TREND MICRO™
IM Security

Proactive Antivirus and Content Security for Instant Messaging Environments

for Microsoft™ Live Communications Server

Getting Started Guide

TREND MICRO™

Document Part No. TIEM12147/41202

Release Date: April 2005

The Getting Started Guide for Trend Micro™ IM Security for Live Communications Server is intended to provide an overview of the product and deployment instructions for your test or production environment. Read it prior to deploying IM Security.

For technical support, please refer to *Getting Support* for contact details. For detailed configuration instructions and protection strategies, refer to the *IM Security Online Help* and *Context sensitive help*, which is accessible from the IM Security management console.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

`www.trendmicro.com/download/documentation/rating.asp`

Contents

Chapter 3: Registering and Installing IM Security

Chapter 4: Getting Started

Chapter 5: Troubleshooting and FAQ

Chapter 6: Getting Support

Preface

Welcome to the Trend Micro™ IM Security for Live Communications Server *Getting Started Guide*. This book contains basic information about the tasks you need to deploy IM Security. It is intended for novice and advanced users who want to learn an overview of, plan, and deploy IM Security.

This Preface discusses the following topics:

IM Security Documentation

The IM Security documentation consists of the following:

- *Online Help*: Web-based documentation that is accessible from the IM Security management console

  The IM Security *Online Help* is accessible from the IM Security management console. It contains explanations about the IM Security components and features, which includes procedures needed to configure the product from the management console and troubleshooting instructions.

- *Getting Started Guide (GSG)*: PDF documentation that is accessible from the Trend Micro Enterprise Protection CD or can be downloaded from the Trend Micro Update Center (`http://www.trendmicro.com/download/`)

  This *GSG* contains instructions on how to deploy IM Security, which includes IM Security deployment planning and testing, installation, and post-installation instructions. See *About this Getting Started Guide* for chapters available in this book.

Tip: Trend Micro recommends checking the corresponding IM Security link from the Update Center (`http://www.trendmicro.com/download`) for updates to the IM Security documentation and program files.

About this Getting Started Guide

This *Getting Started Guide* discusses the following topics:

- *Introducing IM Security*: an overview of the device and its components
- *Registering and Installing IM Security*: recommendations and instructions to help you plan and deploy IM Security servers
- *Getting Started*: post-installation configurations
- *Troubleshooting and FAQ*: troubleshooting tips for issues encountered when installing IM Security or performing post-installation tasks
- *Getting Support*: guidelines to obtain more information

In addition, *Glossary* defines IM Security related terms.

Audience

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

- Antivirus and content security protection
- General network concepts (such as IP addressing, LAN settings)
- Live Communications Server deployment and topologies
- Live Communications Server configuration

Document Conventions

To help you locate and interpret information easily, the IM Security documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and service or process names
Italics	References to other documentation
`Monospace`	Examples, sample command lines, program code, Web URLs, file names, folder names, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

TABLE 1. Conventions used in the IM Security documentation

Chapter 1

Introducing IM Security

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

The topics discussed in this chapter include:

After learning the IM Security concepts in this chapter, proceed by:

- Planning the deployment (see *page 3-2*)
- Checking the IM Security deployment considerations (see *page 2-4*)
- Conducting a pilot deployment (see *page 2-5*)
- Installing IM Security (see *page 3-5*)

IM Security Overview

Trend Micro™ IM Security for Microsoft™ Live Communications Server represents a significant advancement in antivirus protection and content security for instant messaging environments. IM Security protects your Live Communications Server (LCS) environment from viruses, offensive content, and other instant messaging unwanted incidents. The product is designed to provide real-time protection by scanning both instant messages and files.

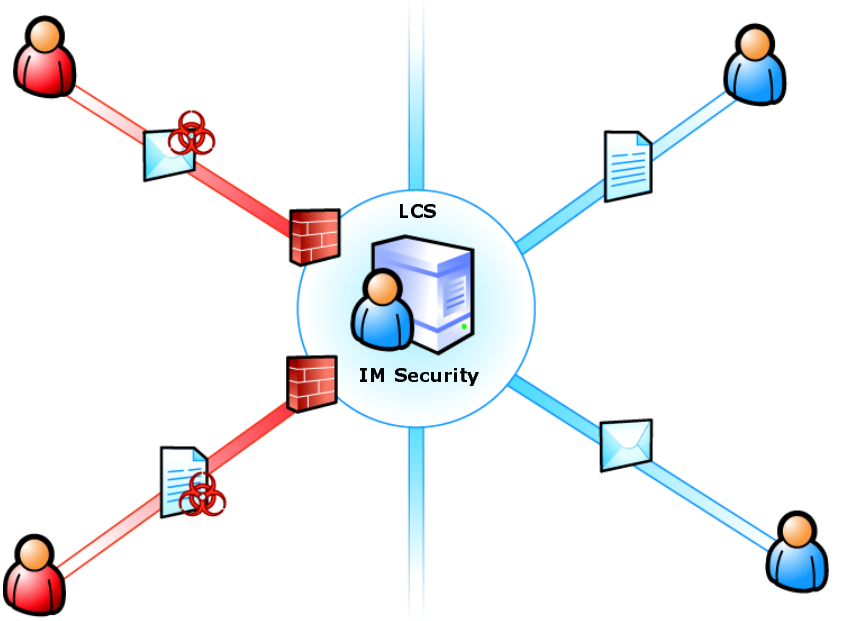


FIGURE 1-1. How IM Security works

IM Security incorporates antivirus scanning, content filtering, and file blocking into one cohesive solution. Refer to the succeeding sections for product features, capabilities, and deployment overview.

Features

IM Security provides the following features:

- *Fast and Simple Installations*
- *Web-based Management Console*
- *Powerful and Creative Antivirus Features*
- *File Blocking*
- *Content Filtering*
- *Updates*
- *Alerts and Notifications*
- *Informative Reports and Logs*

Fast and Simple Installations

IM Security provides a wizard-type Setup program. `Setup.exe` allows you to easily install the product on a single server with Live Communications Server (LCS) 2003 Home Server, LCS 2005 Standard or Enterprise (Front-End) Edition, or LCS 2005 Standard or Enterprise with Service Pack 1 (SP1).

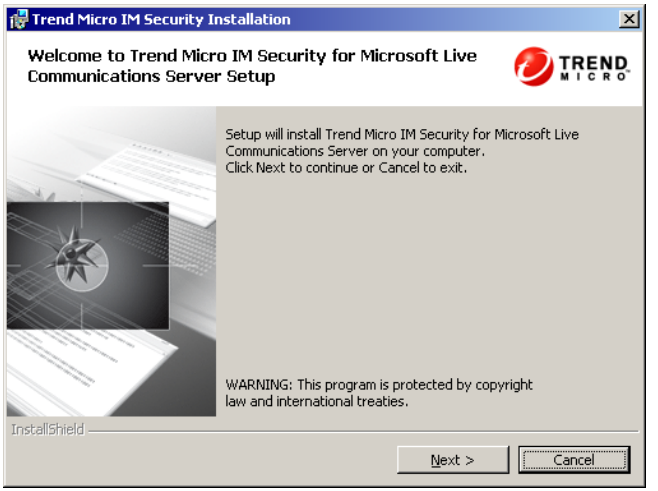


FIGURE 1-2. IM Security Setup Wizard

Installing IM Security provides details on how to install IM Security.

Web-based Management Console

IM Security provides a Web-based management console that allows you to configure IM Security anytime and from anywhere on the network.

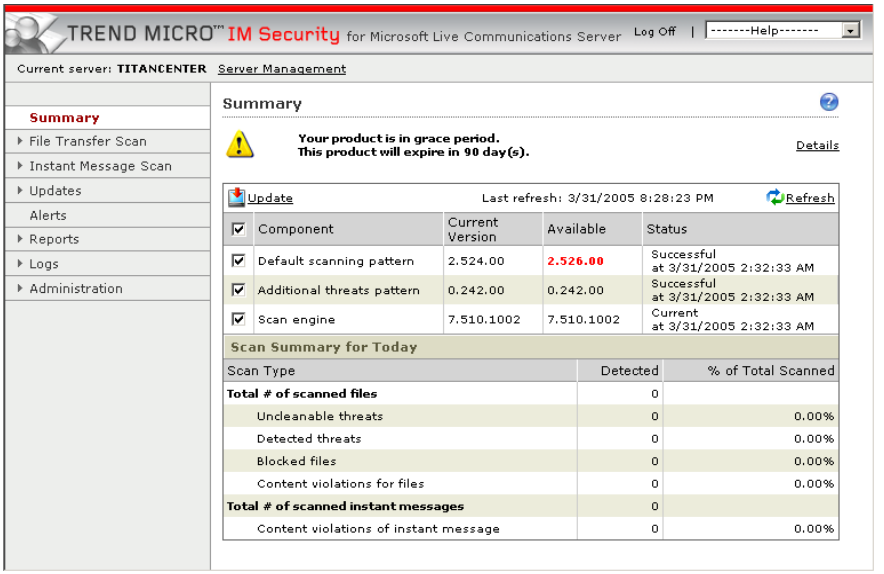


FIGURE 1-3. IM Security management console

The interface has the following areas:

- Header menu: includes links to IM Security help file's **Contents and Index**, Trend Micro Support team's **Knowledge Base**, and other Support tools
- Header section: displays the current server name and **Server Management** link
- Navigation menu: has links to major IM Security features
- Working area: allows you to configure IM Security options

Tip: The IM Security management console is best viewed using a screen area of 1024 x 768 pixels.

Powerful and Creative Antivirus Features

IM Security implements the following virus, spyware, and other grayware scanning methodologies:

- Quickly scan messages and files using multi-threaded in-memory scanning
- Scan for viruses and block files using true file type recognition
- Use Trend Micro ActiveAction (recommended) actions or customize actions against viruses, spyware, and other grayware

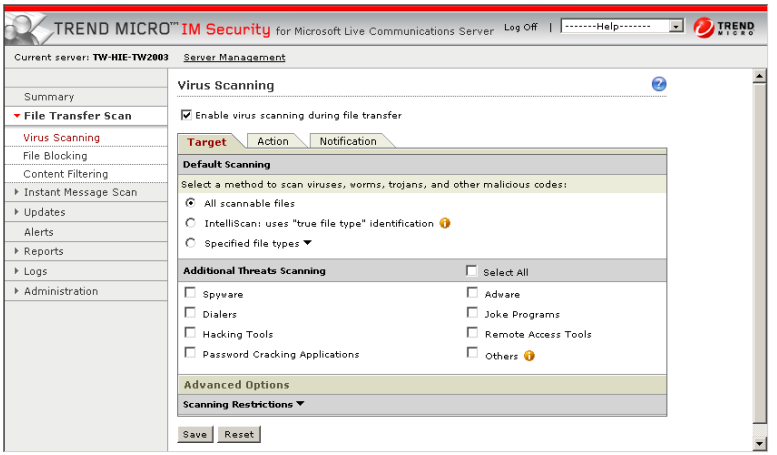


FIGURE 1-4. IM Security virus scanning

File Blocking

You have the option to decide which files to block and what action to take against blocked files.

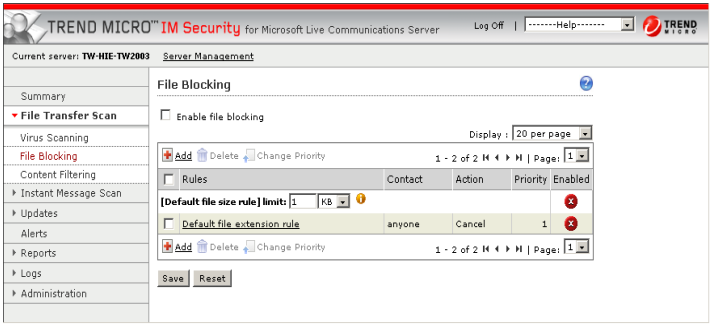


FIGURE 1-5. IM Security file blocking

Content Filtering

IM Security allows you to check messages and files for content deemed harassing, offensive, or otherwise objectionable. In addition, the product provides the option to let you specify the filter action for messages or files with unwanted content.

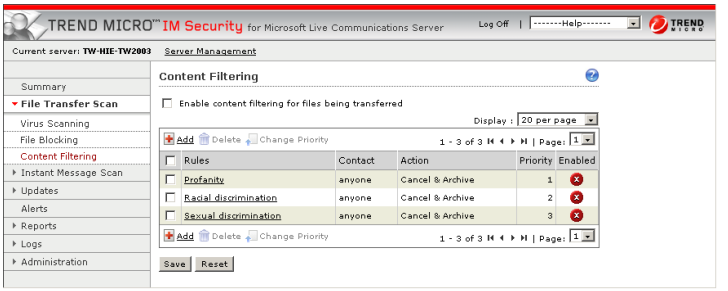


FIGURE 1-6. IM Security file content filtering

Note: IM Security is able to filter content of Microsoft Office files (`*.ppt`, `*.doc`, `*.xls`) and Adobe portable document formats (`*.pdf`).

