TREND MICRO™

1.0 ScanMail™ Mobile Security

Installation Guide

Securing your mobile Exchange messaging

for Microsoft™ Exchange

Messaging Security

Mobile 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-mobile-security-for-microsoft-exchange.aspx

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

Copyright © 2013. Trend Micro Incorporated. All rights reserved.

Document Part No. APEM16093_130830

Release Date: November 2013

Document Version No.: 1.0

Product Name and Version No.: ScanMail™ Mobile Security *for Microsoft™ Exchange* 1.0

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

The user documentation for Trend Micro ScanMail Mobile Security *for Microsoft Exchange* 1.0 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

Preface iii

ScanMail Mobile Documentation iv

Audience iv

Document Conventions v

Chapter 1: Planning ScanMail Mobile Installation

System Requirements 1-2

- ScanMail Mobile with Exchange Server 2013 1-2
- ScanMail Mobile with Exchange Server 2010 1-3

Conducting a Pilot Installation 1-4

- Step 1: Creating an Appropriate Test Site 1-5
- Step 2: Preparing a Rollback Plan 1-5
- Step 3: Executing and Evaluating Your Pilot Installation 1-6

Deployment Strategy 1-6

- Planning for Network Traffic 1-7
- Deploying ScanMail Mobile to Multiple Servers 1-7

About Fresh Installations 1-9

Preparing to Install 1-9

- Installing without Internet Information Services 1-10
- Installing with a Remote SQL Server 1-11
- Additional Requirements for Installing Remotely with Windows 2008 and 2012 1-14

Preinstallation Checklist 1-17

Chapter 2: Installing ScanMail Mobile Security for Microsoft Exchange

Installing on Exchange Server 2013 and 2010 2-2

Chapter 3: Performing Post-Installation Tasks

Verifying a Successful Installation 3-2
About the ScanMail Mobile Management Pack 3-2

Chapter 4: Performing a Silent Installation

About Silent Installation 4-2
Silent Installation Limitations 4-2
Performing Silent Installation 4-2
Using an Existing Preconfigured File 4-3

Chapter 5: Removing ScanMail Mobile

Uninstallation Overview 5-2
Privilege Requirements 5-2
Using the Enterprise Solution DVD 5-3
Using the Windows Control Panel 5-13

Chapter 6: Contacting Trend Micro

Contacting Technical Support 6-2
TrendLabs 6-2
Speeding Up Your Support Call 6-3
Knowledge Base 6-3
Security Information Site 6-4

Appendix A: Preconfigured Files

Appendix B: Glossary

Index

Index IN-1

Preface

Preface

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

This preface discusses the following topics:

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

ScanMail Mobile 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 Mobile features.

- **Installation Guide**: PDF documentation that discusses requirements and procedures for installing 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 are also posted and a dynamic list of the most frequently asked questions 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-mobile-security-for-microsoft-exchange.aspx) for updates to the documentation.

Audience

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

- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies

- Microsoft Exchange Server administration
- Microsoft Exchange Server 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
Important	Information regarding required or default configuration settings and product limitations

Convention	Description
WARNING!	Critical actions and configuration options

Chapter 1

Planning ScanMail Mobile Installation

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

Topics in this chapter:

- *System Requirements on page 1-2*
- *Conducting a Pilot Installation on page 1-4*
- *Deployment Strategy on page 1-6*
- *About Fresh Installations on page 1-9*
- *Preparing to Install on page 1-9*
- *Preinstallation Checklist on page 1-17*

System Requirements

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

ScanMail Mobile with Exchange Server 2013

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

TABLE 1-1. 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 Mobile (2GB RAM recommended)
Disk space	2GB free disk space
Operating system	• 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
Web server	• Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet information Services (IIS) 7.5

Resource	Requirements
SQL server	• SQL Server 2012 • SQL Server 2008 R2 • SQL Server 2008
Browser	• Microsoft™ Internet Explorer™ 7.0 or above **Note** Trend Micro recommends operating Internet Explorer 10 in compatibility view. • Mozilla Firefox™ 3.0 or above

ScanMail Mobile with Exchange Server 2010

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

Table 1-2. System Requirements for Installation with Exchange Server 2010

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

RESOURCE	REQUIREMENTS
Operating system	• Microsoft Windows Server 2012 (64-bit) Standard or Datacenter • Microsoft™ Windows Server™ 2008 with Service Pack 2 or above (64-bit) • Microsoft Windows Server 2008 R2 or above (64-bit)
Mail server	Microsoft Exchange Server 2010 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
SQL server	• SQL Server 2012 • SQL Server 2008 R2 • SQL Server 2008
Browser	• Microsoft™ Internet Explorer™ 7.0 or above **Note** Trend Micro recommends operating Internet Explorer 10 in compatibility view. • Mozilla Firefox™ 3.0 or above

Conducting a Pilot Installation

The following section contains Trend Micro recommendations for installing ScanMail Mobile. 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 1-5*
- *Step 2: Preparing a Rollback Plan on page 1-5*
- *Step 3: Executing and Evaluating Your Pilot Installation on page 1-6*

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

Backing Up ScanMail Mobile Configurations

Before making any changes, back up ScanMail Mobile configurations.

Procedure

1. Stop ScanMail Mobile Security Master Service and SQL Server (SCANMAIL_MOBILE) Service on the target server which has the database you want to back up.
2. Copy the `Conf.mdf`, `Log.mdf`, or `Report.mdf` file.

Restoring ScanMail Mobile Configurations

Use the following procedures to restore ScanMail Mobile configurations if necessary.

Procedure

1. Stop the ScanMail Mobile Security Master Service and SQL Server (SCANMAIL_MOBILE) 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_MOBILE) Service and the ScanMail Mobile Security 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 Mobile Setup program supports installation to a single or multiple local server or remote servers.

When deploying and configuring ScanMail Mobile on your Local Area Network (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 (LAN) segment

Planning for Network Traffic

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

ScanMail Mobile generates network traffic when it does the following:

- Sends alerts and notifications to administrators and other designated recipients

ScanMail Mobile increases the burden on the CPU when it scans email messages. ScanMail Mobile uses multi-threaded scanning which reduces the CPU burden.

Deploying ScanMail Mobile to Multiple Servers

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

Another strategy is to deploy ScanMail Mobile 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 Mobile on Exchange servers exposed to the Internet (this is the default value). ScanMail Mobile 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 1-3. Deploying ScanMail Mobile with Exchange Server

SERVER VERSION	SERVER ROLE	RECOMMENDATION
Exchange Server 2010	Client Access Server: • Outlook Web App allows access to email messages from any web browser • Exchange ActiveSync synchronizes data between mobile devices and Exchange 2010 including email messages, contacts, calendar information, and tasks • POP3 and IMAP4 clients • Availability service • Autodiscover service	• ActiveSync is enabled after installing the Client Access server role on a computer running Microsoft Exchange Server 2010 • By default, all new users are enabled for Exchange ActiveSync **Note** If Exchange ActiveSync is disabled for a user, administrators can manually enable ActiveSync.
Exchange Server 2013	Mailbox Server • The Exchange Server 2013 Mailbox Server role hosts both mailbox and public folder databases while also providing email message storage • The Mailbox Server role includes Client Access protocols, Transport service, mailbox databases, and Unified Messaging components • Exchange ActiveSync is a client protocol that synchronizes mobile devices with the Exchange mailbox	• Exchange ActiveSync is enabled by default after installing Microsoft Exchange 2013 Mailbox Server • By default, all new users are enabled for Exchange ActiveSync **Note** If Exchange ActiveSync is disabled for a user, administrators can manually enable ActiveSync.

Deploying ScanMail Mobile 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 Mobile on each LAN segment separately.

Note

ScanMail Mobile Security *for Microsoft Exchange* is designed to guard your Exchange mail servers. ScanMail Mobile does not provide protection to non-Exchange mail servers, file servers, desktops, or gateway devices. ScanMail Mobile 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.

About Fresh Installations

Perform a fresh installation to install ScanMail Mobile for the first time. Before beginning your installation, consult the preinstallation checklist (*Preinstallation Checklist on page 1-17*).

Note

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

Preparing to Install

To prepare for a smooth installation, preview the information in this section and consult the preinstallation 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 ScanMail Mobile on each of your Microsoft Exchange servers. Perform local and remote installations from one ScanMail Mobile 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 Mobile. You can simultaneously install ScanMail Mobile 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 Mobile fresh installation.

TABLE 1-4. Fresh Installation Minimum Privileges

EXCHANGE VERSION	MINIMUM PRIVILEGES
Exchange Server 2013 Mailbox	Local Administrator and Domain User
Exchange Server 2010 with Client Access Server	Local Administrator and Domain User

Installing without Internet Information Services

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

Procedure

1. Run `cmd.exe`.
2. Navigate to the `SMMS` 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 (for details, see *Installing on Exchange Server 2013 and 2010 on page 2-2*). ScanMail Mobile does not check for IIS and does not install the management console on this server.

Installing with a Remote SQL Server

ScanMail Mobile supports storing the ScanMail Mobile database on a remote SQL server with fresh installs on supported versions of Exchange Server. Prepare a remote SQL server before installing ScanMail Mobile.

Note

ScanMail Mobile 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 Mobile 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 Mobile.

   Note

   ScanMail Mobile supports SQL server accounts; Windows accounts are not supported.

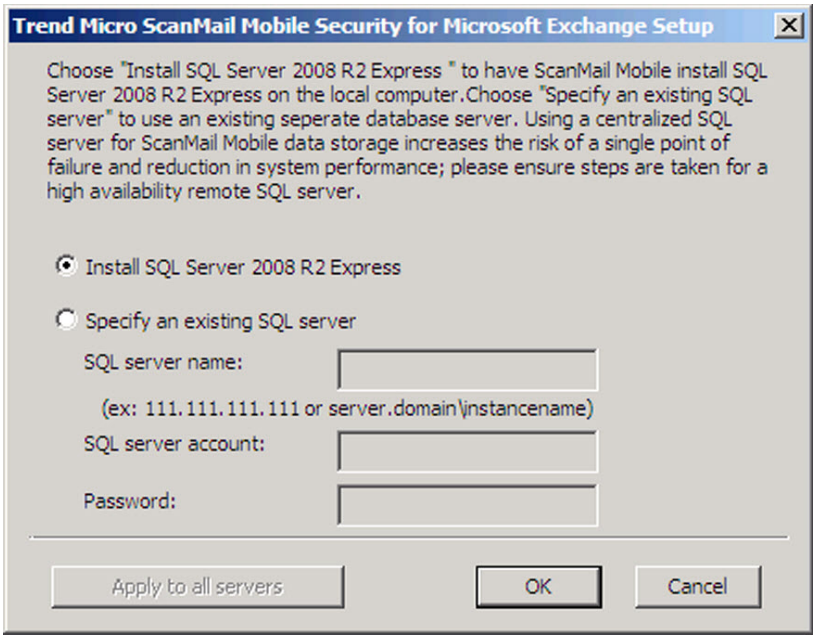
3. During installation, specify the remote SQL server on the following screens:

   Note

   When ScanMail Mobile is installed with a remote SQL server and connection to the server is unavailable, ScanMail Mobile will perform a database reconnect. ScanMail Mobile logs the error to Windows Event Log and adds an entry every hour the server is unavailable. When the server is unavailable, ScanMail Mobile does not scan messages. All messages are sent to the mail database. ScanMail Mobile 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 Mobile will continue message scans.

