TREND MICRO™

IM Security for Microsoft™ Office Communications Server[1]

Instant Protection for Instant Messaging

Administrator's Guide

Messaging Security

Document Part No. TIEM13638/80520

Release Date: September 2008

Patents Pending

The Trend Micro IM Security user documentation contains product feature information and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Preface

Chapter 1: Introducing Trend Micro™ IM Security

Chapter 2: Getting Started with Trend Micro™ IM Security

Chapter 3: Managing Trend Micro™ IM Security

Chapter 5: Troubleshooting and FAQ

Chapter 6: Getting Support

Appendix A: Performance Counters

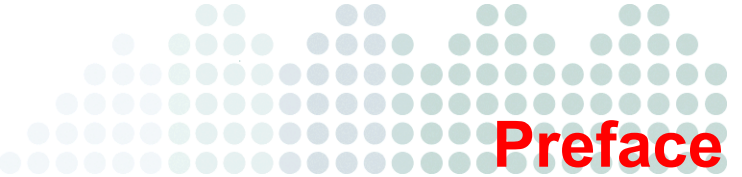
Appendix B: IM Security and TMCM Logs and Actions Comparison

Glossary

Index

List of Figures

List of Tables



Preface

Welcome to the *Trend Micro™ IM Security 1.5 Administrator's Guide*. This guide contains information about product settings and service levels.

This preface discusses the following topics:

Trend Micro™ IM Security Documentation

The Trend Micro IM Security documentation consists of the following:

Online Help—Helps you configure all features through the user interface. You can access the online help by opening the product console and then clicking the help icon ().

Installation and Deployment Guide—Helps you plan for deployment and configure all product settings.

Administrator's Guide—Provides instructions, troubleshooting, and best practices for configuring the product post installation.

Quick Tour—Provides a brief product introduction and highlights useful product features.

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.

The Installation and Deployment Guide, Administrator's Guide, Quick Tour, and readme are available at:

http://www.trendmicro.com/download

Audience

The IM Security documentation is written for IT managers and administrators in medium and large enterprises. The documentation assumes a basic knowledge of networking concepts and security systems, including:

- Antivirus and content security protection
- Network concepts such as IP address and LAN settings
- Network devices and their administration
- Network configuration such as the use of VLAN and SNMP
- Office Communications Server deployment and topologies
- Office 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 IM Security tasks**
Italics	*References to other documentation*
`Monospace`	`Examples, sample command lines, program code, Web URL, file name, and program output`
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Introducing Trend Micro™ IM Security

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

The topics discussed in this chapter 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™ Office Communications Server (OCS) 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 new antispyware work together to stop malware before any damage. Plus, flexible content filtering ensures appropriate IM use and prevents data theft.

