TREND MICRO™

# 1.6.5 TREND MICRO™ IM Security for Microsoft Skype for Business

## Administrator's Guide

Instant Protection for Instant Messaging

Messaging Security

Document Part No.: TIEM16347/140311

Release Date: September 2016

Protected by U.S. Patent No.: Pending

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

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

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

Evaluate this documentation on the following site:

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

### Privacy and Personal Data Collection Disclosure

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

The following link outlines the types of data that IM Security collects and provides detailed instructions on how to disable the specific features that feedback the information.

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

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

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

# Table of Contents

## Preface



## Chapter 1: Introducing Trend Micro IM Security



## Chapter 2: Pre-Installation Tasks

## Chapter 3: Installing and Upgrading IM Security



## Chapter 4: Silent Installation



## Chapter 5: Post-Installation Tasks

# Preface

## Preface

Welcome to Trend Micro™ IM Security. This book contains basic information about the tasks you need to perform to protect your servers. It is intended for novice and advanced users of IM Security who want to manage IM Security.

This preface discusses the following topics:

# IM Security 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 IM Security features.

- **Installation and Deployment 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/trend-micro-im-security.aspx) for updates to the documentation.

# Audience

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

- Antivirus and content security protection

- Data Loss Prevention
- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Microsoft Lync or Skype for Business Server administration
- Microsoft Lync Server 2013 server role configurations
- Microsoft Skype for Business 2015 server role configurations

## 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<br>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

## Introducing Trend Micro™ IM Security

This chapter introduces Trend Micro IM Security and provides an overview of its components and deployment.

Topics include:

# IM Security Overview

Instant messaging can mean instant exposure to fast-moving attacks designed to spread malware, lure victims to malicious sites, and steal data. Trend Micro™ IM Security for Microsoft ™ Skype™ for Business Server secures your real-time IM communications by stopping the wide range of threats—faster than ever. In-the-cloud Web Reputation blocks links to malicious sites before the links can be delivered. Signature-independent zero-day security, leading antivirus, and antispyware work together to stop malware before any damage can occur. Plus, flexible Content Filtering and Data Loss Protection features ensure appropriate IM use and prevent data theft.

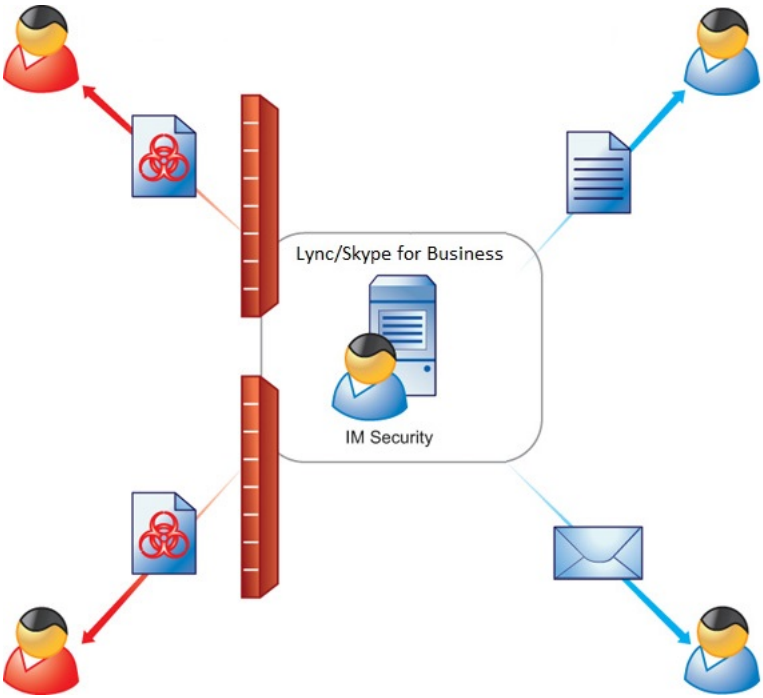



**FIGURE 1-1. IM Security deployment**

IM Security incorporates virus/malware and spyware/grayware scanning, Content Filtering, URL filtering, File Blocking, Data Loss Prevention, and Communication Control into one cohesive solution.

## Features and Benefits

The following table outlines the IM Security features and benefits.

| Feature | Benefit |
|---|---|
| Simple installation | IM Security provides the Setup installation program, which allows administrators to easily install the product on a single server or multiple servers with Lync Server 2013 or Skype for Business Server 2015. |
| Centralized product management | The IM Security web console allows administrators to configure IM Security anytime and from anywhere on the network. |
| Communication Control | Communication Control allows you to manage the Lync and Skype for Business Server features granted to accounts at a company-wide or granular level, or allows you to limit the interactions between specific accounts. |
| File transfer scanning | IM Security protects Lync Server 2013 or Skype for Business Server 2015 and instant messaging (Lync and Skype for Business Client) users from the following security risks associated with file transfers:<br>• Virus/Malware and spyware/grayware<br>• Sensitive or unwanted data transfers<br>• Malicious URLs |
| Instant message scanning | IM Security protects Lync Server 2013 or Skype for Business Server 2015 and instant messaging (Lync and Skype for Business Client) users from the following security risks associated with instant messages:<br>• Sensitive or unwanted data transfers<br>• Malicious URLs |

| Feature | Benefit |
|---|---|
| Configurable disclaimer statements | IM Security supports configurable disclaimer statements for instant messaging sessions. |
| Alerts and notifications | Set alerts to notify administrators or selected IT personnel whenever specific events related to IM Security or Lync/Skype for Business Server occur. Inform administrators and contacts about IM Security actions using customizable notifications. |
| Reports and logs | Monitor IM Security activities using queried logs that detail security risk detections, content security events, and program update events. In addition, IM Security provides the option to send graphical reports using email. |

# File and Instant Messaging Protection

IM Security protects Lync and Skype for Business Server users by providing the following scan filters.

**Table 1-1. Security Scan Filters**

| Scan Filter | Description |
|---|---|
| Virus Scan | Scans for viruses/malware, spyware/grayware, packers, and other security threats |
| File Blocking | Conserves network bandwidth, and prevents transmission of confidential information and malicious code hidden in files |
| Content Filtering | Monitors files and instant messages for inappropriate content |
| Web Reputation (URL filtering) | Protects against malicious websites |
| Data Loss Prevention | Monitors files and instant messages for sensitive content |

The following table presents the order in which IM Security applies file and instant messaging protection.

**TABLE 1-2. IM Security Order of Protection Precedence**

| ORDER | FILE-BASED PROTECTION | IM-BASED PROTECTION |
|---|---|---|
| 1 | File Blocking | Content Filtering |
| 2 | Content Filtering | Web Reputation (URL filtering) |
| 3 | Virus Scan | Data Loss Prevention |
| 4 | Web Reputation (URL filtering) | |
| 5 | Data Loss Prevention | |

IM Security uses all levels of protection to prevent files with viruses/malware, spyware/grayware, malicious URLs, unwanted content, or sensitive data from reaching intended recipients. IM Security uses Content Filtering, Web Reputation, and Data Loss Prevention filtering to prevent instant messages with unwanted content, malicious URLs, or sensitive data from reaching contacts.

## Communication Control

Communication Control manages the access granted to users, either granularly or company-wide, to features available during Lync/Skype for Business client communication. You can choose to block some features from specific users, groups, or even between specific users for a specified period of time.

## Virus Scan

File transfer scanning continually protects your Lync/Skype for Business Server environment. Virus scan scans for viruses/malware, spyware/

grayware, and other security risks that might be present in incoming and outgoing files.


**FIGURE 1-2. How IM Security Virus Scan works**

IM Security performs the following scan related tasks upon receiving a file:

1. Scans the file using the settings specified on the **Virus Scan** screen
2. Applies the virus scan action
3. Sends notifications to the administrator or contacts

IM Security allows you to notify administrators, or the Lync/Skype for Business client contacts involved in the virus/malware detection, through email, IM, SNMP, or Windows Event log.

## File Blocking

File Blocking scans for unwanted files based on file type, name, or size.


**FIGURE 1-3. How IM Security File Blocking works**

IM Security performs the following File Blocking related tasks upon receiving a file:

1. Scans the file and determines whether it matches the criteria set for the File Blocking rules.

   A File Blocking rule defines how IM Security blocks a file based on file type, file or extension name, or file size. If more than one criteria are enabled in a single rule, IM Security uses an OR relationship to connect the enabled criteria.

2. Applies the File Blocking action.

3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators, or the Lync/Skype for Business client contacts involved in the File Blocking event, through email, IM, SNMP, or Windows Event log.

## Content Filtering

Content Filtering protects your Lync/Skype for Business Server environment by filtering all incoming and outgoing files and messages for undesirable content.


**FIGURE 1-4. How IM Security Content Filtering works**

IM Security performs the following Content Filtering related tasks upon receiving a file or message:

1. Evaluates and determines whether content being transferred contains offensive information by comparing it to the list of keywords taken from enabled content filter rules.

   If there are five enabled rules, IM Security uses the keywords from those rules to determine whether a file or message contains unwanted content. IM Security implements an algorithm that consolidates all keywords from enabled rules for filtering. Doing so allows for faster file or message content filtering.

2. Applies the Content Filtering rule action.

   If a file or message matches more than one rule, IM Security applies the filter action specified by the rule with the highest priority.

3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators, or the Lync/Skype for Business client contacts involved in the Content Filtering detection, through email, IM, SNMP, or Windows Event log.

## Web Reputation

Web Reputation protects your Lync/Skype for Business Server environment by validating the authenticity of URLs that users send during messaging sessions and file transfers.

IM Security performs the following tasks upon receiving a URL:

1. Evaluates the URL to determine if it is a web threat or a legitimate URL.

   IM Security determines if a URL is a web threat by analyzing its reputation score. Trend Micro calculates the reputation score using proprietary metrics.

2. Applies the Web Reputation action.

   IM Security takes the action that the administrator specified on the **Web Reputation Actions** screen.

3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators, or the Lync/Skype for Business client contacts involved in the malicious URL detection, through email, IM, SNMP, or Windows Event log.

**Note**

The Web Reputation feature requires an active Internet connection.

## Data Loss Prevention

Data Loss Prevention protects your Lync/Skype for Business Server environment by evaluating the data that users send during messaging

sessions and file transfers to determine if sensitive information (as defined by you) is present in the conversation or files.


**FIGURE 1-5. How IM Security Data Loss Prevention works**

IM Security performs the following tasks when an instant message or file transfer occurs:

1. Scans the instant message or file and evaluates the content against the Data Loss Prevention rules defined by the administrator.

   IM Security evaluates all enabled Data Loss Prevention rules to determine if a template match occurred.

2. Applies the Data Loss Prevention action for any triggered rule.

   IM Security takes the action that the administrator specified on the **DLP Policies** screen under **Delivery Option**.

3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators, or the Lync/Skype for Business client contacts involved in the sensitive data transfer, through email, IM, SNMP, or Windows Event log.

## Reports and Logs

To provide current information about the security of your Lync/Skype for Business Server environment, IM Security is preconfigured to generate reports based on Virus Scan, File Blocking, Content Filtering (file transfers and instant messages), URL filtering (Web Reputation), Data Loss

Prevention, and server traffic. Reports can be generated on demand or scheduled on a daily, weekly, or monthly basis.

Log data can be exported to comma-separated value (CSV) files for further analysis. To prevent logs from consuming excessive disk space, use the **Logs** > **Maintenance** screen to schedule automatic log deletions for older logs.

### Alerts and Notifications

IM Security can issue several types of alerts and notifications in response to program or security events.

IM Security sends alerts in response to IM Security service events, update status, or Lync/Skype for Business Server events. IM Security can be configured to send alerts to network and server administrators and IT employees to inform them of system status, which are critical to network operations.

IM Security sends notifications in response to security events such as virus/malware and spyware/grayware detections, undesirable content or sensitive data transfers, and URL blocking actions. Notifications can be sent to administrators and other Lync/Skype for Business users.

## Protection Strategy

An organization must design a strategy that provides optimal protection for its Lync or Skype for Business server environment. Consider the following when selecting your IM Security protection strategy:

- What is the overall corporate IT security strategy?
- What are the available resources (processor, memory) on servers with Lync or Skype for Business server?
- Where and how can security risks and unwanted content enter the Lync or Skype for Business server environment (for example, file transfer, instant message)?

Trend Micro recommends the following strategies for optimal protection for a Lync or Skype for Business server environment:

- Implement a virus/malware and spyware/grayware scanning regimen
- Create File Blocking rules for unauthorized file types and extensions

**Note**

The IM Security product console provides the recommended file types and extensions to block.

- Create Content Filtering rules for unwanted or offensive keywords in instant messages and file transfers
- Create Data Loss Prevention rules for sensitive data in instant messages and file transfers
- Configure scheduled component updates

These strategies provide excellent protection, while also minimizing the system resource usage.

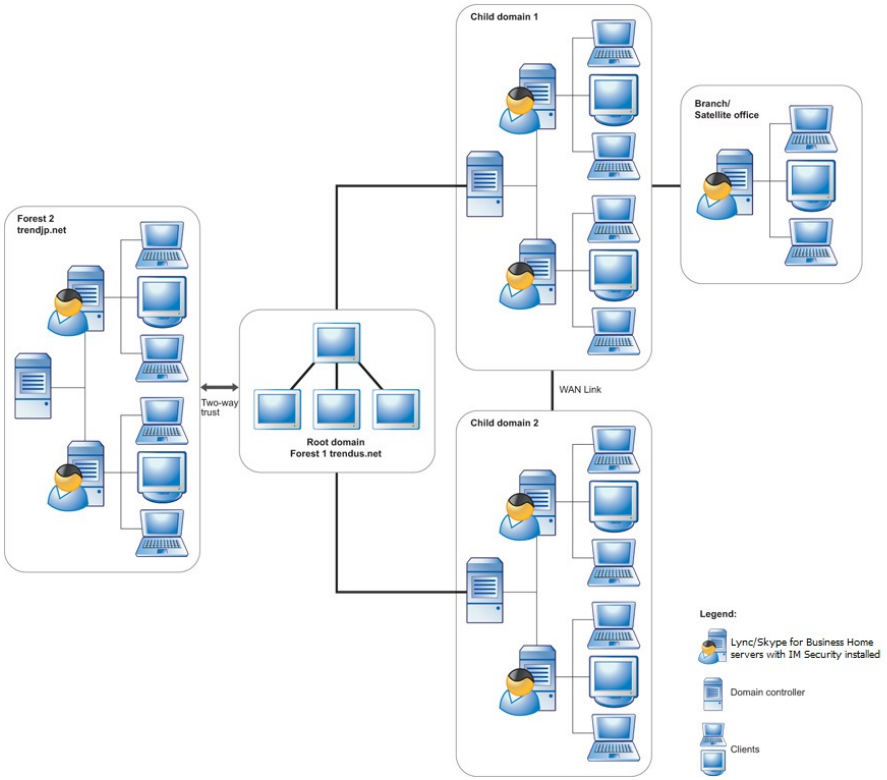



**FIGURE 1-6. A sample protected Lync/Skype for Business Server environment**

## IM Security and Lync/Skype for Business Server Deployment Scenarios

This section, using example configurations from the Microsoft Lync Server 2013/Skype for Business Server 2015 Technical document, is intended to help determine where to install IM Security. For details regarding the different

Lync/Skype for Business Server deployment scenarios, refer to the *Microsoft Lync Server 2013/Skype for Business Server 2015 Planning Guide* and the Microsoft Lync Server 2013/Skype for Business Server 2015 Technical document.

This section uses the three different Pool Configurations as a starting point to demonstrate where to install IM Security.

## Standard Edition Configuration

In a Standard Edition Configuration, a Front-End server hosts one or more Lync/Skype for Business Server services and the Back-End database. If you are using the Standard Edition Configuration, install IM Security on the same Front-End server that hosts the Lync/Skype for Business Server database and services.

Small to Medium Deployment Scenario

If your environment has fewer than 5,000 users, and you intend to utilize all of the Lync/Skype for Business Server services and allow external user access, you can deploy one IM Security protected Front-End server and one Access Edge server. Refer to the *Microsoft Lync Server 2013/Skype for Business Server 2015 Planning Guide* for more details and additional deployment scenarios.

**Note**

In these scenarios, you should only install IM Security on the Standard Edition (Front-End) servers.

## Enterprise Edition: Consolidated Configuration

In an Enterprise Edition: Consolidated Configuration, one or more Front-End servers host the Lync/Skype for Business Server services. The Back-End database is hosted on its own endpoint. If you are using the Enterprise Edition: Consolidated Configuration, install IM Security on each of the Front-End servers that host Lync/Skype for Business Server services.

Centralized Enterprise Deployment Scenario

If your environment has fewer than 30,000 users, deploy multiple IM Security protected front-end servers to utilize all Lync/Skype for Business Server services and provide external user access.

Access Edge servers are required to provide external user access. Refer to the *Microsoft Lync Server 2013/Skype for Business Server 2015 Planning Guide* for more details and additional deployment scenarios.

**Note**

In these scenarios, you should only install IM Security on the Enterprise Edition (Front-End) servers.

## Enterprise Edition: Expanded Configuration

In an Enterprise Edition: Expanded Configuration, one or more Front-End servers host the IM Conferencing. There are separate, dedicated servers that host other Lync/Skype for Business services such as the Office Web Apps Server and the Persistent Chat Server. The Back-End database is hosted on its own endpoint. If you are using the Enterprise Edition: Expanded Configuration, install IM Security on each of the Front-End servers that are hosting IM Conferencing.

Global Enterprise Deployment Scenarios

If your environment has more than 125,000 users distributed globally, deploy multiple IM Security protected Front-End servers to multiple locations. Install additional services on separate, dedicated computers.

**Note**

In these scenarios, you should only install IM Security on the Enterprise Edition (Front-End) servers.

# Chapter 2

## Pre-Installation Tasks

This chapter explains how to plan and prepare for an IM Security deployment.

Topics include:

# Planning for Deployment

Maximizing the benefits that IM Security can bring to an organization requires an understanding of the possible ways to deploy IM Security to servers with Lync Server 2013 or Skype for Business Server 2015 installed. This section provides a deployment overview and deployment considerations.