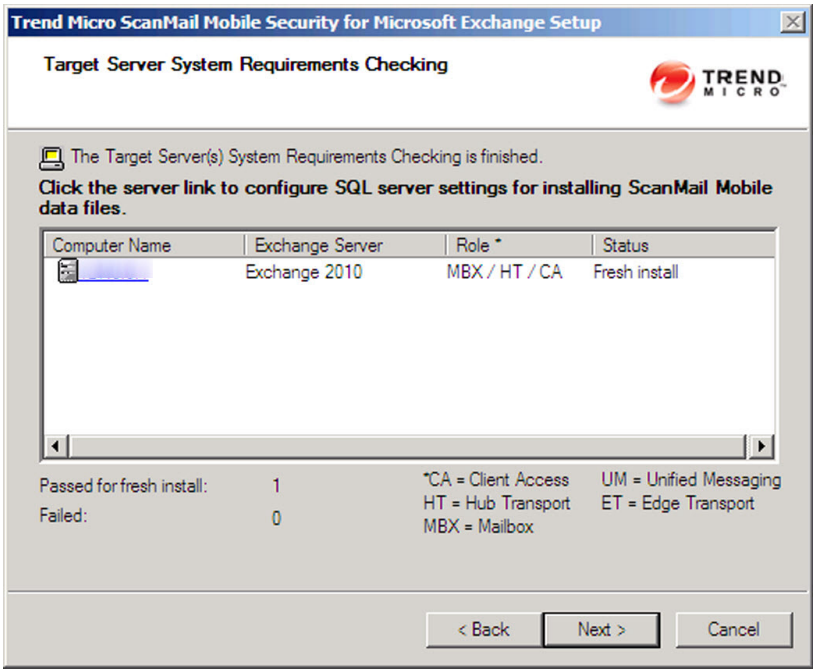
   a. On the **Select Target Server(s)** screen of the ScanMail Setup program, click the server link to configure remote SQL server settings.

The remote SQL configuration screen appears.



b. Type the SQL instance name and SQL account prepared in Step 2. Then, click **OK**.

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



c. Click **Next** to continue with the installation process if the status check was successful.

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

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

4. Complete the rest of the installation process.

Additional Requirements for Installing Remotely with Windows 2008 and 2012

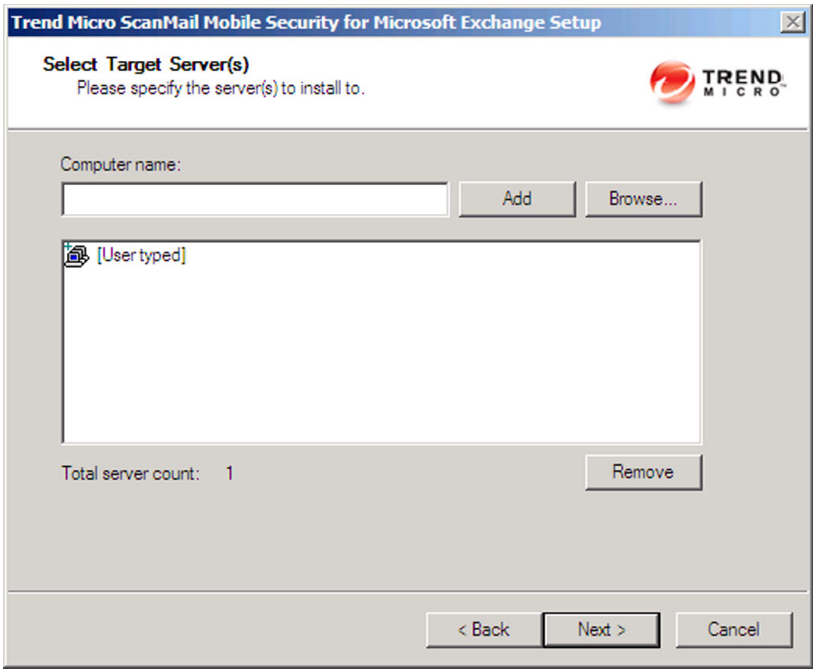
This only applies to Windows 2008 and Windows 2012 operating systems when remotely installing multiple Exchange servers.

Perform the following before installing:

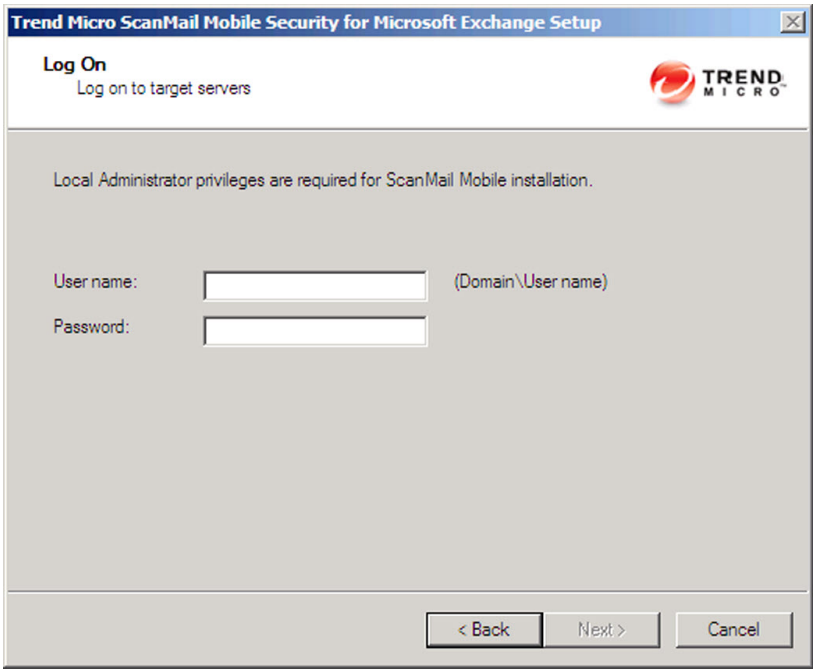
- Prepare an account with domain administrator privileges or domain user privileges. If it is an account with domain user privileges, this account must have local administrator privileges on each Exchange server.
- Enable file sharing on Windows Firewall or disable Windows Firewall on each Exchange server.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

Procedure

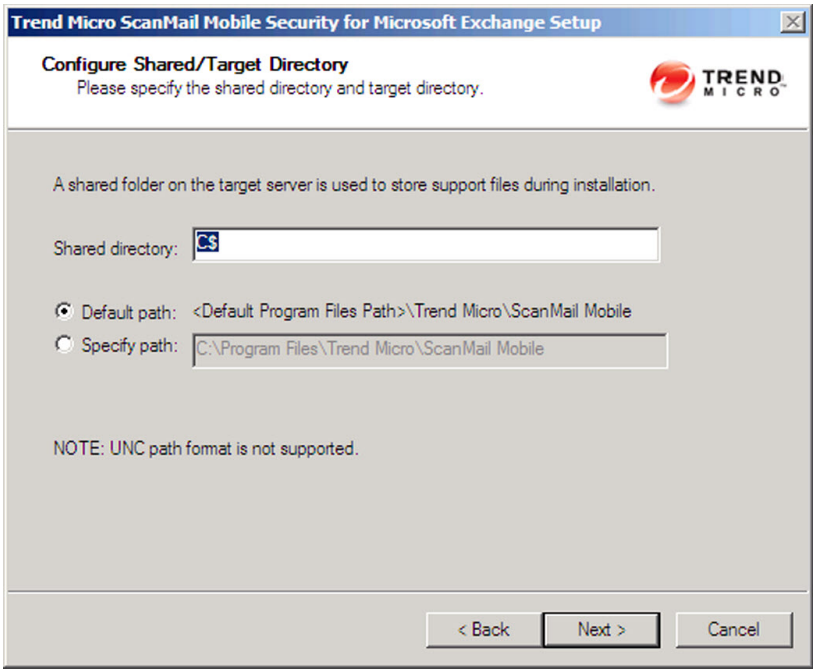
1. Log on to the operating system with an account that has domain administrator privileges and launch the ScanMail Mobile Setup program.
2. Specify the options on the following screens:
    a. On the **Select Target Server(s)** screen of the installation process, **Add** or **Browse** to add multiple target ScanMail Mobile servers that belong to the same domain.



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.



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



3. Complete the rest of the installation process.

Preinstallation Checklist

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

TABLE 1-5. Preinstallation Checklist

ITEM	NOTES
Minimum account privileges	Administrators require Local Administrator privileges.

ITEM	NOTES
Restart	Administrators 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 Mobile 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 Mobile, ScanMail Mobile will only provide a limited service.
Proxy server	During installation, the Setup program prompts for proxy information. If a proxy server handles Internet traffic on the network, type the proxy server information, user name, and password. Administrators can configure proxy settings at a later time from the product console.
CGI component	On Windows 2008, install CGI role service before installing ScanMail Mobile. Add CGI role service from **Windows Server Manager** > **Add Roles** > **Web Server (IIS)** > **Add Role services** > **Application development** > **CGI**.

Chapter 2

Installing ScanMail Mobile Security *for Microsoft Exchange*

Install ScanMail Mobile Security *for Microsoft Exchange* locally or remotely to one or more servers using one easy-to-use Setup program.

Topics in this chapter:

- *Installing on Exchange Server 2013 and 2010 on page 2-2*

Installing on Exchange Server 2013 and 2010

The following lists the steps to install ScanMail Mobile with Exchange 2013 Mailbox Server or Exchange 2010 Client Access Server.