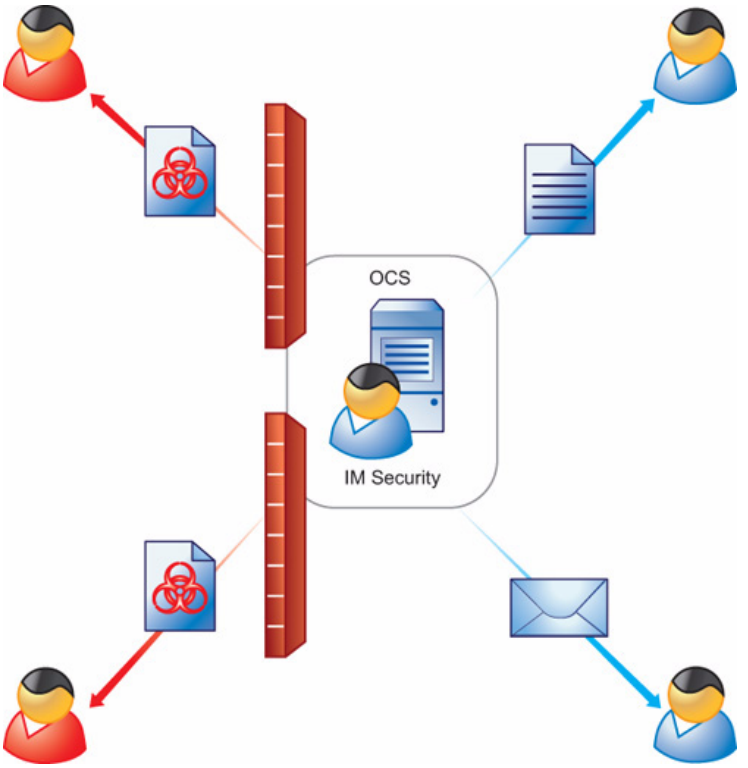


FIGURE 1-1 IM Security deployment

IM Security incorporates virus/malware and spyware/grayware scanning, content filtering, URL filtering, and file blocking into one cohesive solution. Refer to the succeeding sections for product features and capabilities.

What's New

Microsoft™ Office Communications Server 2007 support

IM Security 1.5 supports file transfer and instant message scanning for Microsoft OCS 2007 Standard or Enterprise editions.

Note: IM Security 1.5 can only be installed on a front-end server.

Disclaimer support

IM Security 1.5 supports the insertion of a configurable disclaimer statement into the chat window when a chat session is initiated. The disclaimer statement prompts individuals to acknowledge that their chat sessions are being monitored for corporate security needs.

Web Threat Protection

IM Security 1.5 can detect and block Web-based security risks by validating URLs that users send in chat sessions.

IntelliTrap

IM Security incorporates IntelliTrap technology. Use IntelliTrap to scan for packing algorithms to detect packed files. Enabling IntelliTrap allows IM Security to take administrator-defined actions on infected files or attachments and to send notifications to senders, recipients, or administrators.

Trend Micro Control Manager MCP agent integration

This version of IM Security supports the following Control Manager versions:

- Control Manager 3.5 (Build 1234) + Patch 4 (Build 1504)
- Control Manager 5.0 (Build 1467) + Hotfix 1602 (Build 1602)

The communication between IM Security and Control Manager uses a new protocol called the Trend Micro Control Manager Management Communication Protocol (MCP). IM Security no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of IM Security and Control Manager. The Control Manager Agent can be registered during the IM Security installation. IM Security supports single sign-on from Control Manager. Access the IM Security product console directly from the Control Manager product console without typing a separate user name and password for the IM Security product console.

Configuration Migration tool

IM Security 1.5 includes a configuration migration tool to help migrate IM Security 1.0 settings to IM Security 1.5 when upgrading from Live Communications Server (LCS) to OCS 2007.

Features and Benefits

IM Security provides the following features and benefits:

Simple Installation

IM Security provides a wizard-type Setup program, `Setup.exe`, that allows administrators to easily install the product on a single server with OCS 2007 Standard or Enterprise Edition.

Centralized Product Management

A Web-based product console allows administrators to configure IM Security anytime and from anywhere on the network.

File Transfer Scanning

IM Security protects OCS 2007 and instant messaging (Office Communicator) users from viruses/malware, spyware/grayware, and other security risks associated with file transfers.

Instant Message Scanning

IM Security protects OCS 2007 and instant messaging (Office Communicator) users by checking for unwanted content and malicious URLs in instant messages.

Configurable Disclaimer Statements

Supports configurable disclaimer statements for instant messaging sessions.

Alerts and Notifications

Set alerts to notify administrators or selected IT personnel whenever specific IM Security or OCS related events 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 OCS users with:

- **Virus scan**—Scans for viruses/malware, spyware/grayware, packers, and other security risks.
- **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 Threat Protection (URL filtering)**—Protects against malicious Web sites.

Table 1-1presents the order in which IM Security applies file and instant messaging protections.

TABLE 1-1. IM Security order of protection precedence

ORDER	FILE-BASED PROTECTION	IM-BASED PROTECTION
1	File Blocking	Content Filtering
2	Content Filtering	Web Threat Protection (URL Filtering)
3	Virus/Malware Scanning	

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

The following section explains how IM Security file and IM-based protection works.