## Phase 1: Plan the Deployment

During phase 1, plan how to best deploy IM Security by completing these tasks:

- Review deployment considerations
- Conduct a pilot deployment on a test segment of the network
- Redefine the deployment strategy based on the results of the pilot deployment

## Phase 2: Install IM Security

During phase 2, start implementing the plan created in phase 1. Perform the following tasks:

- Perform pre-installation tasks
- Install IM Security
- Verify a successful installation

## Phase 3: Manage IM Security

During phase 3, manage an IM Security server from the web console. Perform the following tasks:

- Update to the latest IM Security components to help guarantee current protection for Lync/Skype for Business Servers

- Configure scan and filter settings
- Schedule updates and report generation

**Note**

This *Installation and Deployment Guide* discusses phases 1 and 2 and briefly introduces post-installation configuration tasks. Refer to the *IM Security Administrator's Guide* for detailed instructions relating to product administration.

## Deployment Considerations

Consider the following when planning for IM Security deployment:

- If your network environment employs Network Address Translation (NAT) devices, the IM Security protected Lync or Skype for Business Server and the clients need to be located together, behind or in front of the NAT device.
- In the Lync or Skype for Business Server Enterprise environment, install IM Security on each Front-End server to enable virus/malware scanning and content filtering for the entire organization.
- If a firewall exists between the Lync or Skype for Business Server and its clients, ensure that IM Security ports are opened.
- If Lync or Skype for Business Clients connect to Lync or Skype for Business Server through VPN, file transfer connections may not be established when IM Security file transfer scanning feature is enabled.
- For multiple Activation Codes, install IM Security to servers separately. Simultaneous and remote installations are not supported with multiple Activation Codes.
- The Setup program provides the option to enable Secure Sockets Layer (SSL) product console connection.

**Important**

You cannot configure SSL from the product console. SSL must be enabled during installation.

- Setup does not require stopping the Lync or Skype for Business Server services.
- If IM Security is installed with other instant messaging software, a scan conflict may occur.

**Important**

Setup does not detect other instant messaging antivirus applications.

- Remember to exclude the IM Security folders from other server-based, antivirus application scanning.

# Conducting a Pilot Deployment

Trend Micro recommends conducting a pilot deployment in a controlled environment to understand how features work, determine how IM Security can help you accomplish security goals, and estimate the level of support needed after a full deployment. A pilot deployment allows validation of and modifications to the deployment plan.

Perform the following tasks to conduct a pilot deployment:

- Choose a pilot site
- Create a contingency plan
- Deploy and evaluate the pilot

## Choosing a Pilot Site

Choose a pilot site that matches the planned deployment. This includes other security software installations (such as Trend Micro™ OfficeScan™,

ScanMail™, and ServerProtect™) you plan to use. Try to simulate the topology of your production environment.

### Creating a Contingency Plan

Trend Micro recommends creating a contingency plan in case there are issues with the installation, operation, or upgrade of IM Security services or components. Consider your network's vulnerabilities and how you can maintain a minimum level of security if issues arise.

### Deploying and Evaluating a Pilot Deployment

Deploy and evaluate the pilot deployment based on expectations regarding both security enforcement and network performance. Create a list of items that meet and do not meet the expected results experienced through the pilot process.

## Redefining the Deployment Strategy

Identify the potential pitfalls and plan accordingly for a successful deployment, take into consideration how IM Security performed with the antivirus installations on the network. This pilot evaluation can be rolled into the overall production and deployment plan.

## System Requirements

Individual company networks are as unique as the companies themselves. Therefore, different networks have different requirements depending on the level of network complexity. This section includes both the minimum and recommended requirements for the IM Security server.

**TABLE 2-1. Hardware and Software Requirements**

| HARDWARE/ SOFTWARE SPECIFICATIONS | MINIMUM REQUIREMENTS | RECOMMENDED REQUIREMENTS / NOTES |
|---|---|---|
| CPU | Intel™ Pentium™ 4 processor or later | |
| Hard disk space | 1 GB of available disk space | 1.5 GB of available disk space |
| Memory | 512 MB | 1GB<br><br>**Note**<br>Scale the memory with the processor; do not overpopulate with memory. |
| Operating System | • Microsoft™ Windows Server™ 2008 with SP2 (64-bit)<br>• Microsoft™ Windows Server™ 2008 R2 (64-bit)<br>• Microsoft™ Windows Server™ 2012<br>• Microsoft™ Windows Server™ 2012 R2 | **Note**<br>Only Standard, Enterprise, and Datacenter Editions are supported. |
| Microsoft™ Skype™ for Business Server | • Microsoft™ Lync™ Server 2013 (Front End Server), Standard or Enterprise Edition<br>• Microsoft™ Skype™ for Business Server 2015 (Front End Server), Standard or Enterprise Edition | **Note**<br>IM Security can only be installed on the Front-End servers. |

| Hardware/ Software Specifications | Minimum Requirements | Recommended Requirements / Notes |
|---|---|---|
| Web server | Microsoft™ Internet Information Services<br>• 7.0<br>• 7.5<br>• 8.0<br>• 8.5 | |
| Web browser | • Internet Explorer™ 7.0 or later<br>• Mozilla® Firefox® 3.0 or later | |
| Messaging clients | • Microsoft™ Office™ Communicator 2007/2007 R2<br>• Microsoft™ Lync™ 2010<br>• Microsoft™ Lync™ 2013/2013 Basic<br>• Microsoft™ Lync™ for Mobile<br>• Microsoft™ Skype™ for Business 2015/2015 Basic<br>• Microsoft™ Skype™ for Business 2016/2016 Basic<br>• Microsoft™ Skype™ for Business for Mobile | |

| Hardware/ Software Specifications | Minimum Requirements | Recommended Requirements / Notes |
|---|---|---|
| Database engine | • Microsoft™ SQL Server® 2008 Express (32-bit or 64-bit)<br>• Microsoft™ SQL Server® 2008 (32-bit or 64-bit)<br>• Microsoft™ SQL Server® 2008 R2 Express (32-bit or 64-bit)<br>• Microsoft™ SQL Server® 2008 R2 (32-bit or 64-bit)<br>• Microsoft™ SQL Server® 2012 (32-bit or 64-bit)<br>• Microsoft™ SQL Server® 2014 (32-bit or 64-bit)<br>• Microsoft™ SQL Server® 2016 (64-bit) | |
| Active Directory® | • Windows™ 2003<br>• Windows™ 2003 R2<br>• Windows™ 2008<br>• Windows™ 2008 R2<br>• Windows™ 2012<br>• Windows™ 2012 R2 | |
| Display | VGA monitor capable of 1024 x 768 resolution, with at least 256 colors to access the IM Security web console. | |

# Pre-Installation Tasks

Several pre-installation tasks can help to make the installation process easier. Complete the following tasks before installing IM Security:

- If a firewall exists between Lync/Skype for Business server and its clients, open the following ports to ensure IM Security connectivity.

  **TABLE 2-2. Ports for IM Security Connectivity**

| SERVICES | PORTS NEEDED |
|---|---|
| Product console | HTTP: 80<br>HTTPS: 443 |
| File transfer | 6891-6900 |
| Notification | SMTP: 25<br>SNMP: 162 |
| Server Management population through Global Catalog (GC) query | 3268 |

- Log on to the target server using an account with “Domain User” and “Local Administrator” privileges.

  Setup requires that a user with “Domain User” and “Local Administrator” privileges create the IM Security accounts.

- Address considerations of installing IM Security with other instant messaging antivirus products.

  The IM Security Setup program does not detect third-party IM environment antivirus applications. Scan conflicts may occur if third-party instant messaging antivirus applications are installed.

- Check that the target server complies with the system requirements.

  If the server’s specifications do not meet the requirements, Setup will not install IM Security.

- Check the remote SQL server meets the authentication requirements.

  For SQL server authentication, ensure the SQL account meets the following authentication requirement:

  - Database role: “dbcreator”

  For Windows authentication, ensure that the user logged on the target servers meets the following authentication requirements:

  - Database role: “dbcreator”
  - Groups: domain users and local administrators

- Obtain the proxy server and SMTP server settings, and any required authentication information.

  During installation, the Setup program prompts you for proxy information. If a proxy server handles Internet traffic on your network, 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.

- Close all open Microsoft Management Console (MMC) screens.
- Prepare the IM Security Activation Code (AC).

# Chapter 3

## Installing and Upgrading IM Security

This chapter provides instructions for installing and updating IM Security.

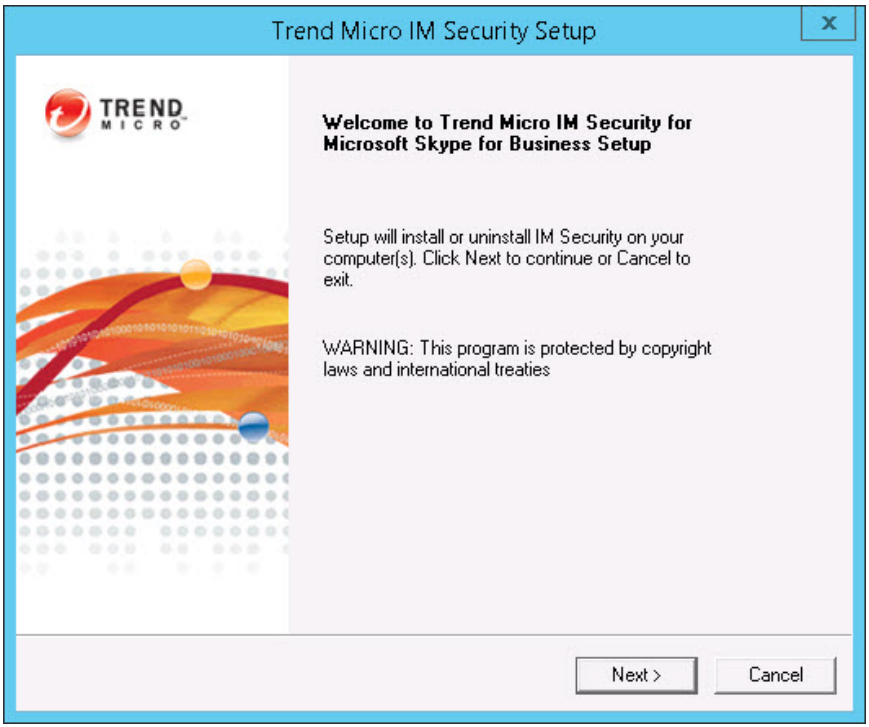
Topics include:

# Installing IM Security

**Procedure**

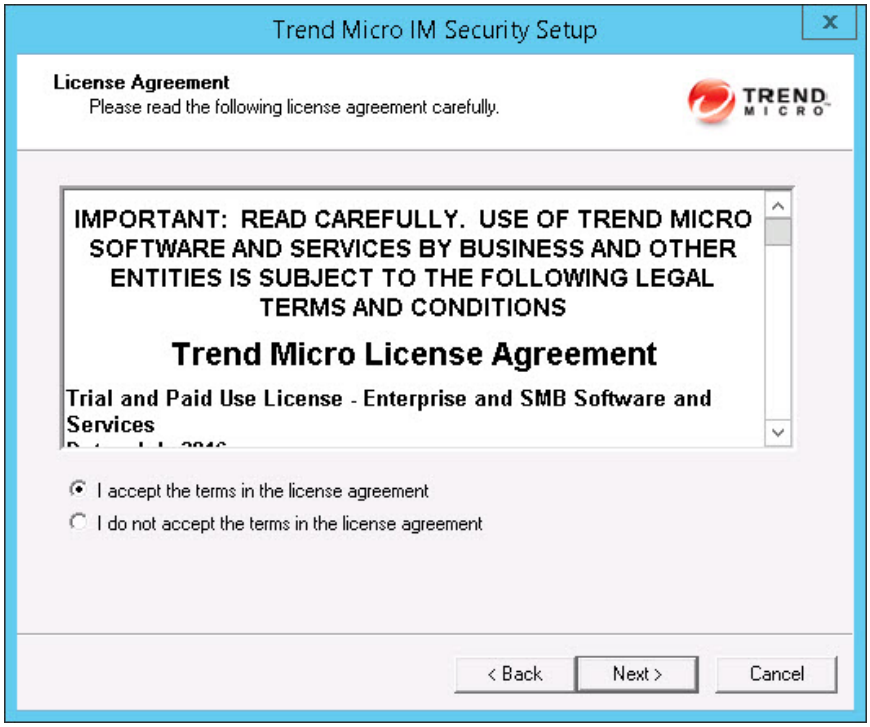
1. Select a source for the Setup program:
   - Trend Micro website
     a. Download IM Security from the Trend Micro website.
     b. Unzip the file to a temporary directory.
     c. Run `setup.exe` to install IM Security.
   - Trend Micro Enterprise Solution DVD
     a. Insert the DVD and follow the online instructions.

The **Welcome to Trend Micro IM Security for Microsoft Skype for Business Setup** screen appears.




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

The **License Agreement** screen appears.

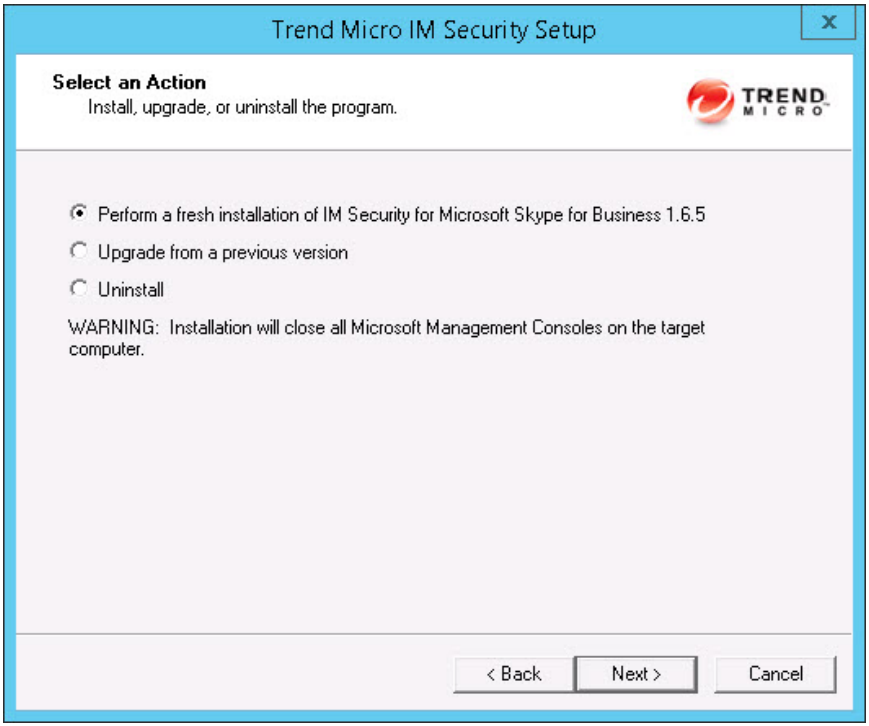



3. Click **I accept the terms in the license agreement** to agree to the terms of the agreement and continue installation. Click **Next** to continue.

**Note**

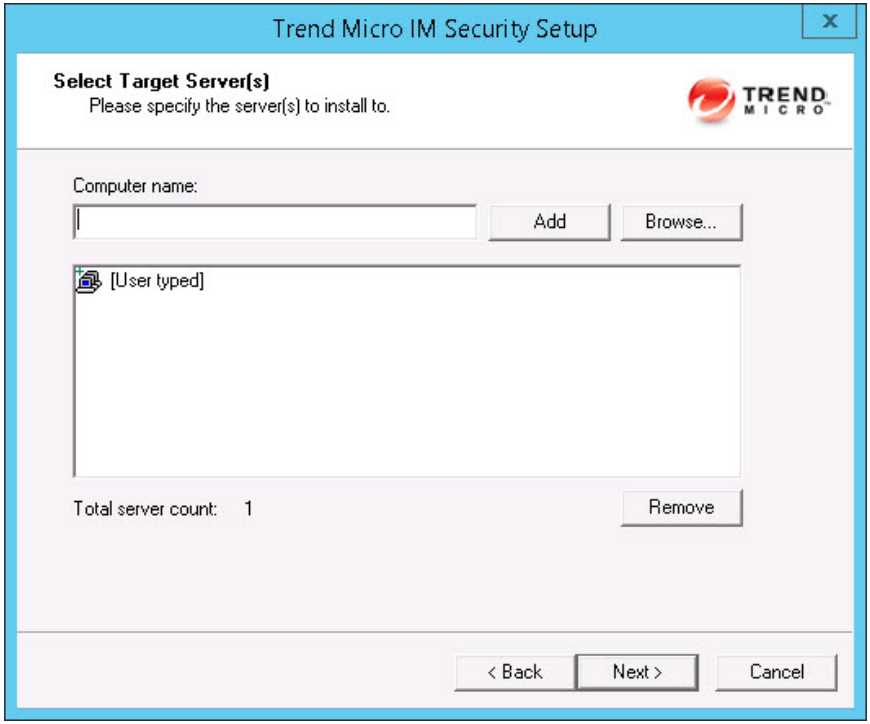
If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the installation without modifying your operating system.

The **Select an Action** screen appears.




4. Select **Perform a fresh installation of IM Security for Microsoft Skype for Business Server 1.6.5** to perform a fresh install. Click **Next** to continue.