Procedure

1. Select a source for the Setup program:
   - Trend Micro website

     http://downloadcenter.trendmicro.com/

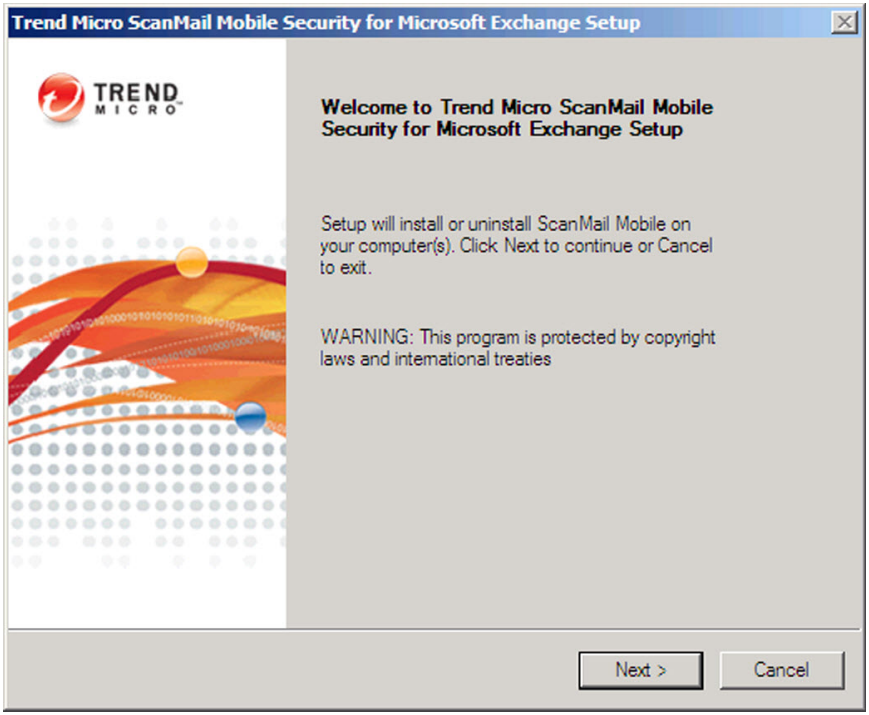
     a. Download ScanMail Mobile from the Trend Micro website.

     b. Unzip the file to a temporary directory.

     c. Run `setup.exe` to install ScanMail Mobile.
   - The Trend Micro Enterprise Solution DVD

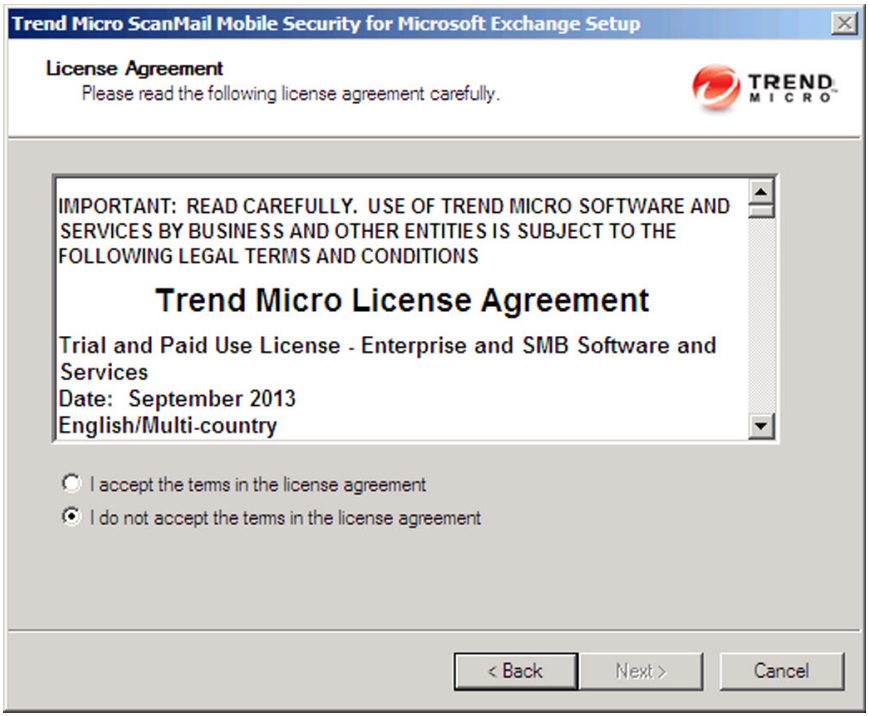
     a. Insert the DVD and follow the online instructions.

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



2. Click **Next**.

The **License Agreement** screen appears.



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

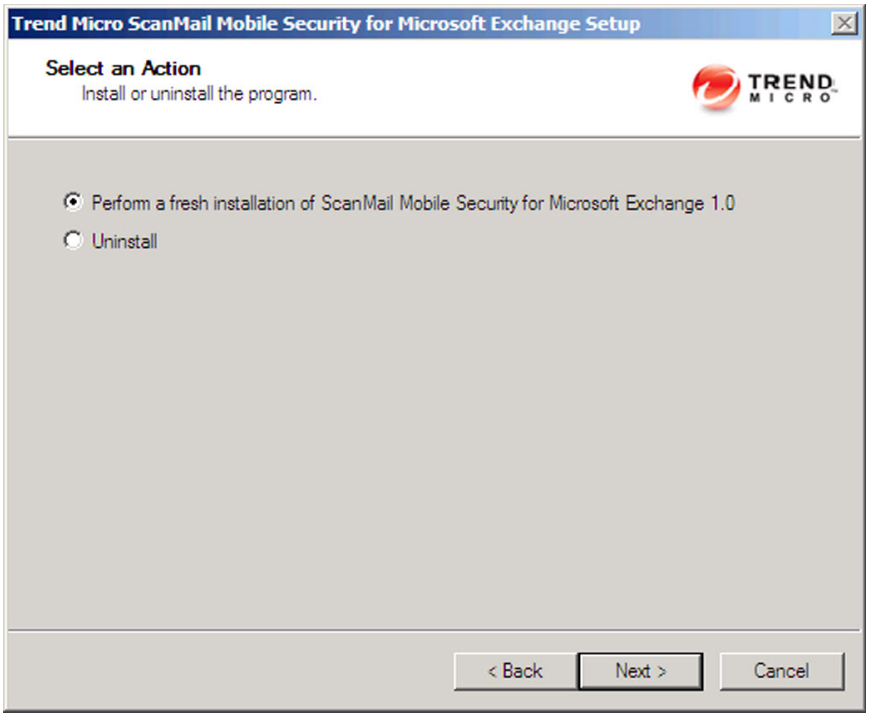
Note

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.

---

4. Click **Next**.

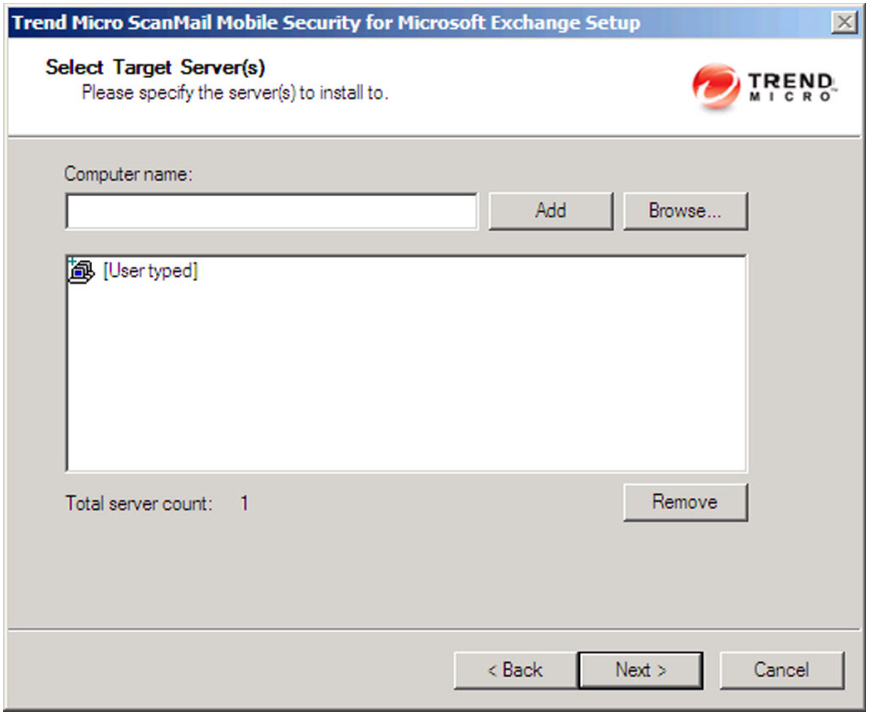
The **Select an Action** screen appears.



5. Select **Perform a fresh installation of ScanMail Mobile Security for Microsoft Exchange 1.0** to perform a fresh install.

6. Click **Next**.

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



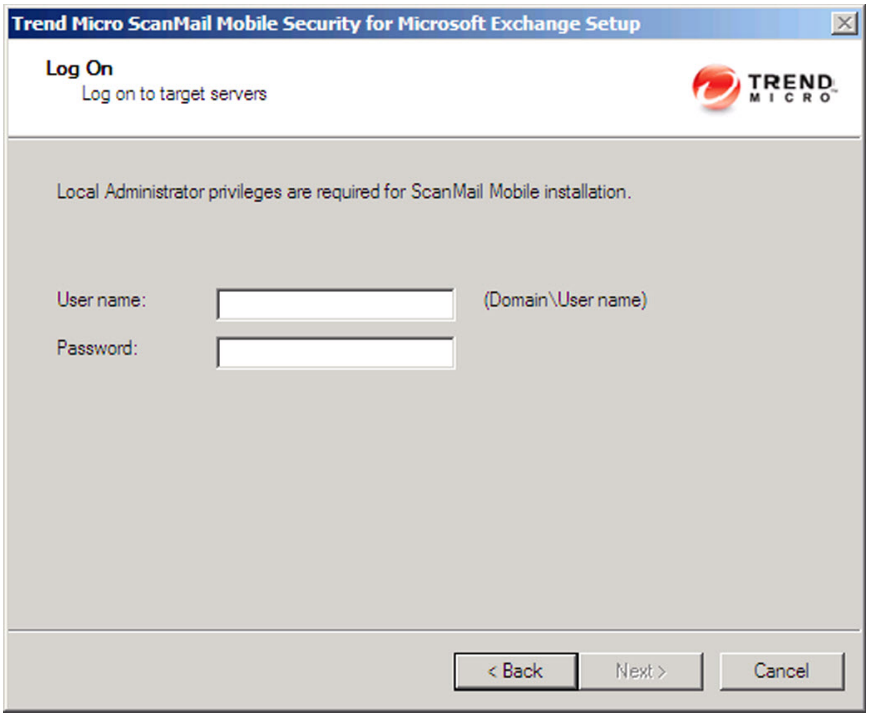
7. Select the computers to which you want to install ScanMail Mobile.

   a. Perform one of the following:

      - 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.