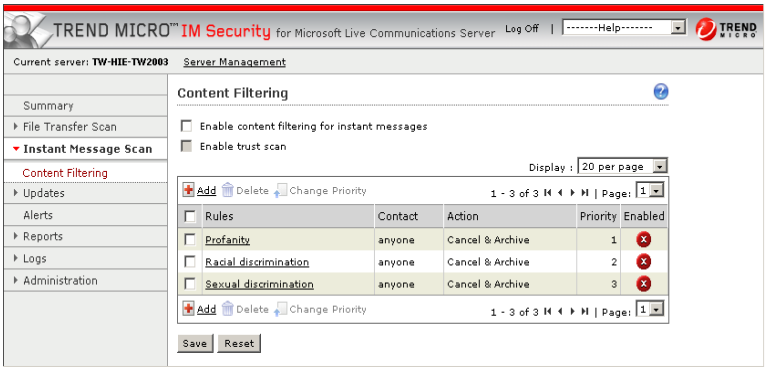


FIGURE 1-7. IM Security instant message content filtering

Updates

Configure scheduled or on-demand component updates. In addition, select Trend Micro ActiveUpdate as the update source or set other locations where new components are available. Refer to the IM Security *Online Help* for details.

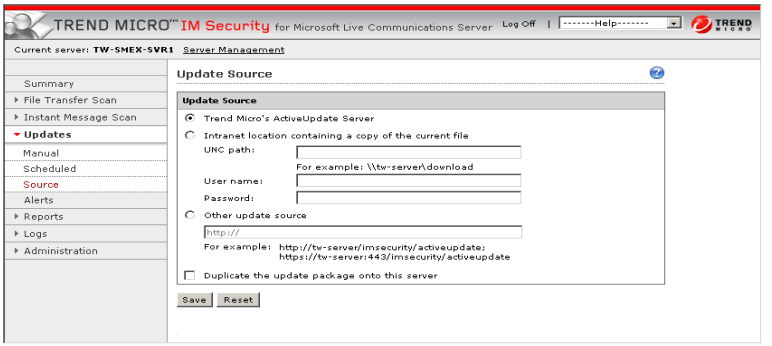


FIGURE 1-8. IM Security Update Source

Alerts and Notifications

Set alerts to notify administrators or selected IT personnel whenever specific IM Security or LCS related events occur.

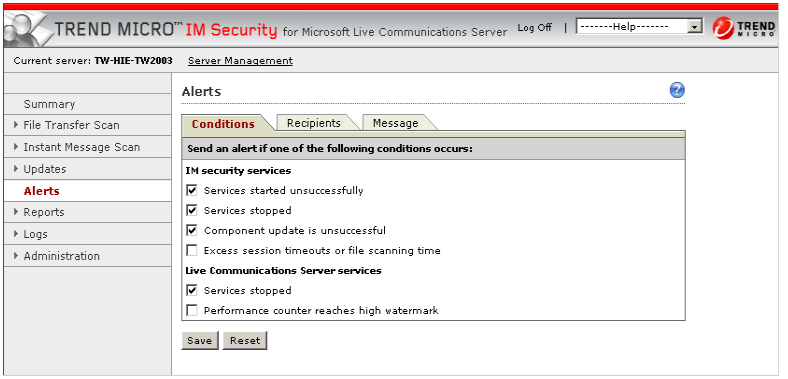


FIGURE 1-9. IM Security alerts

Inform administrators and contacts about IM Security actions using customizable notifications.

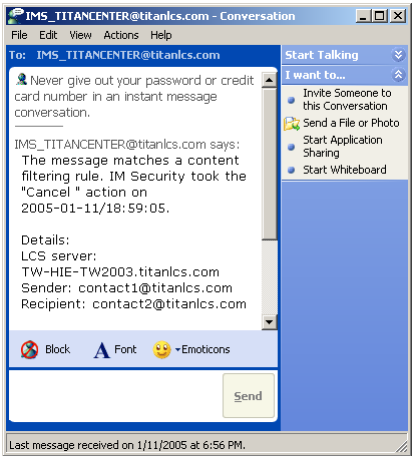


FIGURE 1-10. Sample IM Security notifications via IM

Informative Reports and Logs

Monitor IM Security activities using queried logs that detail system events, viruses, and program update events. In addition, IM Security provides the option to send graphical reports via email.

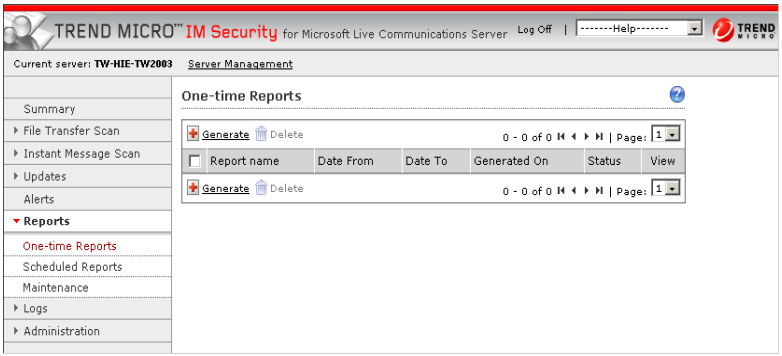


FIGURE 1-11. IM Security reports

Proceed to the next section for details about threat and unwanted content protection.

File and Instant Messaging Protection

IM Security protects Live Communications Server users with:

- Threat, spyware, and other grayware scanning
- File blocking
- Content filtering (files and instant messages)

Table 1-1 presents how IM Security applies its file and instant messaging protections.

ORDER	FILE-BASED PROTECTION	IM-BASED PROTECTION
1	Virus Scanning	Content Filtering
2	File Blocking	
3	Content Filtering	

TABLE 1-1. IM Security protection order

IM Security uses all three levels of protection to prevent files with viruses or spyware/grayware and unwanted content from reaching intended recipients. The product uses its content filtering protection to prevent instant messages with unwanted content from reaching contacts.

The succeeding section explains how IM Security's file and IM-based protection works.

Virus and Spyware/Grayware Scanning

When enabled, file transfer scanning continually protects your instant messaging environment. Virus scanning scans for threats and spyware/grayware that might be present in incoming and outgoing files.

Figure 1-12 depicts how IM Security virus, spyware, and scanning works.

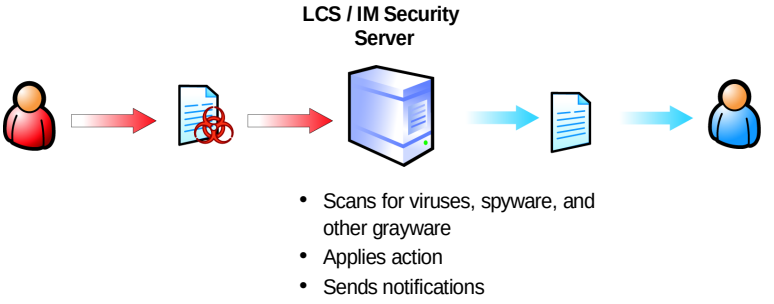


FIGURE 1-12. How IM Security performs virus scanning

IM Security performs the following virus scanning tasks upon receiving a file:

1. Scans the file based on configurations made in the **Virus Scanning** page.
2. Applies the virus scanning action.

   Table 1-2 lists the actions that you can set.
3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators or contacts of the virus detection through email, IM, SNMP, or Windows Event log.

Refer to the following topics in the *Online Help* for details about and instructions to configure file transfer scanning and filtering:

- *Content Filtering*, *File Blocking*, *Virus Scanning*
- *Protect IM Environment(s)*

File Blocking

When enabled, file blocking scans for unwanted files based on file type, name, or size. *Figure 1-13* depicts how IM Security file blocking works.

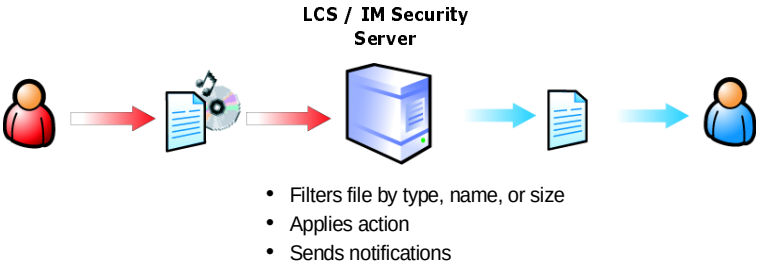


FIGURE 1-13. How IM Security performs file blocking

IM Security performs the following file blocking tasks upon receiving a file:

1. Scans and determines whether a file 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**.

FIGURE 1-14. Block files by file type, name, or size

   If more than one of these criteria are enabled in a single rule, IM Security uses an OR relationship to connect the enabled criteria.

2. Applies the file blocking action.

Table 1-2 lists the actions that you can set.

3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators or contacts of a file blocking event through email, IM, SNMP, or Windows Event log.

Table 1-2 defines the Virus Scanning and File Blocking actions.

ACTION	VIRUS SCANNING	FILE BLOCKING
ActiveAction	✔	✘
Cancel file transfer	✔	✔
Clean	✔	✘
Deliver	✔	✔
Quarantine	✔	✘
Archive*	✘	✔ **

TABLE 1-2. Virus scanning and file blocking actions

* In addition to one of the above actions, the Archive action can be configured per rule). An LCS Archiving Service must be available to enable querying archived messages. For more information about Archiving Service, please refer to the LCS documentation.

** File Blocking saves files in the IM Security Archive directory (for example `<root>:\Program Files\Trend Micro\IM Security\Archive`).

Refer to the following topics in the Online Help for details about and instructions to configure file transfer scanning and filtering:

- *Content Filtering, File Blocking, Virus Scanning*
- *Protect IM Environment(s)*

Content Filtering

When enabled, content filtering protects your instant messaging environment by filtering all incoming and outgoing files and messages for undesirable content.

Figure 1-15 depicts how IM Security file or instant message content filtering works.

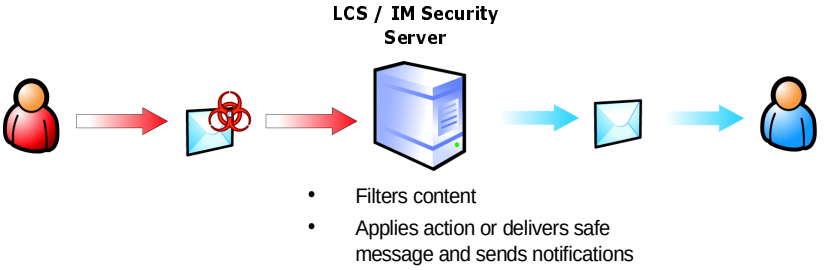


FIGURE 1-15. How IM Security performs content filtering

IM Security performs the following content filtering tasks upon receiving a file/message:

1. Evaluates and determines whether a file/message being transferred contains offensive information by comparing their content with 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/message contains unwanted offensive content. The product implements an algorithm that consolidates all keywords from enabled rules for filtering. Doing so allows faster file or message content filtering.

2. Applies the content filtering rule action.

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

   Table 1-3 lists the content filtering actions that you can set.

3. Sends notifications to the administrator or contacts.

   IM Security allows you to notify administrators or contacts of the content filter rule matching through email, IM, SNMP, or Windows Event log.

The following table defines the Content Filtering actions.

ACTION	FILE CONTENT FILTERING	INSTANT MESSAGE CONTENT FILTERING
Cancel instant message transfer	✔	✔
Deliver	✔	✔
Replace entire content	✘	✔
Replace keyword	✘	✔
Archive*	✔ **	✔ ***

TABLE 1-3. Content filtering actions

* In addition to one of the above actions, the Archive action can be configured per rule. An LCS Archiving Service must be available to enable querying archived messages. For more information about Archiving Service, please refer to the LCS documentation.

** File Content Filtering saves files in the IM Security Archive directory (for example `<root>:\Program Files\Trend Micro\IM Security\Archive`).

*** Instant Message Content Filtering saves messages in the IM Security database (for example `<root>:\Program Files\Trend Micro\IM Security\Database\IMSecurityDB.mdf`).

Refer to the following sections in the *Online Help* for details about:

- *Content Filtering*
- *Protect IM Environment(s)*

Protection Strategy

An organization must design a strategy that provides optimal protection for its instant messaging environment. The key decision factors for selecting an appropriate IM Security protection strategy are:

- What is the overall corporate IT security strategy?
- What are the available resources (processor, memory) on available servers with Live Communications Server?
- Where and how can threats and unwanted content enter the Live Communications Server environment (for example, file transfer, instant message)?

Trend Micro recommends the following strategies for optimal antivirus protection for a Live Communications Server environment:

- Implementation of virus, spyware, and other grayware scanning
- Creation of file blocking rules for unauthorized file types and extensions

Tip: The IM Security management console provides the recommended file types and extensions to block.

- Creation of content filtering rules for unwanted or offensive keywords present in instant messages and files being transferred
- Configuration of scheduled component update

These strategies provide very good antivirus protection, while also minimizing the system resource usage. Refer to the *Online Help* for instructions on how to implement these strategies.

Figure 1-16 illustrates a sample environment after deploying IM Security.