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




5. Select the computers to which you want to install IM Security.

   a. Perform one of the following:

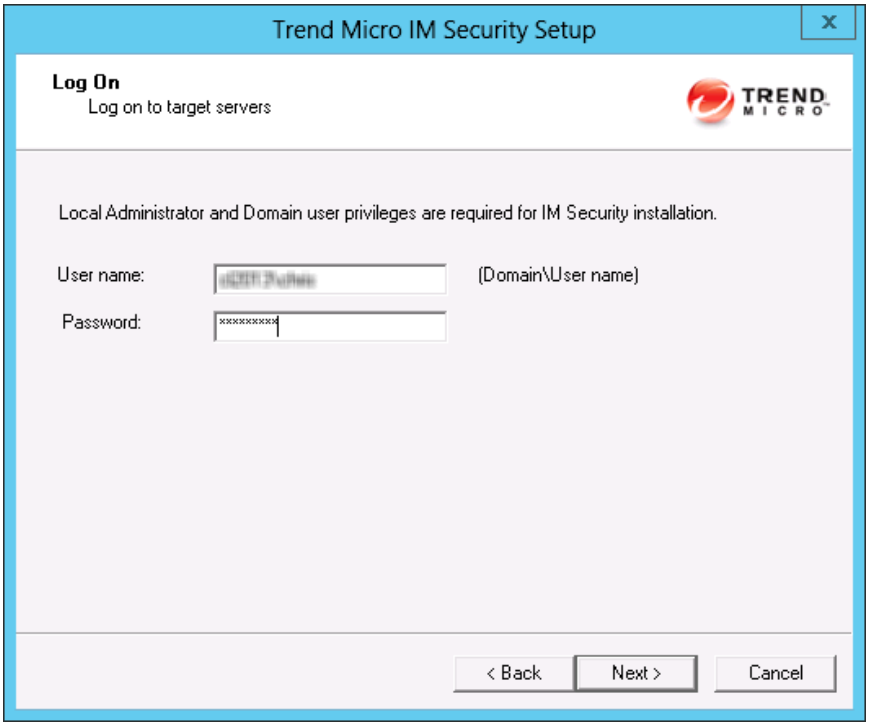
      - Type the name of the server to which you want to install in the **Computer name** field and click **Add** to add the computers to the list of servers.
      - Click **Browse** and browse the computers that are available on your network, then double-click the computers you want to add to the list.
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

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

**Note**

The Setup program can install IM Security 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 IM Security supports IPv6.

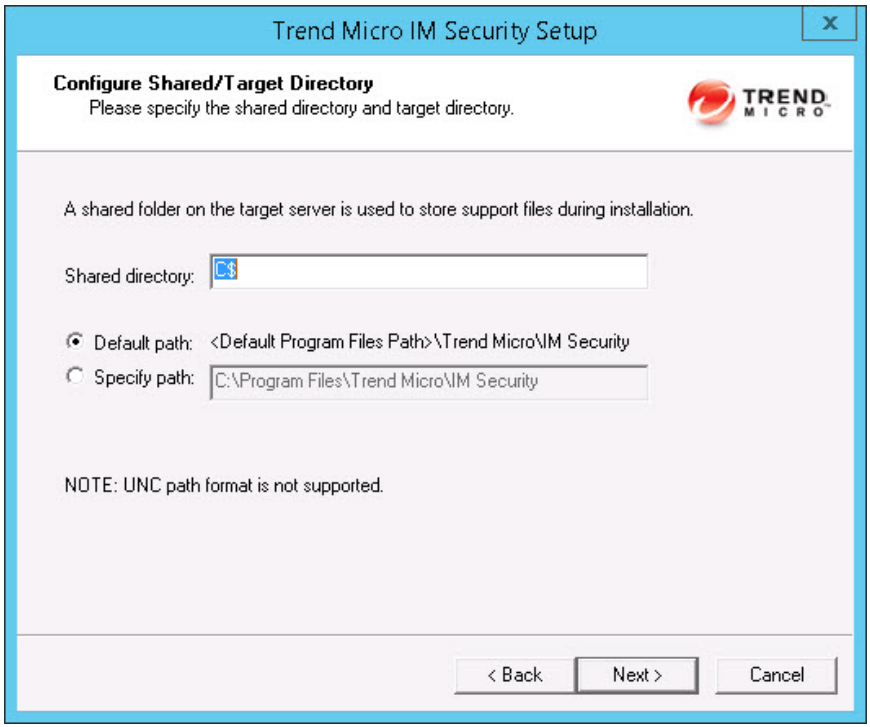
The **Log On** screen appears.




6. Log on to the target servers where you want to install IM Security. Use an account with “Domain User” and “Local Administrator” privileges.

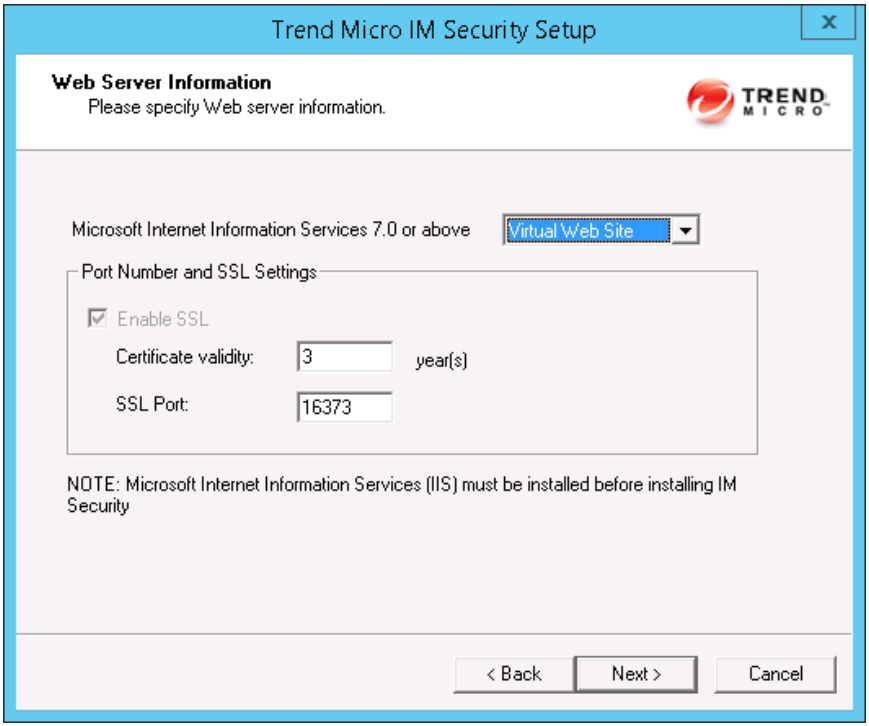
Type the user name and password to log on to the target server to install IM Security. Click **Next** to continue.

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



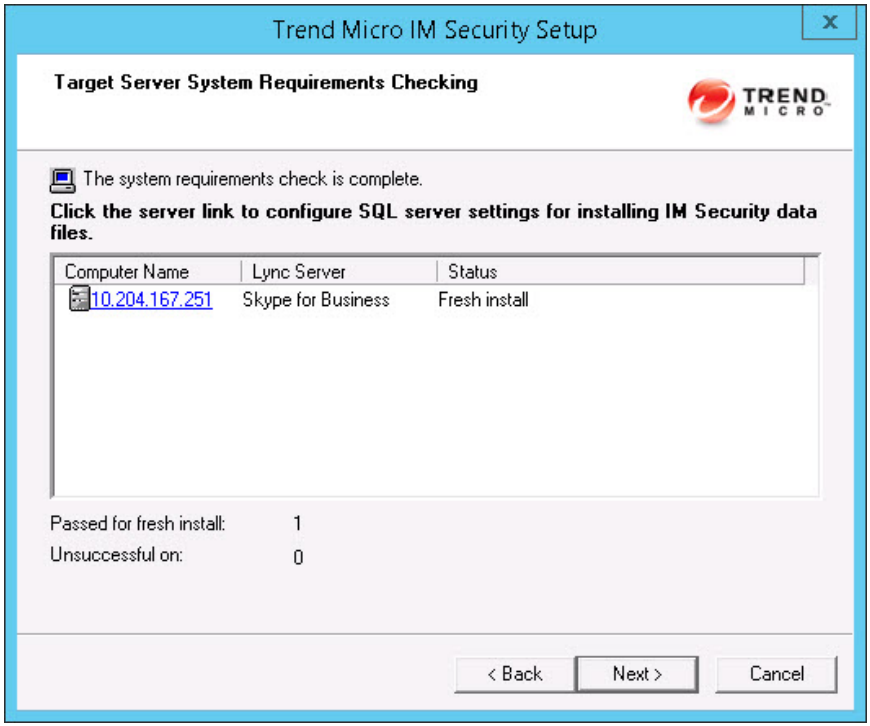

7. Type the directory share name for which the specified user has access rights or keep the default temporary share directory, `C$`. The Setup program uses the shared directory to copy temporary files during installation and is only accessible to the administrator. Select **Default path** or **Specify path** and type the directory path on the target server where you will install IM Security. Click **Next** to continue.

The **Web Server Information** screen appears.




8. 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.

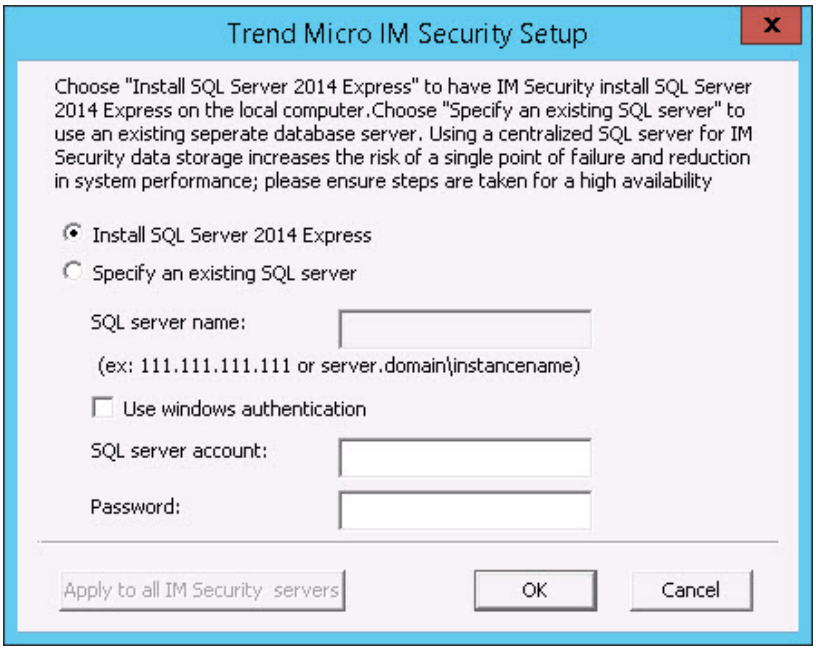
The **Target Server System Requirements Checking** screen appears.




9. Review the settings.

   a. To install IM Security on a remote SQL server, click the virtual server on which to install IM Security data files.

The **SQL Server Selection** screen appears.




b. 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 name, SQL server account, and password.

**Note**

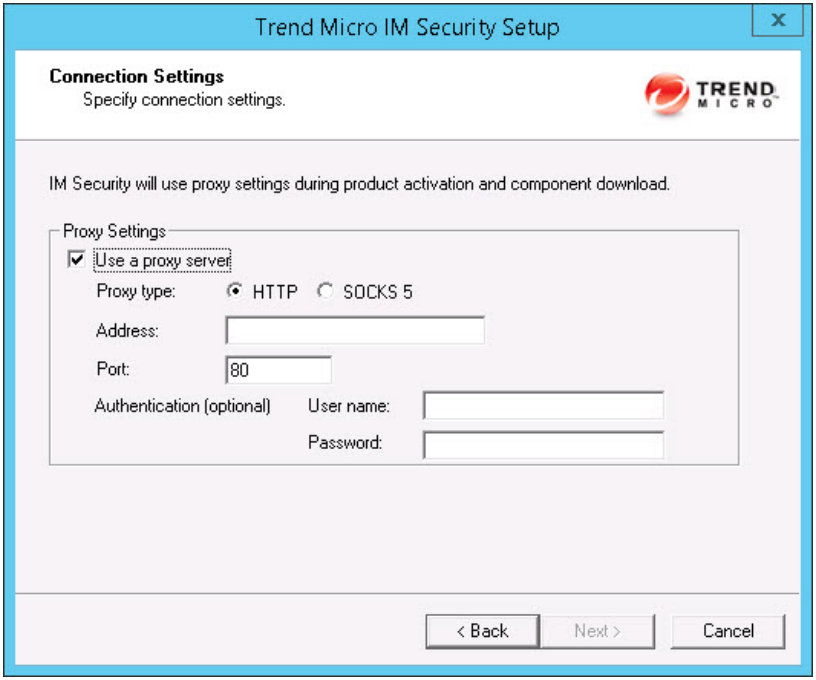
Using a centralized SQL server for IM Security data storage increases the risk of a single point of failure and reduction in performance. Ensure that steps are taken for a high-availability remote SQL server.

c. Click **OK**.

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

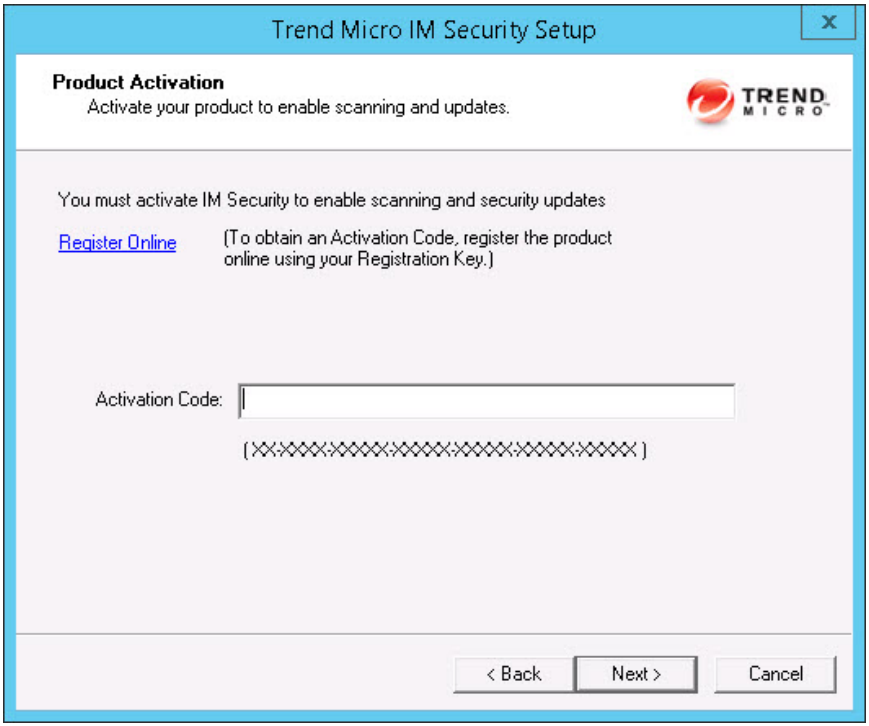
d. Check that the user name and password are correct. Click **Next**.

The **Connection Settings** screen appears.




10. 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.

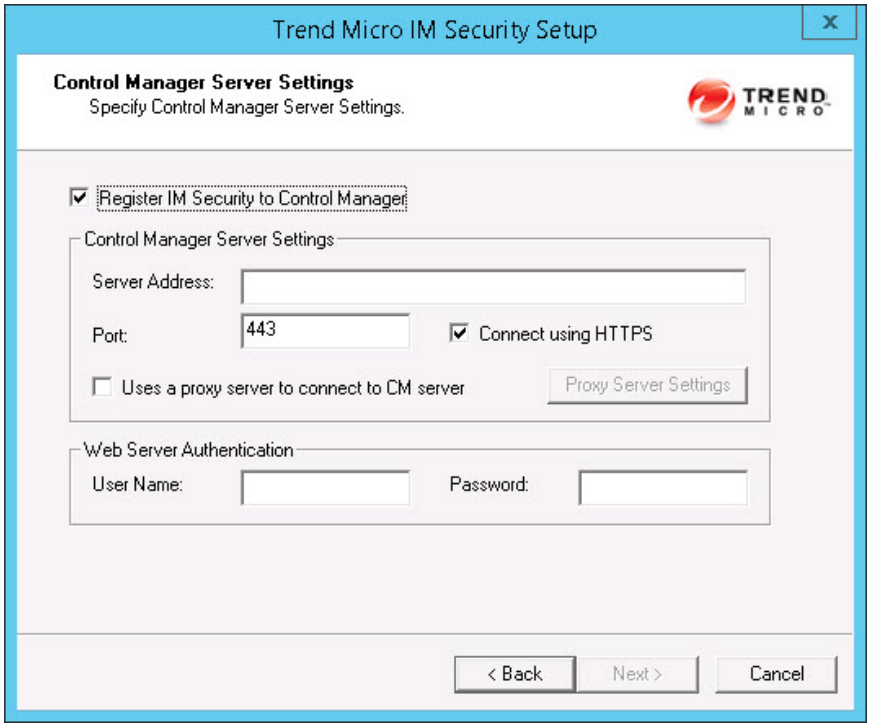



**11.** Type the activation code. Click **Next**.

**Note**

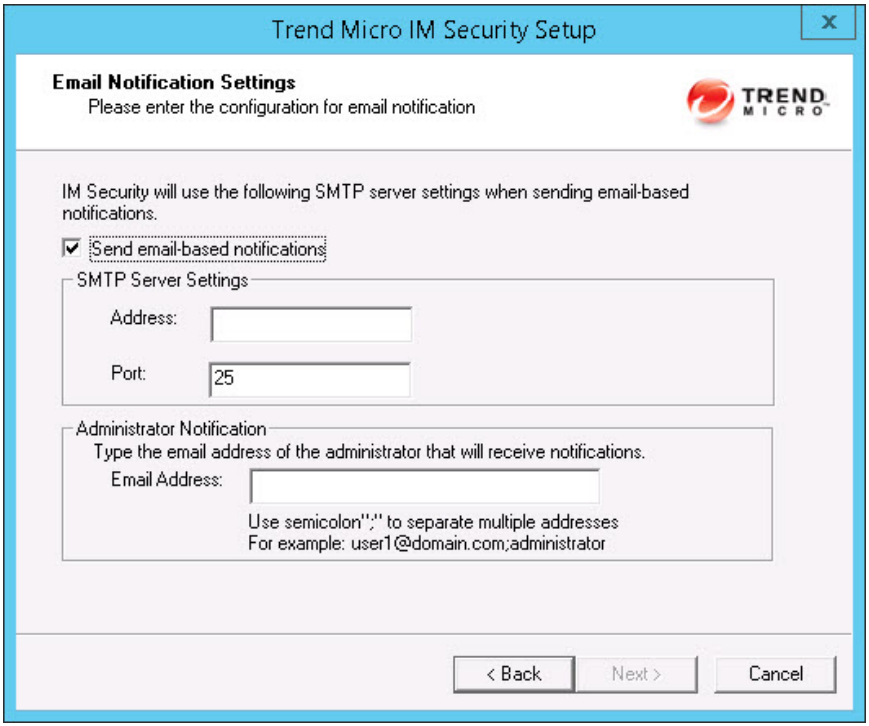
You can copy an Activation Code and paste it in the input field of the Activation Code on this screen.