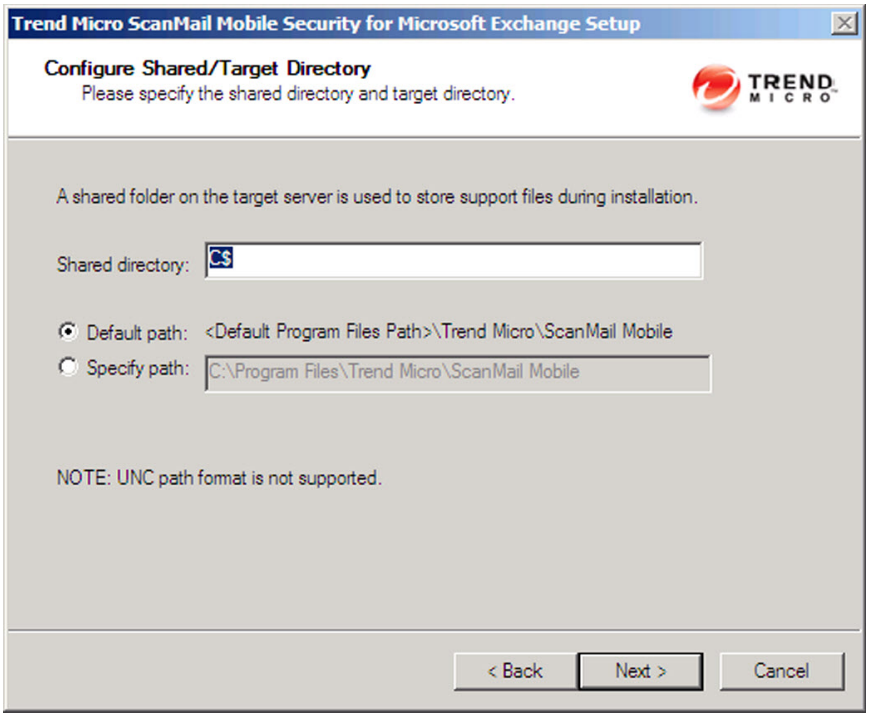


Note

The Setup program can install ScanMail Mobile 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 Mobile supports IPv6.

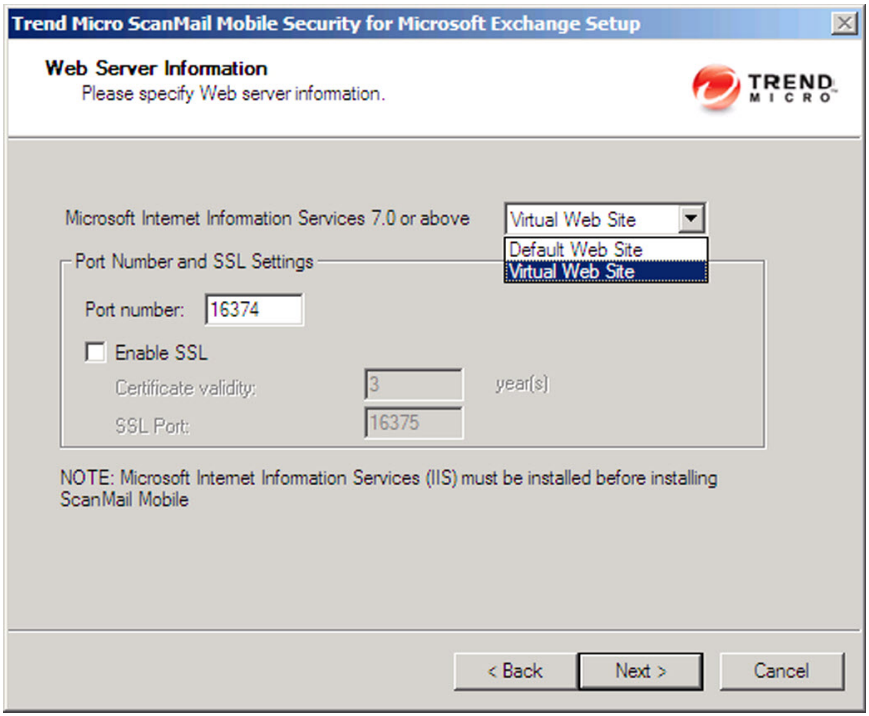
8. Log on to the target servers where you want to install ScanMail Mobile. Use an account with Domain User privileges and Local Administrator privileges. Type the user name and password to log on to the target server to install ScanMail Mobile.

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



9. Specify the shared folder:
10. Click **Next**.

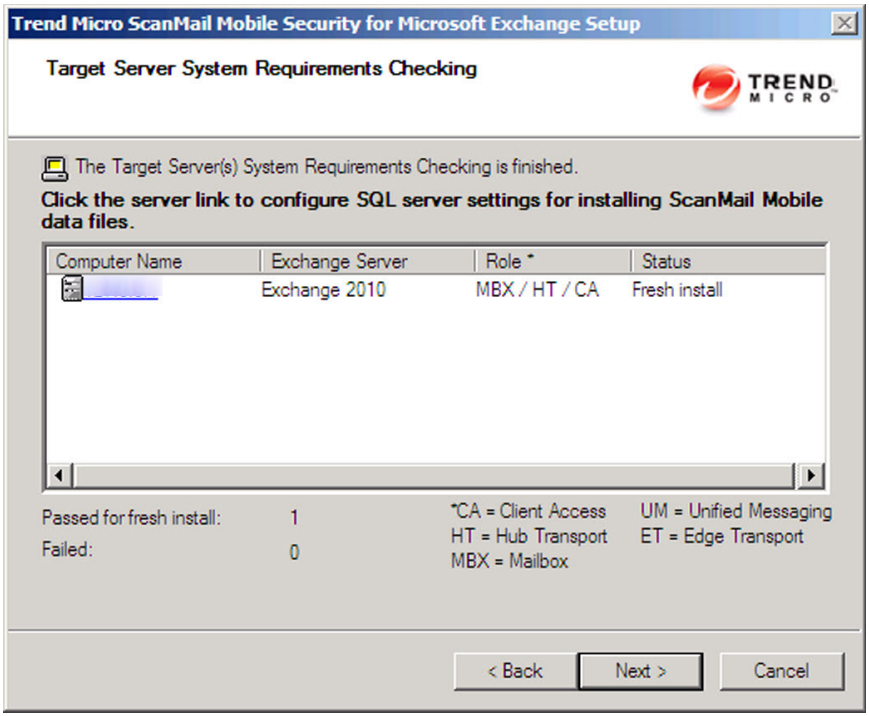
The **Web Server Information** screen appears.



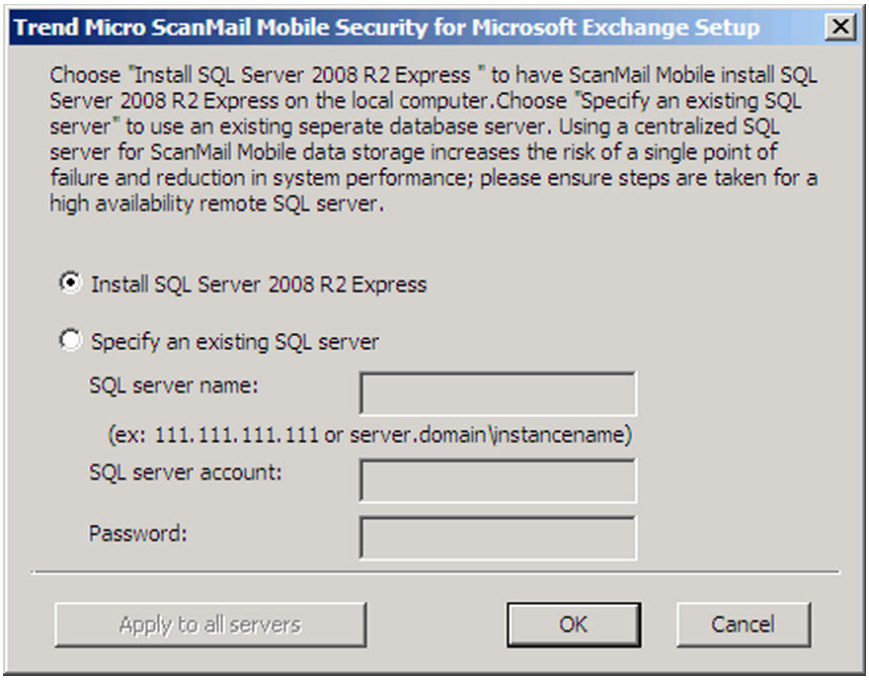
11. Select **IIS Default Web Site** or **Virtual Web Site**. Next to **Port number** type the port to use as a listening port for this server. You also have the option of enabling Secure Socket Layer (SSL) security. Select **Enable SSL** check box to use this feature.

12. Click **Next**.

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



13. Review the settings. To install ScanMail Mobile on a remote SQL server, click the server on which to configure remote SQL server settings.



14. Select one of the following:

    - **Install SQL Server 2008 R2 Express**: Installs SQL Server R2 2008 Express on the local computer.
    - **Specify an existing SQL server**: Uses an existing database server. Type the SQL server name, SQL server account, and password.