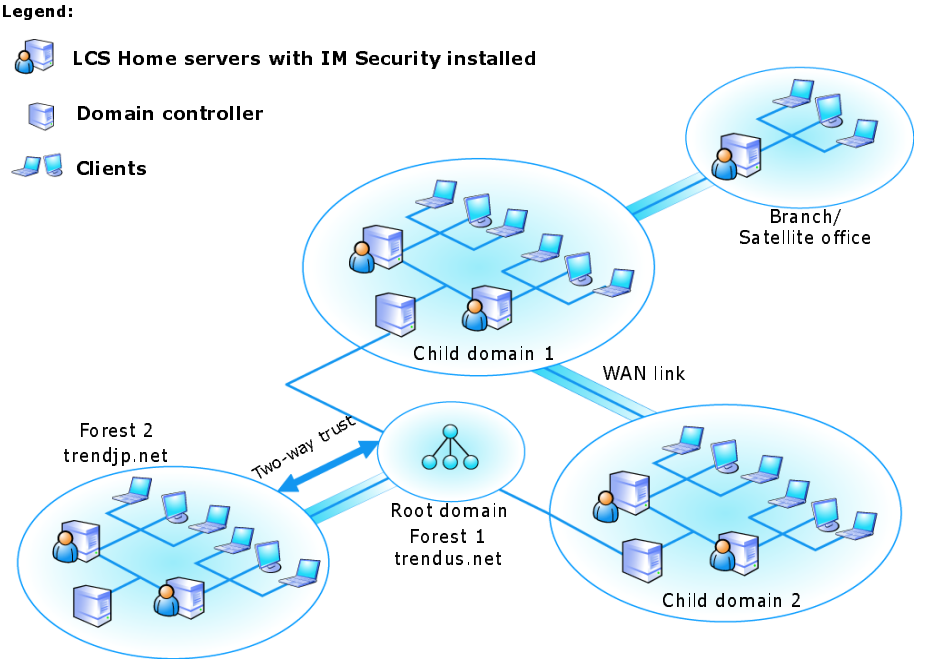


FIGURE 1-16. A sample protected LCS environment

Proceed to the next section for details about IM Security deployment.

Chapter 2

Testing and Performing Pre-installation Tasks

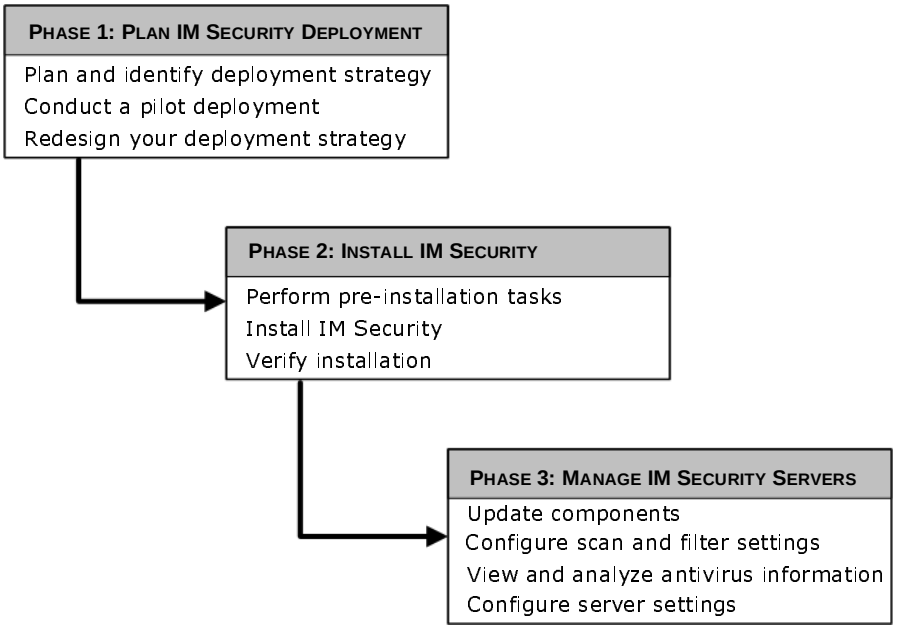
This chapter explains how to plan and prepare for an IM Security deployment.

The topics discussed in this chapter include:

Planning for Deployment

To maximize the benefits IM Security can bring to your organization, you will need an understanding of the possible ways to deploy IM Security to servers with Live Communications Server installed. This section provides a deployment overview and considerations.

Deployment Overview



Phase 1: Plan the Deployment

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

- Take into account the deployment considerations (*page 2-4*)
- Conduct a pilot deployment on a test segment of your network (see *page 2-5*)
- Redefine your deployment strategy based on the results of the pilot deployment (see *page 2-5*)

Phase 2: Install IM Security

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

- Perform pre-installation tasks (see *page 2-7*)
- Install IM Security (see *page 3-5*)
- Verify successful installation (see *page 4-8*)

Phase 3: Manage IM Security Servers

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

- Update to the latest IM Security components to help guarantee current protection for LCS servers
- Configure scan and filter settings
- Schedule update and report generation

Note: This *Getting Started Guide* discusses phases 1 (see *page 2-4*) and 2 (see *page 2-7*) and briefly introduces post-installation configuration tasks (see *page 4-1*). Refer to the IM Security *Online Help* for detailed instructions relating to product administration.

Deployment Considerations

Consider the following when planning for an IM Security deployment:

- Windows Messaging does not support LCS servers and clients behind a Network Address Translator (NAT)

  If you are using a NAT, file transfer will not work unless you have a Universal Plug and Play NAT (UPnP NAT). Make sure that your NAT is UPnP-compliant.

- In an LCS Home Server setup, you need to install IM Security on each Home server to enable virus scanning and content filtering for your entire organization
- Setup does not detect the presence of LCS Archiving Service in a target environment

  To make use of the Archive action in **File Blocking** and **Content Filtering**, as well as the **View Details** link available in **Logs** > **Query** > **Content filtering for IM results**, an LCS Archiving Service must be present and properly configured in your environment. An LCS Archiving Service is an optional component in an IM Security deployment. Refer to Microsoft LCS documentation for more information about the LCS Archiving Service.

- If a firewall exists between an LCS server and its clients, ensure IM Security ports are opened (see *page 2-7*)
- If you have multiple Activation Codes, you must install IM Security to servers separately (that is, simultaneous and remote installation is not possible)
- The Setup program provides you with the option to enable Secure Sockets Layer (SSL) management console connection

  Use SSL to help ensure secure communications between your Web browser and the IM Security server.

  Note: You cannot configure SSL from the management console. SSL must be enabled during installation.

- Setup does not require stopping the LCS services
- Remove other instant messaging antivirus applications before installing IM Security. Otherwise, a scanning conflict may occur

  Setup does not detect other instant messaging antivirus applications.

- Remember to exclude the IM Security folders from other server-based antivirus application's scanning (see *Preparing Other Antivirus Applications*)

Conducting a Pilot Deployment

Trend Micro recommends conducting a pilot deployment in a controlled environment to help you understand how features work, determine how IM Security can help your organization accomplish its security goals, and estimate the level of support you will likely need after a full deployment. A pilot deployment allows you to validate and, if necessary, redesign your deployment plan.

Perform the following tasks to conduct a pilot deployment:

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

Choosing a Pilot Site

Choose a pilot site that matches your planned deployment. This includes other antivirus installations (such as Trend Micro™ OfficeScan™, ScanMail™, and ServerProtect™) you plan to use. Try to simulate the type of topology that would serve as an adequate representation 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 retain a minimum level of security if issues arise.

Deploying and Evaluating your Pilot

Deploy and evaluate the pilot 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 your Deployment Strategy

Identify the potential pitfalls and plan accordingly for a successful deployment, especially considering how IM Security performed with the antivirus installations on your 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 describes both the minimum and recommended requirements for an IM Security server.

Tip: Use these values to obtain an idea on how to allocate server resources that can support the users' needs in your organization.

The following table lists the system requirements for IM Security.

HARDWARE/SOFTWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
CPU	Intel Pentium™ 550MHz or faster processor
Hard disk space (program and database folders)	200MB of available disk space
Memory	512MB
Windows Server™ 2003	Standard or Enterprise edition
Microsoft™ Live Communications Server	2003 Home Server, 2005 Standard or Enterprise (Front-End) Server, or 2005 Standard or Enterprise Server with Service Pack 1 **Note:** The LCS Archiving Service is an optional component in an IM Security deployment. If you want to archive instant messages traffic to and from your IM environment, install this component. You can then use the IM Security management console's **Logs** > **Query** option to search for and view archived messages.
Web server	Microsoft Internet Information Services 6.0 or Apache Web server 2.0
Web browser	Internet Explorer™ 5.5 or Netscape™ Navigator 7.2
Java Virtual Machine (JVM)	Microsoft JVM or Sun JVM version 1.4.1_02 **Note:** For more information about Microsoft JVM, please visit http://www.microsoft.com/mscorp/java/.
Messaging clients	Windows Messenger 5.0 or 5.1

TABLE 2-1. IM Security minimum system requirements

Recommended System Requirements

In addition to the minimum system requirements, consider the following system requirements to obtain optimum IM Security performance:

- Scale the memory with the processor; do not overpopulate with memory
- Use a VGA monitor capable of 1024 x 768 resolution, with at least 256 colors whenever accessing the IM Security management console (*page 4-10*)

Pre-installation Tasks

Several pre-installation tasks can help to make the installation process easier. Complete the following tasks before installing IM Security (see *page B-4* for the checklist version):

- If a firewall exists between an LCS server and its clients, open the ports described in *Table 2-2* to ensure IM Security connectivity

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

TABLE 2-2. Ports for IM Security connectivity

- Log on to the target server using an account with **Domain Admins** privilege

  Setup requires a user with Domain Admins privilege to create the IM Security accounts (*page 4-2*).

- Disable or uninstall other IM environment antivirus applications

  The IM Security Setup program does not detect third-party IM environment antivirus applications. Disable or uninstall third-party antivirus applications to prevent scanning conflicts.

- Check the target server complies with the system requirements

  If the server's specifications do not meet the requirements (see *page 2-6*), Setup will not install IM Security.

- Obtain the proxy server and SMTP server settings and authentication information (if necessary)

  During installation, the setup program prompts you to enter proxy information. If a proxy server handles Internet traffic on your network, you must type the proxy server information, your user name, and your password to receive pattern file and scan engine updates. If you leave the proxy information blank during installation, you can configure it at a later time from the management console.
- Close opened Microsoft Management Console (MMC) screens
- Prepare the IM Security Activation Code (see *page 3-2*)

After completing the pre-installation tasks, proceed by registering (see *page 3-2*) or installing IM Security (see *page 3-5*).

Chapter 3

Registering and Installing IM Security

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

The topics discussed in this chapter include:

Registering and Obtaining an Activation Code

Use your Registration Key to register your product on the Trend Micro Online Registration Web site. Register your products to ensure eligibility to receive the latest security updates and other product and maintenance services. After completing the registration, Trend Micro sends an email message that includes an IM Security Activation Code, which you can then use to activate IM Security.

IM Security has two types of Activation Code:

- Evaluation AC

  An Evaluation AC allows you to implement IM Security's full functionalities for a limited evaluation period. During the evaluation period, IM Security performs virus scanning, file blocking, and content filtering, as well as component update.

- Standard AC

  A Standard AC allows you to implement IM Security's full functionalities.

Tip: For information on purchasing a standard version Registration Key from a reseller, see **Trend Micro Sales Web page**.

Table 3-1 defines how IM Security behaves depending on the Activation Code activation and expiration.

Feature	Standard Version		Evaluation Version	
	Activated	Expired	Activated	Expired
File/IM scanning and filtering	✔	✔	✔	✘
ActiveUpdate	✔ (when the # of seats is not exhausted)	✘	✔ (when the # of seats is not exhausted)	✘
Management console access	✔	✔	✔	✔

Table 3-1. How IM Security behaves depending on the license version and status

The management console displays the remaining number of days before an evaluation or full version AC expires. Trend Micro recommends registering and obtaining a full version AC before the expiry date to allow uninterrupted LCS environment protection.

Tip: You may register IM Security during installation (see *page 3-16*).

To register IM Security and obtain an Activation Code:

Note: These Web screens and workflows are subject to change without prior notice.

1. Using a Web browser, go to **Trend Micro Online Registration** (`http://olr.trendmicro.com`). The **Online Registration** page of the Trend Micro Web site opens.

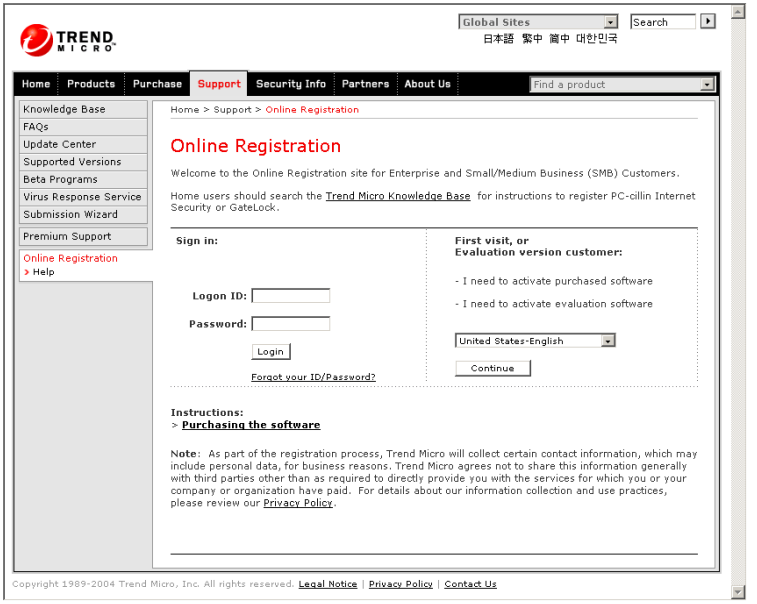


FIGURE 3-1. Trend Micro Online Registration

2. Perform one of the following:
   - If you already have an account with the Online Registration Web site, log on using your **logon ID** and **password**
   - Otherwise, if you are a new customer, select your **location** and click **Continue** under **First Visit...**
3. On the **Enter Registration Key** page, type or copy the **IM Security Registration Key**, and then click **Continue**.
4. On the **License Agreement** page, read the license agreement and then click **I accept**.
5. On the **Confirm Product Information** page, click **Continue Registration**.
6. Fill out the online registration form, and then click **Submit**.
7. Click **OK** twice.

