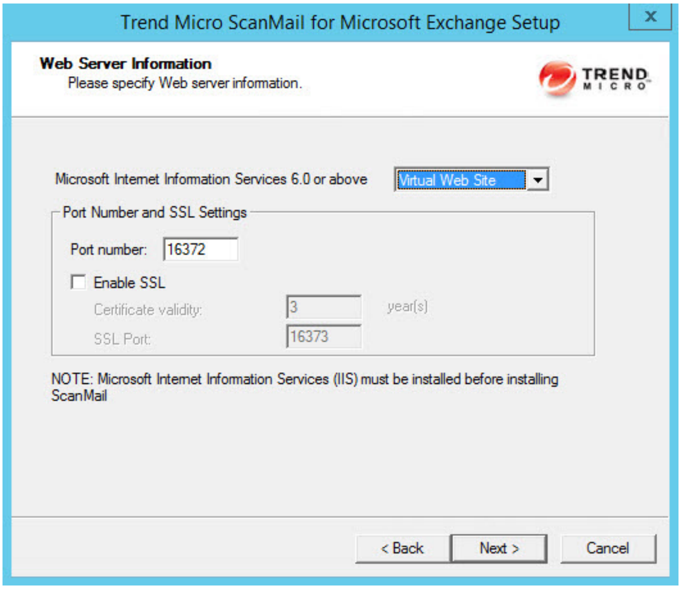
● Default path: <Default Program Files Path>\Trend Micro\Smex

○ Specify path: C:\Program Files\Trend Micro\Smex

NOTE: UNC path format is not supported.

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 **Specify path** and type the directory path on the target server where you will install ScanMail. Click **Next** to continue.

The **Web Server Information** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Web Server Information

Please specify Web server information.

Microsoft Internet Information Services 6.0 or above: Virtual Web Site

Port Number and SSL Settings

Port number: 16372

☐ Enable SSL

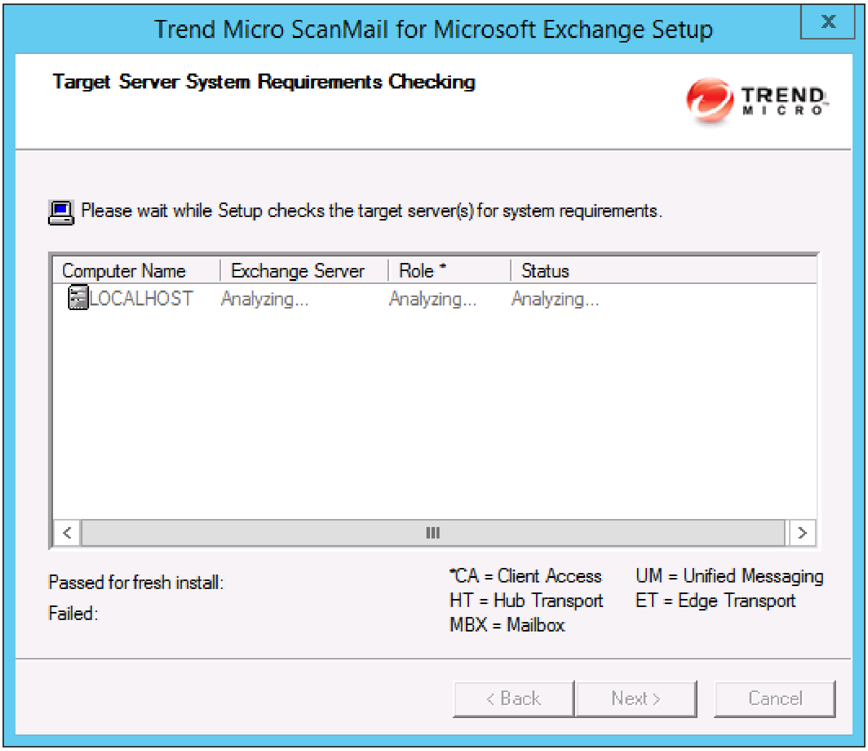
Certificate validity: 3 year(s)

SSL Port: 16373

NOTE: Microsoft Internet Information Services (IIS) must be installed before installing ScanMail

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



Trend Micro ScanMail for Microsoft Exchange Setup

Target Server System Requirements Checking

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

Computer Name	Exchange Server	Role *	Status
LOCALHOST	Analyzing...	Analyzing...	Analyzing...

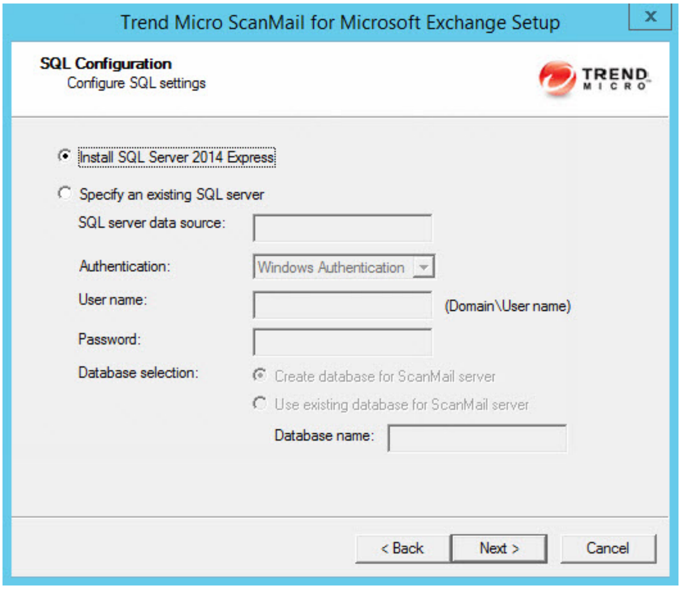
Passed for fresh install:

Failed:

*CA = Client Access
HT = Hub Transport
MBX = Mailbox
UM = Unified Messaging
ET = Edge Transport

10. Review the settings. Click **Next**.

The **SQL Configuration** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

SQL Configuration
Configure SQL settings

● Install SQL Server 2014 Express

○ Specify an existing SQL server

SQL server data source:

Authentication: Windows Authentication

User name: (Domain\User name)

Password:

Database selection: ● Create database for ScanMail server
○ Use existing database for ScanMail server

Database name:

11. Select one of the following:

    - Select **Install SQL Server 2014 Express** to install SQL Server 2014 Express on the local computer.

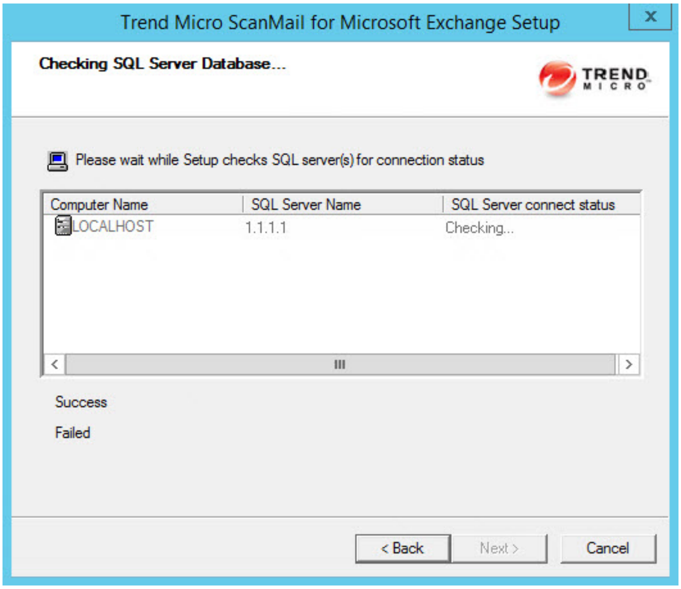
    - Select **Specify an existing SQL server** to use an existing database server. Type the SQL server data source, user name, and password.

    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.

12. Click **Next**.

The **Checking SQL Server Database** screen appears.



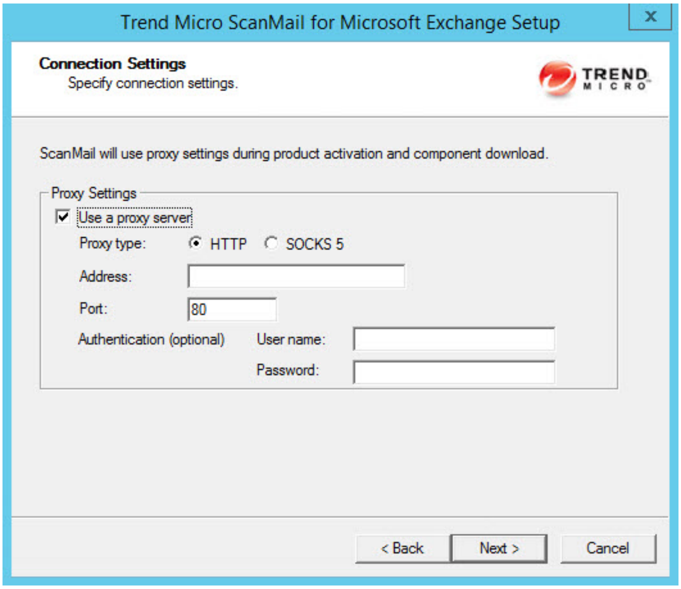
Checking SQL Server Database...

Please wait while Setup checks SQL server(s) for connection status

Computer Name	SQL Server Name	SQL Server connect status
LOCALHOST	1.1.1.1	Checking...

13. Click **Next** to continue.

The **Connection Settings** screen appears.



Connection Settings
Specify connection settings.

ScanMail will use proxy settings during product activation and component download.

Proxy Settings

☑ Use a proxy server

Proxy type: ● HTTP ○ SOCKS 5

Address:

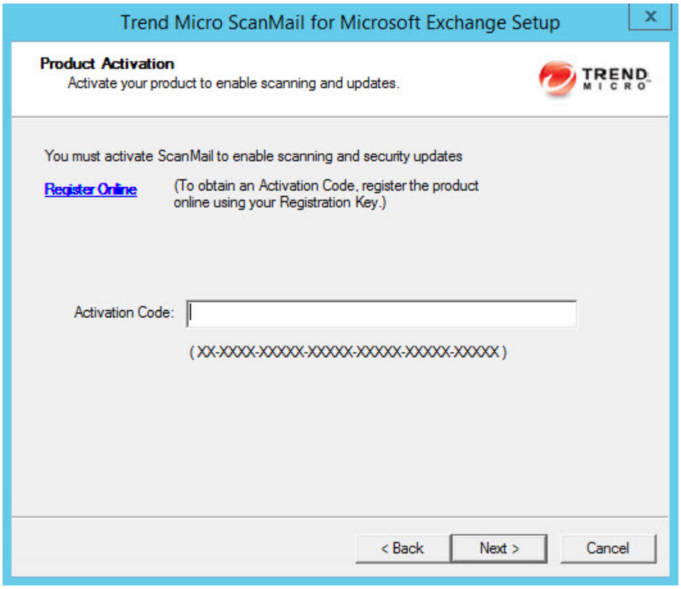
Port: 80

Authentication (optional) User name:

Password:

14. If a proxy server handles Internet traffic on your network, select **Use a proxy server** 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 **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.