    Note

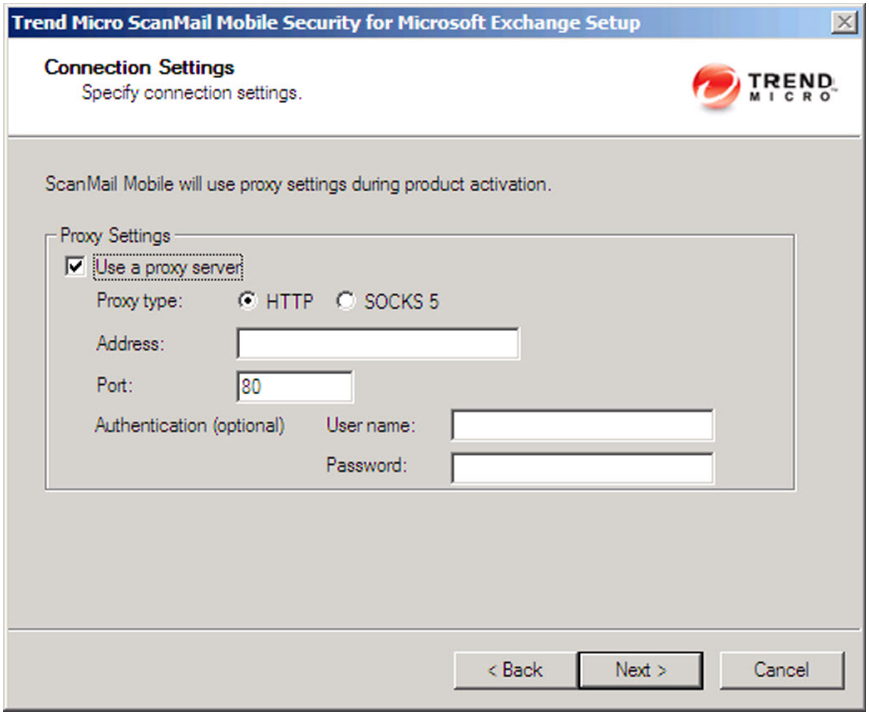
    Using a centralized SQL server for ScanMail Mobile data storage increases the risk of a single point of failure and reduction in performance. Ensure that steps are taken for a high availability remote SQL server.

15. Click **OK**.

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

16. Click **Next**.

    The **Connection Settings** screen appears.



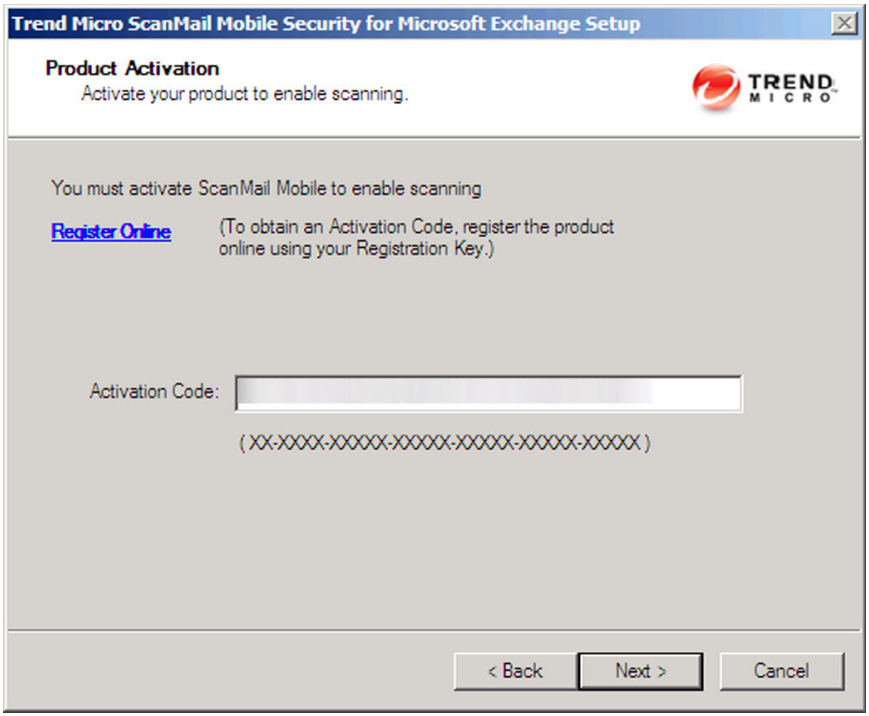
17. If a proxy server handles Internet traffic on your network, select **Use a proxy server** and then type the proxy hostname or address and port number that your proxy uses.

    - 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.

    By default, the proxy server is disabled.

18. Click **Next**.

The **Product Activation** screen appears.



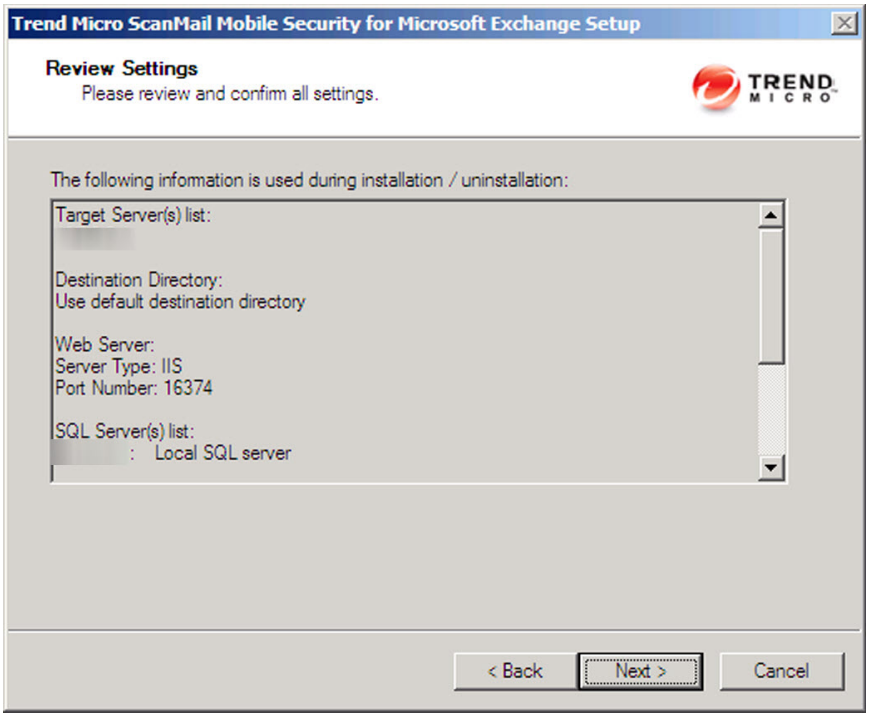
19. Type the activation code.

Note

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

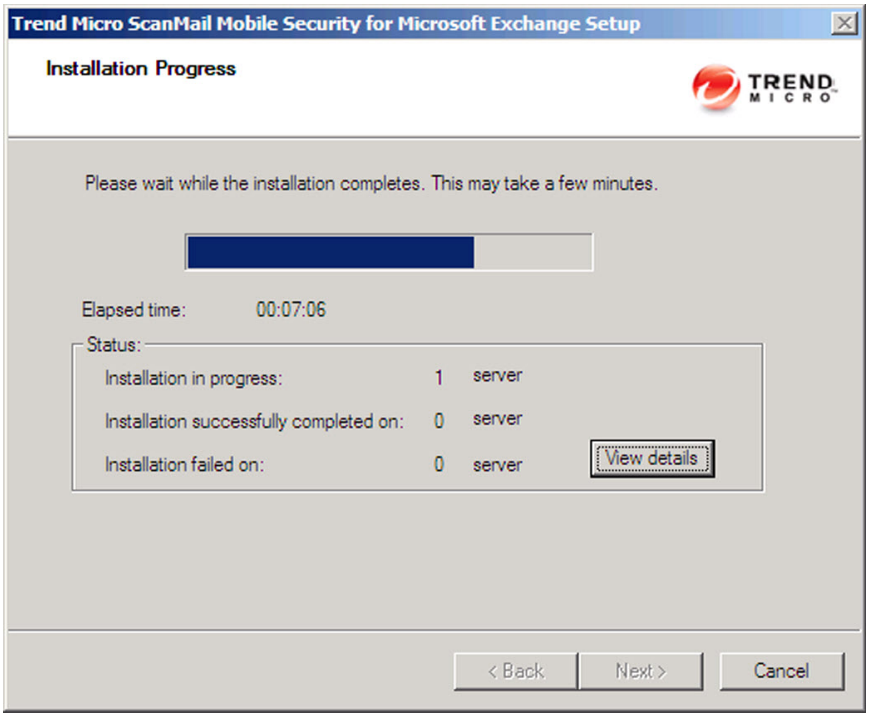
20. Click **Next**.

The **Review Settings** screen appears.



21. Click **Next**.

The **Installation Progress** screen appears.



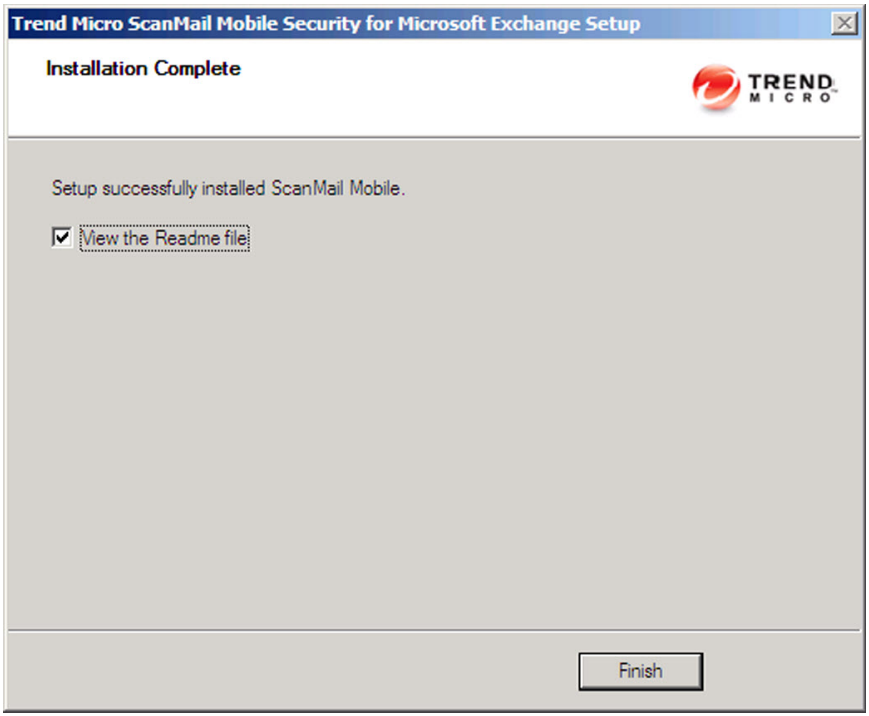
22. Click **View details** to display a list of each computer to which you are installing ScanMail Mobile and the status of each computer.

23. Click **Next**.

Note

ScanMail Mobile installs Microsoft™ SQL Server 2008 R2 Express for configurations, logs, and reports on 64-bit computers. ScanMail Mobile sets the Microsoft SQL Server 2008 R2 Express security level to the highest.

The **Installation Complete** screen appears.