After completing the registration, Trend Micro sends an Activation Code via email, which you can then use to activate IM Security. Perform one the following methods to activate IM Security:

- During installation (see *page 3-16*)
- After installation via the management console (see *page 3-24*)

Installing IM Security

This section provides details about IM Security installation. Ensure that you have performed the *Pre-installation Tasks* before running Setup.

To install IM Security:

1. Wait while Setup installs RTC Client API 2.1 and MSDE 2000 IM Security instance (see *page 3-5*).

   Note: Skip this step if you are upgrading from a previous IM Security build or if you have not removed these programs from a previous IM Security installation.

2. Set the product and database installation folder (see *page 3-9*).
3. Configure the Web server and proxy server settings (see *page 3-12*).
4. Activate the product and set World Virus Tracking participation (see *page 3-16*).
5. Set administrator and notification accounts (see *page 3-18*).

Step 1: Wait while Setup installs RTC Client API 2.1 and MSDE 2000 IM Security instance.

1. Do one of the following to navigate to the Setup program (`Setup.exe`):
   - If you are installing from the Trend Micro Enterprise Protection CD, go to the IM Security folder on the CD

     View product **Information**, **System Requirements**, or complete IM Security **Documentation** in the corresponding view pane.
   - If you downloaded the software from the Trend Micro Update Center, navigate to the relevant folder on your server

2. Double-click `Setup.exe` to launch the wizard installation program.

   The **Setup Prompt** screen appears.

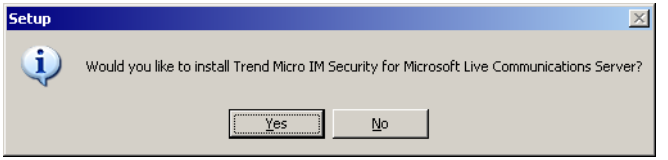


FIGURE 3-2. Setup Prompt screen

3. Click **Yes** to start.

   Setup performs one of the following tasks:

   - If you are installing IM Security for the first time, Setup initially installs RTC Client API 1.2 and Microsoft SQL Server Desktop Engine (MSDE) 2000 instance before displaying the **Welcome** screen

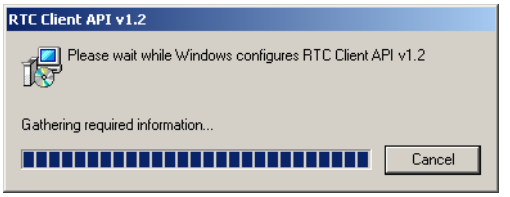


FIGURE 3-3. Installing RTC Client API 1.2 MSDE 2000 instance

IM Security uses RTC Client API to send IM-based notifications.

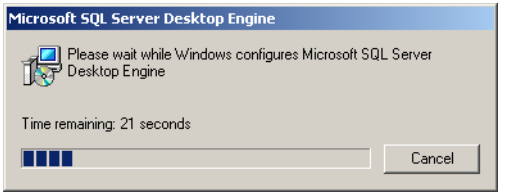


FIGURE 3-4. Installing MSDE 2000 instance

IM Security uses MSDE to store logs to the IM Security database.

- If you have installed IM Security before and have not removed RTC API 1.2 and MSDE 2000, Setup proceeds to the IM Security installation and displays the **Welcome** screen

FIGURE 3-5. Welcome screen

4. Click **Next >**. The **License Agreement** screen appears.

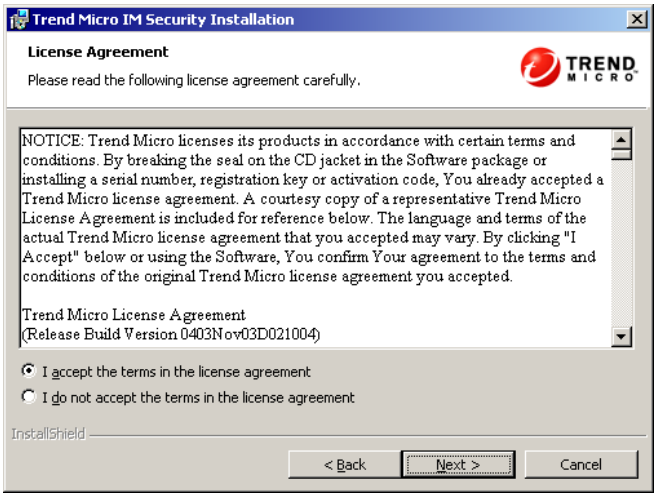


FIGURE 3-6. License Agreement screen

Select **I accept the terms in the license agreement** to continue with the installation. Otherwise, select **I do not accept the terms in the license agreement**; the installation will end, and Setup will close.

Step 2: Set the product and database installation folder.

1. Click **Next >**. The **Installation Folder** screen appears.

   Specify the complete path and folder name where you want to install IM Security. Accept or modify the default destination folder (`c:\Program Files\Trend Micro\IM Security`).

FIGURE 3-7. Installation Folder screen

2. Click **Next >**. The **Database Installation Folder** screen appears.

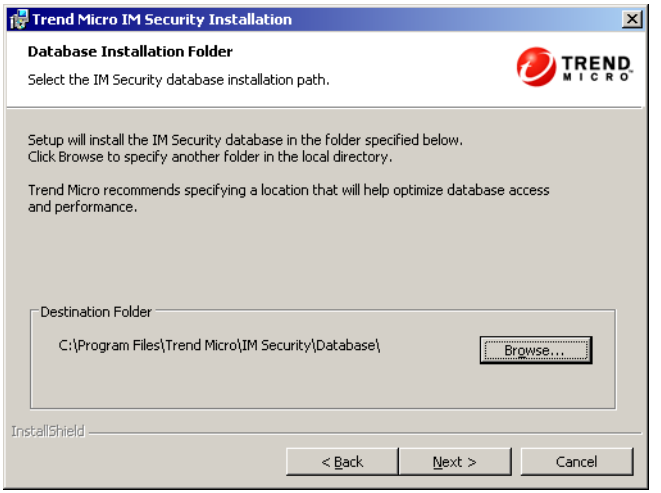


FIGURE 3-8. Database Installation Folder screen

Specify the full path where you want to install the IM Security database (`IMSSecurityDB.mdf`) and database log file (`IMSecurityDB.ldf`). Accept or modify the default installation folder (`c:\Program Files\Trend Micro\IM Security\Database`).

Tip: Trend Micro recommends specifying a location that is the same as the IM Security program folder. In addition, do not move the database and database log file from its installation path to avoid connectivity issues.

---

3. Click **Next >**. The **System Information** screen appears.

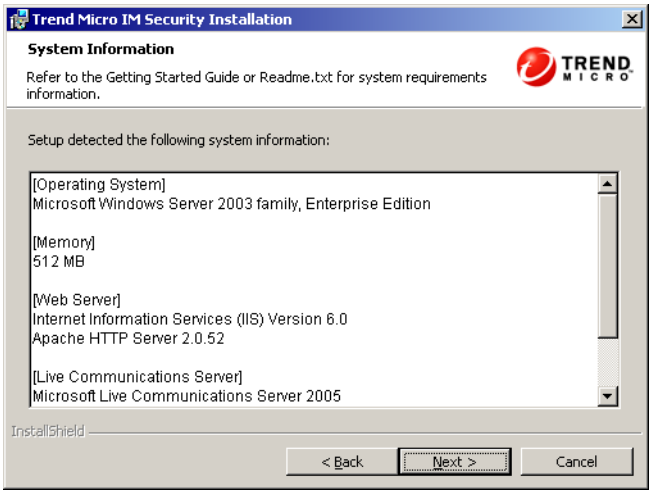


FIGURE 3-9. System Information screen

Setup checks the local server for compliancy with the system requirements and displays the server's specification.

Step 3: Configure the Web, Simple Mail Transfer Protocol (SMTP), and proxy server settings.

1. Click **Next >**. The **Web Server** screen appears.

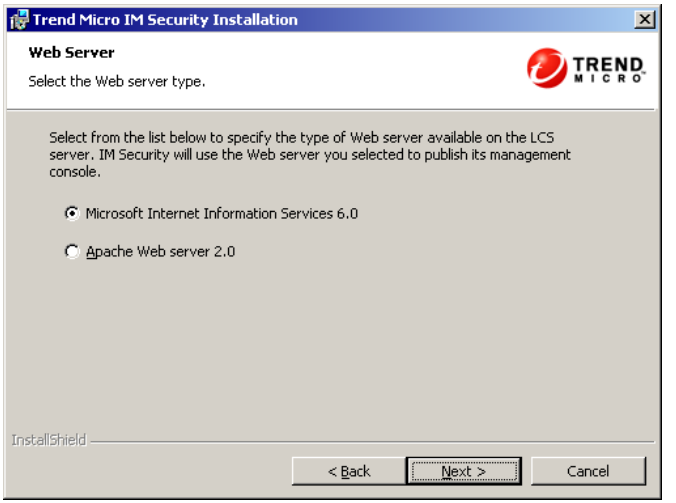


FIGURE 3-10. Web Server screen

Select the Web server installed on the target server: **Microsoft IIS** or **Apache Web server**. IM Security will use this server to publish its management console.

Tip: Before running Setup, install a Web server application on the target server. See *Pre-installation Tasks* for additional tasks that you should perform before installing IM Security.

---

2. Click **Next >**. The **Web Server Settings** screen appears.

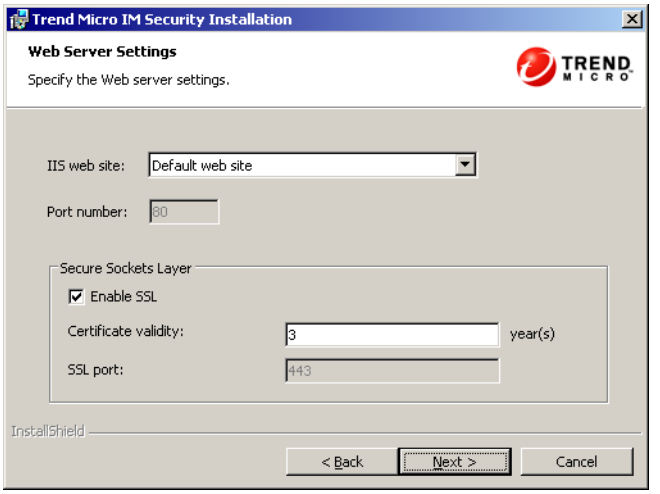


FIGURE 3-11. IIS Web Server Settings screen

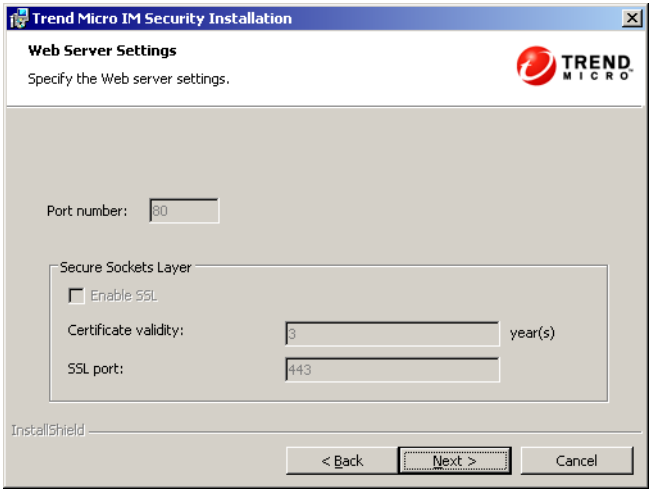


FIGURE 3-12. Apache Web Server Settings screen

Set the Web server port and encrypted connection configuration. M Security will use these settings to encrypt communication between the management console to the IM Security server.

a. If you selected **IIS Web server** (*Figure 3-11*), select the site that will host the management console Web pages. This option is not available when Apache Web server is selected.

b. Accept or type a new **port number** that Setup will use for management console access (only applies to IIS).

If you changed the HTTP port to another value other than the default number (80), including the port number in the URL is necessary.

c. Under **Secure Sockets Layer**, select **Enable SSL** to enable secure communication between your Web browser and the IM Security server.

Tip: Enabling SSL is only available during installation. Trend Micro recommends this option to help ensure secure communication.

---

d. Type the **certificate validity** and if necessary, modify the allocated SSL port.

3. Click **Next >**. The **Proxy Server Settings** screen appears.

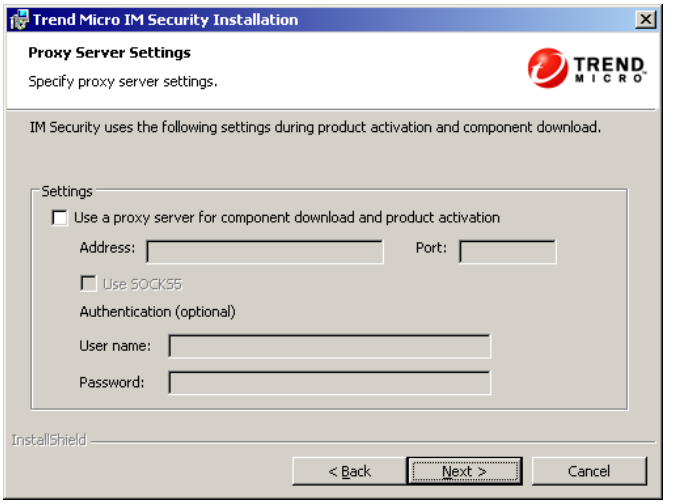


FIGURE 3-13. Proxy Server Settings screen

If you use a proxy server to connect to the Internet, select **Use a proxy server for component download and product activation**, and then set the following:

- **Proxy server**: type the FQDN, IP address, or NetBIOS name of the server
- **Port**: type the proxy port number
- **Use SOCKS5**: select this option if the proxy server is using SOCKS5 protocol
- **User name**: type a logon name that can access the proxy server

  Provide both the domain and logon names, for example: `mydomain\admin`.
- **Password**: type the password for the user name

Step 4: Activate the product and World Virus Tracking program participation.