Product Activation

Activate your product to enable scanning and updates.

You must activate ScanMail to enable scanning and security updates

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

Activation Code:

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

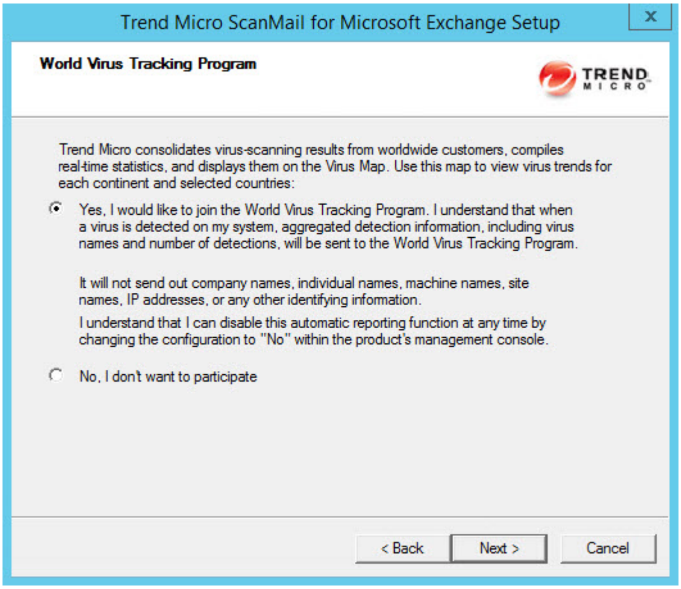
15. Type the activation code.

Note

You can copy an Activation Code and paste it in the input field of the Activation Code on this screen.

16. Click **Next**.

The **World Virus Tracking Program** screen appears.



World Virus Tracking Program

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

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

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

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

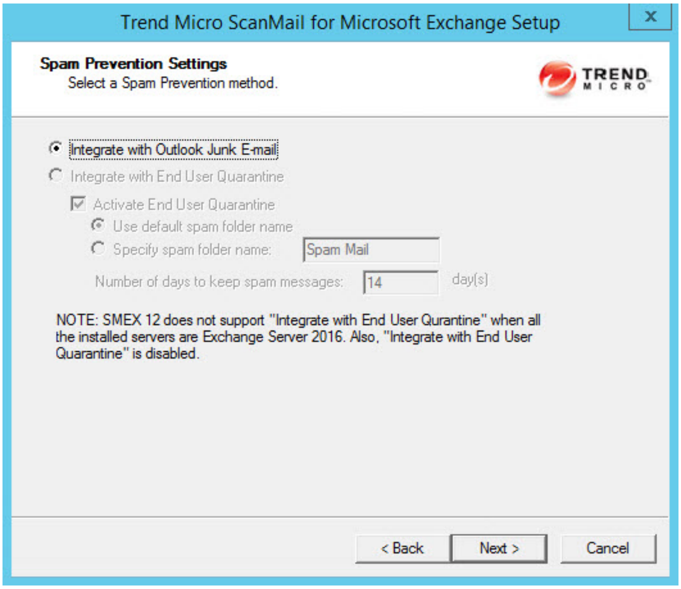
○ No, I don't want to participate

17. Read the statement and click **Yes** to enroll. If you decline to participate, you can still proceed with the installation. Click **Next** to continue.

    - During a fresh installation, the **Spam Prevention Settings** screen appears.

    - During an upgrade installation, the **Control Manager Server Settings** screen appears.

18. For upgrade installations, skip to step 17. On the **Spam Prevention Settings** screen, perform the following tasks:



Trend Micro ScanMail for Microsoft Exchange Setup

Spam Prevention Settings

Select a Spam Prevention method.

● Integrate with Outlook Junk E-mail

○ Integrate with End User Quarantine

☑ Activate End User Quarantine

● Use default spam folder name

○ Specify spam folder name: Spam Mail

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

NOTE: SMEX 12 does not support "Integrate with End User Qurantine" when all the installed servers are Exchange Server 2016. Also, "Integrate with End User Quarantine" is disabled.

a. Select one of the following folder options for storing ScanMail detected spam messages:

Tip

Trend Micro recommends that administrators who want to use the End User Quarantine feature activate the feature during installation. Trend Micro does not recommend using End User Quarantine in the following environments:

- The Exchange Mailbox server role is installed on a domain controller
- The Exchange Client Access server role is installed on a domain controller (even if the Mailbox server role is installed on a member server)

- 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.

Important

End User Quarantine is not supported on Exchange Server 2016.

i. Select **Activate End User Quarantine** to create the spam folder during the installation process.

ii. Select to use the default spam folder name or specify a new name for the spam folder.

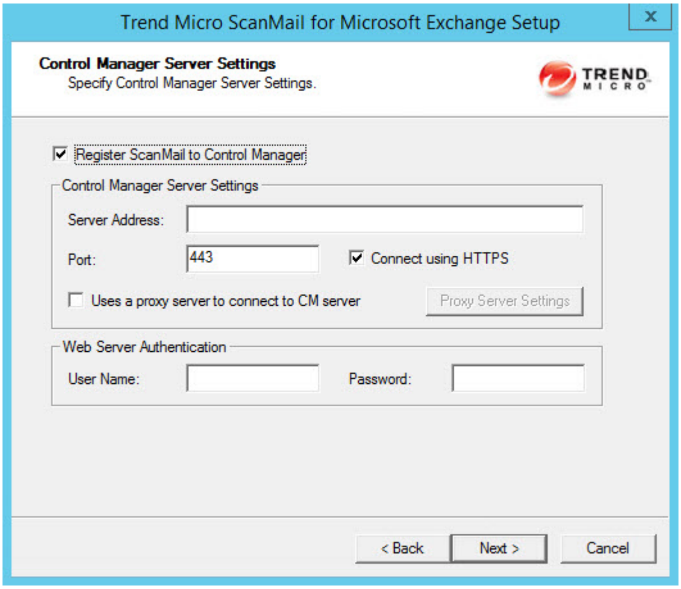
iii. Specify the **Number of days to keep spam messages**.

b. Click **Next** to continue.

Note

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

The **Control Manager Server Settings** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Control Manager Server Settings

Specify Control Manager Server Settings.

☑ Register ScanMail to Control Manager

Control Manager Server Settings

Server Address:

Port: 443 ☑ Connect using HTTPS

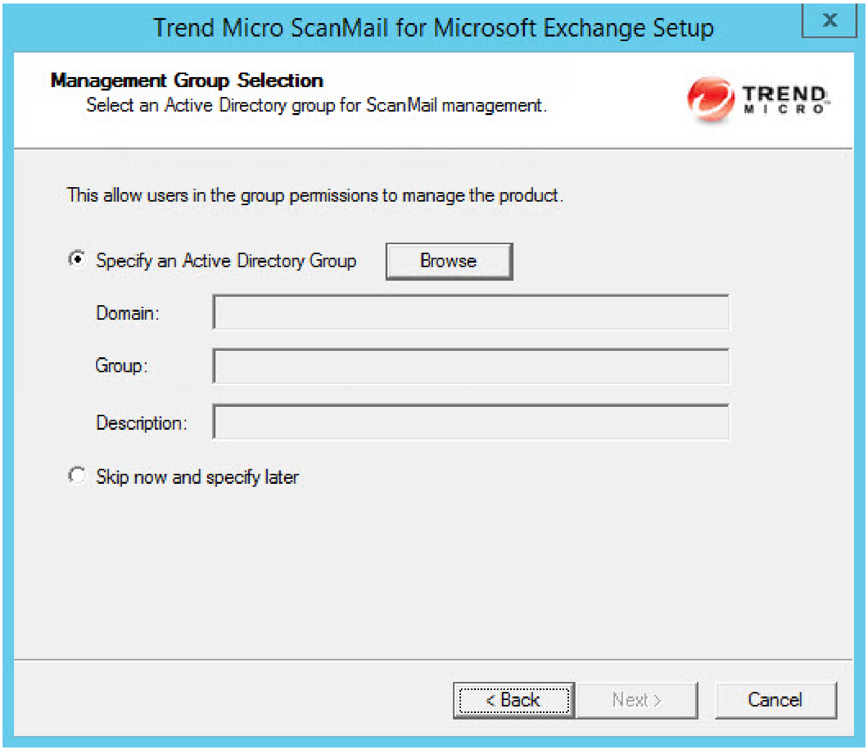
□ Uses a proxy server to connect to CM server

Web Server Authentication

User Name: Password:

19. Specify the Control Manager server settings and specify the proxy server settings if you use a proxy server between your ScanMail server and Control Manager server. Click **Next** to continue.

    The **Management Group Selection** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Management Group Selection

Select an Active Directory group for ScanMail management.

This allow users in the group permissions to manage the product.

● Specify an Active Directory Group

Domain:

Group:

Description:

○ Skip now and specify later

20. On the **Management Group Selection** screen:

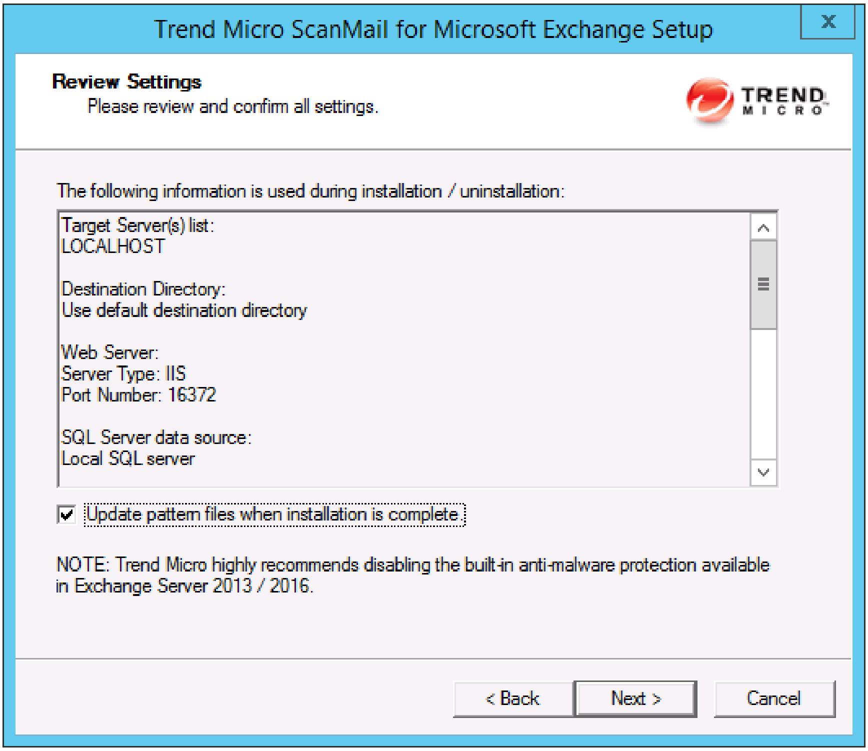
    a. Configure an Active Directory Group to have ScanMail management privileges by:

       - Clicking **Specify an Active Directory Group.**

       - Selecting **Skip now and specify later** to configure this feature after installation.

b. Click **Next** to continue.