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




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

    The **Email Notification Settings** screen appears.

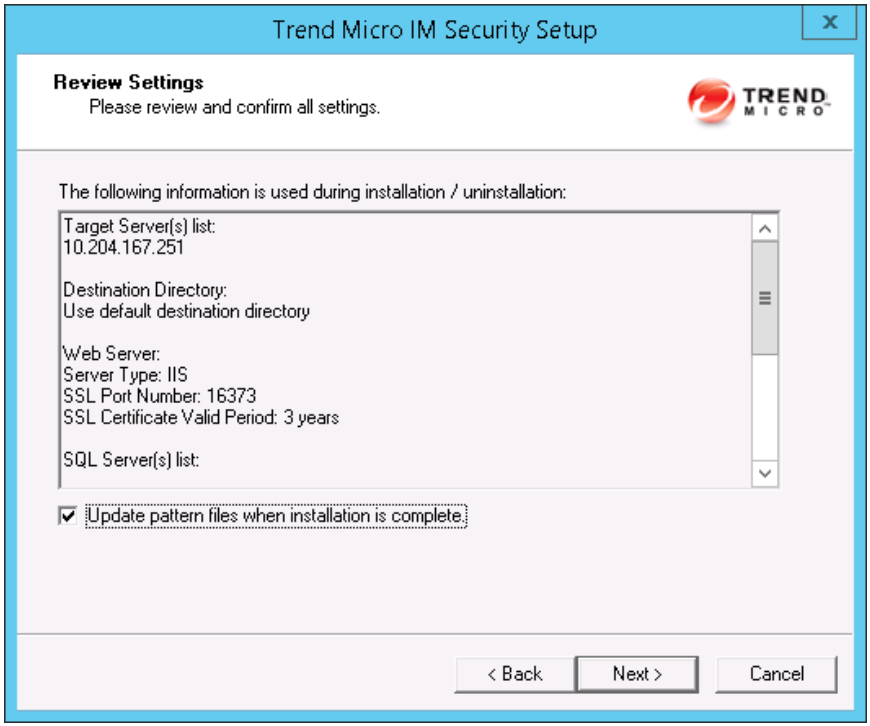



13. Specify the SMTP server settings that IM Security uses when sending email-based notifications. Click **Next** to continue.

**Tip**

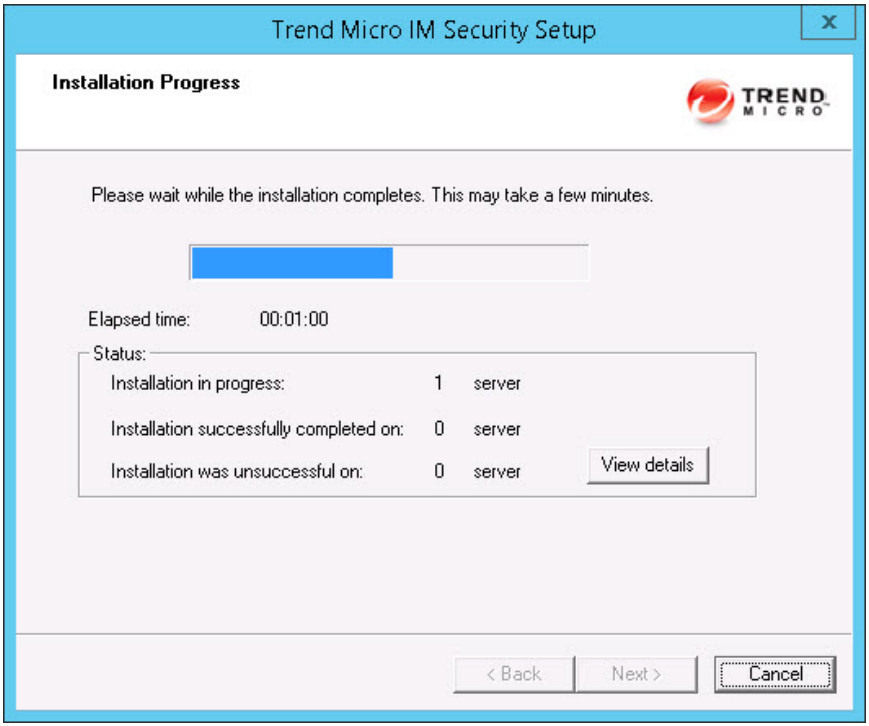
You can configure the SMTP server settings after the installation completes through the web console on the **Administrator Notification** screen (**Administration** > **Notification Settings**).

The **Review Settings** screen appears.




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.

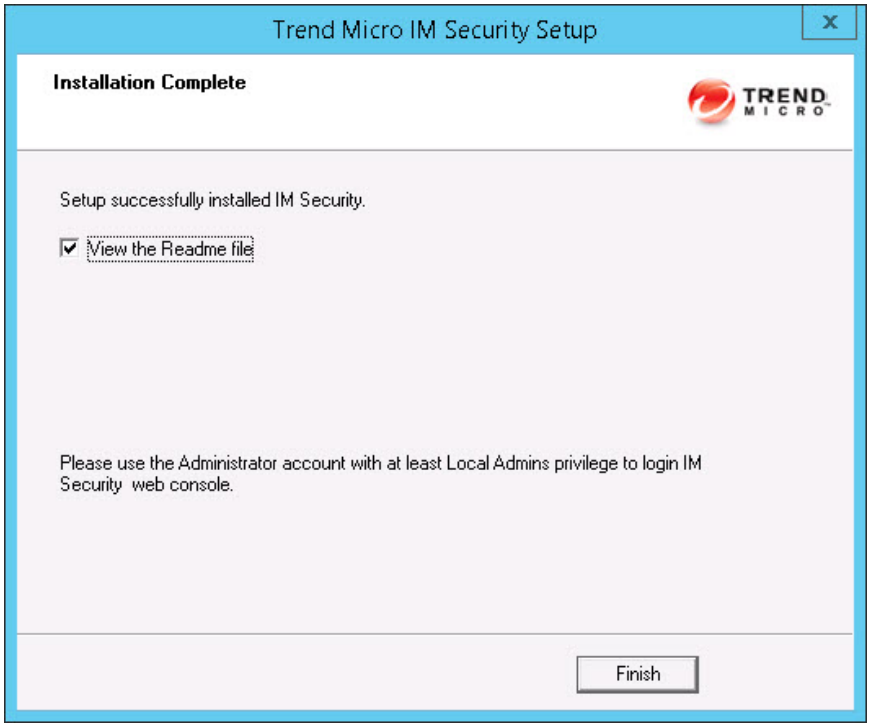



15. Click **View details** to display a list of each computer to which you are installing IM Security and the status of each computer. Click **Next** when the installation completes.

**Note**

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

The **Installation Complete** screen appears.




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

17. Use an administrator account with local administrator privileges to log on to the IM Security product console.

# Upgrading IM Security

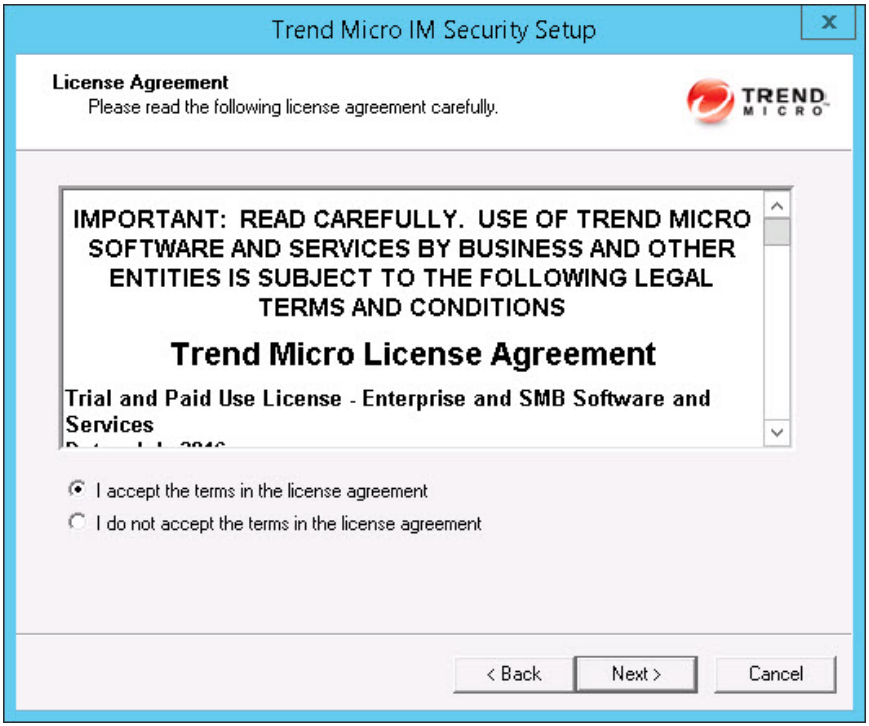
**Procedure**

1. Select a source for the Setup program:
   - Trend Micro website.
     a. Download IM Security from the Trend Micro website.
     b. Unzip the file to a temporary directory.
     c. Run `setup.exe` to install IM Security.
   - The Trend Micro Enterprise Solution DVD.
     a. Insert the DVD and follow the online instructions.

The **Welcome to Trend Micro IM Security for Microsoft Skype for Business Setup** screen appears.


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

The **License Agreement** screen appears.

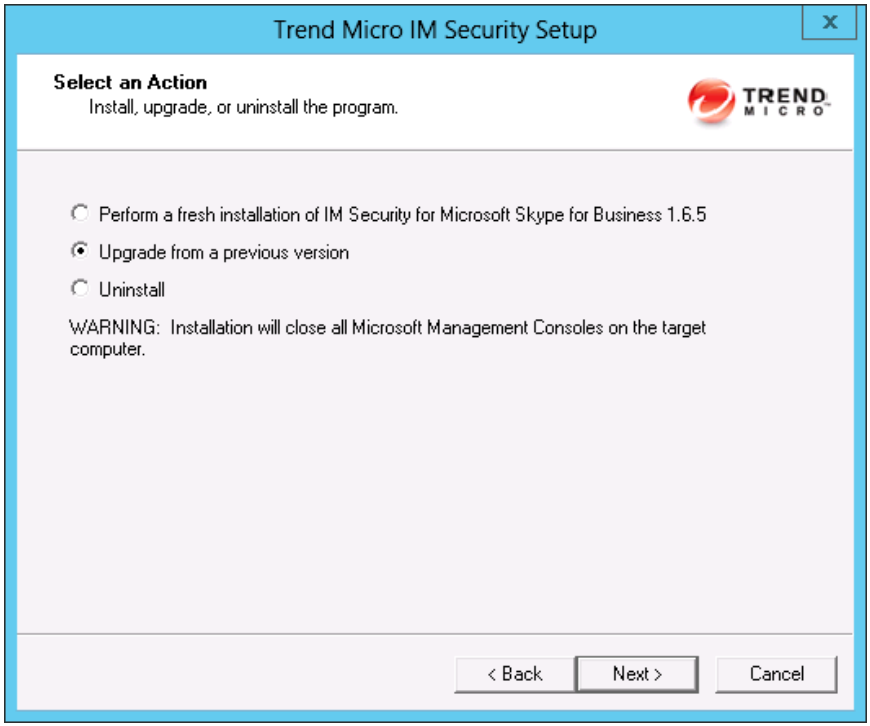



3. Click **I accept the terms in the license agreement** to agree to the terms of the agreement and continue installation. Click **Next** to continue.

**Note**

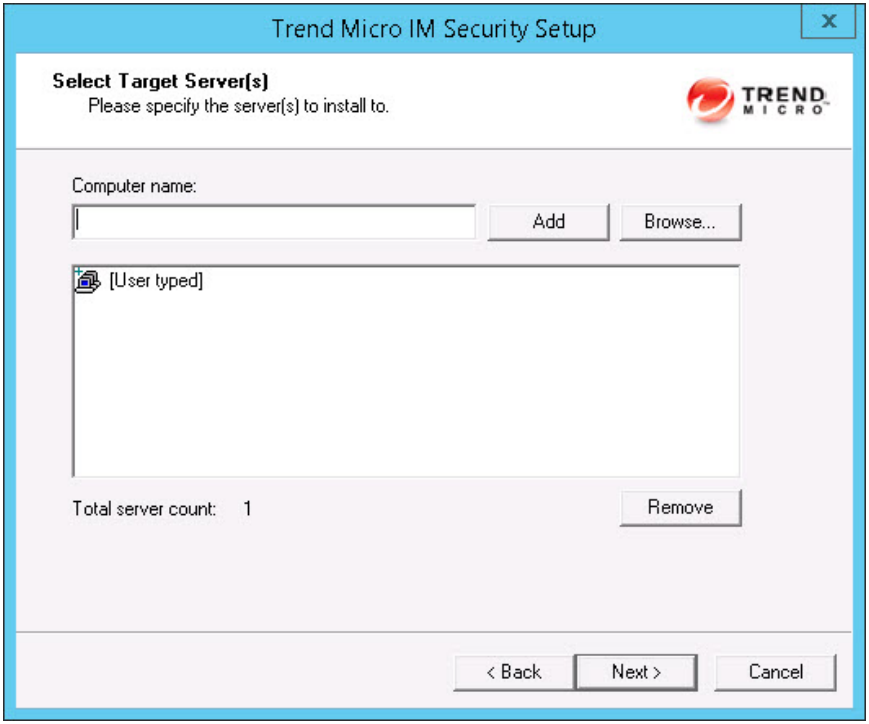
If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the installation without modifying your operating system.

The **Select an Action** screen appears.




4. Select **Upgrade from a previous version** to upgrade an existing version of IM Security. Click **Next** to continue.

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



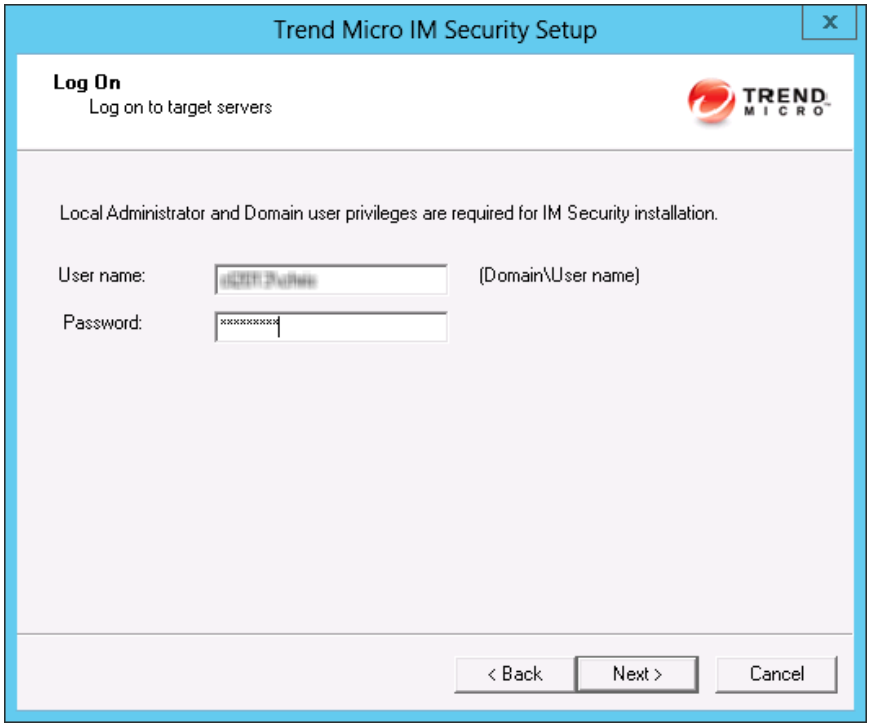

5. Select the computers to which you want to install IM Security.

   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.



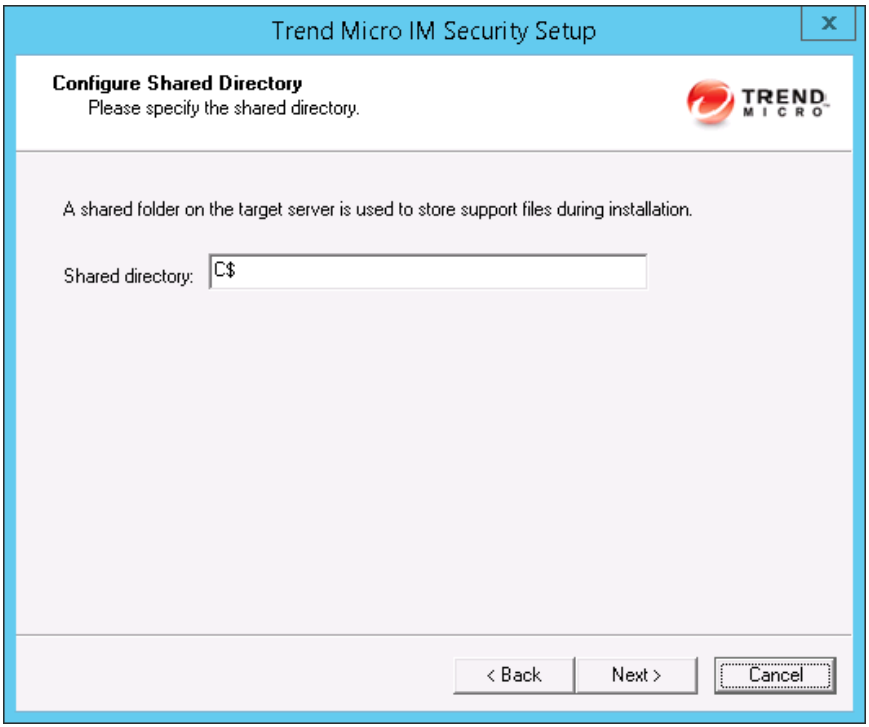

**Note**

The Setup program can install IM Security 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 IM Security supports IPv6.

6. Log on to the target servers where you want to install IM Security. Use an account with “Domain User” and “Local Administrator” privileges.