1. Click **Next >**. The **Product Activation** screen appears.

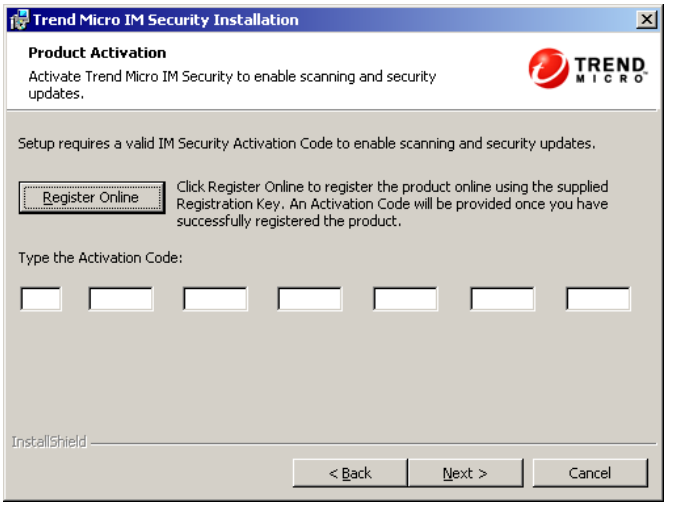


FIGURE 3-14. Product Activation screen

If you have not obtained an IM Security **Activation Code**, click **Register Online** and follow the Online Registration prompts to obtain an Activation Code (see instructions available on *page 3-2*). Otherwise, type or paste the acquired **Activation Code** in the fields provided.

Tip: You may skip this step and activate IM Security using the management console > **Administration** > **Product License** page at a later time (see *page 3-24*).

---

2. Click **Next >**. The **World Virus Tracking** screen appears.

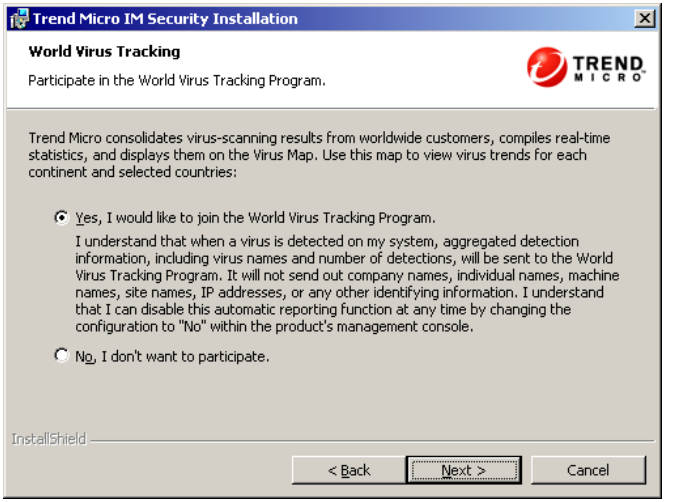


FIGURE 3-15. World Virus Tracking screen

Select **Yes, I would like to join the World Virus Tracking Program**. If you wish to join this program at a later time, use the management console's **Administration** > **World Virus Tracking** option to participate.

Step 5: Set IM Security administrator account(s).

1. Click **Next** >. The Administrator Account screen appears.

FIGURE 3-16. Administrator Account screen

Create the administrator account or specify an existing Active Directory user that Setup will designate as the IM Security administrator:

- If you are creating a new account, specify a user name that is easy to remember and descriptive of IM Security management duties (for example, `ims_admin`)

  In addition, provide a strong password to help secure product administration.

  Note: Setup displays a message if the password provided does not meet the required complexity and length.

- If you are specifying an existing account, Setup adds the account to the **IM Security Admins** group

2. Click **Next >**. The **IM Notification Account** screen appears.

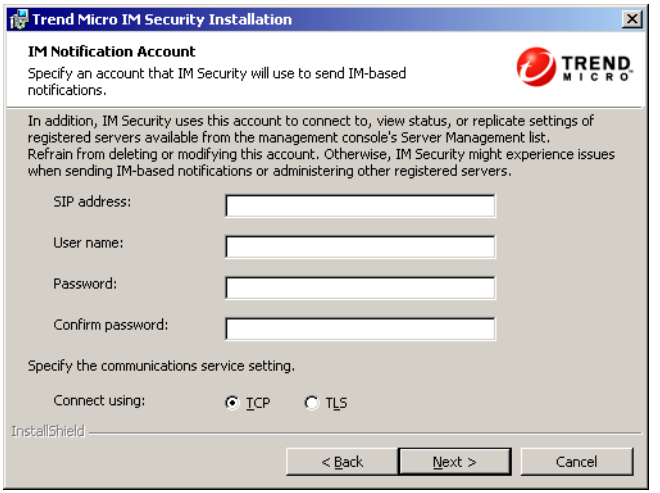


FIGURE 3-17. IM Notification Account screen

a. Create an account or specify an existing Active Directory user that IM Security will use to send IM-based notifications.

- If you are creating a new account, accept the predefined SIP address and user name

  Otherwise, specify a SIP address and user name that are easy to remember and descriptive of IM Security notification duties (for example, `ims_notification_agent`)

- If you are specifying an existing account (**user name** or **SIP address**), Setup displays an error and requires you to specify a new or unique Active Directory user

b. Specify a strong password to help secure product administration.

c. Select the communication service setting that IM Security will use whenever it sends IM-based notifications.

Tip: Transmission Control Protocol (TCP) sends instant messages in plain text. Alternatively, Transport Layer Security (TLS) sends encrypted instant messages.

Setup creates the **IM Security Admins** Active Directory group, and then adds the administrator and notification accounts to the group.

3. Click **Next >**. The **Email Notification Settings** screen appears.

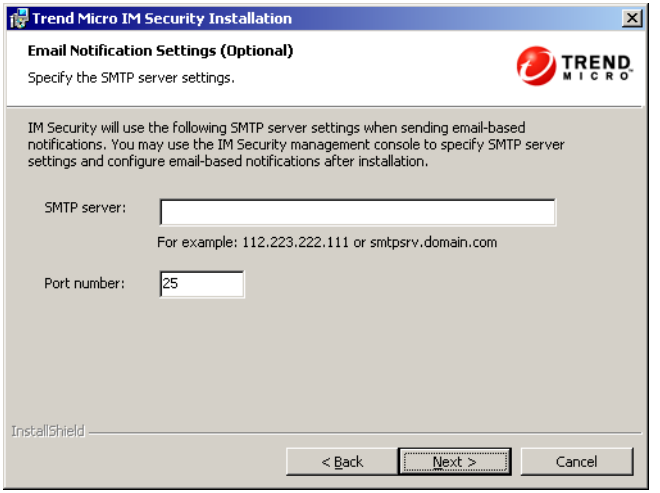


FIGURE 3-18. Email Notification Settings screen

Configure the **SMTP server** and **port number** that IM Security will use to send notifications and alerts via email. If you want to set the SMTP server at a later time, use the IM Security management console's **Administration** > **Notification Settings** page.

4. Click **Next** >. The **Ready to Install** screen appears.

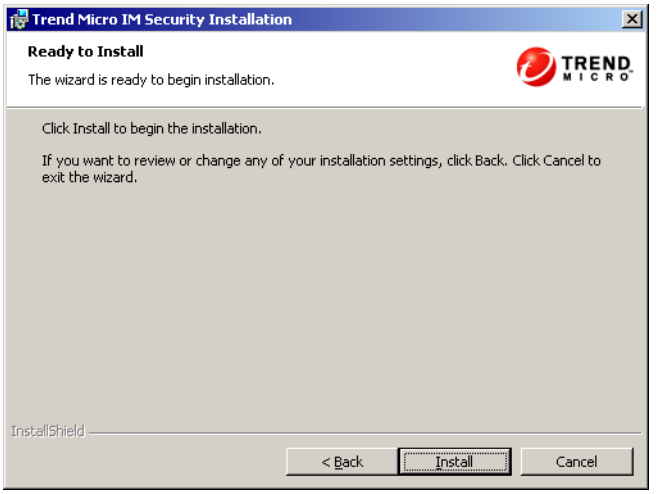


FIGURE 3-19. Ready to Install screen

Click **Back** to modify specific installation settings.

5. Click **Next >**. Setup installs IM Security files, services, and other components to the target server.

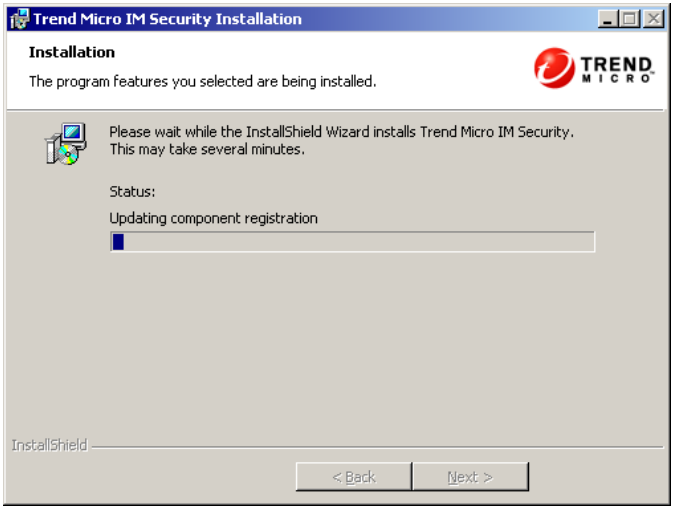


FIGURE 3-20. Installation screen

6. Click **Finish**. The **Installation Complete**d screen allows you to view the product ReadMe or manually update its antivirus and content security components.

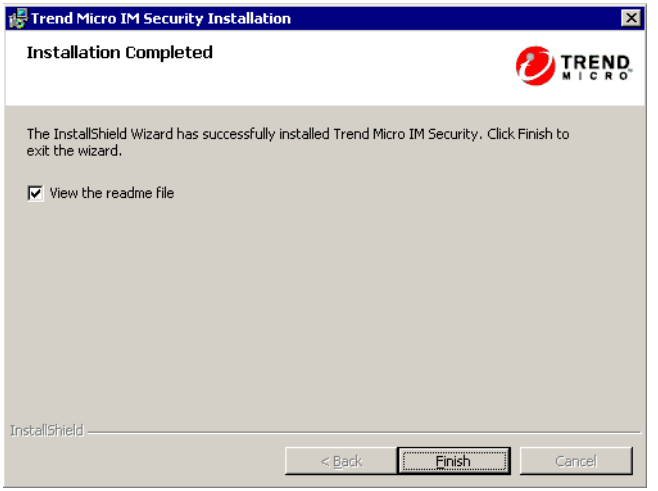


FIGURE 3-21. Installation Completed screen

See *Verifying a Successful Installation* to confirm whether IM Security has been successfully installed.

Trend Micro recommends performing the post-installation procedures to establish a security baseline for your Live Communications Server environment. See *Getting Started* for instructions.

See *Installation* for help when issues occur during IM Security installation.

Activating IM Security

Activate IM Security to keep your antivirus and content security components current. To activate your product, register online and obtain an Activation Code using your Registration Key.

- If you have purchased the standard version AC from a Trend Micro reseller, the Registration Key is included in the product package

  Register online and obtain an Activation Code to activate the product.

- Otherwise, if you are using an evaluation version

  The evaluation version is fully functional for 30 days, after which IM Security tasks will continue to load, but no virus scanning, message filtering, nor component update will occur.

  Obtain a standard Registration Key from your reseller and then follow the instructions to activate the product.

After you have obtained an Activation Code either from your product package or purchased through a Trend Micro reseller, activate IM Security to use all of its functions, including downloading updated program components.

Tip: Setup provides an option to activate IM Security during installation (see *page 3-16*).

To activate IM Security using the management console:

1. Access the IM Security management console (see *page 4-10*).
2. On the left-hand menu, click **Administration** > **Product License**. The **Product License** page appears.
3. Click **Enter a New Code**, and then type the full version AC in **New Activation Code**.
4. Click **Activate**.

IM Security is now activated. Standard maintenance support is included in the initial purchase of IM Security license and consists of one year of component updates, product version upgrades, and telephone and online technical support.

Removing IM Security

Uninstallation removes the following IM Security components (refer to *page 4-2* for details):

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

Note: Removal will automatically remove RTC Client API 1.2 and MSDE 2000 IM Security instance. Do not remove these components before uninstalling IM Security.

To uninstall IM Security:

1. Go to **Start** > **Control Panel** > **Add/Remove Programs**.
2. Select **Trend Micro IM Security for Microsoft Live Communications Server**, and then click **Remove**.
3. At the prompt, select **Yes** to remove IM Security.