The **Review Settings** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Review Settings

Please review and confirm all settings.

The following information is used during installation / uninstallation:

Target Server(s) list:
LOCALHOST

Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

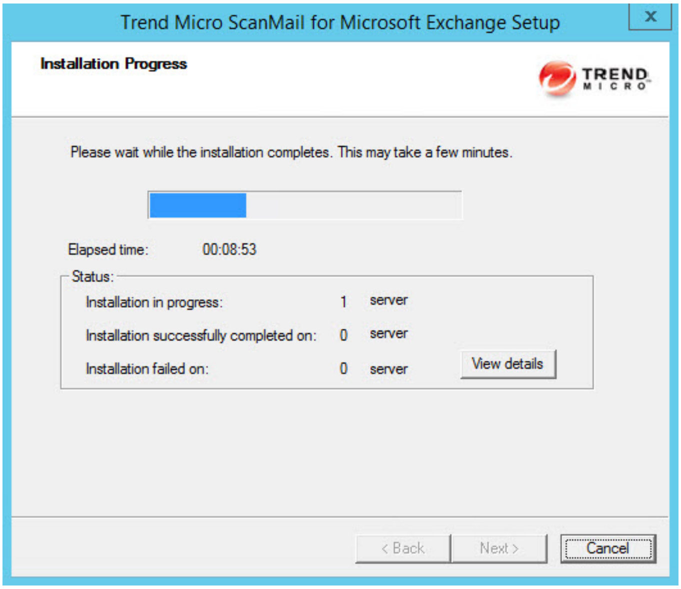
SQL Server data source:
Local SQL server

☑ Update pattern files when installation is complete

NOTE: Trend Micro highly recommends disabling the built-in anti-malware protection available in Exchange Server 2013 / 2016.

21. 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.



Please wait while the installation completes. This may take a few minutes.

Elapsed time: 00:08:53

Status:

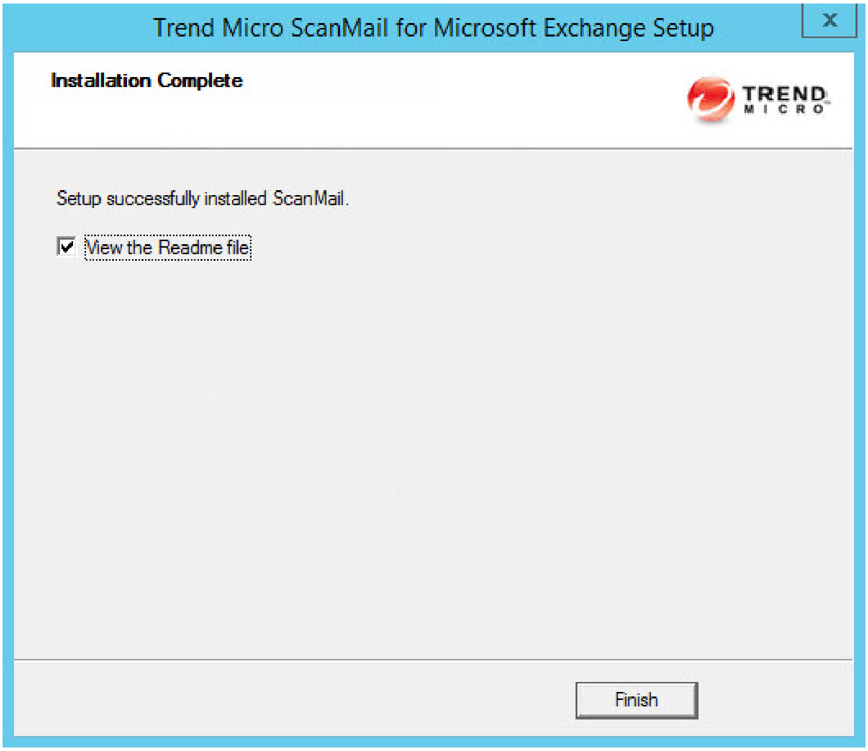
Installation in progress: 1 server

Installation successfully completed on: 0 server

Installation failed on: 0 server

22. Click **View details** to display a list of each computer to which you are installing ScanMail and the status of each computer. Click **Next** when the installation completes.

The **Installation Complete** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Installation Complete

Setup successfully installed ScanMail.

☑ View the Readme file

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

Chapter 3

Upgrading ScanMail with Exchange 2010 Servers

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

Topics in this chapter:

Upgrading Scan Mail on Exchange 2010 Servers

The following lists the steps to install ScanMail with Exchange Server 2010.

Procedure

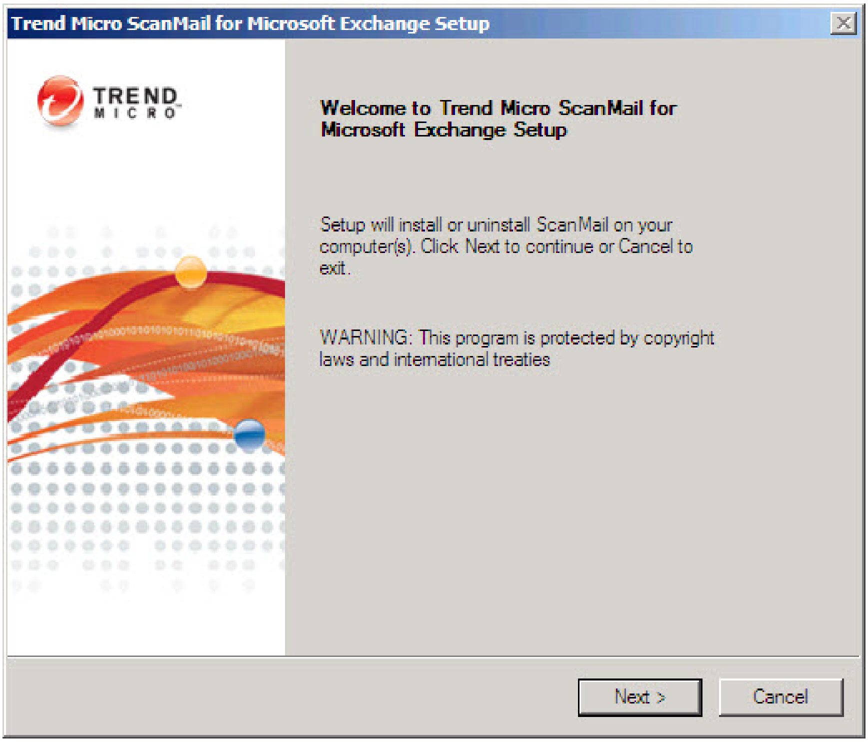
1. Obtain the Setup program:

   a. Download ScanMail from the Trend Micro website.

   b. Unzip the file to a temporary directory.

   c. Run `setup.exe` to install ScanMail.

The **Welcome to Trend Micro ScanMail for Microsoft Exchange Setup** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

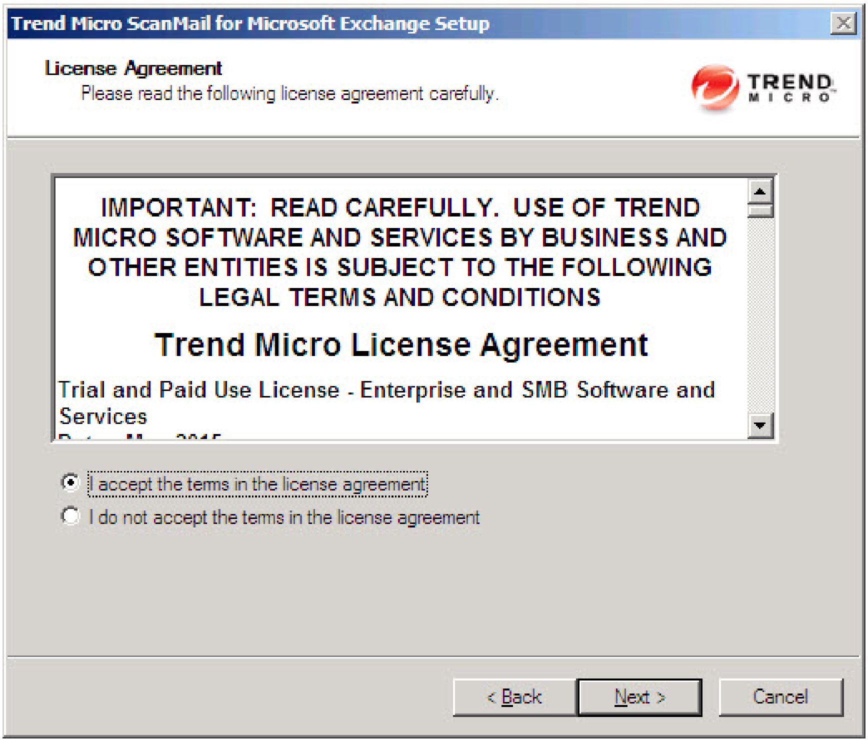
Welcome to Trend Micro ScanMail for Microsoft Exchange Setup

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

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

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

The **License Agreement** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

License Agreement

Please read the following license agreement carefully.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

● I accept the terms in the license agreement

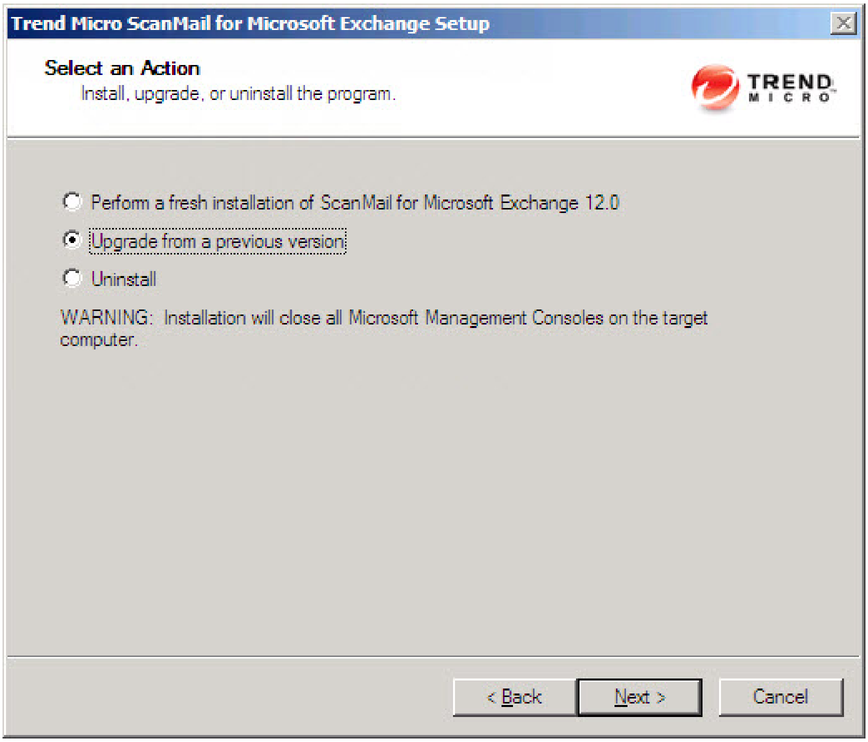
○ I do not accept the terms in the license agreement

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.