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

Chapter 3

Performing Post-Installation Tasks

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

Topics in this chapter:

- *Verifying a Successful Installation on page 3-2*
- *About the ScanMail Mobile Management Pack on page 3-2*

Verifying a Successful Installation

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

TABLE 3-1. Successful Installation Verification

ITEM	SETTINGS
Installation folder	`C:\Program Files\Trend Micro\ScanMail Mobile`
Services	• ScanMail Mobile Security for Microsoft Exchange Master Service • ScanMail Mobile Security for Microsoft Exchange Remote Configuration Server • ScanMail Mobile Security for Microsoft Exchange System Watcher
Registry keys (All versions)	`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail Mobile Security for Exchange`

About the ScanMail Mobile Management Pack

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

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

Chapter 4

Performing a Silent Installation

Install ScanMail Mobile to one or more servers using silent installation.

Topics in this chapter:

- *About Silent Installation on page 4-2*
- *Performing Silent Installation on page 4-2*

About Silent Installation

This version of ScanMail Mobile 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 Mobile records the installation process into a preconfigured file.
- In recording mode, ScanMail Mobile 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.
- 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 Mobile Security *for Microsoft Exchange* directory.

3. Type `Setup /R` to start recording mode.

4. Copy the preconfigured file (`setup-xxx.iss`) to the ScanMail Mobile Security *for Microsoft Exchange* directory when the recording completes.

   For details about the preconfigured file settings, see *Preconfigured Files on page A-1*.

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

   For example:

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

   Note

   The password is not and cannot be encrypted in the file.

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 4-1. Silent Installation Setting Parameters

PARAMETER	DESCRIPTION
`Setup /H |Help| ?`	Displays the **Help** screen.

PARAMETER	DESCRIPTION
`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 5

Removing ScanMail Mobile

This chapter describes how to remove ScanMail Mobile.

Topics in this chapter:

- *Uninstallation Overview on page 5-2*
- *Using the Enterprise Solution DVD on page 5-3*
- *Using the Windows Control Panel on page 5-13*

Uninstallation Overview

Uninstallation removes the following components:

- ScanMail Mobile product console
- All program files
- Program folders
- Entries made to the registry

Uninstallation of ScanMail Mobile 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 Mobile from the Windows Control Panel or the Uninstall program.
- Do not manually uninstall ScanMail Mobile.

Privilege Requirements

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

TABLE 5-1. Minimum Privileges Required for Uninstalling ScanMail Mobile

EXCHANGE VERSION	MINIMUM PRIVILEGES
Exchange Server 2013 Mailbox	Local Administrator and Domain User
Exchange Server 2010 with Client Access Server	Local Administrator and Domain User

Using the Enterprise Solution DVD

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

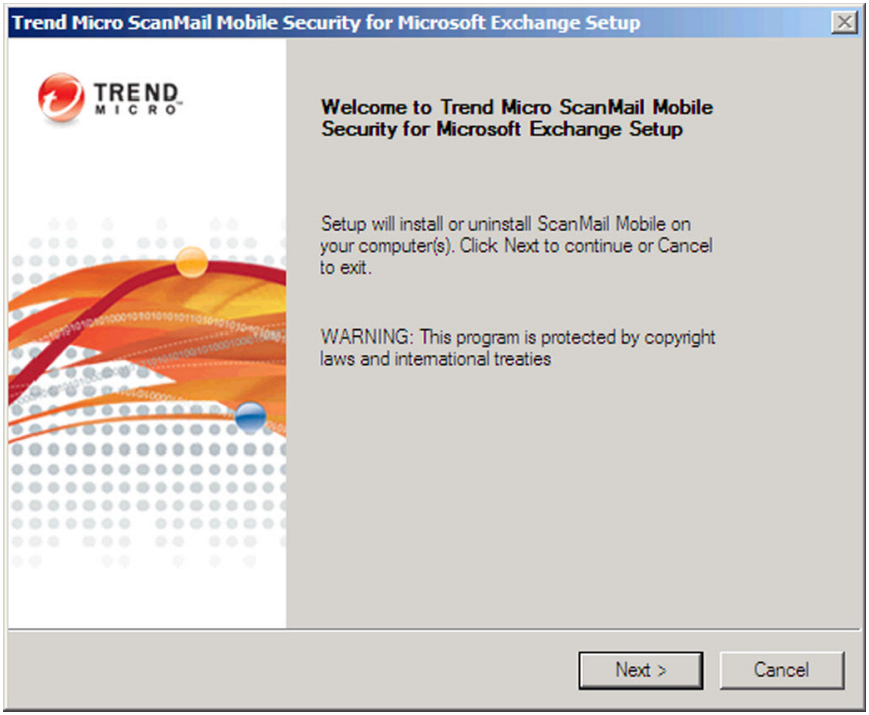
Procedure

1. To remove ScanMail Mobile, run `setup.exe` from the Trend Micro Enterprise Solution DVD.
2. Select uninstall when prompted.

Note

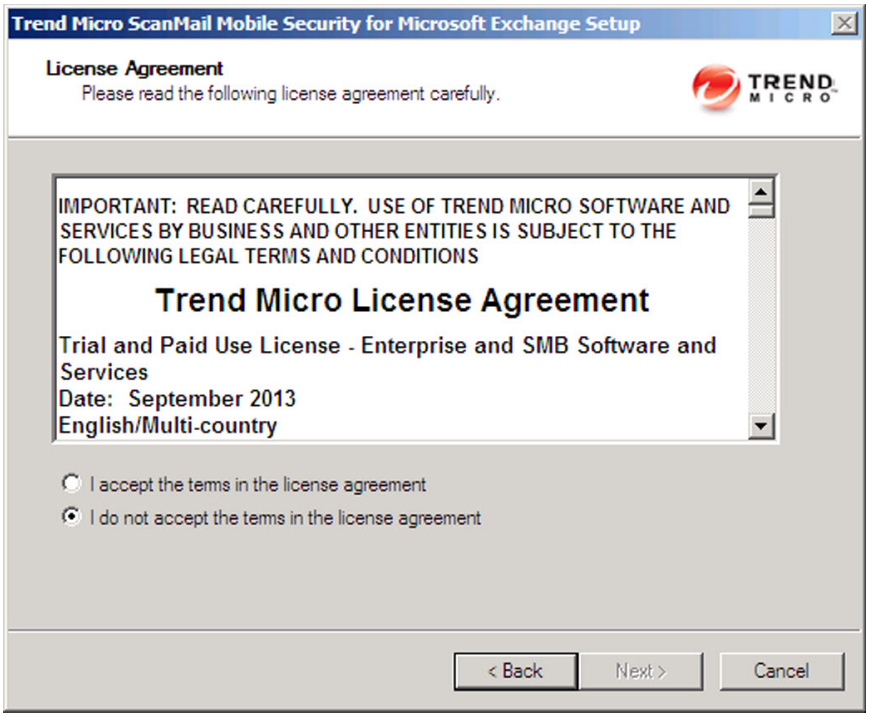
If, at any time, you click **Cancel** from the Setup program, the program will display an **Exit Setup** dialog box. When you click **Yes** from this dialog box, the uninstallation aborts.

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



3. Click **Next**.

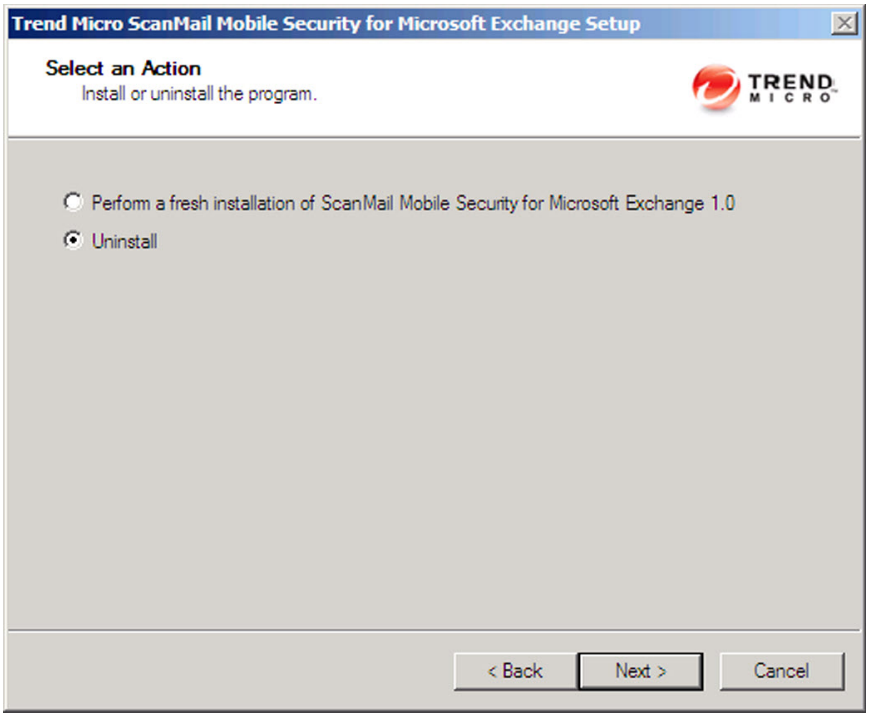
The **License Agreement** screen appears.



4. Agree to the terms of the agreement by selecting **I accept the terms in the license agreement**. If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the process without modifying your operating system.

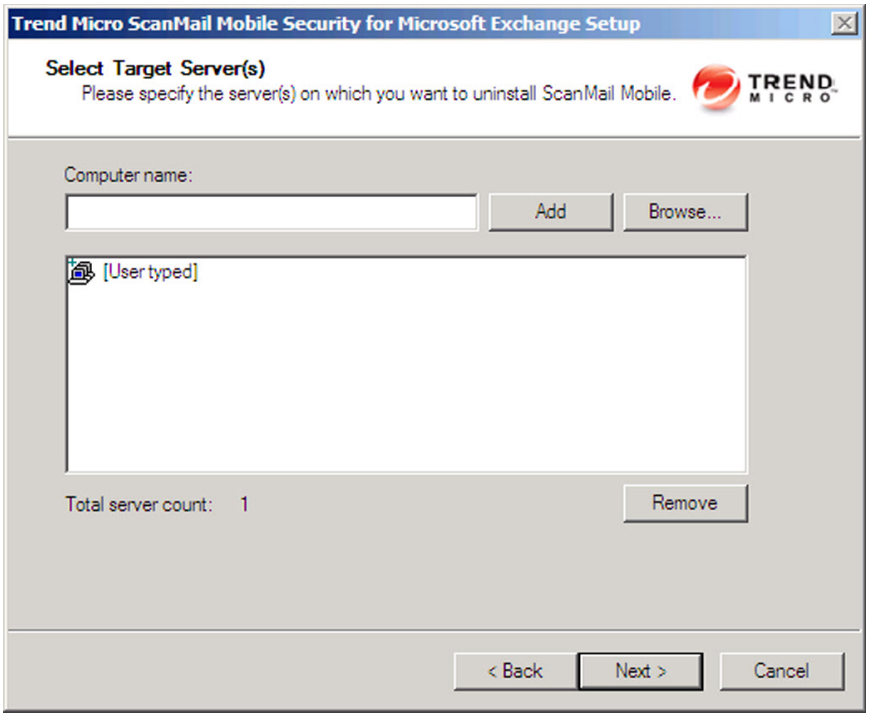
5. Click **Next**.