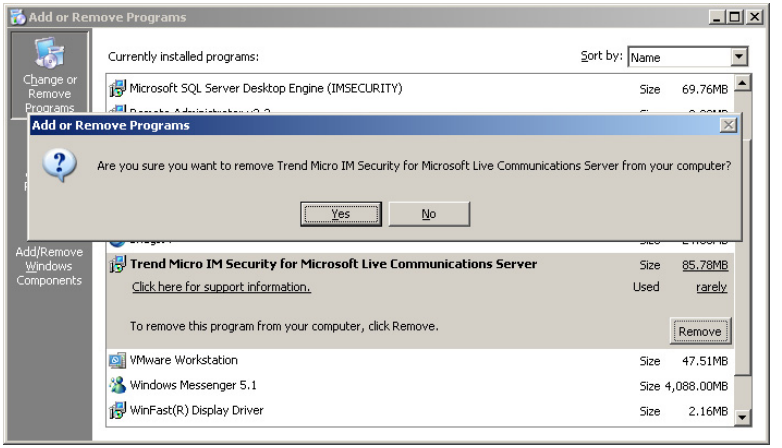


FIGURE 3-22. Removing IM Security

IM Security is removed from the server.

Chapter 4

Getting Started

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

The topics discussed in this chapter include:

System Changes

The following server changes occur after running a successful IM Security installation:

Note: These changes are thoroughly described in the succeeding sections.

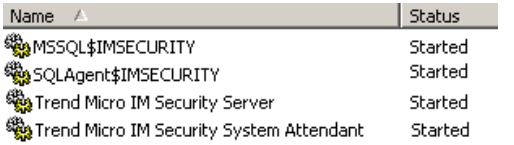
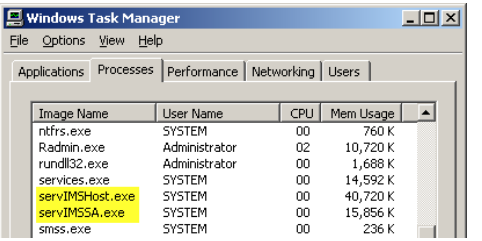
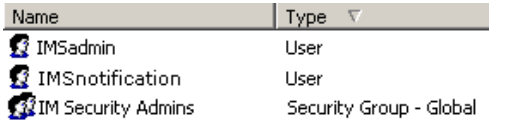
COMPONENT	DETAILS
Product and SQL agent services	Setup adds four services  **FIGURE 4-1. Services**
Task Manager processes	Setup adds two processes:  **FIGURE 4-2. Processes**
Active Directory objects	Setup adds two (2) users and one (1) group based on what you configure during installation (see *page 3-5*):  **FIGURE 4-3. Active Directory objects**

TABLE 4-1. System changes after installing IM Security

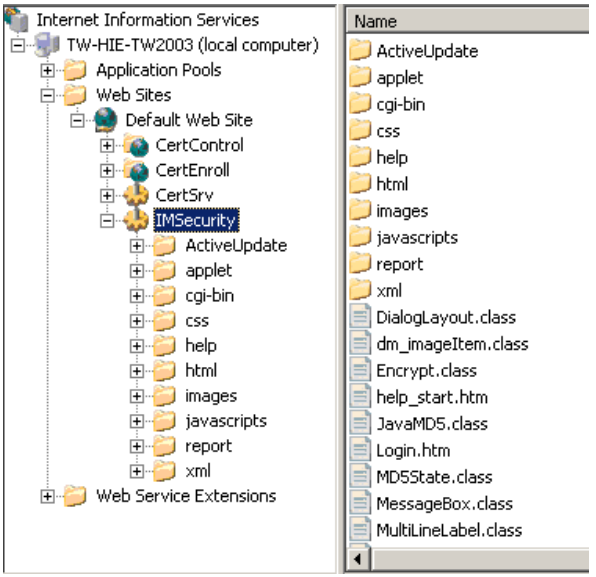
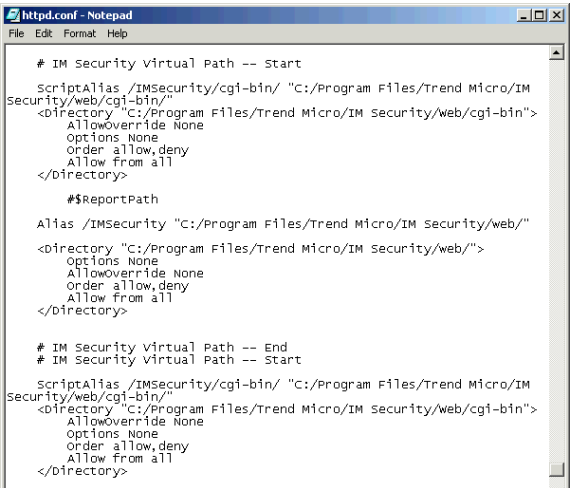
COMPONENT	DETAILS
IIS Web site **Note:** If you have Apache installed, see *Figure 4-5*.	Depending on the **Web Server Type** screen, Setup follows your Web server settings (see *page 3-13*):  **FIGURE 4-4. IIS changes**

TABLE 4-1. System changes after installing IM Security

COMPONENT	DETAILS

Apache Web site
 	
Note: If you have IIS installed, see *Figure 4-4*.
	Setup follows your Web server settings (see *page 3-13*)
	 
	httpd.conf - Notepad
	File Edit Format Help
	
	`# IM Security Virtual Path -- Start`
	
	`ScriptAlias /IMSecurity/cgi-bin/ "C:/Program Files/Trend Micro/IM Security/web/cgi-bin/"`
	`<Directory "C:/Program Files/Trend Micro/IM Security/web/cgi-bin">`
	`AllowOverride None`
	`Options None`
	`Order allow,deny`
	`Allow from all`
	`</Directory>`
	
	`#$ReportPath`
	
	`Alias /IMSecurity "C:/Program Files/Trend Micro/IM Security/web/"`
	
	`<Directory "C:/Program Files/Trend Micro/IM Security/web/">`
	`Options None`
	`AllowOverride None`
	`Order allow,deny`
	`Allow from all`
	`</Directory>`
	
	`# IM Security Virtual Path -- End`
	`# IM Security Virtual Path -- Start`
	
	`ScriptAlias /IMSecurity/cgi-bin/ "C:/Program Files/Trend Micro/IM Security/web/cgi-bin/"`
	`<Directory "C:/Program Files/Trend Micro/IM Security/web/cgi-bin">`
	`AllowOverride None`
	`Options None`
	`Order allow,deny`
	`Allow from all`
	`</Directory>`
	
	FIGURE 4-5. Apache changes

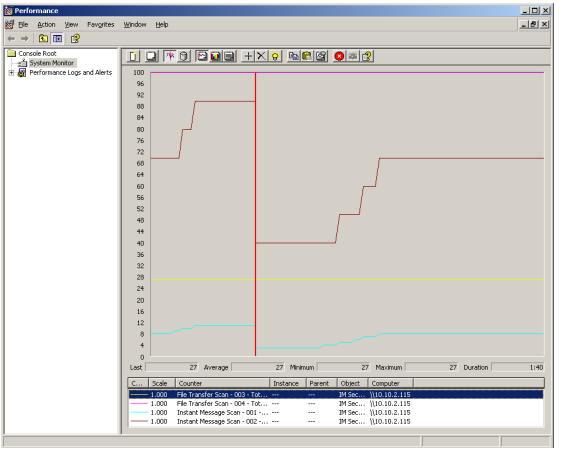
Performance Counter objects	Setup adds Performance Counter objects, which you can then select to view IM Security performance.  Performance File Action View Favorites Window Help Console Root System Monitor Performance Logs and Alerts 100 96 92 88 84 80 76 72 68 64 60 56 52 48 44 40 36 32 28 24 20 16 12 8 4 0 Last 27 Average 27 Minimum 27 Maximum 27 Duration 1:40 Color Scale Counter Instance Parent Object Computer 1.000 File Transfer Scan - 003 - Tot... --- --- IM Sec... \\10.10.2.115 1.000 File Transfer Scan - 004 - Tot... --- --- IM Sec... \\10.10.2.115 1.000 Instant Message Scan - 001 -... --- --- IM Sec... \\10.10.2.115 1.000 Instant Message Scan - 002 -... --- --- IM Sec... \\10.10.2.115 **FIGURE 4-6. Sample Performance Counter view**

TABLE 4-1. System changes after installing IM Security

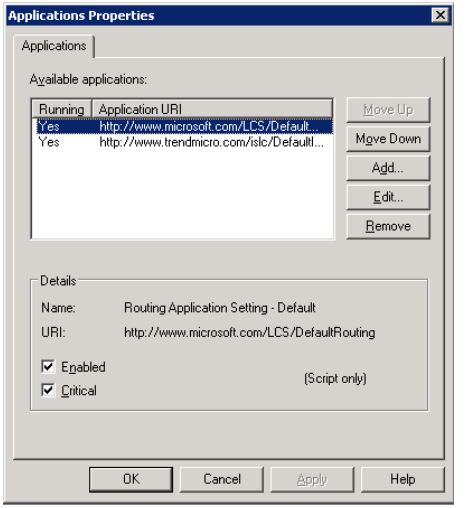
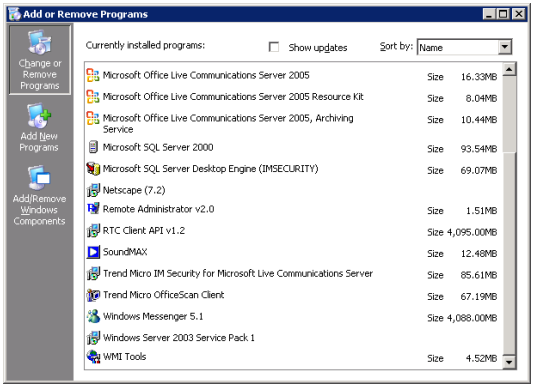
COMPONENT	DETAILS
LCS Properties update	Setup updates the LCS > **Applications** > **Properties** and adds an IM Security-related entry.  **FIGURE 4-7. LCS changes**
Add/Remove Programs items	Setup creates three Add/Remove Programs items: **Trend Micro IM Security for Microsoft Live Communications Server**, **RTC Client API v1.2**, and **Microsoft SQL Server Desktop Engine (IMSECURITY)**. 

TABLE 4-1. System changes after installing IM Security

Services

Setup adds the following services:

SERVICE	DESCRIPTION
Trend Micro IM Security Server	The core IM Security service. **Trend Micro IM Security Server** depends on Windows Management Instrumentation (WMI), MSSQL$IMSECURITY, and **Trend Micro IM Security System Attendant** services. It is responsible for core IM Security processes (management console access, saving configuration, and invoking the scan, update, report, and notification processes).
Trend Micro IM Security System Attendant	Monitors the service status of Live Communications Server and IM Security Server services. The service depends on the WMI and MSSQL$IMSECURITY services.
MSSQL$IMSECURITY	IM Security SQL server instance. `<root>:\Program Files\IMSecurityDBEngineMSSQL$IMSECURITY\Binn\sqlservr.exe –sIMSECURITY` controls this service.
SQLAgent$IMSECURITY	The IM Security SQL agent is used to perform scheduled and maintenance tasks. `<root>:\Program Files\IMSecurityDBEngineMSSQL$IMSECURITY\Binn\sqlagent.EXE -i IMSECURITY` controls this service.

TABLE 4-2. IM Security services

Tip: Use the Windows **Services** Panel to check for the status of IM Security services.

Processes

Setup adds the following processes:

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

TABLE 4-3. IM Security processes

Tip: Use Windows **Task Manager** to check whether these processes are running.

Program Folders

Setup adds the following program folders (if the default Setup settings are kept):

FOLDER NAME	DESCRIPTION
`c:\Program Files\Trend Micro\IM Security`	IM Security program files/folder path.
`c:\Program Files\Trend Micro\IM Security\Database`	IM Security database file and transaction log folder path.
`c:\Program Files\Microsoft SQL Server\MSSQL$IMSECURITY`	The IM Security Microsoft Database Engine (MSDE) 2000 program path.

TABLE 4-4. IM Security program folders

Preparing Other Antivirus Applications

If you are running Trend Micro ServerProtect or other antivirus product on the IM Security server, exclude the IM Security Quarantine, Backup and Temp directories from scanning. Otherwise, a scanning conflict will occur.

If you are using ServerProtect, refer to the ServerProtect documentation for instructions to exclude IM Security folders from scanning.

Verifying a Successful Installation

Trend Micro recommends using the European Institute for Computer Antivirus Research (EICAR) test script as a safe way to confirm that IM Security virus scanning is running and working properly.

WARNING! *Depending on how you have configured your IM Security servers, you might need to disable antivirus products for the duration of the EICAR test (otherwise, the virus might be detected before it arrives at the IM Security server). This leaves your servers vulnerable to infection. For this reason, Trend Micro recommends that you only use the EICAR test in a test environment or pilot deployment (see page 2-5).*

Alternatively, go to `http://www.trendmicro.com/en/security/test/overview.htm` and download a copy of the industry standard EICAR test script to your hard drive. The EICAR file is a text file with a `*.com` extension. It is inert. It is not a virus, it does not replicate, and it does not contain a payload. Never use real viruses to test your antivirus installation.

To test IM Security with EICAR:

1. If necessary, disable antivirus products that might detect the EICAR test file before it arrives at your LCS server.
2. Open an ASCII text file and copy the following 68-character string to it.
   `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 it.