Virus Scan

When enabled, file transfer scanning continually protects your instant messaging 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 in 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 contacts of the virus/malware 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 Scan*
- *Protect IM Environment(s)*

File Blocking

When enabled, 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 contacts of a file blocking event 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 Scan*
- *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 1-4 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 contacts of the content filter rule violation 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*
- *Protect IM Environment(s)*

Web Threat Protection

When enabled, Web Threat Protection protects your instant messaging environment by validating the authenticity of URLs that users send during messaging sessions.

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 threat protection action.

   IM Security takes the action that the administrator specified in the Web Threat Protection Actions screen.

3. Sends notifications to the administrator or contacts.

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

Note: The Web Threat Protection feature requires an active Internet connection.

Refer to the *Online Help* for details about and instructions for configuring Web Threat Protection.

Reports and Logs

To provide current information about the security of your instant messaging evironment, IM Security is pre-configured to generate reports based on virus scan, file blocking, content filtering (file transfers and instant messages), URL filtering (Web Threat Protection), 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 OCS 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, filtering violations, and URL blocking actions. Notifications can be sent to administrators and other OCS users.

Trend Micro Technology in IM Security

This section explains IM Security technology and how it protects your OCS and instant messaging environments.

Program Components

To ensure up-to-date protection against the latest security risks, perform a manual update or set a scheduled update for the following components:

- **Pattern files**—These files are the Virus pattern, Spyware pattern, IntelliTrap pattern, and IntelliTrap exception pattern. These files contain the binary "signatures" or patterns of known security risks. When used in conjunction with the scan engine, IM Security is able to detect known risks as they pass through OCS. New pattern files are typically released at the rate of several per week.
- **Scan engine**—This is the component that analyzes each file's binary patterns and compares them against the binary information in the pattern files. If there is a match, the file is determined to be malicious.
- **URL Filtering Engine**—IM Security utilizes the Trend Micro URL Filtering Engine to perform URL categorization and reputation rating based on the data supplied by the Trend Micro Web Threat Protection feature. Trend Micro recommends setting a weekly update to ensure that your installation has the most current URL Filtering Engine.

ActiveUpdate

ActiveUpdate is a service common to many Trend Micro products. ActiveUpdate connects to the Trend Micro Internet update server to enable downloads of pattern files, the scan engine, and the URL filtering engine.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. Updates are available on a regularly scheduled interval that you configure, or on-demand. The ActiveUpdate feature can be utilized by accessing the **Updates > Source** screen.

Virus Pattern

The Trend Micro scan engine uses an external data file, called the virus pattern file, to keep current with the latest viruses/malware and other Internet risks such as Trojans, mass mailers, worms, and mixed attacks. New virus pattern files are created and released several times a week, and any time a particularly malicious risk is discovered.

All Trend Micro antivirus programs using the ActiveUpdate feature can detect whenever a new virus pattern is available at the server, and/or can be scheduled to automatically poll the server every hour, day, week, and so on to get the latest file.

How Scanning Works

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Because each virus contains a unique binary "signature" or string of tell-tale characters that distinguishes it from any other code, the virus experts at TrendLabs capture inert snippets of this code to include in the pattern file. The engine then compares certain parts of each scanned file to the data in the virus pattern file looking for a match.

Pattern files use the following naming format:

```
lpt$vpn.###
```

where ### represents the pattern version (for example, 400). To distinguish a given pattern file with the same pattern version and a different build number, and to accommodate pattern versions greater than 999, the IM Security product console displays the following format:

roll number.pattern version.build number (format: xxxxx.###.xx)

- roll number—this represents the number of rounds when the pattern version exceeded 999 and could be up to five digits.
- pattern version—this is the same as the pattern extension of lpt$vpn.### and contains three digits.
- build number—this represents the patch or special release number and contains two digits.

If multiple pattern files exist in the same directory, only the one with the highest number is used. Trend Micro publishes new pattern files on a regular basis (typically several times per week), and recommends configuring a daily automatic update on the **Updates > Scheduled** screen. Updates are available to all Trend Micro customers with valid maintenance contracts.