Trend Micro ScanMail for Microsoft Exchange Setup

Select an Action

Install, upgrade, or uninstall the program.

○ Perform a fresh installation of ScanMail for Microsoft Exchange 12.0

● Upgrade from a previous version

○ Uninstall

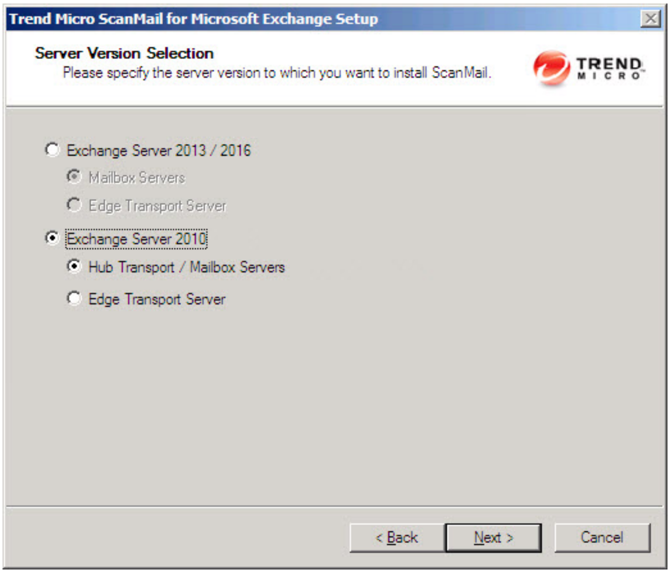
WARNING: Installation will close all Microsoft Management Consoles on the target computer.

4. Select an action.

   a. Select **Upgrade from a previous version** to upgrade an existing version of ScanMail. For more information about upgrading, see *About Upgrading to ScanMail 12.0 on page 1-25*.

   b. Click **Next** to continue.

The **Server Version Selection** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Server Version Selection

Please specify the server version to which you want to install ScanMail.

○ Exchange Server 2013 / 2016

● Mailbox Servers

○ Edge Transport Server

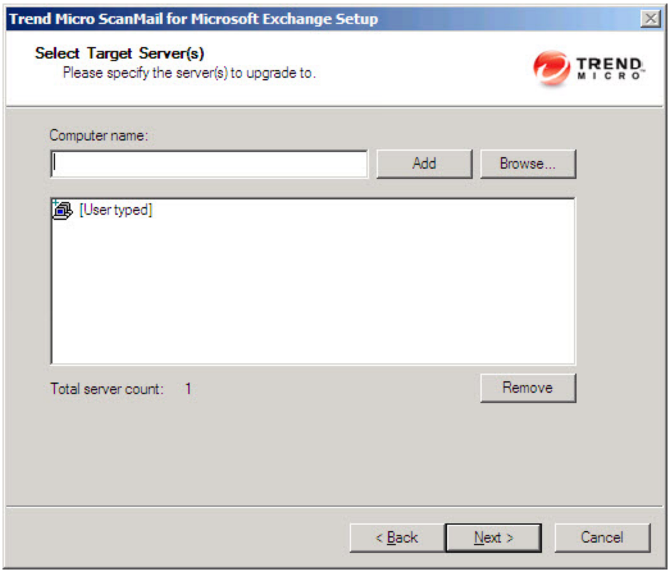
● Exchange Server 2010

● Hub Transport / Mailbox Servers

○ Edge Transport Server

5. Select **Exchange Server 2010** and specify **Hub Transport / Mailbox Servers** or **Edge Transport Server** to upgrade ScanMail. Click **Next** to continue.

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



Trend Micro ScanMail for Microsoft Exchange Setup

Select Target Server(s)

Please specify the server(s) to upgrade to.

Computer name:

[User typed]

Total server count: 1

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

   a. Perform one of the following:

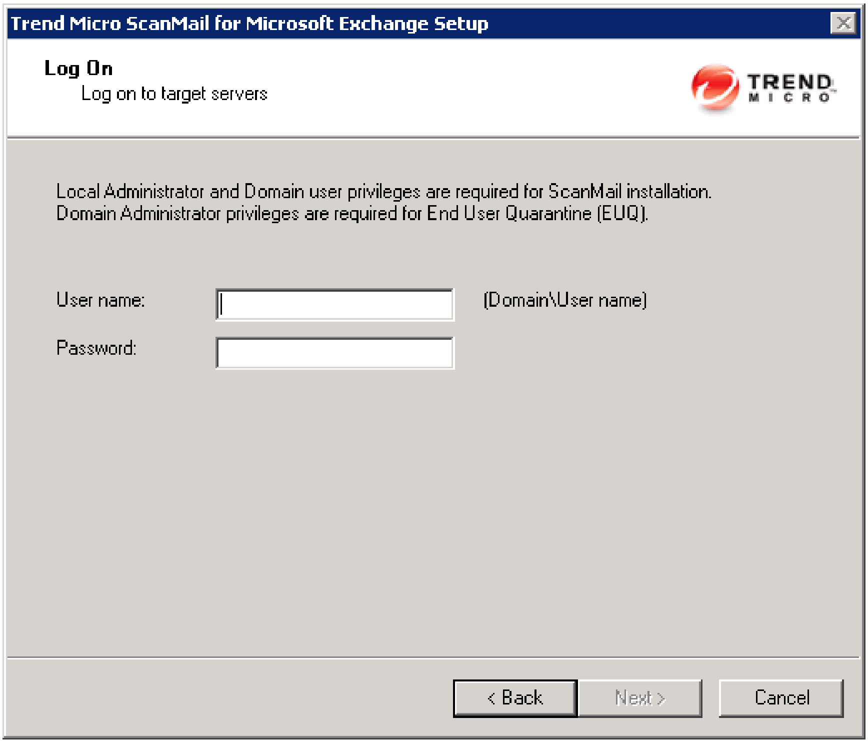
      - Type the name of the server to which you want to install in the **Computer name** field and click **Add** to add the computers to the list of servers.

      - 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.


Trend Micro ScanMail for Microsoft Exchange Setup

Log On

Log on to target servers

Local Administrator and Domain user privileges are required for ScanMail installation.
Domain Administrator privileges are required for End User Quarantine (EUQ).

User name: (Domain\User name)

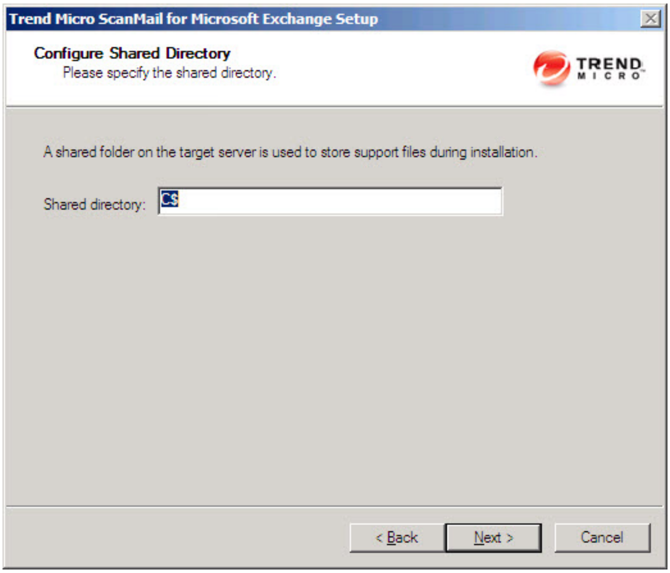
Password:

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.



Trend Micro ScanMail for Microsoft Exchange Setup

Configure Shared Directory

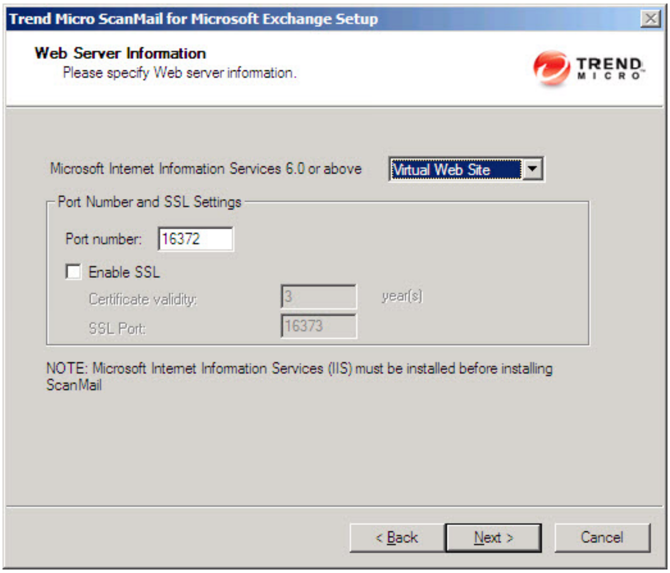
Please specify the shared directory.

A shared folder on the target server is used to store support files during installation.

Shared directory: C$

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 **Specify path** and type the directory path on the target server where you will install ScanMail. Click **Next** to continue.

The **Web Server Information** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Web Server Information

Please specify Web server information.