4. Start Windows Messenger and send `eicar_test.com` to one of your contacts (preferably to another network administrator or IT personnel).
5. Access the management console and query virus scan logs.

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

Alternatively, check the IM notification sent to the `eicar_test.com` recipient and to your account.

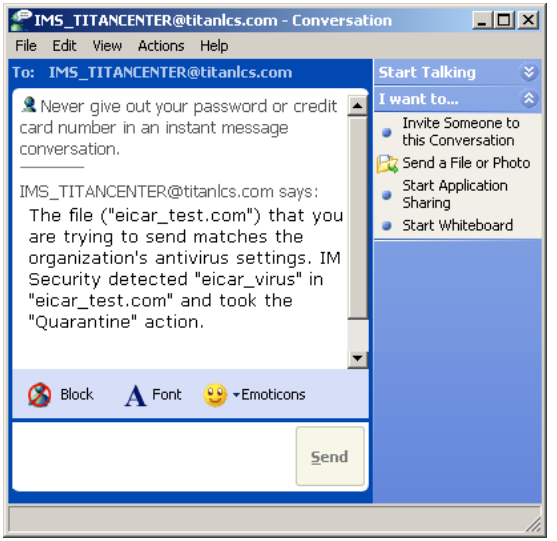


FIGURE 4-8. Sample IM-based notifications sent by the IM Security notification account

Note: Virus scanning enables IM-based notifications to sender and recipient by default. See *page 4-13* for details about IM Security default settings.

IM Security opens a new **Conversation** window when sending notifications coming from the IM Security notification account. In the sample notification above (*Figure 4-8*), `IMS_TITANCENTER` is the notification account (see *page 3-19*).

Accessing the IM Security Management Console

Use one of the following methods to access the management console:

- Locally on the IM Security server (see *page 4-10*)
- Remotely via HTTPS or HTTP (see *page 4-11*)

Tip: During installation, decide whether to enable the SSL protocol to enable HTTPS transmission.

Accessing the Management Console Locally

If you have local access to the IM Security server, configure IM Security settings by opening the management console locally.

To access the management console locally from the IM Security server:

1. Click **Start** > **All Programs** > **Trend Micro IM Security for Microsoft Live Communications Server** > **IM Security Management Console**. A browser opens and displays the **Logon** page.

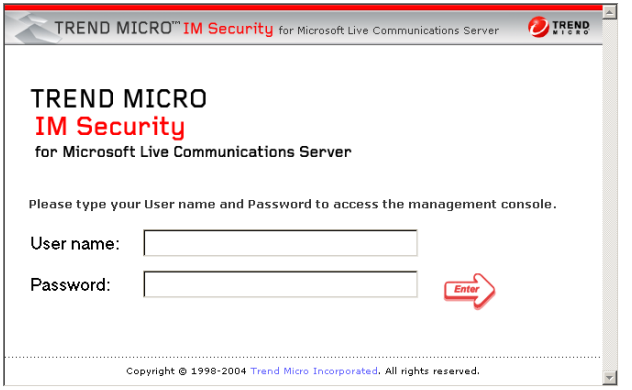


FIGURE 4-9. Management console Logon page

Tip: Ensure that you are using a compatible browser. Otherwise, the management console page will not be accessible. See *page 2-6* for browser requirements or *page 5-4* for troubleshooting management console access issues.

2. Type the **user name** and **password** in the field provided.

> **Tip:** The user name and password correspond to the **Administrator Account** you set up during IM Security installation (see *page 3-18*).

3. Click  .

The **Summary** page displays.

You can only access one instance of the management console from one computer.

Accessing the Management Console Remotely

Setup enables secure sockets layer (SSL) management console connection when the **Enable SSL** option is selected during installation. This allows IM Security to encrypt the configuration data as it passes from the IM Security management console to the IM Security server. Alter the management console URL to use the HTTPS protocol through port 443.

To access the management console remotely:

1. Type one of the following addresses in your browser's **Address** field to open the Log on page:
   - `https://<host name>:<port>/IMSecurity`

     Where:
     - `<host name>` is the IM Security server's fully qualified domain name (FQDN), IP address, or server name
     - `<port>` is the port to be used during an HTTPS session (for example, `443`)

     When accessing a secured IM Security site, it automatically sends its certificate, and Internet Explorer displays a lock icon () on the status bar.
   - `http://<host name>/IMSecurity`

     Where `<host name>` is the IM Security server's fully qualified domain name (FQDN), IP address, or server name. If the HTTP port is modified to another value other than the default port number (80), including the port number in the URL is necessary.

   See *Table 4-5* for differences between HTTPS and HTTP access.

2. Type the IM Security administrator account's **user name** and **password** in the fields provided.
3. Click 

.

The management console index page, **Summary**, displays.

The following table lists the differences between HTTPS and HTTP access:

CAPABILITIES	HTTPS	HTTP
Secure transmission	✔	✘
Plain text transmission	✘	✔
Viewable registered servers (**Server Management**)	✔	✔

TABLE 4-5. Differences between HTTPS and HTTP access

Checking Default Settings

Table 4-6 enumerates the default settings implemented in a successful IM Security installation.

PAGE	DEFAULT VALUE
Virus Scanning	**Enable virus scanning**: Enabled **Target**: All scannable files **Action**: ActiveAction **Notification**: Sender and Recipient (IM only)
File Blocking	**Enable file blocking**: Disabled **Default rules**: Disabled
File Transfer Scan > Content Filtering	**Enable content filtering**: Disabled **Default rules**: Disabled
Instant Message Scan > Content Filtering	**Enable content filtering**: Disabled **Enable trust scan**: Disabled **Default rules**: Disabled
Manual Update	**Components**: All components selected
Scheduled Update	**Enable scheduled update**: Enabled **Components selected**: Default and additional threat patterns **Schedule**: Daily at 2:30AM
Update Source	**Source**: Trend Micro's ActiveUpdate Server
Alerts	**IM Security conditions enabled**: Services started unsuccessfully Services stopped Component update is unsuccessful **Live Communications Server conditions enabled**: Services stopped **Recipients**: Write to Windows Event log
One-time and Scheduled Reports	Empty
Log Maintenance	**Manual**: All logs, Delete logs older than 30 days **Scheduled**: Enabled (same setting as manual)

TABLE 4-6. IM Security default settings

PAGE	DEFAULT VALUE

Folders	**Quarantine Folder (Virus Scanning)**:
	`<Installation path>\quarantine\`
	
	Backup Folder (Virus Scanning):
	`<Installation path>\backup\`
	
	Archive Folder (File Blocking):
	`<Installation path>\archive\`
	
	Archive Folder (File Transfer Content Filtering):
	`<Installation path>\archive\`

Debug Logs	Disabled

TABLE 4-6. IM Security default settings

WARNING! *Clicking **Reset** from any of the management console pages instructs IM Security to restore the default settings for a specific 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.*

Updating Components

Complete the following task before updating IM Security components:

- Configure proxy server settings (optional)

  Depending on how you configured your **Proxy Server** during installation, you may skip this step.

- Set the update source (optional)

  Use the default update source–ActiveUpdate.

- Update components manually

Tip: Set scheduled update to ensure automatic component updates. This help ensure the currency of your antivirus and unwanted content protection.

Configuring Proxy Server Settings

If your system uses a proxy server to access the Internet, use the **Proxy Settings** page to set proxy server settings for the following IM Security features:

- ActiveUpdate or other Update Source
- Product Registration
- World Virus Tracking

To configure the proxy server settings:

1. Access the management console (see *page 4-10*).
2. Click **Administration** > **Proxy** on the navigation menu.
3. On the **Proxy** page, select **Use a proxy server for component download and product activation**.
4. Under **Proxy Server**, configure the following:
   - Type the **server name** or **IP address** of the proxy server and its **port number**
   - Click **Use SOCKS5** if SOCKS5 protocol is used
5. Under **Proxy Authentication**, type the **user name** and **password** used to access the proxy server.
6. Click **Save** to apply settings.

Ensure the correctness of the proxy server settings. Otherwise, component update or product registration might not work.

Setting the Update Source

Set the update source to define the location where IM Security downloads the latest antivirus and content security component. The source specified in the **Update Source** page applies to both manual and scheduled updates.

Here are some common scenarios why the update source needs to be changed:

- Downloading a special build of the pattern file or scan engine from a different source
- During product troubleshooting (that is, when being instructed to do so by a technical support engineer)
- Using an alternative update server on your intranet to avoid multiple connections to the Internet

To set the update source:

1. Access the management console (see *page 4-10*).
2. Click **Updates** > **Source** on the navigation menu. The **Update Source** page appears.

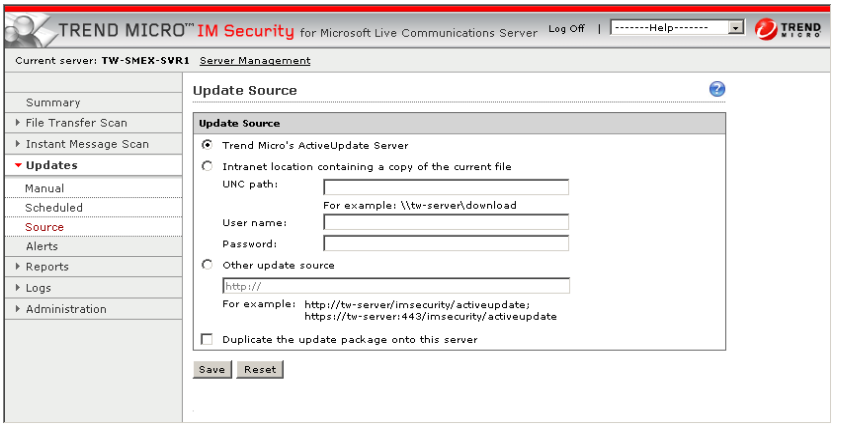


FIGURE 4-10. Update Source page

3. If necessary, select the location from which IM Security receives updates. The default location is the **Trend Micro ActiveUpdate server**.

Tip: To ensure the latest component version, retain the default setting.

4. If the IM Security server corresponding to this instance of the management console is the update source for other IM Security servers, select **Duplicate the update package onto this server**. This option instructs IM Security to download the update package (pattern file and scan engine) to the IM Security server. You can then set the current server as the update source for other servers.
5. Click **Save** to apply settings.

When you invoke a manual or scheduled update, IM Security will download the component from the set source.

Updating Components Manually

To help ensure up-to-date protection, update the default scanning pattern, spyware/grayware pattern, and scan engine immediately after installing IM Security or during virus outbreaks.

To update components manually:

1. Access the management console (see *page 4-10*).
2. Click **Updates** > **Manual** on the navigation menu. The **Manual Update** page appears.

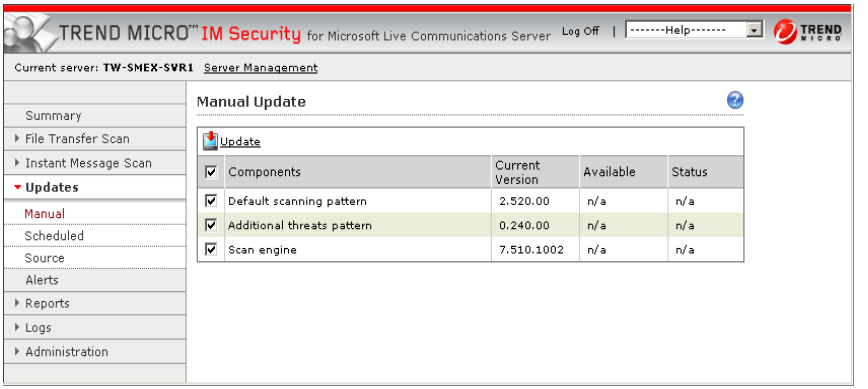


FIGURE 4-11. Manual Update page

3. Select the antivirus and content security components that IM Security will download.

Tip: Trend Micro recommends checking for the latest version of the default scanning pattern, spyware/grayware pattern, and scan engine components.

4. Click **Update** to invoke manual update.

Clicking **Update** instructs IM Security to read the **Manual Update** page settings, check for, and download the latest components from the update source.

Chapter 5

Troubleshooting and FAQ

This chapter describes how to troubleshoot issues that may arise with IM Security.

The topics discussed in this chapter include:

Installation

One of the following issues may occur during IM Security:

- Setup stops responding
- Setup reports a successful installation, but IM Security services are not started
- Setup stops because the minimum system requirements are not met

To troubleshoot IM Security installation issues:

1. Check the Setup debug log (`c:\IMSecurity_Install.log`) for possible error messages.

   Note: Trend Micro Technical Support providers use the debug log to understand installation issues.

2. Verify and ensure that a user with **Domain Admins** privileges is logged on to the server where IM Security should be installed.

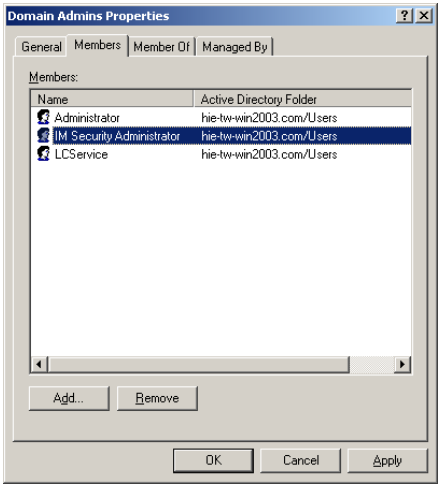


FIGURE 5-1. Use an account with *Domain Admin* privileges when installing IM Security

3. Revisit and ensure that none of the conditions described under *Deployment Considerations* has been violated.
4. Verify whether the system requirements have been met (see *page 2-6*).