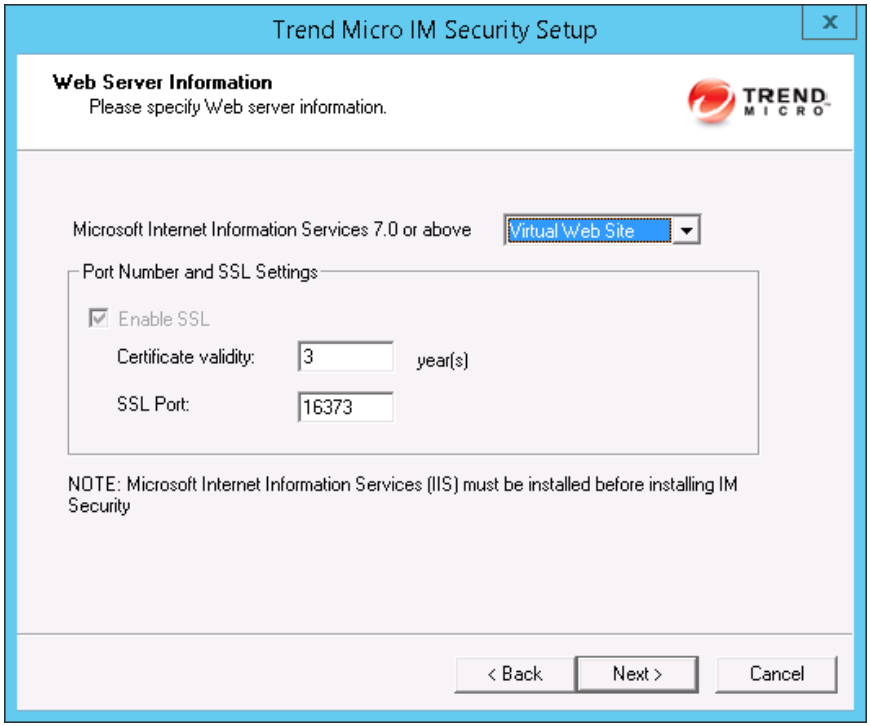
Type the user name and password to log on to the target server to install IM Security. Click **Next** to continue.

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



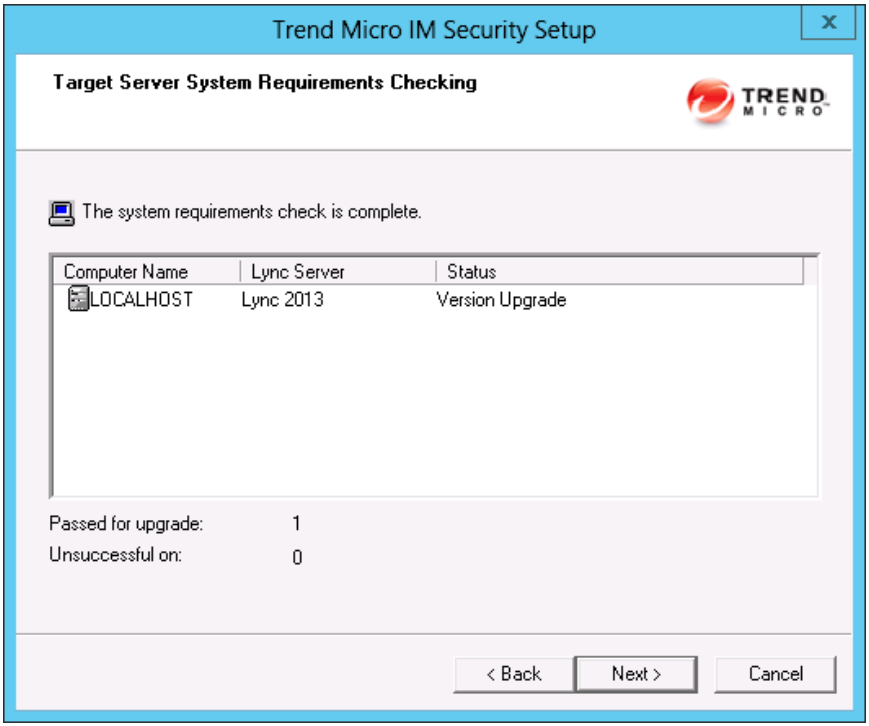

7. Type the directory share name for which the specified user has access rights or keep the default temporary share directory, `C$`. The Setup program uses the shared directory to copy temporary files during installation and is only accessible to the administrator. Click **Next** to continue.

The **Web Server Information** screen appears.



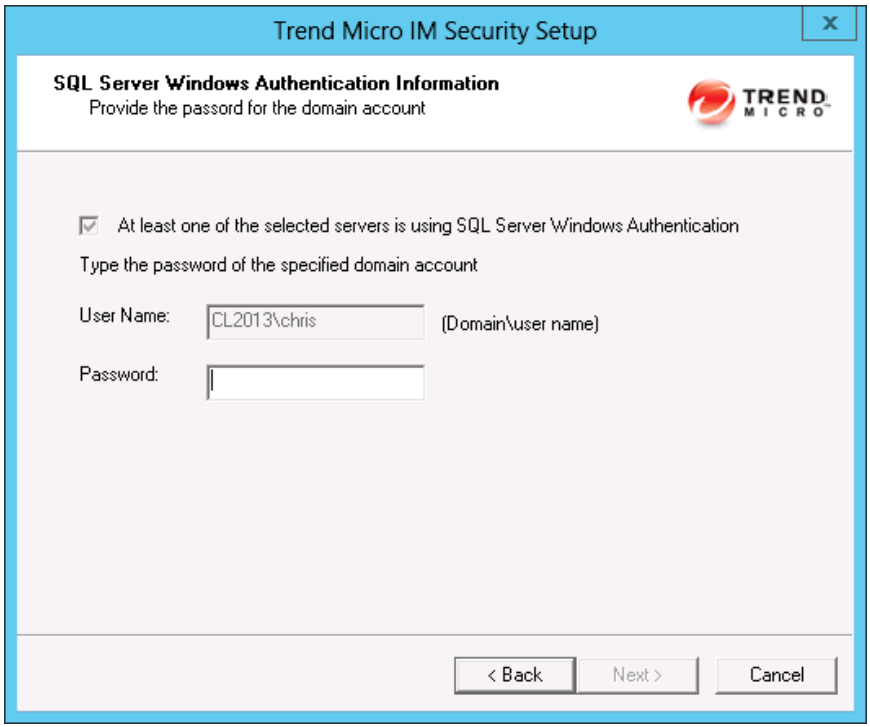

8. Select **IIS Default Web Site** or **Virtual Web Site**. Next to **SSL Port**, type the port number to use as a listening port for this server. Click **Next** to continue.

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



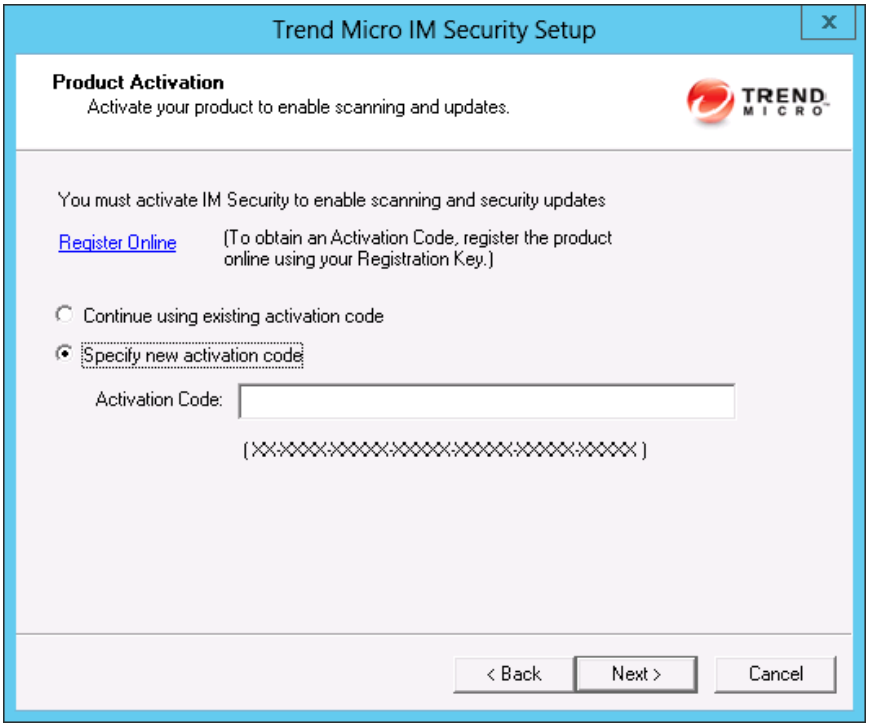

9. Review the settings. Click **Next >** to continue.

The **SQL Server Windows Authentication Information** screen or the **Product Activation** screen as shown in step 10 appears.




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

The **Product Activation** screen appears.




11. Perform one of the following options:

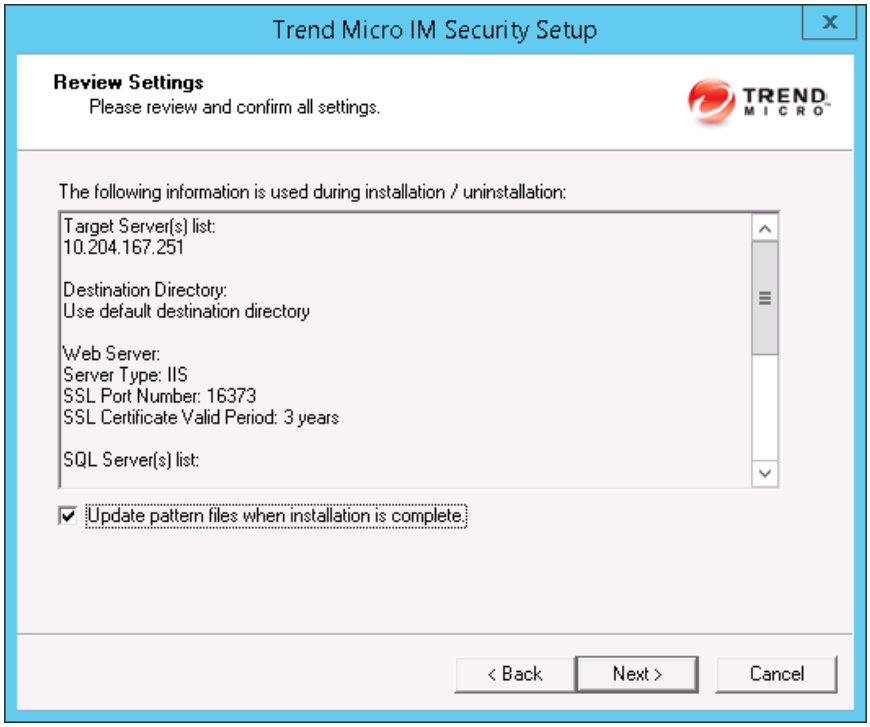
    - Select **Continue using existing activation code**.
    - Select **Specify new activation code**. Type the activation code.

    **Note**

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

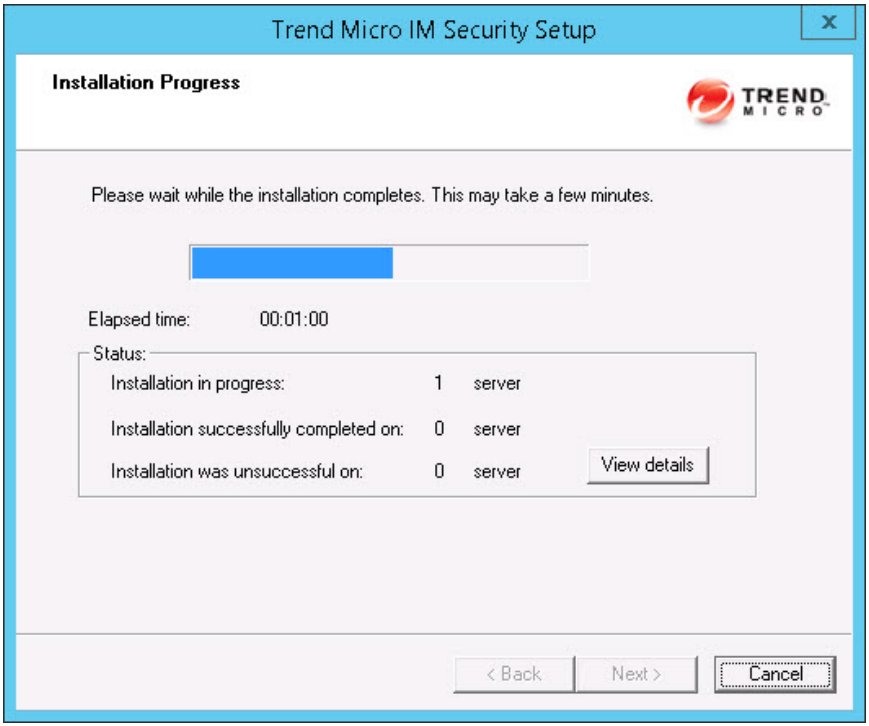
12. Click **Next**.

The **Review Settings** screen appears.




13. 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.

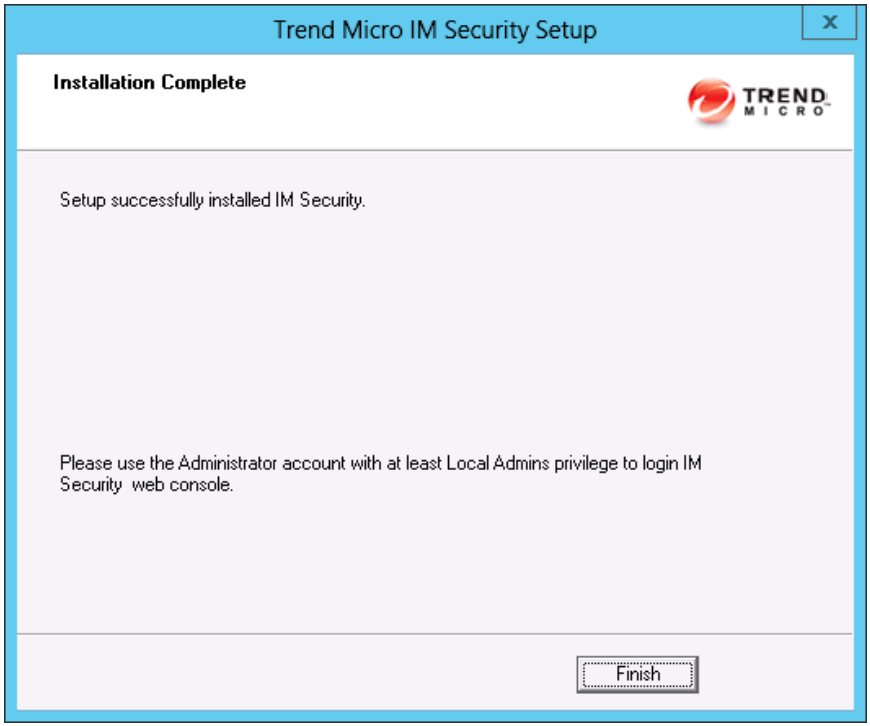



14. Click **View details** to display a list of each computer to which you are installing IM Security and the status of each computer. Click **Next** when the installation completes.

**Note**

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

The **Installation Complete** screen appears.




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

16. Use an administrator account with local administrator privileges to log on to the IM Security product console.

# Chapter 4

# Silent Installation

Install IM Security to one or more servers using silent installation.

Topics in this chapter:

# About Silent Installation

This version of IM Security supports silent installation. The steps in silent installation follow the same steps as regular installation or upgrade.

The differences between the standard installation process and silent installation include the following:

- The **Welcome** screen displays a message reminding you that IM Security records the installation process into a pre-configured file.
- In recording mode, IM Security only records the user name and password and does not log on to the target servers.
- Once the recording completes, the file name and location information is listed on the setup screen.
- The **Target Server System Requirements Checking** screen does not display.

## Silent Installation Limitations

The following lists the limitations for silent installation:

- Silent installations are only supported on local computers.
- Generate the pre-configured file by using recording mode the first time. Then, modify settings in the pre-configured file. However, do not modify settings in the **Do not edit** sections.
- For version/build upgrades, record settings using the new package. Silent installation will keep the previous settings when an upgrade is performed.
- Record settings separately for target servers with different languages. Do not apply pre-configured files recorded on an English operating system to a target server with a German operating system.

# Performing Silent Installation

**Procedure**

1. Launch a Windows command prompt.
2. Locate the `IM Security` directory.
3. Type `Setup /R` to start recording mode.
4. Copy the pre-configured file (`C:\Windows\Temp\setup-ims.iss`) to the installation package directory (`C:\IMS`) when the recording completes.
5. Type `Setup /S <pre-configured filename>` to perform silent installation.

## Using an Existing Pre-Configured 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. |
| `Setup /R <config_file path>` | Starts recording mode. If the path is empty, the default path is the Windows directory `C:\Windows\Temp\setup-ims.iss` |
| `Setup /S <config_file>` | Performs a silent installation with the file name you specify. |

The IM Security silent installation also supports remote database. You can edit the pre-configured file to configure remote database information.

**Note**

If you have configured the local database, you do not need to edit the pre-configured file.

To edit the pre-configured file, open the pre-configured file `setup-ims.iss` in a file editor, and edit the following items at the bottom of the file:

**TABLE 4-2. Silent Installation Setting Parameters**

| PARAMETER | DESCRIPTION |
|---|---|
| `RemoteSQLServerName` | The IP address or server name of the remote SQL server. |
| `RemoteSQLUserName` | The logon user name of remote SQL server. |
| `RemoteSQLPassword` | The logon password of remote SQL Server. |
| `SQLWindowsAuthentication` | The authentication mode of remote SQL server.<br>• 0: SQL server authentication<br>• 1: Windows authentication |

# Chapter 5

## Post-Installation Tasks

Trend Micro recommends performing specific tasks after installing and activating IM Security.

Topics include:

# Verify Server Changes

The following tables list server changes that occur after successfully installing IM Security.