The **Select an Action** screen appears.



6. Select **Uninstall** to remove ScanMail Mobile from the target server(s).

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

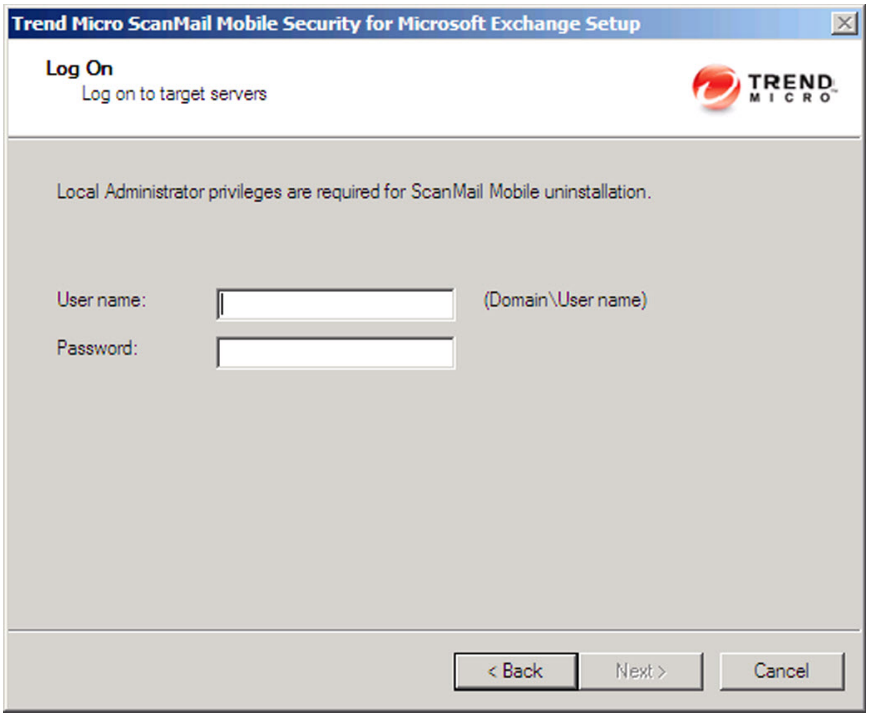


7. Select the computers from which you want to uninstall ScanMail Mobile:

   - Type the name of the server from which you want to uninstall 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.

8. Click **Next**.

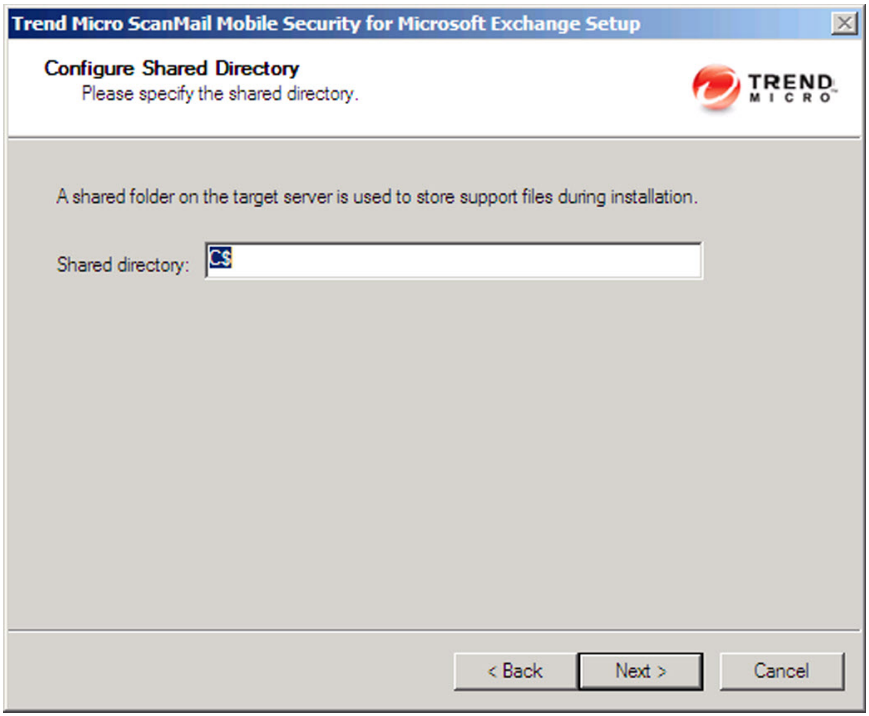
The **Log On** screen appears.



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

10. Click **Next**.

The **Configure Shared Directory** screen appears.

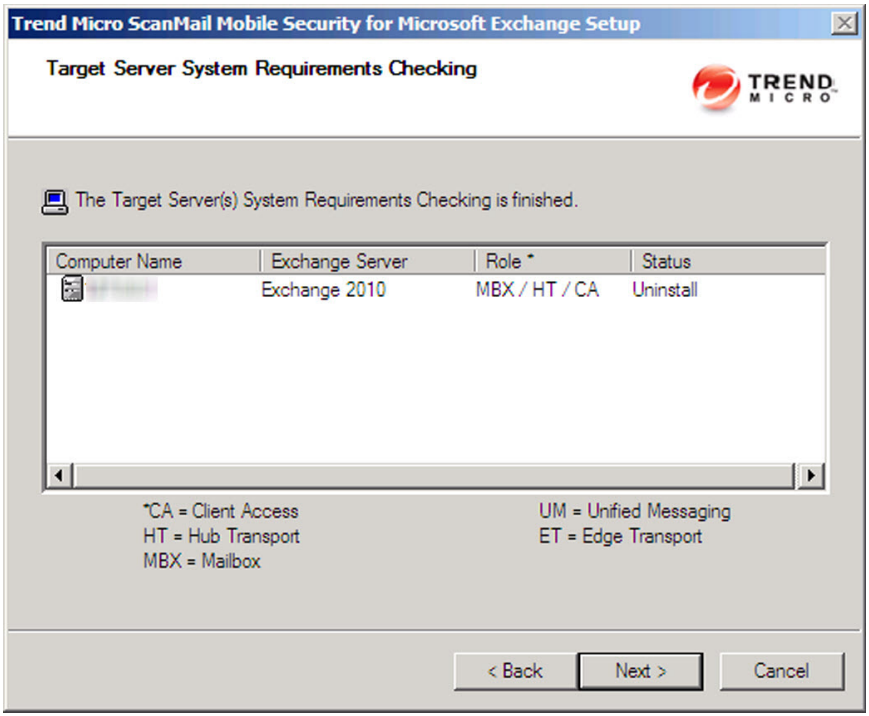


11. Specify the shared directory for the target servers from where you will uninstall ScanMail Mobile.

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

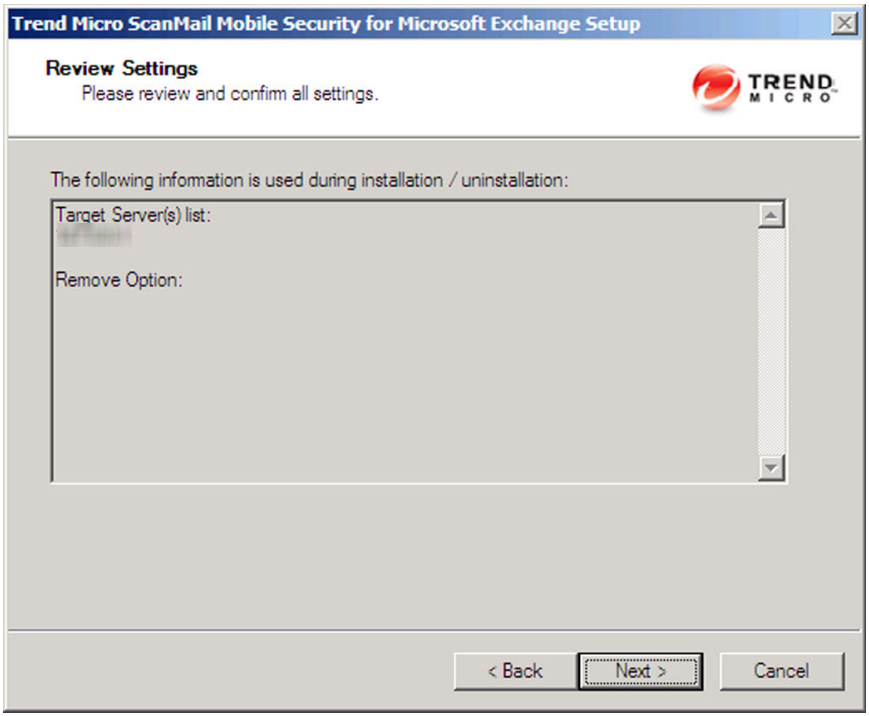
b. Click **Next**.

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



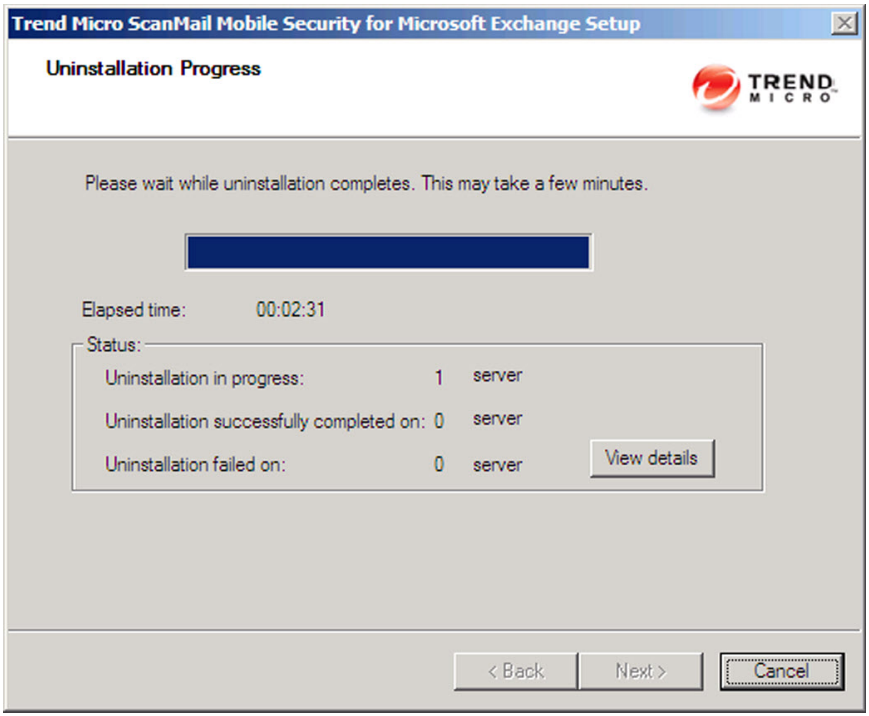
12. View the screen and ensure the settings for the uninstallation are correct.
13. Click **Next**.