If the above steps do not work, contact your Trend Micro support provider (see *page 6-2*).

Product Registration and Activation

One of the following issues may occur that leads to unsuccessful registration and/or activation:

- Product registration is successful, however, no Activation Code (AC) was received from Trend Micro
- Unable to activate IM Security during installation or through the management console

To troubleshoot product activation issues:

1. Register IM Security to obtain an AC (see *page 3-2*).

   Note: Do not use the Registration Key (RK) when activating IM Security. Otherwise, product activation will not work. A Registration Key is used to register a product to the **Trend Micro Online Registration** (`http://olr.trendmicro.com`). Alternatively, an Activation Code is used to activate a product's features during or right after installation.

2. Verify the AC used. Be sure to use the following format when specifying the AC:

   `XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

3. If there are messages or logs related to product activation, check for the possible solutions offered by the logs or messages.

   Tip: Refer to the *Online Help* > *View Summaries, Logs, and Reports* section for instructions to query logs.

4. Ensure the number of LCS clients does not exceed the number of seats for which the license is valid. Otherwise, product activation will not work.

   Tip: The **Product License** > **Seat status** field displays the number of seats available and used. Refer to the *Online Help* > *Administer Servers* section for instructions to view product license information.

If the above steps do not work, contact your Trend Micro support provider (see *page 6-2*).

Management Console Access Issues

One of the following issues may occur when trying to access the IM Security management console:

- Inaccessible management console
- Missing **User name and Password** field
- Unrecognized **User name** and **Password**

To troubleshoot management console access issues:

1. Ensure the latest Microsoft or Sun Java Virtual Machine (JVM) is installed on the IM Security server (see *page 2-6*). Otherwise, the **User name and Password** field will not appear on the management console.

Note: IM Security supports Microsoft JVM and Sun JVM version 1.4.1_02. For more information about Microsoft JVM, please visit `http://www.microsoft.com/mscorp/java/`.

FIGURE 5-2. Missing User name and Password field– install the latest Microsoft or Sun JVM

2. Use the Windows **Services** panel to verify whether **Trend Micro IM Security Host Service** is started.

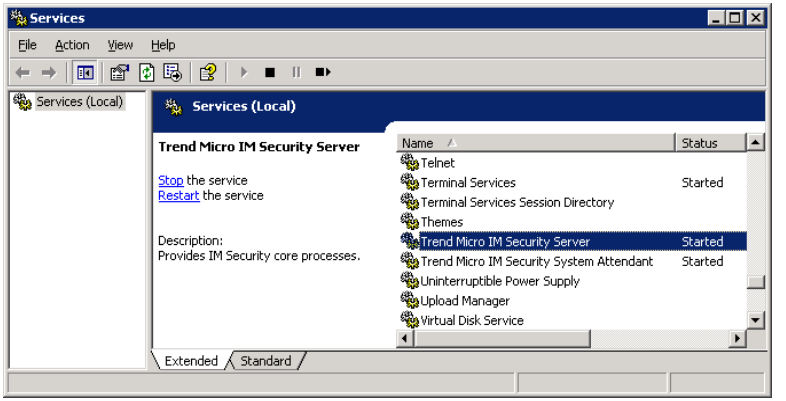


FIGURE 5-3. Inaccessible management console– ensure IM Security Host Service is started

3. Verify the Web service (IIS or Apache) is started.
4. Verify whether the IM Security administrator account has not been changed. Otherwise, obtain the latest user name and password of the administrator account.
5. Check the network connection, and verify the ports needed by the management console are accessible (see *page 2-7*).
6. Check whether the following settings are true:
   - Both IM Security and Microsoft SharePoint™ Portal Server are installed on the same server
   - The IM Security management console belongs to the Microsoft Internet Information Services (IIS) Default Web site

   If all of the above conditions are true, the management console will be inaccessible. SharePoint prevents access to other Web sites by default. To exclude the IM Security Web site, add **IMSecurity** in the **Excluded path** of Sharepoint Central Administration **virtual server settings**. Refer to the *Online Help > Troubleshooting* section for detailed instructions.

If the above steps do not work, contact your Trend Micro support provider (see *page 6-2*).

Component Update Issues

If you configured the update source to download antivirus and content security components from **Trend Micro ActiveUpdate**, and the latest components cannot be downloaded, check the connection from the IM Security server to the ActiveUpdate server.

To troubleshoot ActiveUpdate issues:

1. Check whether the IM Security server is connected to your network.

   In addition, verify your network connection and server status.

2. Run the following commands to make sure the IM Security server can resolve the ActiveUpdate server's FQDN (see *Figure 5-4*).

   `nslookup`

   `ping`

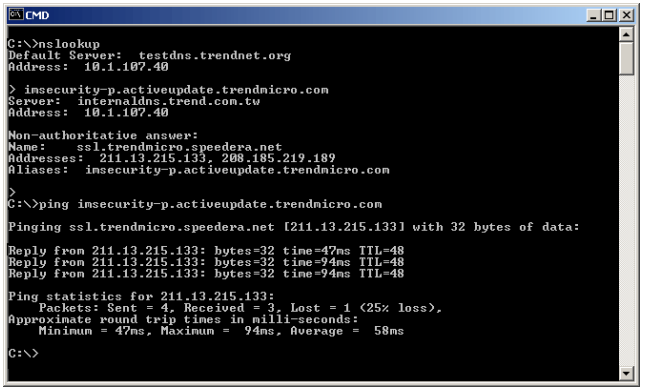


FIGURE 5-4. Use *ping* and *nslookup* to test connection between IM Security and ActiveUpdate servers

3. Use `telnet` to connect to the ActiveUpdate server at port 80 to make sure the IM Security server can connect via HTTP.

If the above steps do not work, contact your Trend Micro support provider (see *page 6-2*).

Frequently Asked Questions

This section answers the following common questions about IM Security:

General Product Knowledge

- What is IM Security?
- How does IM Security protect my LCS server?
- Can IM Security scan files or filter messages transmitted using non-LCS IM chats via MSN/Windows Messenger?
- Can IM Security filter content of all file types?
- What are the instant messaging applications that IM Security supports?
- What are the instant messaging clients that IM Security supports?

Installation, Registration, and Activation

- Can I specify another agent notification account sometime after the IM Security installation?
- Where can I get a Registration Key or Activation Code?

Please refer to the *IM Security Online Help* > *Frequently Asked Questions* topic for more answers to management related questions.

What is IM Security?

Trend Micro™ IM Security is an application that provides antivirus and content security protection to Microsoft Live Communications Server environments.

How does IM Security protect my LCS server?

IM Security provides real-time virus, spyware, and other grayware scanning, file blocking, and content filtering. Refer to the *Online Help* > *Protect IM Environments* section for details.

Can IM Security scan files or filter messages transmitted via non-LCS IM chats via MSN/Windows Messenger?

IM Security can only scan files or filter messages transmitted via Microsoft Live Communications Server.

Can IM Security filter content of all file types?

No. IM Security is able to filter content of Microsoft Office files (`*.ppt`, `*.doc`, `*.xls`) and Adobe portable document formats (`*.pdf`).

What are the instant messaging applications that IM Security supports?

As of this release, IM Security protects servers where Microsoft Live Communications Server is installed.

What are the instant messaging clients that IM Security supports?

IM Security supports the following messaging clients:

- Windows Messenger 5.0
- Windows Messenger 5.1

Where can I get a Registration Key or Activation Code?

Refer to the Trend Micro Web site (`http://kb.trendmicro.com/solutions/search/main/search/solutionDetail.asp?solutionId=16326`) for details.

Can I specify another agent notification account sometime after the IM Security installation?

IM Security only allows a single agent notification account. You may specify a new account by using the Agent Account Tool.

Chapter 6

Getting Support

Trend Micro is committed to providing service and support that exceeds our user's expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter includes the following topics:

Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try and find a solution to your questions:

- **Check your documentation**: the *Troubleshooting and FAQ* section of this *Getting Started Guide* and *Online Help* provide comprehensive information about IM Security

  Search both documents to see if they contain your solution.

- **Visit our Technical Support Web site**: our Technical Support Web site contains the latest information about all Trend Micro products

  The support Web site has answers to previous user inquiries. To search the Knowledge Base, visit

  `http://kb.trendmicro.com`

In addition to phone support, Trend Micro provides the following resources:

- Email support

  `support@trendmicro.com`

- Readme: late-breaking product news, installation instructions, known issues, and version specific information
- Product updates and patches

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

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

`http://www.trendmicro.com/en/about/contact/overview.htm`

To speed up the issue resolution, when you contact our staff please provide as much of the following information as you can:

- IM Security Activation Code
- Version
- Exact text of the error message, if any
- Steps to reproduce the problem

Sending Infected File Samples

You can send viruses, infected files, Trojan programs, spyware, and other grayware to Trend Micro. More specifically, if you have a file that you think is some kind of threat but the scan engine is not detecting it or cleaning it, you can submit the suspicious file to Trend Micro using the following Web address:
`subwiz.trendmicro.com`

Please include in the message text a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any viruses it may contain.

Reporting False Positives

Report false positive detections to `false@support.trendmicro.com`.

Trend Micro Technical Support replies to your message within twenty-four (24) hours.

Introducing TrendLabs

Trend Micro TrendLabs^{SM} is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

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

For more information about TrendLabs, please visit:

`www.trendmicro.com/en/security/trendlabs/overview.htm`

Other Useful Resources

Trend Micro offers a host of services through its Web site, `www.trendmicro.com`.

Internet-based tools and services include:

- Virus Map: monitors virus incidents around the world
- HouseCall™: Trend Micro online virus scanner
- Virus risk assessment: the Trend Micro online virus protection assessment program for corporate networks

Glossary

Tip: For faster glossary search when viewing this appendix online, use the Acrobat Reader's **Find** option to search for a term.

A B **C** D **E** **F** **G** **H** I

J K **L** **M** **N** **O** **P** Q **R**

S **T** **U** **V** **W** X Y Z

A

Top

Alerts
Refer to messages that include IM Security service, update status, or Live Communications Server events. Use the Alerts page to configure alerts.

B

Top

Blocking rules
See file blocking rules.

C

Top

Content filtering rules
In IM Security, content filtering rules refer to rules that instruct IM Security how to filter messages and files for unwanted content.

E

Top

Events
Refer to IM Security or Live Communications Server actions that trigger or instruct IM Security to send alerts or notifications.

F

Top

False positives
Occurs when a valid Web site, URL, message, or file is incorrectly determined by software to be of an unwanted type.

File blocking rules
Short for file transfer blocking rules. File blocking rules are rules that instruct IM Security to block unwanted or infected files from being transferred from one contact to another.

File content filtering rules
Short for file transfer content filtering rules. File content filtering rules are rules that instruct IM Security to apply the set action for files with unwanted content.

L

Top

LHA
Compressed file archive created by LHA/LHARC (lha255b.exe).

Logs
A time-sequential record of IM Security events.

N

Top

NMS
In the SNMP management architecture, one or more computers on the network acts as a network management station (NMS) and polls the managed devices to gather information about their performance and status.

Notifications
Refer to messages generated by IM Security about virus scanning, file blocking, and content filtering events.

P

Top

Pattern file
Pattern file is a Trend Micro component that provides rules and signatures to detect viruses, spyware, and other grayware. IM Security uses the scan engine, virus pattern, and spyware/grayware pattern to detect known viruses, spyware, and other grayware.

R

Top

Reports
A collection of logs about virus and content security events that occur in an IM Security network. Generate reports to consolidate logs in an organized and graphically appealing format.

S

Top

Scan engine
The antivirus component that identifies viruses, spyware, and other grayware present in files transferred in a Live Communications Server environment.

SNMP
Simple Network Management Protocol (SNMP) is a set of communication specifications for managing network devices, such as bridges, routers, and hubs over a TCP/IP network.

SOCKS5
The SOCKS5 protocol, also known as authenticated firewall traversal (AFT), is an open Internet standard (rfc1928) for network proxies at the transport layer.

T

Top

Traps
Notifications sent by managed devices to the NMS when certain events occur, such as a shutdown or authentication error.

W

Top

Windows event log
The **Alerts** > **Recipients** screen allows you to enable Windows event logging. When enabled, view logs through the Windows **Event Viewer** screen.

Worms
A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems, often via email.

Appendix B

IM Security Deployment Checklists

Use the following checklists to record relevant system information:

- *Installation Checklist* on page B-2
- *Ports Checklist* on page B-3
- *Pre-installation Tasks Checklist* on page B-4

They will be needed from time to time.

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: AC:	
IP address	10.1.104.255	
Administrator account	IMS_admin	
Agent notification account	IMS_notification	
WEB SERVER INFORMATION		
IP address	10.1.104.225	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Uses SOCKS5	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
Management Console and Update/Deploy components	80	
File transfer	6891-6900	
SMTP	25	
SNMP	162	
Server Management population	3268	

Pre-installation Tasks Checklist

Before installing IM Security, complete the following tasks:

COMPLETED?	PRE-INSTALLATION TASKS
☐	If a firewall exists between an LCS server and its clients, open the ports described in *Table 2-2* to ensure IM Security connectivity.
☐	Log on to the target server using an account with **Domain Admins** privilege.
☐	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 (see page 3-2).

Index

T

U

V

W