**TABLE 5-1. System Changes**

| COMPONENTS | DETAILS |
|---|---|
| Product and SQL agent services | Setup adds the following services:<br>• Trend Micro IM Security Server<br>• Trend Micro IM Security System Attendant<br>When installing using a local SQL database, Setup also installs the following:<br>• SQL Server (IMSECURITY)<br>• SQL Server Agent (IMSECURITY) |
| Task Manager processes | Setup adds two processes:<br>• servIMSHost.exe<br>• servIMSSA.exe |
| IIS website | Depending on the **Web Server Type** screen, Setup follows your web server settings. |
| Performance Counter objects | Setup adds Performance Counter objects, which you can then select to view IM Security performance. |
| Lync/Skype for Business Server Properties update | Setup updates the Lync/Skype for Business Server Application list (**Topology** > **Server Application**) and adds an entry for IM Security. |
| Programs and Features items | Setup creates the following Programs and Features items:<br>• Trend Micro IM Security for Microsoft Skype for Business<br>• SQL Server 2014 Express SP1 |

**TABLE 5-2. Services**

| SERVICES | DESCRIPTION |
|---|---|
| Trend Micro IM Security Server | The core IM Security service<br><br>Trend Micro IM Security Server depends on Windows Management Instrumentation (WMI), SQL Server, and Trend Micro IM Security System Attendant services. It is responsible for core IM Security processes, which include product console access, saving configuration, and invoking the scan, update, report, and notification processes. |
| Trend Micro IM Security System Attendant | Monitors the service status of Lync/Skype for Business Server and IM Security Server services<br><br>The service depends on the WMI and SQL Server services. |

**Note**

Use the Windows Services Panel to verify the status of IM Security services.

**TABLE 5-3. Processes**

| PROCESS NAME | DESCRIPTION |
|---|---|
| `servIMSSA.exe` | The Trend Micro IM Security System Attendant Service process |
| `servIMSHost.exe` | The IM Security main process |

**TABLE 5-4. Default Program Folders**

| FOLDER NAME | DESCRIPTION |
|---|---|
| `c:\Program Files\Trend Micro\IM Security` | IM Security program files/folder path |

## Prepare Other Antivirus Applications

If you are using another antivirus product on the IM Security server, exclude the IM Security Archive, Quarantine, Backup, Download and Temp directories from real-time, manual, or scheduled scans.

## About the IM Security Management Pack

IM Security provides full support for Systems Center Operations Manager (SCOM) 2007 R2, 2012 and 2012 R2. Administrators can import the IM Security management package to System Center Operations Manager (SCOM) from the following path in the IM Security installation package to use IM Security with Systems Center Operations Manager (SCOM):

```
\Management Pack
\Trend.Micro.IM.Security.for.Microsoft.Skype.for.Business.xml
```

## Verifying a Successful Installation

IM Security recommends verifying installation by testing IM Security 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.

**Procedure**

1. If necessary, disable security products that might detect the EICAR test file before it arrives at your Lync/Skype for Business Server.
2. Open an ASCII text file and copy the following 68-character string to the file.