Microsoft Internet Information Services 6.0 or above: Virtual Web Site

Port Number and SSL Settings

Port number: 16372

☐ Enable SSL

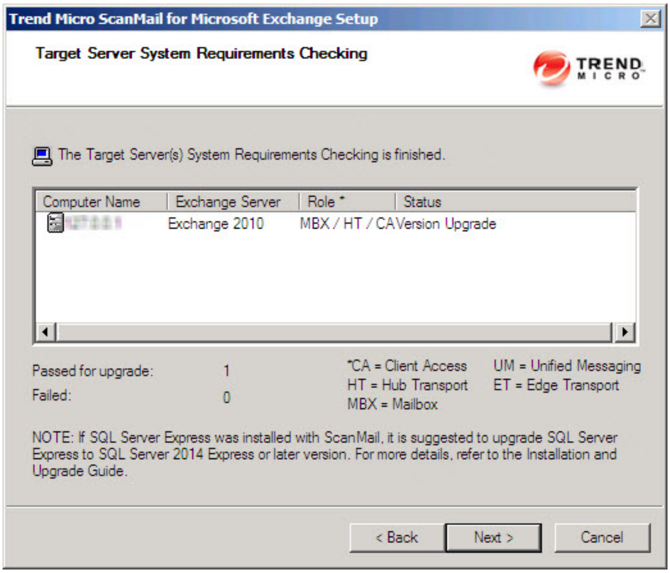
Certificate validity: 3 year(s)

SSL Port: 16373

NOTE: Microsoft Internet Information Services (IIS) must be installed before installing ScanMail

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



Trend Micro ScanMail for Microsoft Exchange Setup

Target Server System Requirements Checking

The Target Server(s) System Requirements Checking is finished.

Computer Name	Exchange Server	Role *	Status
[redacted]	Exchange 2010	MBX / HT / CA	Version Upgrade

Passed for upgrade: 1

Failed: 0

*CA = Client Access
HT = Hub Transport
MBX = Mailbox
UM = Unified Messaging
ET = Edge Transport

NOTE: If SQL Server Express was installed with ScanMail, it is suggested to upgrade SQL Server Express to SQL Server 2014 Express or later version. For more details, refer to the Installation and Upgrade Guide.

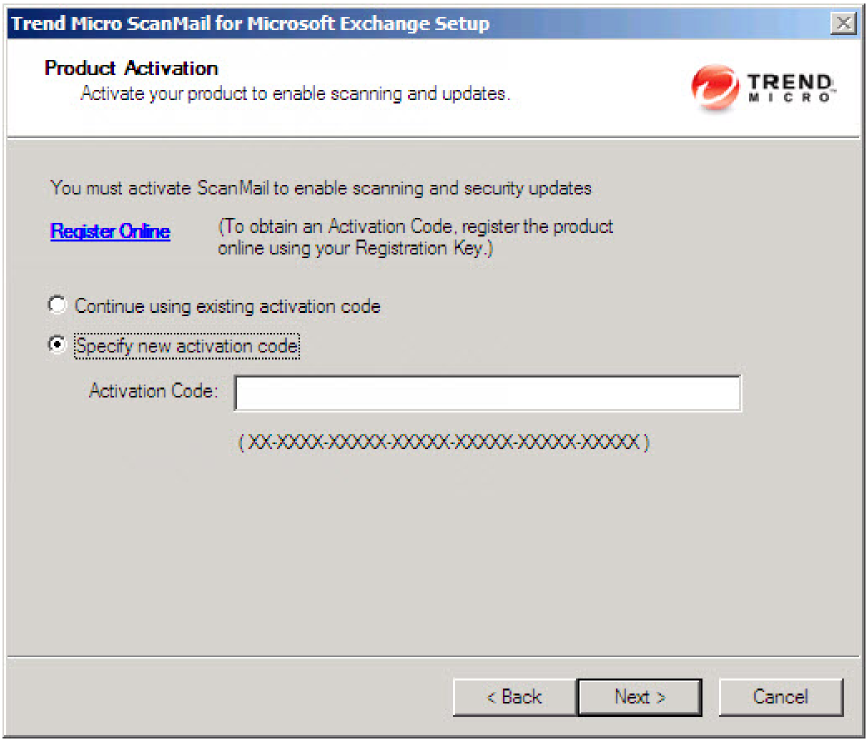
10. Review the settings.

Note

Trend Micro recommends upgrading SQL Server Express to version 2014 on the ScanMail 11.0 SP1 server being upgraded.

11. Click **Next** to continue.

The **Product Activation** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Product Activation

Activate your product to enable scanning and updates.

You must activate ScanMail to enable scanning and security updates

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

○ Continue using existing activation code

● Specify new activation code

Activation Code:

(XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

12. Perform one of the following options:

    - Select **Continue using existing activation code**.

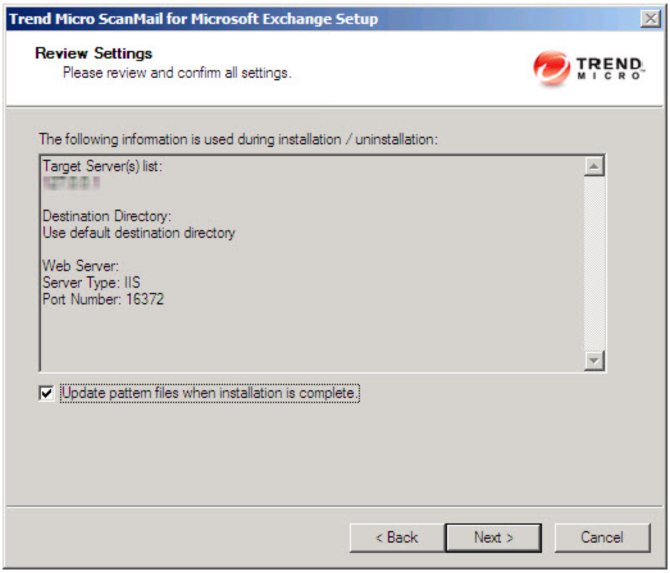
    - Select **Specify new activation code**. Type the activation code.

Note

You can copy an Activation Code and paste it in the input field of the Activation Code on this screen.

13. Click **Next**.

The **Review Settings** screen appears.



Review Settings

Please review and confirm all settings.

The following information is used during installation / uninstallation:

Target Server(s) list:
[redacted]

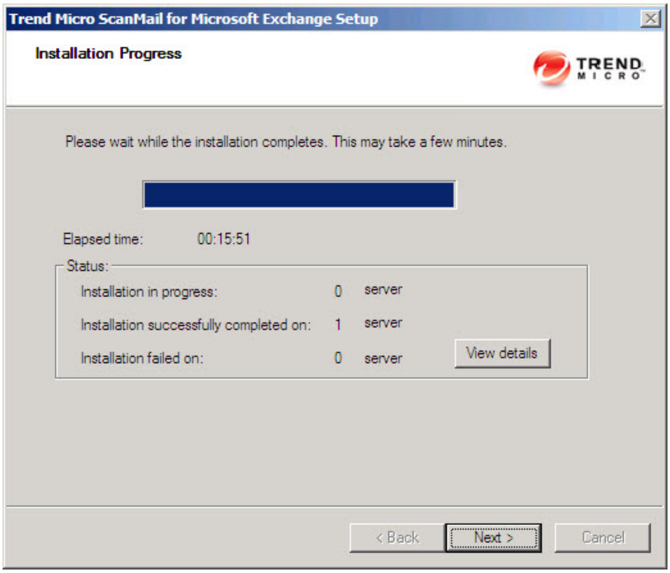
Destination Directory:
Use default destination directory

Web Server:
Server Type: IIS
Port Number: 16372

☑ Update pattern files when installation is complete.

14. 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.



Please wait while the installation completes. This may take a few minutes.

Elapsed time: 00:15:51

Status:

Installation in progress: 0 server

Installation successfully completed on: 1 server

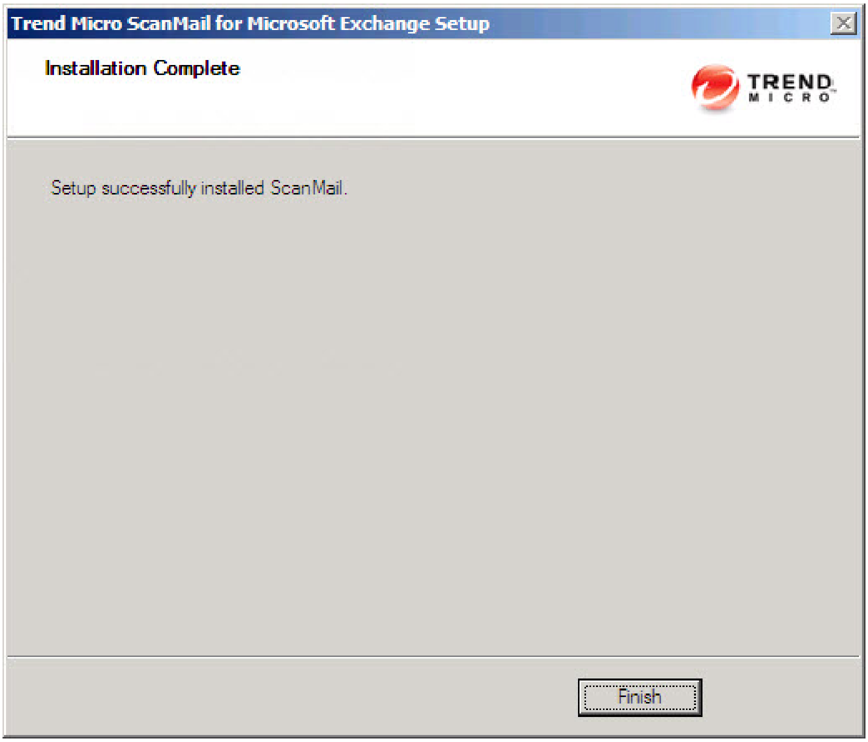
Installation failed on: 0 server

15. 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.

Note

ScanMail installs Microsoft™ SQL Server 2014 Express for configurations, logs, and reports on 64-bit computers. ScanMail sets the Microsoft SQL Server 2014 Express security level to the highest.

The **Installation Complete** screen appears.



Setup successfully installed ScanMail.

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

Chapter 4

Performing Post-Installation Tasks

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

Topics in this chapter:

Verifying a Successful Installation

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

Table 4-1. Successful Installation Verification

Item	Settings
Installation folder	`C:\Program Files\Trend Micro\SMEX\`
Services	• ScanMail for Microsoft Exchange Master Service • ScanMail EUQ Monitor Service **Note** This service is disabled for Exchange Server 2016 environments. • ScanMail for Microsoft Exchange Remote Configuration Server **Note** This service is not added to Exchange Server Edge Transport server roles. • ScanMail for Microsoft Exchange System Watcher
Registry keys (All versions)	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange`

ITEM	SETTINGS
Registry keys - Hub Transport with Mailbox Servers - Mailbox Servers	- `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.

About the ScanMail Management Pack

ScanMail provides full support for Systems Center Operations Manager (SCOM) 2007 and 2012. Administrators can import the ScanMail management package to System Center Operations Manager (SCOM) from the following path in the ScanMail installation package to use ScanMail with Systems Center Operations Manager (SCOM):

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

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

Procedure

1. Connect a valid mail client to the Exchange Server being tested.
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

Procedure

1. Connect a valid mail client to the Exchange Server being tested.

2. Download a copy of the standard industry EICAR test file 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

Procedure

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.