Note: There is no need to delete the old pattern file or take any special steps to "install" the new one.

Incremental Updates of the Virus Pattern File

ActiveUpdate supports incremental updates of the virus pattern file. Rather than download the entire 7 or 8MB pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software and deploy pattern files throughout your environment.

Spyware Pattern

As new hidden programs (grayware) that secretly collect confidential information are written, released into the public, and discovered, Trend Micro collects their telltale signatures and incorporates the information into the spyware pattern file.

The spyware pattern file, is stored in the following:

```
engine\vsapi\primary\ssaptn.###
```

where ### represents the pattern version. This format distinguishes a given pattern file with the same pattern version and a different build number. It also accommodates pattern versions greater than 999. The IM Security console displays the following format:

```
roll number.pattern version.build number (format: xxxxx.###.xx)
```

- roll number—this represents the number of rounds when the pattern version exceeded 999 and could be up to five digits.

- pattern version—this is the same as the pattern extension of tmaptn.### and contains three digits.
- build number—this represents the patch or special release number and contains two digits.

About Spyware and Grayware

In addition to computer viruses, the IM Security pattern files include signatures for many other potential risks. These additional risks are not viruses since they do not replicate and spread. However, they can perform unwanted or unexpected actions, such as collecting and transmitting personal information without the user's explicit knowledge, displaying pop-up windows, or changing the browser's home page.

IM Security can be optionally configured to scan for the following additional risks:

- **Spyware**—Software that secretly collects and transmits information without the user's explicit knowledge or consent.
- **Dialers**—Software that secretly dials a telephone number, typically an international or pay-per call number, through the user's modem.
- **Hacking tools**—Software that can be used for malicious hacking purposes.
- **Password cracking applications**—Software designed to defeat computer passwords and other authentication schemes.
- **Adware**—Software that monitors and collects information about a user's browsing activities to display targeted advertisements in the user's browser or through pop-up windows.
- **Joke programs**—Programs that mock computer users or generate some other sort of humorous display.
- **Remote access tools**—Programs designed to allow access to a computer, often without the user's consent.
- **Others**—Files that do not fit into the other additional risks classifications. Some of these may be tools or commercial software that have legitimate purposes, in addition to having the potential for malicious actions.

The Additional Threats Scanning feature can be accessed from the **File Transfer Scan > Virus Scan** screen.

Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. Originally developed in response to the first computer viruses the world had seen, the scan engine today is exceptionally sophisticated. It is capable of detecting Internet worms, mass-mailers, Trojan horse risks, network exploits and other risks, as well as viruses. The scan engine detects the following types of risks:

- "in the wild," or actively circulating
- "in the zoo," or controlled viruses that are not in circulation, but are developed and used for research and "proof of concept"

In addition to having perhaps the longest history in the industry, the Trend Micro scan engine has also proven in test after test to be one of the fastest—whether checking a single file, scanning 100,000 files on a desktop machine, or scanning email traffic at the Internet gateway. Rather than scan every byte of every file, the engine and pattern files work together to identify not only tell-tale characteristics of virus code, but the precise location within a file where viruses would hide. If a virus is detected, it can be removed and the integrity of the file restored.

The scan engine includes an automatic clean-up routine for old pattern files (to help manage disk space), as well as incremental pattern updates (to help minimize bandwidth).

In addition, the scan engine is able to decrypt all major encryption formats (including MIME and BinHex). It also recognizes and scans common compression formats, including Zip, Arj, and Cab. Most Trend Micro products also allow administrators to determine how many layers of compression to scan (up to a maximum of 20), for compressed files contained within a compressed file.

It is important that the scan engine remain current with the latest risks. Trend Micro ensures this in two ways:

- Frequent updates to the scan engine's data-file, called the default scanning file, which can be downloaded and read by the engine without the need for any changes to the engine code itself
- Technological upgrades in the engine software prompted by a change in the nature of virus risks, such as the rise in mixed risks like SQL Slammer

In both cases, updates can be automatically scheduled, or an update can be initiated on-demand.