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
   FILE!$H+H*
   ```

3. Save the file as `eicar_test.com` to a temporary directory and then close the file.
4. Start the Lync/Skype for Business client and transfer the `eicar_test.com` file to one of your contacts (preferably to another network administrator or IT personnel).
5. Access the product console and query virus scan logs.

   IM Security detects the EICAR test file as **eicar_virus**, quarantines `eicar_test.com`, logs the event, and sends notifications to the sender and recipient.

**Note**

- Virus Scan enables IM-based notifications to the sender and recipient by default.
- IM Security opens a new conversation window when sending notifications from the IM Security notification account.

# Checking Default Settings

The following table enumerates the default settings implemented in a successful IM Security installation.

**TABLE 5-5. Default Settings**

| SCREEN | DEFAULT VALUE |
|---|---|
| **Communication Control** | • **Enable Communication Control**: Disabled<br>• **Default rules**: All enabled |
| **File Transfer Scan** > **Virus Scan** | • **Enable Virus Scan for File Transfer Scan**: Enabled<br>• **Target**: All scannable files<br>• **Action**: ActiveAction<br>• **Notification**: Sender and Recipient (IM only) |
| **File Transfer Scan** > **File Blocking** | • **Enable File Blocking**: Disabled<br>• **Default rules**: Disabled |
| **File Transfer Scan** > **Content Filtering** | • **Enable Content Filtering for File Transfer Scan**: Disabled<br>• **Default rules**: Disabled |

| Screen | Default Value |
|---|---|
| **File Transfer Scan** > **Web Reputation** | • **Enable Web Reputation for File Transfer Scan**: Enabled<br>• **Target**: Security Level is Medium<br>• **Action**: Replace all and Archive<br>• **Notification**: Sender and Recipient (IM only) |
| **File Transfer Scan** > **DLP Policies** | • **Enable Data Loss Protection for File Transfer Scan**: Disabled<br>• **Policies**: All disabled |
| **Instant Message Scan** > **Content Filtering** | • **Enable Content Filtering for Instant Message Scan**: Disabled<br>• **Default rules**: Disabled |
| **Instant Message Scan** > **Web Reputation** | • **Enable Web Reputation for Instant Message Scan**: Enabled<br>• **Target**: Security Level is Medium<br>• **Action**: Replace all and Archive<br>• **Notification**: Sender (IM only) |
| **Instant Message Scan** > **DLP Policies** | • **Enable Data Loss Protection for Instant Message Scan**: Disabled<br>• **Policies**: All disabled |
| **Updates** > **Manual** | • **Components**: All components selected |
| **Updates** > **Scheduled** | • **Enable scheduled update**: Enabled<br>• **Components selected**: Virus Pattern, Spyware Pattern, IntelliTrap Pattern, and IntelliTrap Exception Pattern<br>• **Schedule**: Daily at 2:30AM |

| Screen | Default Value |
|---|---|
| **Updates** > **Source** | • **Source**: Trend Micro ActiveUpdate Server<br>• **Allow other servers to download updates from this server**: Disabled |
| **Alerts** | IM Security alerts:<br>• Services do not start successfully<br>• Services are unavailable<br>• Component update is unsuccessful<br>Lync/Skype for Business Server alerts:<br>• Services are unavailable<br>Recipients:<br>• Write to Windows Event log |
| One-time and Scheduled Reports | • Empty |
| **Logs** > **Maintenance** | • **Manual**: All logs, Delete logs older than 30 days<br>• **Scheduled**: Enabled (same setting as manual) |

| Screen | Default Value |
|---|---|
| **Administration** > **Directories** | • **Quarantine Directory (Virus Scan)**: `<Installation path>\quarantine\`<br>• **Backup Directory (Virus Scan)**: `<Installation path>\backup\`<br>• **Archive Directory (File Blocking)**: `<Installation path>\archive\`<br>• **Archive Directory (File Transfer Content Filtering)**: `<Installation path>\archive\`<br>• **Archive Directory (File Transfer Web Reputation)**: `<Installation path>\archive\`<br>• **Archive Directory (File Transfer Data Loss Prevention)**: `<Installation path>\archive\` |
| **Administration** > **Debug Logs** | • Disabled |

**WARNING!**

Clicking **Reset** on any of the product web console screens restores the default settings for that page. If there are customizations or additional rules that you have created after installing IM Security, those settings/rules will be removed after clicking **Reset** and confirming the action.

## About IM Security Updates

Security software can only be effective if it is using the latest technology. Since new viruses/malware and other malicious codes are constantly being released, it is crucial that you regularly update your IM Security components to protect against new security threats.

IM Security components available for updating are:

- Virus Pattern
- Virus Scan Engine
- Spyware Pattern
- IntelliTrap Pattern
- IntelliTrap Exception Pattern
- URL Filtering Engine

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

## Updating IM Security - Prerequisite Tasks

**Procedure**

1. Register your software.
2. If a proxy server handles Internet traffic on your network, you must set the proxy server information.
3. Configure your update method and source.
   - Methods include **Manual Update** and **Scheduled Update**.
   - Sources include the ActiveUpdate server, the Internet, the intranet UNC PATH, and Control Manager.

## Configuring Proxy Settings

Proxy servers are used for added security and more efficient use of bandwidth. If your network uses a proxy server, configure the proxy settings to connect to the Internet, download the updated components necessary to keep IM Security updated, and check the license status online.

**Procedure**

1. Click **Administration** > **Proxy**.

2. Select **Use a proxy server for Web Reputation, updates, and product license notifications**. Select this check box to use a proxy server for web reputation queries to Trend Micro reputation servers, updates, and product license notifications.
3. Type the proxy server name or IP address.
4. Type the **Port**.
5. (Optional) Select **Use SOCKS 5 proxy protocol**.
6. If the proxy server requires authentication, specify the user name and password.

## Configuring Manual Updates

Trend Micro recommends manually updating your scan engines and pattern files immediately after installing IM Security or whenever there is an outbreak.

**Procedure**

1. Click **Updates** > **Manual**.
2. Select the component(s) that you want to update.
3. Click **Update**.

   IM Security begins downloading the components and displays a progress bar that shows you the elapsed time and the percentage of the download remaining. IM Security downloads the current components from the specified source.

## Configuring Scheduled Update

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

**Procedure**

1. Select a source from which your updates will be downloaded.
   a. Click **Updates** > **Source**.

      The **Update Source** screen appears.

   b. Select a download source.

   c. Click **Save**.

2. Set up your schedule.
   a. Click **Updates** > **Scheduled**.

   b. Click **Enable schedule updates** to have IM Security begin to update according to your schedule.

   c. Set the **Update Schedule**.

      i. Select an update frequency: by minutes, by hours, by days, or weekly.

      ii. Set the start time for the schedule by selecting the hour and minute. Each time the update occurs, the download begins at this time.

3. Select the components for downloading from the update source.
   a. Select the components that IM Security downloads during each scheduled update.

      **Tip**

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

   b. Click **Save**.

      IM Security will begin downloading the selected components according to your schedule.

## Configuring the Download Source

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

**Procedure**

- **Trend Micro ActiveUpdate server**: Select this option to download from the default update server.

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

- **Intranet location containing a copy of the current file**: Select this option to download from an Intranet location.

  Download components from an Intranet source that receives updated components.

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

  **Note**

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

- **Other update source**: Select this option to specify an update source different from the default. The update source must begin with "`http://`".

  Download components from an Internet or other source.

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

- **Allow other servers to download updates from this server**: Select this option to allow other IM Security servers to download updates from this server.

  Click **Allow other servers to download updates from this server** to set IM Security to create a duplicate copy of the update package on the current server. Normally, IM Security only downloads components that the user has set it to download or the increments of the components that it needs. When you set IM Security to duplicate the update package, it will download all the components that are available for downloading.

  This option instructs IM Security to download the update package (pattern file and scan engine) onto the IM Security server `<root>:\Program Files\Trend Micro\IM Security\ActiveUpdate` folder.

# Chapter 6

# Removing IM Security

This chapter describes how to remove IM Security.

Topics in this chapter:

# IM Security Uninstallation

Uninstallation removes the following IM Security components:

- Web server entries
- All program files and folders
- WMI entries
- Active Directory objects
- Performance Counter objects

# Using the Enterprise Solution DVD

You can use the Trend Micro Enterprise Solution DVD to uninstall IM Security.

Using the Setup program to uninstall IM Security removes all related components and programs. IM Security recommends using the `Setup.exe` program to uninstall IM Security.

---

**Procedure**

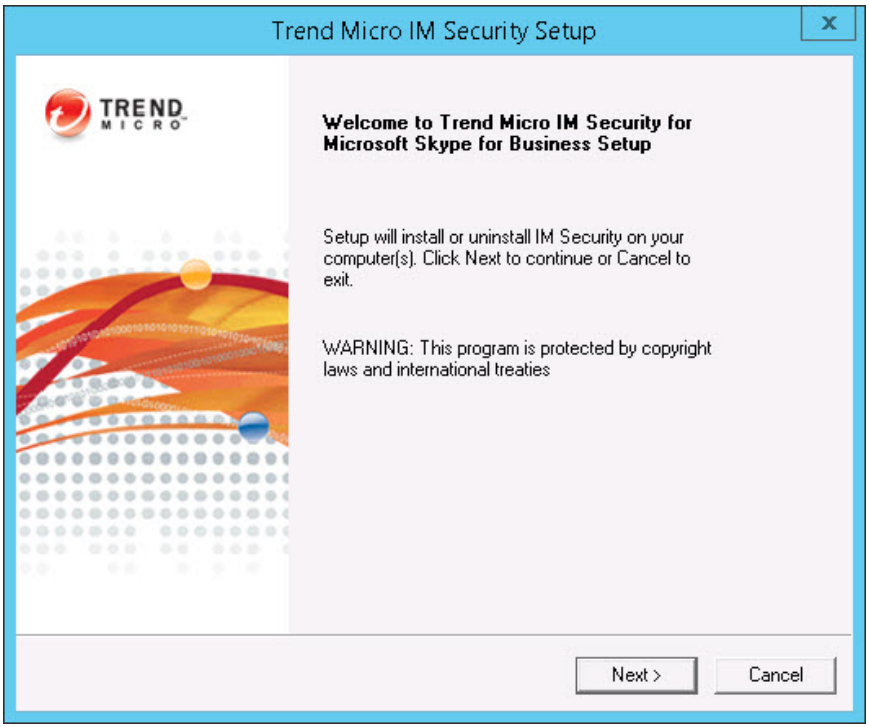
1. To remove IM Security, run `setup.exe` from the Trend Micro Enterprise Solution DVD. Select uninstall when prompted.

   **Note**

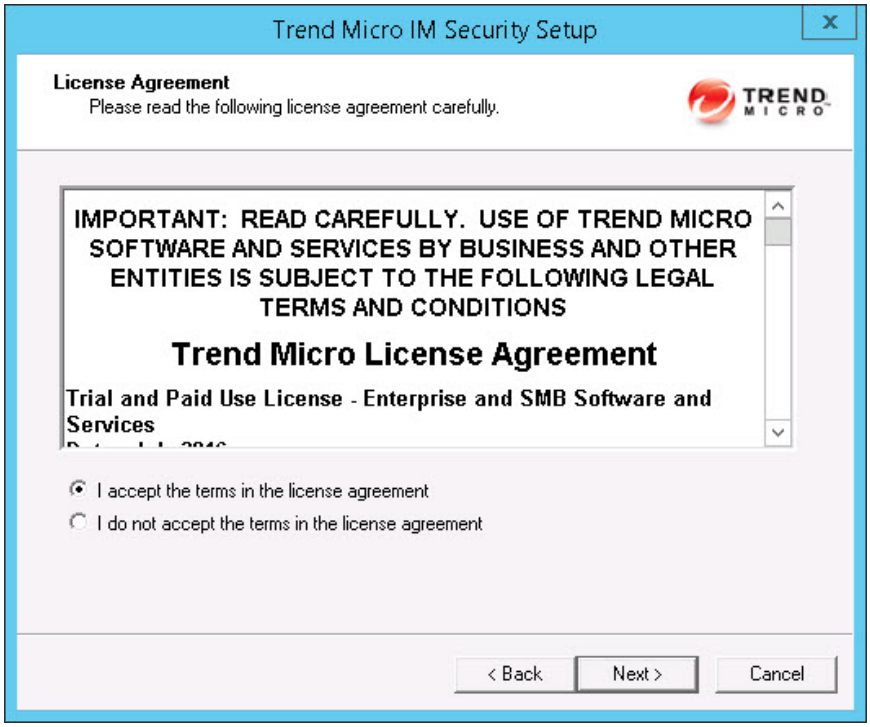
   If, at any time, you click **Cancel** from the Setup program, the program will display an **Exit Setup** dialog box. When you click **Yes** from this dialog box, the uninstallation aborts.

The **Welcome to Trend Micro IM Security for Microsoft Skype for Business Server Setup** screen appears.



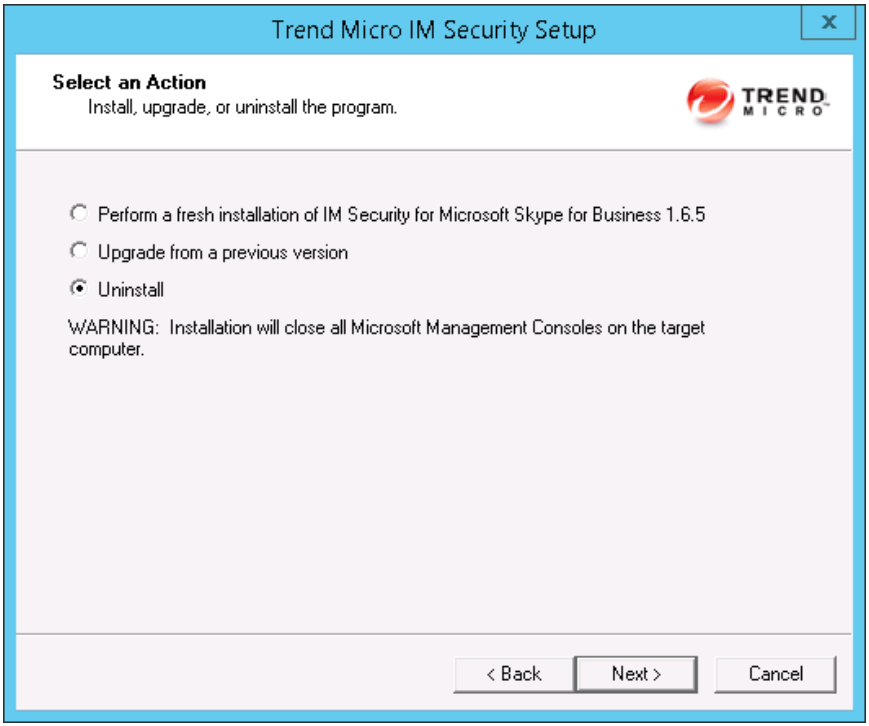

2. Click **Next** to continue with the uninstallation.

The **License Agreement** screen appears.



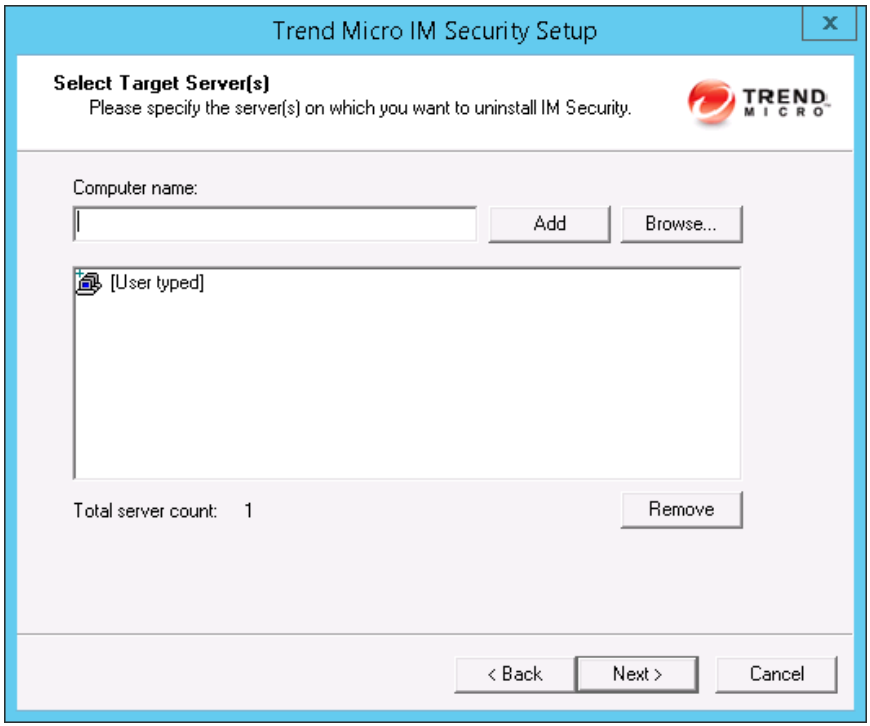

3. If you do not accept the terms, click **I do not accept the terms in the license agreement**. This terminates the process without modifying your operating system. Agree to the terms of the agreement by selecting **I accept the terms in the license agreement** and click **Next** to continue with the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

The **Select an Action** screen appears.




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

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



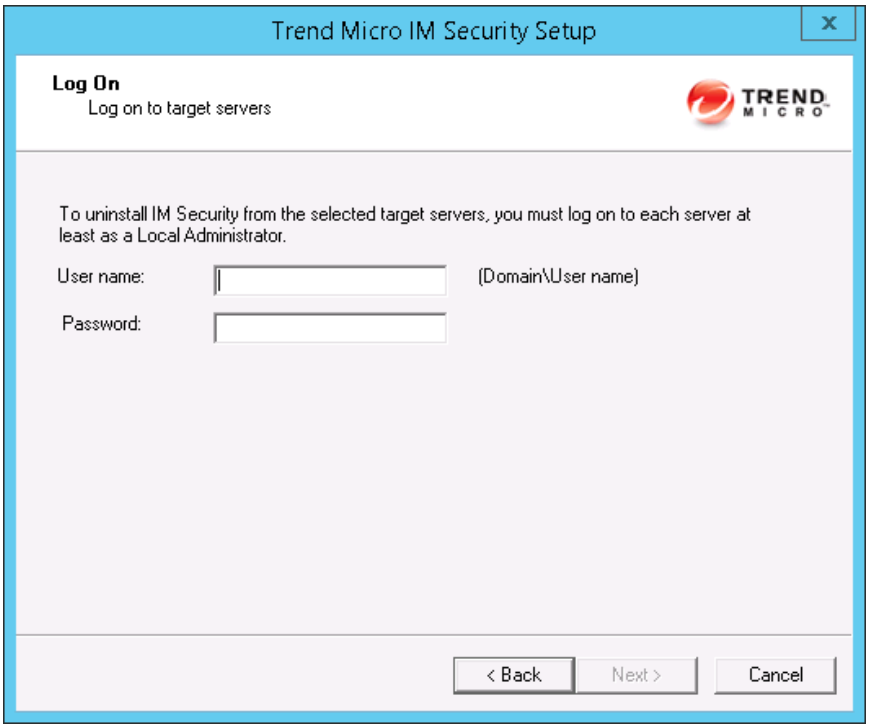

5. To uninstall IM Security from a server:

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

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

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

The **Log On** screen appears.

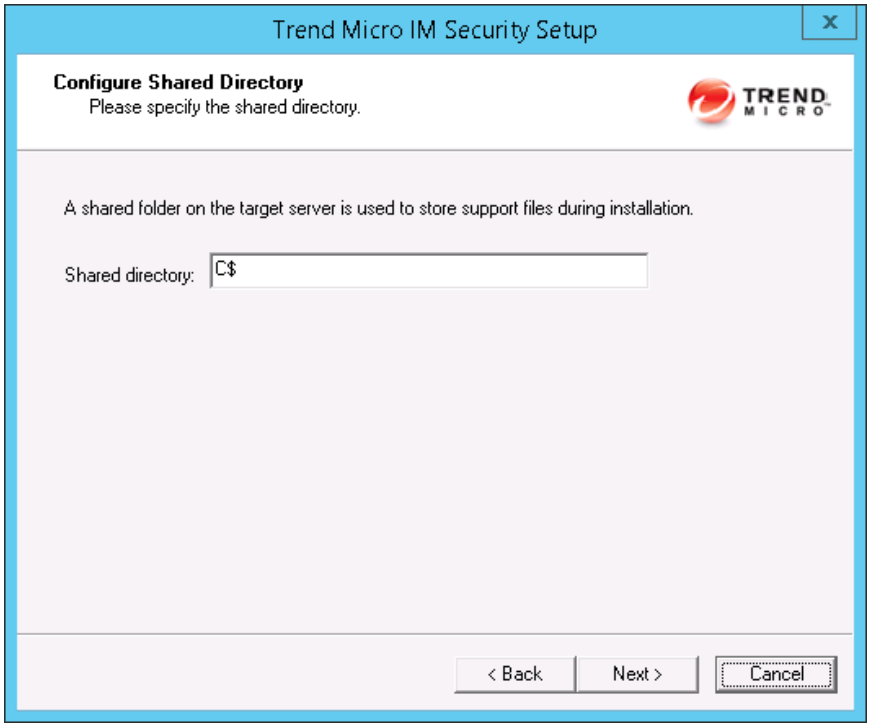



6. Type the user name and password to log on to the target server to uninstall IM Security. Click **Next** to continue.

**Note**

You must log on with an account with "Domain User" and "Local Administrator" privileges to uninstall IM Security.

The **Configure Shared Directory** screen appears.

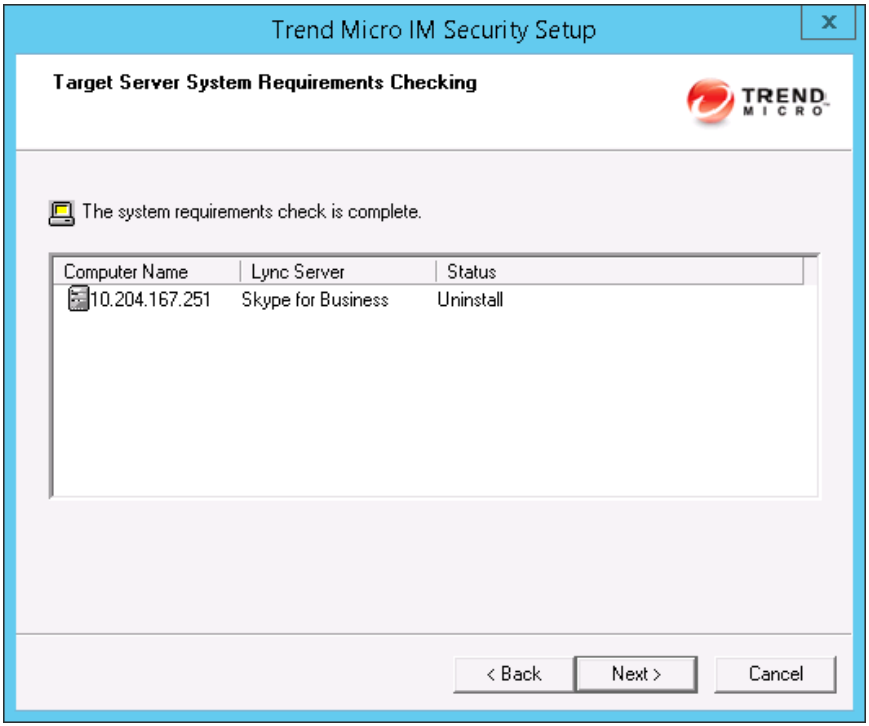



7. Use this screen to specify the shared directory for the target servers from where you will uninstall IM Security.

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

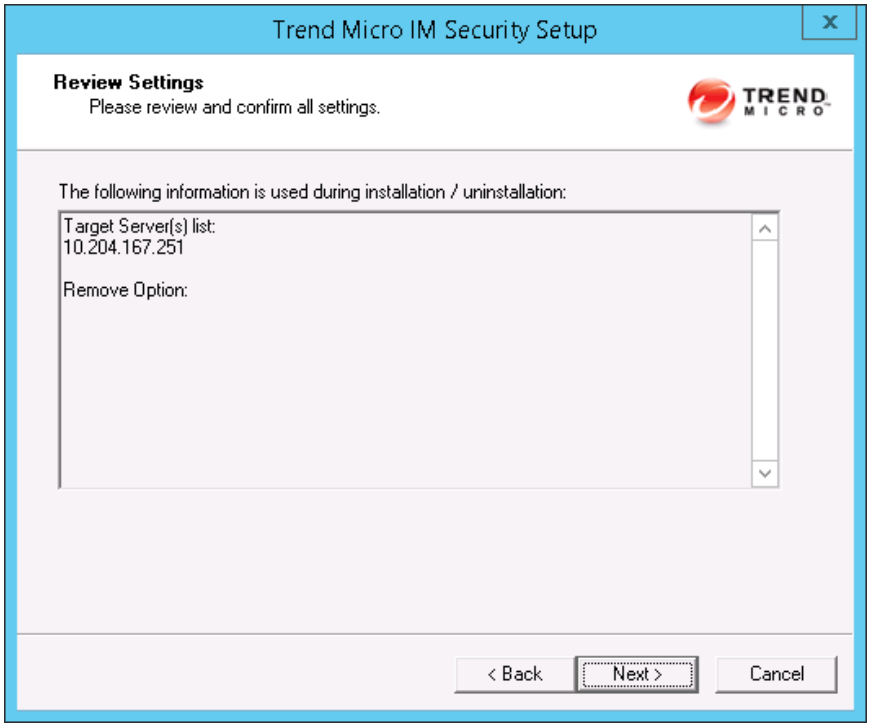
   b. Click **Next**.

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



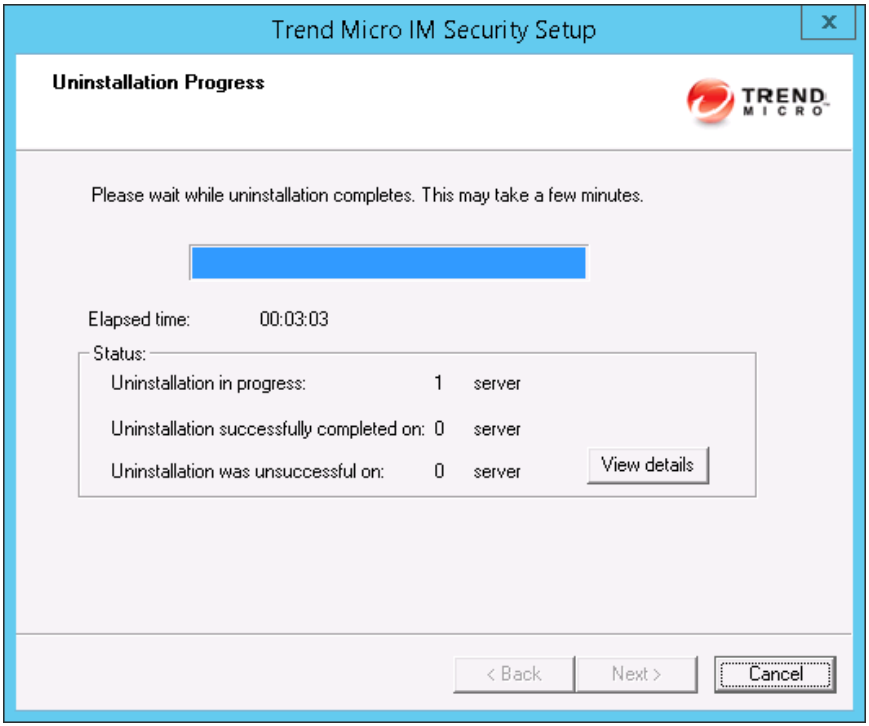

8. View the screen and ensure the settings for the uninstallation are correct and click **Next** to continue.

The **Review Settings** screen appears.



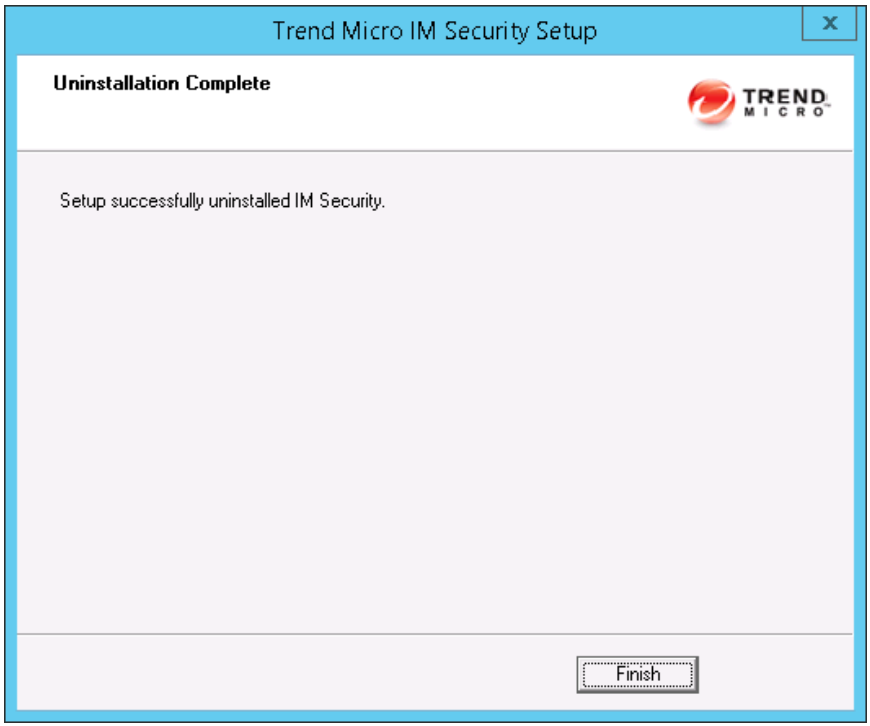

9. Review your settings and click **Next** to begin the uninstallation progress.

The **Uninstallation Progress** screen appears.




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

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




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

    The Setup program removes IM Security from the selected servers.

## Using the Windows Control Panel

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

**Procedure**

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

# Chapter 7

## Technical Support

Learn about the following topics:

# Troubleshooting Resources

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

## Using the Support Portal

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

**Procedure**

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

   **Tip**

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

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

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

## Threat Encyclopedia

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

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

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

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

## Contacting Trend Micro

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

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

- Worldwide support offices:

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

- Trend Micro product documentation:

http://docs.trendmicro.com

### Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

## Sending Suspicious Content to Trend Micro

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

### Email Reputation Services

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

https://ers.trendmicro.com/

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

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

### File Reputation Services

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

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

Record the case number for tracking purposes.

### Web Reputation Services

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

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

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

## Other Resources

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

### Download Center

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

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

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

## Documentation Feedback

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

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

# Appendix A

## Deployment Checklist

Use the following checklists to record relevant system information:

# Pre-Installation Tasks Checklist

Before installing IM Security, complete the following tasks:

| Completed ? | Pre-installation Tasks |
|---|---|
| | If a firewall exists between the Lync/Skype for Business Server and its clients, open the necessary ports to ensure IM Security connectivity.<br>For details, see *Ports Checklist on page A-3*. |
| | Log on to the target server using an account with “Domain User” and “Local Administrator” privileges. |
| | Disable or uninstall other IM environment antivirus applications. |
| | Check the target server’s compliancy to the system requirements. |
| | Obtain the proxy server and SMTP server settings and authentication information (if necessary). |
| | Close opened Microsoft Management Console (MMC) screens. |
| | Prepare the IM Security Activation Code. |

# Installation Checklist

The following server address information is required during installation, and for configuring the IM Security server to work with your network. Record them here for easy reference.

| Information Required | Sample | Your Value |
|---|---|---|
| IM Security server information | | |
| Registration Key (RK) and Activation Code (AC) | RK:<br>AC: | |
| IP address | `10.1.104.255` | |

| Information Required | Sample | Your Value |
|---|---|---|
| Administrator account | IMS_admin | |
| Web server information | | |
| IP address | `10.1.104.225` | |
| Fully Qualified Domain Name (FQDN) | `server.company.com` | |
| NetBIOS (host) name | yourserver | |
| | No | |
| Proxy server Information | | |
| IP address | `10.1.174.225` | |
| Fully Qualified Domain Name (FQDN) | `proxy.company.com` | |
| NetBIOS (host) name | proxyserver | |
| SMTP server information | | |
| IP address | `10.1.123.225` | |
| Fully Qualified Domain Name (FQDN) | `mail.company.com` | |
| NetBIOS (host) name | mailserver | |
| SNMP Trap information | | |
| Community name | trendmicro | |
| IP address | `10.1.194.225` | |

## Ports Checklist

IM Security uses the following ports for the indicated purposes.

| Service | Sample Port Value | Your value |
|---|---|---|
| Product Console and Update/ Deploy components | 16372/16373 | |
| File transfer | 6891-6900 | |
| SMTP | 25 | |
| SNMP | 162 | |
| Server Management population | 3268 | |

# Appendix B

## Glossary

| Term | Explanation |
|---|---|
| 100BaseT | An alternate term for “fast Ethernet”, an upgraded standard for connecting computers into a local area network (LAN). 100BaseT Ethernet can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than 10BaseT.<br><br>Also see 10BaseT. |
| 10BaseT | The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. Ethernet is a standard for connecting computers into a local area network (LAN). The maximum cable distance is 100 meters (325 feet), the maximum devices per segment is 1, and the maximum devices per network are 1024.<br><br>Also see 100BaseT. |
| access (verb) | To read data from or write data to a storage device, such as a computer or server. |
| access (noun) | Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities. |

| TERM | EXPLANATION |
|---|---|
| action | The operation to be performed when:<br>• a virus has been detected<br>• spam has been detected<br>• a content violation has occurred<br>• an attempt was made to access a blocked URL<br>• file blocking has been triggered, or<br>• sensitive data is detected.<br>Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.<br>Also see target and notification. |
| activate | To enable your software after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the **Product License** screen. |
| Activation Code | A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: `SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4`<br>Also see Registration Key. |
| active FTP | Configuration of FTP protocol that allows the client to initiate "handshaking" signals for the command session, but the host initiates the data session. |
| 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.<br>ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD. |

| TERM | EXPLANATION |
|---|---|
| ActiveX | A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of web pages. |
| ActiveX malicious code | An ActiveX control is a component object embedded in a web page which runs automatically when the page is viewed. ActiveX controls allow web developers to create interactive, dynamic web pages with broad functionality such as HouseCall, Trend Micro's free online scanner.<br><br>Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to high. |
| address | Refers to a networking address (see IP address) or an email address, which is the string of characters that specify the source or destination of an email message. |
| administrator | Refers to “system administrator”; the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security. |
| administrator account | A user name and password that has administrator-level privileges. |
| administrator email address | The address used by the administrator of your Trend Micro product to manage notifications and alerts. |
| adware | Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called **spyware**. |
| alert | A message intended to inform a system's users or administrators about a change in the operating conditions of that system or about some kind of error condition. |
| anti-relay | Mechanisms to prevent hosts from “piggybacking” through another host’s network. |

| TERM | EXPLANATION |
|---|---|
| antivirus | Computer programs designed to detect and clean computer viruses. |
| archive | A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a `.zip` file. |
| attachment | A file attached to (sent with) an email message. |
| audio/video file | A file containing sounds, such as music, or video footage. |
| authentication | The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).<br><br>The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures.<br><br>Also see public-key encryption and digital signature. |
| binary | A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra. |
| block | To prevent entry into your network. |
| bridge | A device that forwards traffic between network segments based on data link layer information. These segments have a common network layer address. |
| browser | A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or pages) and of navigating from one node to another. A browser acts as a client to a remote web server. |
| cache | A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc. |

| TERM | EXPLANATION |
|---|---|
| case-matching | Scanning for text that matches both words and case. For example, if dog is added to the content-filter, with case-matching enabled, messages containing Dog will pass through the filter; messages containing dog will not. |
| cause | The reason a protective action, such as URL-blocking or file-blocking, was triggered. This information appears in log files. |
| clean | To remove virus code from a file or message. |
| client | A computer system or process that requests a service of another computer system or process (a server) using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture. |
| client-server environment | A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds. |
| 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 your Trend Micro product 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. |
| content violation | An event that has triggered the Content Filtering policy. |
| cookie | A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your web browser for later use. The next time you access a website for which your browser has a cookie, your browser sends the cookie to the web server, which the web server can then use to present you with customized web pages. For example, you might enter a website that welcomes you by name. |