Spam Folder Configuration

Important

The End User Quarantine spam folder is only available for Exchange Server 2013 environments.

- Trend Micro Spam Folder

  ScanMail creates a spam folder on all of the mailboxes on the Exchange server where you installed ScanMail. During the installation, the installation program prompted you to name this folder and it will have the name that you specified.

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

- Spam detection levels

  ScanMail also configures the spam detection level defaults. The spam detection level filters out spam messages arriving at the Exchange server.

  - **High**: This is the most rigorous level of spam detection. ScanMail monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those email messages that ScanMail filters as spam when they are actually legitimate email messages.

  - **Medium**: ScanMail monitors at a high level of spam detection with a moderate chance of filtering false positives.

- **Low**: This is the default setting. This is most lenient level of spam detection. ScanMail will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.

Chapter 5

Silent Installation

Install ScanMail to one or more servers using silent installation.

Topics in this chapter:

About Silent Installation

This version of ScanMail supports silent installation. The steps in silent installation follow the same steps as regular installation.

The differences between the silent and standard installation processes are:

- The **Welcome** screen displays a message reminding you that ScanMail records the installation process into a preconfigured 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 are listed on the setup screen.
- The **Checking Target Server System Requirements** and **Selecting Target Server(s)** 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 preconfigured file by using recording mode the first time. Then, modify settings in the preconfigured 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 preconfigured files recorded on an English operating system to a target server with a German operating system.

Performing Silent Installation

Procedure

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

Using an Existing Preconfigured File

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

TABLE 5-1. 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 6

Removing ScanMail

This chapter describes how to remove ScanMail.

Topics in this chapter:

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.

Privilege Requirements

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

TABLE 6-1. Minimum Privileges Required for Uninstalling ScanMail

EXCHANGE VERSION	MINIMUM PRIVILEGES	FEATURE LIMITATION WITHOUT DOMAIN ADMINISTRATOR PRIVILEGES
Exchange Server 2016 Mailbox Servers	• Local Administrator • Domain User • Exchange Organization Management Group	N/A
Exchange Server 2013 Mailbox Servers	• Local Administrator • Domain User • Exchange Organization Management Group	Manual removal of EUQ mailbox required.
Exchange Server 2016, 2013 or 2010 Edge Transport	Local Administrator	N/A
Exchange Server 2010 Hub/Mailbox/Cluster	• Local Administrator • Domain User • Exchange Organization Management Group	Manual removal of EUQ mailbox required.

Using the Setup Program

You can use the `setup.exe` program to uninstall ScanMail.

Procedure

1. To remove ScanMail, run `setup.exe`.

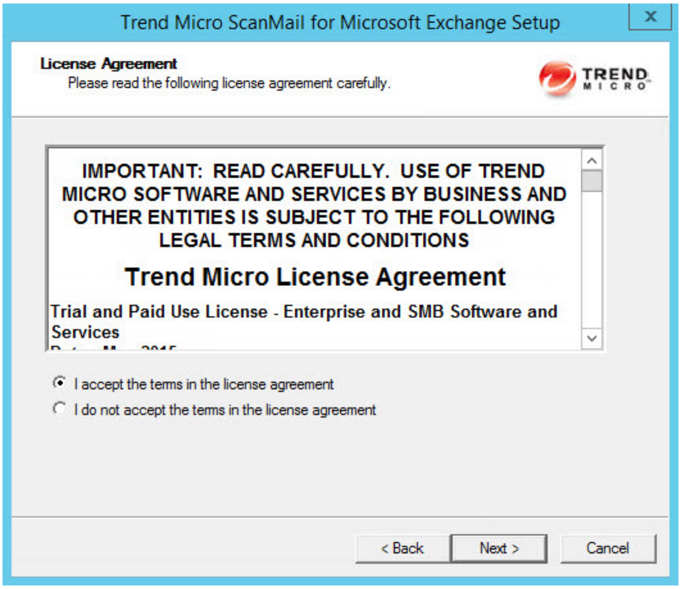
Note

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.

The **Welcome to Trend Micro ScanMail for Microsoft Exchange Setup** screen appears.

2. Click **Next**.

   The **License Agreement** screen appears.



License Agreement

Please read the following license agreement carefully.

IMPORTANT: READ CAREFULLY. USE OF TREND MICRO SOFTWARE AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS

Trend Micro License Agreement

Trial and Paid Use License - Enterprise and SMB Software and Services

● I accept the terms in the license agreement

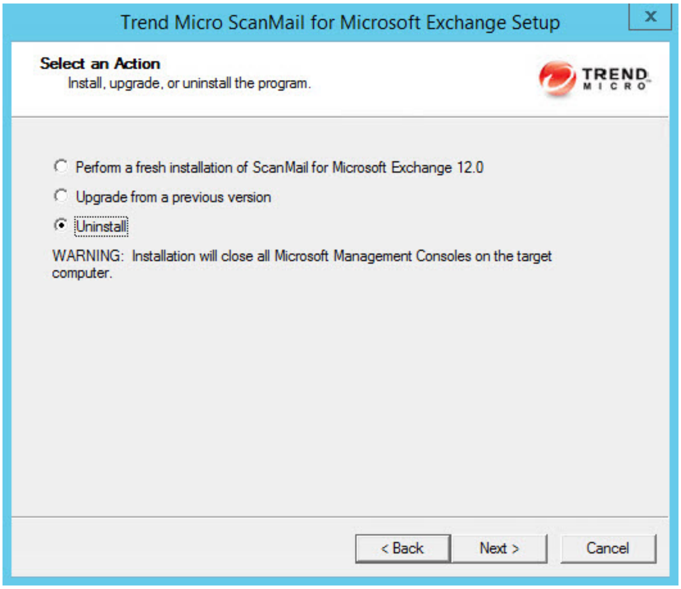
○ I do not accept the terms in the license agreement

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.



Trend Micro ScanMail for Microsoft Exchange Setup

Select an Action

Install, upgrade, or uninstall the program.

○ Perform a fresh installation of ScanMail for Microsoft Exchange 12.0

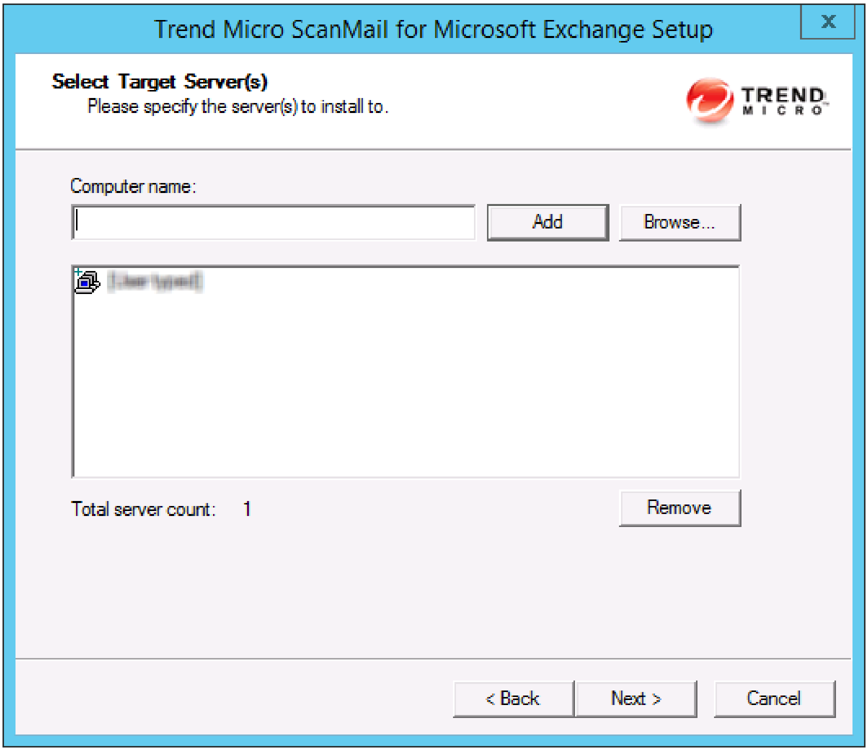
○ Upgrade from a previous version

● Uninstall

WARNING: Installation will close all Microsoft Management Consoles on the target computer.

4. Select **Uninstall** to remove ScanMail from your server(s).

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



Trend Micro ScanMail for Microsoft Exchange Setup

Select Target Server(s)

Please specify the server(s) to install to.

Computer name:

[redacted]

Total server count: 1

5. To uninstall ScanMail from a server:

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

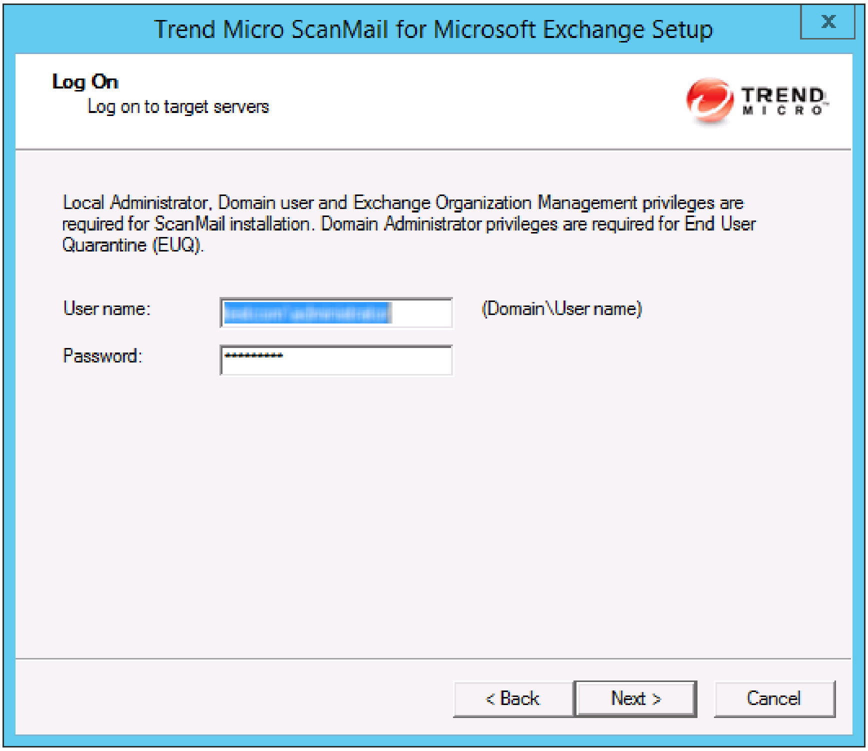
- Type the name of the target server in the **Computer name** field and click **Add** to add the computers to the list of servers.

- 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**.

The **Log On** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Log On

Log on to target servers

Local Administrator, Domain user and Exchange Organization Management privileges are required for ScanMail installation. Domain Administrator privileges are required for End User Quarantine (EUQ).