The **Review Settings** screen appears.



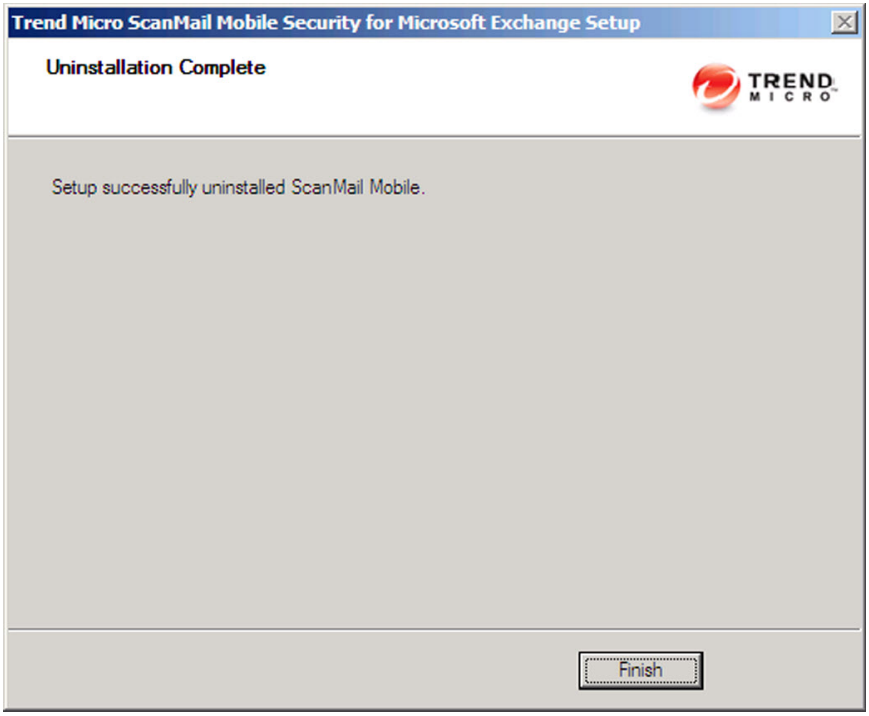
14. Review your settings.
15. Click **Next**.

The **Uninstallation Progress** screen appears.



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

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



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

    The Setup program removes ScanMail Mobile from the selected servers.

Using the Windows Control Panel

You can remove ScanMail Mobile using the Microsoft™ Windows™ Control Panel, but you must remove Microsoft SQL Server 2008 R2 Express separately after uninstallation. Using the Setup program to uninstall ScanMail Mobile removes all related components and programs.

Tip

Trend Micro recommends using the `Setup.exe` program to uninstall ScanMail Mobile.

Procedure

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

Note

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

Chapter 6

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 6-2*
- *Speeding Up Your Support Call on page 6-3*
- *Knowledge Base on page 6-3*
- *Security Information Site on page 6-4*

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

Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use the Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in the Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

The Knowledge Base can be accessed by all Trend Micro customers as well as anyone using an evaluation version of a product. Visit:

http://esupport.trendmicro.com/

And, if you can't find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 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 Mobile banner at the top of any ScanMail Mobile 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=smmstemp` • `ShareName=C$` **Note** This is the default setting and can be changed. • `TargetDir=C:\Program Files\Trend Micro\ScanMail Mobile` **Note** This is the default setting and can be changed.

SECTION	CONTENTS
	• `UseDefaultProgPath=0` or `1` **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 • `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>`
SMTP	`EnableSMTPScanning=1` **Note** 0 is disable, 1 is enable
Do NOT edit these settings	• `LogonPassword=<Your configuration>` **Note** Password does not display. • `ProxyPassword=<Your configuration>`

SECTION	CONTENTS
	Note Password does not display. • `ConsolePassword=<Your configuration>` **Note** Password does not display.
InstallOption	• `RequestActionType=1`
RemoteSQL	• `RemoteSQLServerName=<Your configuration>` • `RemoteSQLUserName=<Your configuration>` **Note** A dbcreator role is required. • `RemoteSQLPassword=<Your configuration>`

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 Mobile See also, Registration Key
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
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
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.

TERM	DESCRIPTION
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).
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.
Dynamic Host Control Protocol (DHCP)	A device, such as a computer or switch, must have an IP address to be connected to a network, but the address does not have to be static A DHCP server, using the Dynamic Host Control Protocol, can assign and manage IP addresses dynamically every time a device connects to a network.
Dynamic IP Address (DIP)	A Dynamic IP address is an IP address that is assigned by a DHCP server The MAC address of a computer will remain the same, however, the computer may be assigned a new IP address by the DHCP server depending on availability.

TERM	DESCRIPTION
End-User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking I accept during installation. Clicking I do not accept 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.
Executable file	A binary file containing a program in machine language which is ready to be executed (run)
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
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 Mobile server and/or client program
HTTP (Hypertext Transfer Protocol)	The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents It conventionally uses port 80.

TERM	DESCRIPTION
HTTPS (Hypertext Transfer Protocol Secure)	A variant of HTTP used for handling secure transactions
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)
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building
License	Authorization by law to use ScanMail Mobile Security *for Microsoft Exchange*
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.
Message size	The number of bytes occupied by a message and all its attachments

TERM	DESCRIPTION
Notification	A message that is forwarded to one or more of the following: • System administrator • Sender of a message • Recipient of a message • Other email address • SNMP and Windows event log The purpose of the notification is to communicate that an event has occurred, such as a virus being detected in a message
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.
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.
Post Office Protocol 3 (POP3)	POP3 is a standard protocol for storing and transporting email messages from a server to a client email application
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database See also, Activation Code.
Scan	To examine items in a file in sequence to find those that meet a particular criteria
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

TERM	DESCRIPTION
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.
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 Mobile uses the subject from the message header to determine the message subject.
Sync	The process of ensuring that data in two or more locations is updated to contain identical information
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
Undesirable content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail

TERM	DESCRIPTION
Wildcard	For ScanMail Mobile, an asterisk (*) represents any character For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on.
Zip file	A compressed archive (in other words, “zip file”) from one or more files using an archiving program such as WinZip

Index

A

ActiveUpdate, 1-7

C

configurations
- backing up, 1-5
- Exchange Server 2010, 1-8
- Exchange Server 2013, 1-8
- restoring, 1-5, 1-6

contacting
- technical support, 6-4

D

deploying, 1-8
- Exchange Server 2010
  - configurations, 1-8
  - recommendations, 1-8
  - server roles, 1-8
- Exchange Server 2013
  - configurations, 1-8
  - recommendations, 1-8
  - server roles, 1-8
- in the demilitarized zone (DMZ), 1-7
- on Exchange Server 2010, 1-8
- on Exchange Server 2013, 1-8
- on multiple LAN segments, 1-9
- strategies, 1-7
- to multiple servers, 1-7

deployment strategy, 1-6

Domain User, 1-9

E

enhanced security, 1-9

Enterprise Solution DVD, 5-3

Exchange Server 2010
- client access server, 2-2
- configurations, 1-8
- deploying to, 1-8
- privileges, 1-9, 1-17

Exchange Server 2013
- configurations, 1-8
- deploying to, 1-8
- mailbox server
  - installation, 2-2
- privileges, 1-9, 1-17

F

fresh installation, 1-9
- privileges, 1-9

I

IIS
- installing without, 1-10

installation
- Exchange Server 2010
  - client access server, 2-2
- Exchange Server 2013
  - mailbox server, 2-2
- preparing, 1-9
- privileges, 1-17
- remotely to Windows 2008, 1-14
- remotely to Windows 2012, 1-14
- remote Windows 2008 requirements, 1-14
- remote Windows 2012 requirements, 1-14
- silent install, 4-2
  - preconfigured file, A-1
- verification, 3-2
  - installation folder, 3-2

registry keys, 3-2
services, 3-2
without IIS, 1-10
with remote SQL server, 1-11
Internet Information Services
installing without, 1-10
InterScan Messaging Security Suite, 1-9
InterScan VirusWall, 1-9
IPv6, 2-7

L
Local Administrator, 1-9

M
minimum privileges, 1-9
multiple LAN segments, 1-9

N
network traffic, 1-7
ActiveUpdate, 1-7
planning for, 1-7

O
OfficeScan, 1-9

P
pilot installation, 1-4
Step 1 - Creating an Appropriate Test Site, 1-5
Step 3 - Executing and Evaluating, 1-6
preconfigured file, A-1
pre-installation, 1-17
privileges
Domain User, 1-9
Local Administrator, 1-9

R
rollback plan, 1-5, 1-6
backing up configurations, 1-5
restoring configurations, 1-5, 1-6

S
security information site, 6-4
silent installation, 4-2, A-1
about, 4-2
limitations, 4-2
performing, 4-2
preconfigured file, A-1
silent installations
preconfigured files, 4-3
setting parameters, 4-3
SQL
remote server, 1-11
security level default, 2-15

T
TrendLabs, 6-2
Trend Micro
download website, 1-5

U
uninstallation, 5-2, 5-3
Enterprise Solution DVD, 5-3
overview, 5-2
privileges
uninstallation, 5-2
Wizard, 5-3
URLs
email technical support, 6-4
security information site, 6-4
Trend Micro downloads, 1-5

W
Windows 2008, 1-14
multiple Exchange servers, 1-14
privileges, 1-14
requirements, 1-14

Windows 2012, 1-14
multiple Exchange servers, 1-14
privileges, 1-14
requirements, 1-14
Windows Firewall, 1-14

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM16093/130830