| TERM | EXPLANATION |
|---|---|
| daemon | A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking. |
| damage routine | The destructive portion of virus code, also called the payload. |
| Data Loss Prevention (DLP) | A scan filter that determines if data being transferred contains sensitive information as defined by the administrator using templates, expressions, and keyword lists. |
| 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. |
| De-Militarized Zone (DMZ) | From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers. |
| Denial of Service (DoS) attack | Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped. |
| dialer | A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge. |
| digital signature | Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption.<br><br>Also see public-key encryption and authentication. |
| directory | A node, which is part of the structure in a hierarchical computer file system. A directory typically contains other nodes, folders, or files. For example, `C:\Windows` is the Windows directory on the `C:\` drive. |
| directory path | The subsequent layers within a directory where a file can be found, for example, the directory path for the ISVW for SMB Quarantine directory is:<br><br>`C:\Programs\Trend Micro\ISVW\Quarantine` |

| Term | Explanation |
|---|---|
| disclaimer | A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message. |
| domain (administrative) | A group of computers sharing a common database and security policy. |
| 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. |
| DOS virus | Also referred to as “COM” and “EXE file infectors”. DOS viruses infect DOS executable programs- files that have the extensions `*.COM` or `*.EXE`. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs. |
| download (noun) | Data that has been downloaded, for example, from a website via HTTP. |
| download (verb) | To transfer data or code from one computer to another. Downloading often refers to transfer from a larger host system (especially a server or mainframe) to a smaller client system. |
| dropper | Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system. |

| TERM | EXPLANATION |
|---|---|
| encryption | Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes. |
| End User License Agreement (EULA) | An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking I accept during installation. Clicking I do not accept will, of course, end the installation of the software product.<br><br>Many users inadvertently agree to the installation of spyware and adware into their computers when they click **I accept** on EULA prompts displayed during the installation of certain free software. |
| Ethernet | A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable. |
| EXE file infector | An executable program with a `.exe` file extension.<br><br>Also see DOS virus. |
| Executable and Linkable Format (ELF) | An executable file format for Unix and Linux platforms. |
| executable file | A binary file containing a program in machine language which is ready to be executed (run). |

| Term | Explanation |
|---|---|
| exploit | An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers. |
| false positive | An email message that was caught by the spam filter and identified as spam, but is actually not spam. |
| file | An element of data, such as an email message or HTTP download. |
| file-infecting virus | File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a predetermined time or perform some other malicious action.<br><br>In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable |
| file name extension | The portion of a file name (such as `.dll` or `.xml`) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run. |
| 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. |
| File Transfer Protocol (FTP) | A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files. |

| TERM | EXPLANATION |
|---|---|
| filtering, dynamic | IP service that can be used within VPN tunnels. Filters are one way GateLock controls traffic from one network to another. When TCP/IP sends data packets to the firewall, the filtering function in the firewall looks at the header information in the packets and directs them accordingly. The filters operate on criteria such as IP source or destination address range, TCP ports, UDP, Internet Control Message Protocol (ICMP), or TCP responses. Also see tunneling and Virtual Private Network (VPN). |
| firewall | A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines. |
| Frequently Asked Questions (FAQ) | A list of questions and answers about a specific topic. |
| gateway | An interface between an information source and a web server. |
| grayware | A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools. |
| group file type | Types of files that have a common theme, for example:<br>• Audio/Video<br>• Compressed<br>• Executable<br>• Images<br>• Java<br>• Microsoft Office |
| Graphical User Interface (GUI) | The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command line interface where communication is by exchange of strings of text. |
| hacking tool | Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited. |

| Term | Explanation |
|---|---|
| hard disk (or hard drive) | One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks. |
| header (networking definition) | Part of a data packet that contains transparent information about the file or the transmission. |
| heuristic rule-based scanning | Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions. |
| host | A computer connected to a network. |
| hub | This hardware is used to network computers together (usually over an Ethernet connection). It serves as a common wiring point so that information can flow through one central location to any other computer on the network thus enabling centralized management. A hub is a hardware device that repeats signals at the physical Ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management. |
| Hypertext Transfer Protocol (HTTP) | The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80. |
| Hypertext Transfer Protocol Secure (HTTPS) | A variant of HTTP used for handling secure transactions. |
| ICSA | ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, cryptography, and PC firewall products in the world today. |
| image file | A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, via a digital camera, or they may be generated by computer using graphics software. |
| incoming | Email messages or other data routed into your network. |

| TERM | EXPLANATION |
|---|---|
| installation script | The installation screens used to install Unix versions of Trend Micro products. |
| 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 | A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet. |
| Internet Protocol (IP) | An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet. |
| interrupt | An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an interrupt handler routine. |
| “in the wild” | Describes known viruses that are actively circulating.<br>Also see “in the zoo”. |
| “in the zoo” | Describes known viruses that are currently controlled by antivirus products.<br>Also see “in the wild”. |
| intranet | Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet. |
| IP | Internet Protocol—See IP address. |
| IP address | Internet address for a device on a network, typically expressed using dot notation such as `123.123.123.123`. |

| Term | Explanation |
|---|---|
| IP gateway | Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached. |
| IT | Information technology, to include hardware, software, networking, telecommunications, and user support. |
| Java applets | Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow web developers to create interactive, dynamic web pages with broader functionality.<br><br>Authors of malicious code have used Java applets as a vehicle for attack. Most web browsers, however, can be configured so that these applets do not execute; sometimes by simply changing browser security settings to high. |
| Java file | Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java applets. (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.) |
| Java malicious code | Virus code written or embedded in Java.<br><br>Also see Java file. |
| JavaScript virus | JavaScript is a simple programming language developed by Netscape that allows web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently.<br><br>A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in web pages and download to a user's desktop through the user's browser.<br><br>Also see VBscript virus. |

| TERM | EXPLANATION |
|---|---|
| joke program | An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system. |
| keylogger | Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers. |
| Kilobyte (KB) | 1024 bytes of memory. |
| license | Authorization by law to use a Trend Micro product. |
| license certificate | A document that proves you are an authorized user of a Trend Micro product. |
| Lightweight Directory Access Protocol (LDAP) | An internet protocol that email programs use to locate contact information from a server. For example, suppose you want to locate all persons in Boston who have an email address containing the name “Bob”. An LDAP search would enable you to view the email addresses that meet this criteria. |
| link (also called hyperlink) | A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link. |
| listening port | A port utilized for client connection requests for data exchange. |
| load balancing | Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation. |

| TERM | EXPLANATION |
|---|---|
| Local Area Network (LAN) | Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area. |
| log storage directory | Directory on your server that stores log files. |
| logic bomb | Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met. |
| macro | A command used to automate certain functions within an application. |
| MacroTrap | A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction). |
| macro virus | Macro viruses are often encoded as an application macro and included in a document. 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. |
| Mail Transfer Agent (MTA) | The program responsible for delivering email messages.<br>Also see SMTP server. |
| malware (malicious software) | Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans. |
| management console | The user interface for your Trend Micro product. |

| TERM | EXPLANATION |
|---|---|
| mass mailer (also known as a Worm) | A malicious program that has high damage potential, because it causes large amounts of network traffic. |
| Media Access Control (MAC) address | An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type. |
| Megabyte (MB) | 1024 kilobytes of data. |
| Microsoft Office file | Files created with Microsoft Office tools such as Excel or Microsoft Word. |
| Millions of bits per second (Mbps) | A measure of bandwidth in data communications. |
| mixed threat attack | Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats. |
| Network Address Translation (NAT) | A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don’t have to get a registered IP address for every machine in your network. |
| network virus | A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure. |

| Term | Explanation |
|---|---|
| notification<br><br>(Also see action and target) | A message that is forwarded to one or more of the following:<br>• system administrator<br>• sender of a message<br>• recipient of a message, file download, or file transfer<br>The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download. |
| 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. |
| online help | Documentation that is bundled with the GUI. |
| open source | Programming code that is available to the general public for use or modification free of charge and without license restrictions. |
| operating system | The software which handles tasks such as the interface to peripheral hardware, scheduling tasks, and allocating storage. In this documentation, the term also refers to the software that presents a window system and graphical user interface. |
| outgoing | Email messages or other data leaving your network, routed out to the Internet. |
| parameter | A variable, such as a range of values (a number from 1 to 10). |
| partition | A logical portion of a disk.<br><br>Also see sector, which is a physical portion of a disk. |
| passive FTP | Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above). |
| password cracker | An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources. |

| TERM | EXPLANATION |
|---|---|
| pattern file (also known as Official Pattern Release) | 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. |
| payload | Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive. |
| policies | Policies provide the initial protection mechanism for the firewall, allowing you to determine what traffic passes across it based on IP session details. They protect the Trusted network from outsider attacks, such as the scanning of Trusted servers. Policies create an environment in which you set up security policies to monitor traffic attempting to cross your firewall. |
| port | A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it. |
| protected network | A network protected by IWSA (InterScan web Security Appliance). |
| proxy | A process providing a cache of items available on other servers which are presumably slower or more expensive to access. |
| proxy server | A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester. |
| public-key encryption | An encryption scheme where each person gets a pair of “keys”, called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key.<br><br>Also see authentication and digital signature. |
| purge | To delete all, as in getting rid of old entries in the logs. |

| TERM | EXPLANATION |
|---|---|
| quarantine | To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server. |
| queue | A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach. |
| recipient | The person or entity to whom an email message is addressed. |
| registration | The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen.<br><br>https://olr.trendmicro.com/registration |
| Registration Key | A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: `SM-27RT-UY4Z-39HB-MNW8`<br><br>Also see Activation Code |
| relay | To convey by means of passing through various other points. |
| remote access tool (RAT) | Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security. |
| removable drive | A removable hardware component or peripheral device of a computer, such as a zip drive. |
| replicate | To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce. |
| router | This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues. |
| scan | To examine items in a file in sequence to find those that meet a particular criteria. |

| TERM | EXPLANATION |
|---|---|
| scan engine | The module that performs antivirus scanning and detection in the host product to which it is integrated. |
| script | A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with “script” are “macro” or “batch file.” |
| sector | A physical portion of a disk.<br><br>Also see partition, which is a logical portion of a disk. |
| seat | A license for one person to use a Trend Micro product. |
| Secure Socket Layer (SSL) | Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. |
| server | A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers. |
| server farm | A server farm is a network where clients install their own computers to run web servers, e-mail, or any other TCP/IP based services they require, making use of leased permanent Internet connections with 24-hour worldwide access. Instead of expensive dedicated-line connections to various offices, servers can be placed on server farm networks to have them connected to the Internet at high-speed for a fraction of the cost of a leased line. |
| shared drive | A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses. |
| signature | Also see virus signature. |

| Term | Explanation |
|---|---|
| signature-based spam detection | A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect “new” spam that isn’t an exact match for text in the spam signature file.<br><br>Also see rule-based spam detection.<br><br>Also see false positive. |
| Simple Mail Transfer Protocol (SMTP) | A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages. |
| Simple Mail Transfer Protocol (SMTP) server | A server that relays email messages to their destinations. |
| Simple Network Management Protocol (SNMP) | A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention. |
| Simple Network Management Protocol (SNMP) trap | A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring.<br><br>Also see SNMP. |
| spam | Unsolicited email messages meant to promote a product or service. |
| spyware | Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used. |

| TERM | EXPLANATION |
|---|---|
| subnet mask | In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of `255.255.255.0` specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of `255.255.0.0`.<br><br>A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them.<br><br>Also see IP address. |
| target | The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.<br><br>(Also see action and notification) |
| Telnet | The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session. |
| top-level domain | The last and most significant component of an Internet fully qualified domain name, the part after the last .. For example, host `wombat.doc.ic.ac.uk` is in top-level domain uk (for United Kingdom). |
| Total Solution CD | A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers. |
| traffic | Data flowing between the Internet and your network, both incoming and outgoing. |

| TERM | EXPLANATION |
|---|---|
| Transmission Control Protocol (TCP) | A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet. |
| trigger | An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This may trigger the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient. |
| Trojan Horse | A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder. |
| true-file type | Used by IntelliScan, 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). |
| trusted domain | A domain from which your Trend Micro product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. Messages from dominion-japan.com are always accepted into the dominion.com network, without checking for spam, since the messages are from a known and trusted source. |
| trusted host | A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network. |

| TERM | EXPLANATION |
|---|---|
| tunneling | A method of sending data that enables one network to send data via another network's connections. Tunneling is used to get data between administrative domains which use a protocol that is not supported by the internet connecting those domains.<br><br>With VPN tunneling, a mobile professional dials into a local Internet Service Provider's Point of Presence (POP) instead of dialing directly into their corporate network. This means that no matter where mobile professionals are located, they can dial a local Internet Service Provider that supports VPN tunneling technology and gain access to their corporate network, incurring only the cost of a local telephone call.<br><br>When remote users dial into their corporate network using an Internet Service Provider that supports VPN tunneling, the remote user as well as the organization knows that it is a secure connection. All remote dial-in users are authenticated by an authenticating server at the Internet Service Provider's site and then again by another authenticating server on the corporate network. This means that only authorized remote users can access their corporate network, and can access only the hosts that they are authorized to use. |
| tunnel interface | A tunnel interface is the opening, or doorway, through which traffic to or from a VPN tunnel passes. A tunnel interface can be numbered (that is, assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface.<br><br>Also see Virtual Private Network (VPN). |
| tunnel zone | A tunnel zone is a logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier. |
| Universal Resource Locator (URL) | A standard way of specifying the location of an object, typically a web page, on the Internet, for example, `www.trendmicro.com`. The URL maps to an IP address using DNS. |

| TERM | EXPLANATION |
|---|---|
| VBscript virus | VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a **Click Here for More Information** button on a web page.<br><br>A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in web pages and download to a user's desktop through the user's browser.<br><br>Also see JavaScript virus. |
| virtual IP address (VIP address) | A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header. |
| Virtual Local Area Network (VLAN) | A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard. |
| Virtual Private Network (VPN) | A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption. |
| virtual router | A virtual router is the component of Screen OS that performs routing functions. By default, Trend Micro GateLock supports two virtual routers: Untrust-VR and Trust-VR. |
| virtual system | A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same Trend Micro GateLock remote appliance; each one can be managed by its own virtual system administrator. |

| TERM | EXPLANATION |
|---|---|
| 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.<br><br>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 kit | A template of source code for building and executing a virus, available from the Internet. |
| virus signature | A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy. |
| virus trap | Software that helps you capture a sample of virus code for analysis. |
| virus writer | Another name for a computer hacker, someone who writes virus code. |
| web | The World Wide Web, also called the web or the Internet. |
| web server | A server process running at a website which sends out web pages in response to HTTP requests from remote browsers. |
| wildcard | A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a wildcard, can be used for any number or suit in the card deck. |
| working directory | The destination directory in which the main application files are stored, such as `/etc/iscan/iwss`. |

| Term | Explanation |
|---|---|
| workstation (also known as client) | A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time. |
| 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. |
| zip file | A compressed archive (in other words, “zip file) from one or more files using an archiving program such as WinZip. |
| Zip of Death | A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network. |
| zone | A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone). |

# 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: TIEM17569/160926