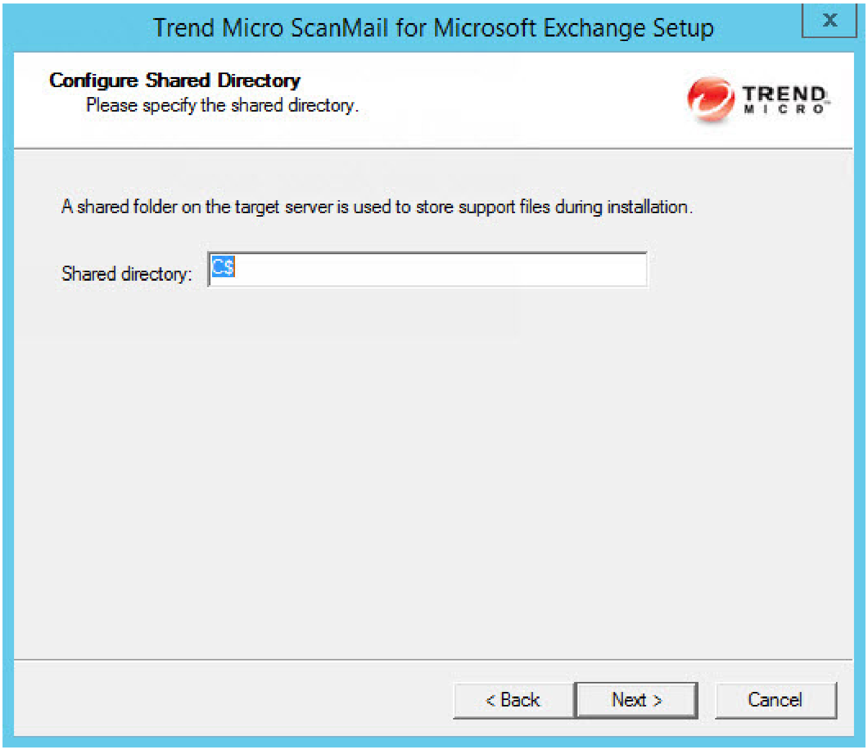
User name: [redacted] (Domain\User name)

Password: **********

6. Type the user name and password to log on to the target server to uninstall ScanMail.

7. Click **Next**.

The **Configure Shared/Target Directory** screen appears.



Trend Micro ScanMail for Microsoft Exchange Setup

Configure Shared Directory

Please specify the shared directory.

A shared folder on the target server is used to store support files during installation.

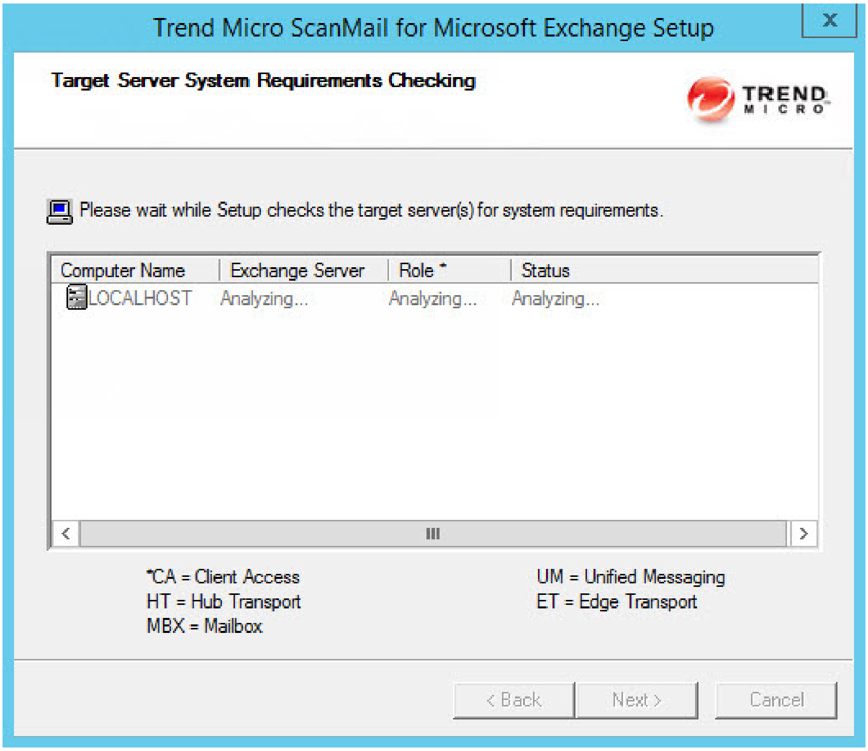
Shared directory: C$

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

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

   b. Click **Next**.

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



Trend Micro ScanMail for Microsoft Exchange Setup

Target Server System Requirements Checking

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

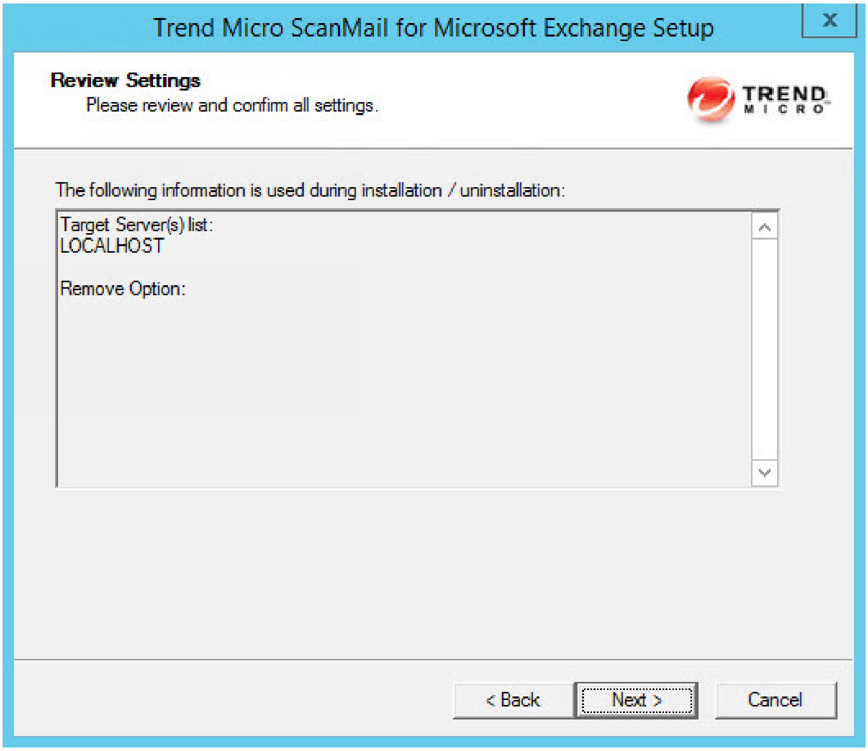
Computer Name	Exchange Server	Role *	Status
LOCALHOST	Analyzing...	Analyzing...	Analyzing...

*CA = Client Access
HT = Hub Transport
MBX = Mailbox
UM = Unified Messaging
ET = Edge Transport

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

10. Click **Next**.

The **Review Settings** screen appears.



Review Settings

Please review and confirm all settings.

The following information is used during installation / uninstallation:

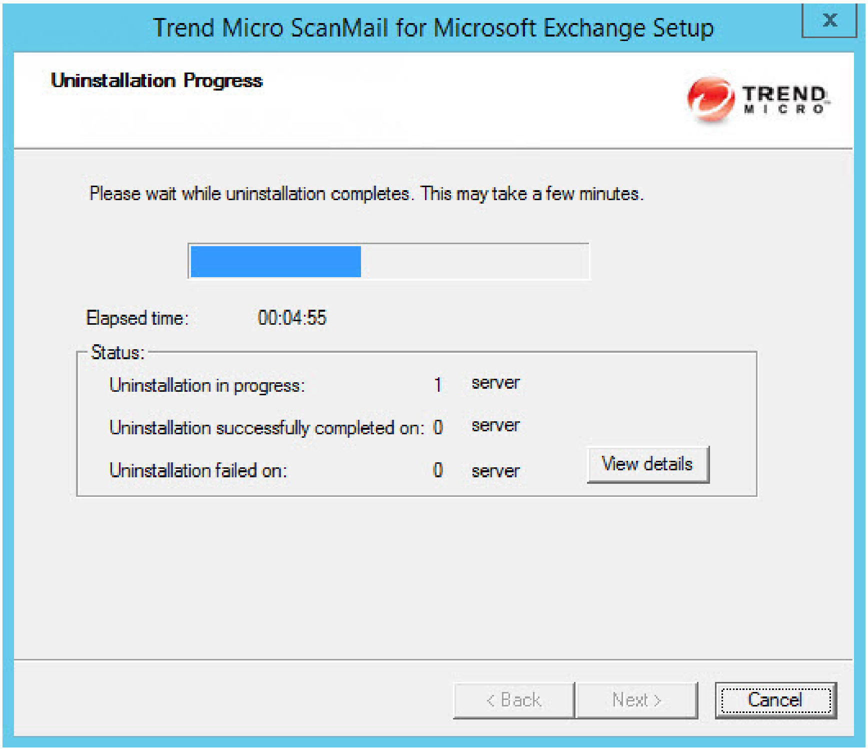
Target Server(s) list:
LOCALHOST

Remove Option:

11. Review your settings.

12. Click **Next**.

The **Uninstallation Progress** screen appears.



Uninstallation Progress

Please wait while uninstallation completes. This may take a few minutes.

Elapsed time: 00:04:55

Status:

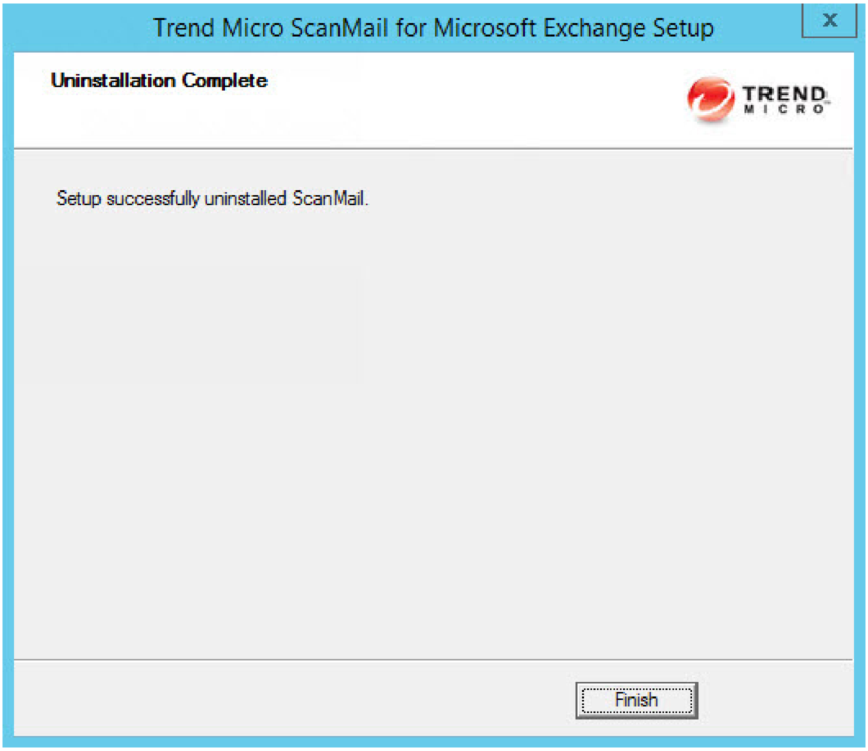
Uninstallation in progress: 1 server

Uninstallation successfully completed on: 0 server

Uninstallation failed on: 0 server

13. When the uninstallation is complete, click **Next** to proceed.

The **Uninstallation Complete** screen appears to inform you that the servers successfully uninstalled.



Uninstallation Complete

Setup successfully uninstalled ScanMail.

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

    The Setup program removes ScanMail from the selected servers.

Using the Windows Control Panel

You can remove ScanMail using the Microsoft™ Windows™ Control Panel. Using the Setup program to uninstall ScanMail removes all related components and programs. Trend Micro recommends using the `Setup.exe` program to uninstall ScanMail.

Procedure

1. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**.

2. Click the Trend Micro ScanMail *for Microsoft Exchange* program 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.

Manually Removing from Exchange 2013 / 2016 Servers

Manually remove ScanMail from Exchange 2013/2016 server, including cluster servers, by following the instructions below.

Procedure

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. Remove ScanMail transport agent from Exchange 2013/2016.

   a. Type the following commands:

      - `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. 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`

4. 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`

5. 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**.

6. 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.

7. Delete ScanMail from the **Start** menu.

   ```
   C:\Documents and Settings\All Users\Start Menu\Programs
   \Trend Micro ScanMail for Microsoft Exchange.
   ```

8. Delete all files and sub folders in the folder that ScanMail installed to. For example:

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

9. Delete all files and sub folders in `<Shared Directory>\SMEXtemp\`. This is the shared directory that was specified during installation. The default is `C$`.

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 Edge Transport or Hub Transport Servers

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

Procedure

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.

   a. Type the following commands:

   ```
   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`

     Note

     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`

  Note

  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 2014 Express 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 2008 on remote servers:

   a. Use SQL Server Management Studio Express to connect to the remote SQL server which has the ScanMail installation.

   b. Delete the ScanMail database:

      - `ScanMail_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 Mailbox Servers

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

Procedure

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 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`

    > **Note**
    >
    > 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`

        > **Note**
        >
        > 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 2014 Express 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 2008 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 database:

- `ScanMail_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**.

Chapter 7

Contacting Trend Micro

This chapter discusses how to contact Trend Micro to receive help, research security threats, and find the latest product solutions.

Topics include:

- *Contacting Technical Support on page 7-2*
- *Speeding Up Your Support Call on page 7-3*
- *Using the Support Portal on page 7-3*
- *Security Information Site on page 7-4*

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at http://esupport.trendmicro.com
- Get the latest Trend Micro product documentation at http://docs.trendmicro.com

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Operating System and Service Pack version
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Browser version
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

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.

Security Information Site

Comprehensive security information is available at the Trend Micro website:

http://about-threats.trendmicro.com

In the ScanMail banner at the top of any ScanMail screen, click the **Help** drop down, then **Security Info**.

Information available:

- List of viruses and malicious mobile code are currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Appendix A

Preconfigured Files

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

Table A-1. Preconfigured Files

Section	Contents
Logon	• `LogonUserDomain=<User's configuration>` • `LogonUserName=<User's configuration>`
Directory	• `TempDir=smex80temp` • `ShareName=C$` **Note** This is the default setting and can be changed. • `TargetDir=C:\Program Files\Trend Micro\Smex` **Note** This is the default setting and can be changed. • `UseDefaultProgPath=0` or `1`

SECTION	CONTENTS
	Note 0 uses your configuration and 1 uses the default
Activation	`MasterACCode=<User's configuration>`
Proxy	• `UseProxy=0` **Note** 0 is disable, 1 is enable • `DoAUAfterInstall=0` **Note** 0 is disable, 1 is enable • `ProxyURL=<Your configuration>` • `ProxyPort=<Your configuration>` **Note** The range is 1 to 65535 • `ProxyUsername=<Your configuration>` • `EnableSocks5=0` or `1` **Note** 0 is disable, 1 is enable
Web	• `WebServerType=0` **Note** 0 is IIS, 1 is Apache • `IISSiteType=0` or `1`

Section	Contents
	Note 0 is Virtual Web Site, 1 is Default Web Site. This setting is only applicable when IIS is selected. • `WebPort=<Your configuration>` **Note** The range is 1 to 65535 • `EnableSSL=0` or `1` **Note** 0 is disable, 1 is enable • `SSLPort=<Your configuration>` **Note** The range is 1 to 65535 • `SSLValidPeriodCertificate=<Your configuration>`
WTC	`WTCEnable=0` or `1` **Note** 0 is disable, 1 is enable
ServerManagement	• `CreateNewConsoleAccount=0` or `1` **Note** 0 uses the current or skip, 1 creates a new account • `ConsoleUsername=<Your configuration>` • `ActivateServerManagement=0` or `1`

Section	Contents
	Note 0 is deactivate, 1 is activate
SMTP	`EnableSMTPScanning=1` **Note** 0 is disable, 1 is enable
EUQ	• `ActivateEUQ=0` or `1` **Note** 0 is deactivate, 1 is activate • `IntegrateWithOutook2K3JunkMailFolder=0` or `1` **Note** 0 is disable, 1 is enable • `UseDefaultSpamFolderName=0` or `1` **Note** 0 uses your configuration and 1 uses the default • `SpamFolderName=Spam Mail` **Note** This is default folder name and can be changed. • `SpamMsgRetainDay=14` **Note** This is default setting and can be changed. The range is 0 to 30.

SECTION	CONTENTS
CMAgent	• `RegisterCMAgent=0` or `1` **Note** 0 is disable, 1 is enable • `CMServerAddress=<Your configuration>` • `CMServerPortNumber=443` **Note** The range is 1 to 65535 • `ConnectCMServerUsingHTTPS=0` or `1` **Note** 0 is disable, 1 is enable • `ConnectCMServerUsingProxy=0` or `1` **Note** 0 is disable, 1 is enable • `ConnectCMServerProxyAddress=<Your configuration>` • `ConnectCMServerUseSOCKS5=0` or `1` **Note** 0 is disable, 1 is enable • `ConnectCMServerProxyUserName=<Your configuration>` • `CMServerWebUserName=<Your configuration>` • `ConnectCMServerProxyPortNumber=80`

Section	Contents
	Note The range is 1 to 65535
Do NOT edit these settings	- `LogonPassword=<Your configuration>` **Note** Password does not display. - `ExchangeType=1, 2, 3` or `4` **Note** - 1 is "Exchange 2010 Edge Transport Server" - 2 is "Exchange 2010 Hub Transport Server / Mailbox Server" - 3 is "Exchange 2013 / 2016 Mailbox Server" - 4 is "Exchange 2013 / 2016 Edge Transport Server" - `ProxyPassword=<Your configuration>` **Note** Password does not display. - `ConsolePassword=<Your configuration>` **Note** Password does not display. - `EUQInstallLangID=1033` **Note** Do not change this setting.

Section	Contents
	• `EUQDefaultLangID=9` **Note** Do not change this setting. • `ConnectCMServerProxyPassword=<Your configuration>` **Note** Password does not display. • `CMServerWebPassword=<Your configuration>` **Note** Password does not display. • `ConsoleGroup=<User's configuration>` **Note** For example: `DomainName\Group`, do not modify the group name • `ServerManagementGroupSid=` **Note** Do not modify the SID
Cluster	• `VirtualServers=<Your configuration>` • `[VirtualServerName]` (type the virtual server name here) • `DiskResourceName=<Your configuration>` • `SMEXFolderPath=<Your configuration>` • `RemoteSQLServerDataSource=<Your configuration>`

SECTION	CONTENTS
	• `RemoteSQLWindowsAuthentication` **Note** 0 indicates SQL account authentication; 1 indicates Windows authentication. • `RemoteSQLUserName=<Your configuration>` **Note** If you configure `RemoteSQLWindowsAuthentication` to use Windows authentication, the user name is the Windows account. • `RemoteSQLPassword=<Your configuration>` **Note** The Remote SQL password is encrypted.
RemoteSQL	• `RemoteSQLServerDataSource=<Your configuration>` • `RemoteSQLUserName=<Your configuration>` **Note** A dbcreator role is required. If you configure `RemoteSQLWindowsAuthentication` to use Windows authentication, the user name is the Windows account. • `RemoteSQLPassword=<Your configuration>` **Note** The Remote SQL password is encrypted. • `RemoteSQLWindowsAuthentication`

SECTION	CONTENTS
	Note 0 indicates SQL account authentication; 1 indicates Windows authentication. - `RemoteSQLExistingDatabase=<Your configuration>` **Note** If left blank, ScanMail creates a new database.
InstallOption	`WaitIISAdminToUnloadSMTPHook=-1` **Note** - 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.

Appendix B

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 See also, 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

Term	Description
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.
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.
Domain Name System (DNS)	A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses
Domain Name System (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.

Term	Description
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.
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 ends 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
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.

TERM	DESCRIPTION
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
HTML, VBScript, or JavaScript viruses	Viruses that reside in web pages and are downloaded through a browser.
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.
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

Term	Description
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.
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.
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
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.

Term	Description
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 website that lures users into providing personal details, such as credit card information. Links to phish sites are often sent in bogus email messages disguised as legitimate messages from well-known businesses.
Ping	A utility that sends an ICMP echo request to an IP address and waits for a response The Ping utility can determine if the machine with the specified IP address is online or not.
Ping of Death	A Denial of Service attack where a hacker directs an oversized ICMP packet at a target computer. This can cause the computer's buffer to overflow, which can freeze or reboot the machine.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application
Quarantine entire message	To place email messages in an isolated directory (the Quarantine Directory) on the ScanMail scanner. Items placed in the quarantine directory are indexed in the ScanMail database.
Quarantine message part	To move the email message body or attachment to a restricted access folder, removing it as a security risk to the Exchange environment. ScanMail replaces the message part with the text/file you specify.

Term	Description
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database See also, 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

Term	Description
Trojan horses	Executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter.
True file type	A virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).
Undesirable content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail
Unsolicited email	See Spam
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

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: SMEM127297/160113