The Trend Micro scan engine is certified annually by international computer security organizations, including the International Computer Security Association (ICSA).

About Scan Engine Updates

By storing the most time-sensitive virus information in pattern files, Trend Micro is able to minimize the number of scan engine updates while at the same time keeping protection up-to-date. Nevertheless, Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- New scanning and detection technologies have been incorporated into the software
- A new, potentially harmful virus is discovered that cannot be handled by the current engine
- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:
`http://www.trendmicro.com`

Component Version Information

To know which pattern file, scan engine, URL filtering engine or program build you are running, click **Summary** in the main menu. The version in use is shown in the **Current Version** column in the **Update** section of the **Scan Summary**.

About IntelliScan

Most antivirus solutions today offer you two options in determining which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file name extensions (considered the most vulnerable to infection) are scanned. But recent developments involving files being "disguised" through having their extensions changed has made this latter option less effective. IntelliScan is a Trend Micro technology that identifies a file's "true file type," regardless of the file name extension.

Note: IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus infection.

True File Type

When set to scan true file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named "family.gif," it does not assume the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that has been deceptively named to avoid detection.

True file type scanning works in conjunction with Trend Micro IntelliScan, to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher risk.

For example, .gif and .jpg files make up a large volume of all Web traffic, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. However, this does not mean that they are entirely safe. It is possible for a malicious hacker to give a harmful file a "safe" file name to smuggle it past the scan engine and onto the network. The file could not run until it was renamed, but IntelliScan would not stop the code from entering the network.

Note: For the highest level of security, Trend Micro recommends scanning all files.

The IntelliScan scanning feature can be accessed from the **File Transfer Scan > Virus Scan** screen.

Protection Strategy

An organization must design a strategy that provides optimal protection for its instant messaging environment. Consider the following when selecting an IM Security protection strategy:

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

Trend Micro recommends the following strategies for optimal protection for an OCS 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
- Configure scheduled component updates

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

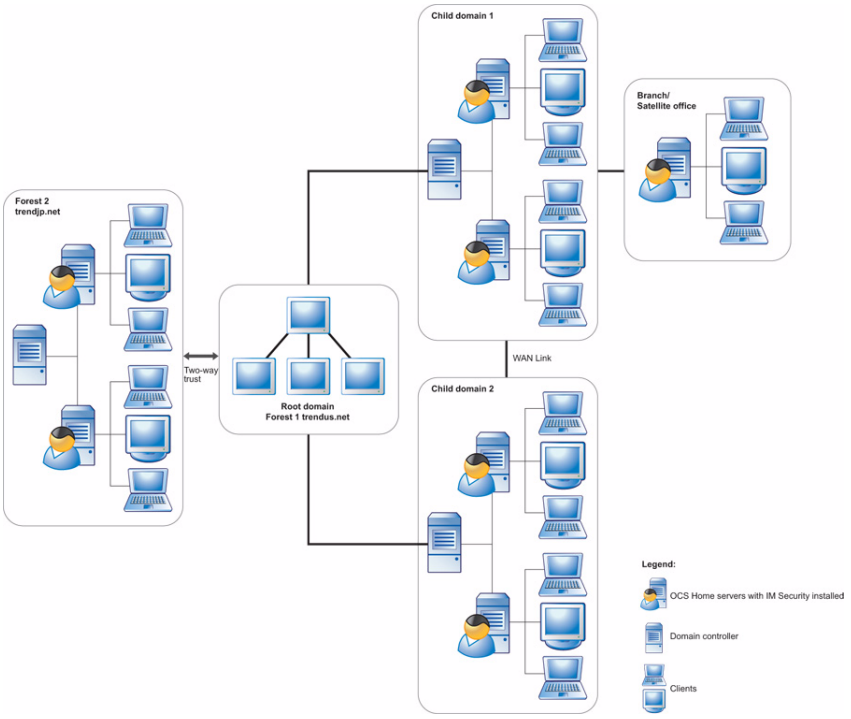


FIGURE 1-5 A sample protected OCS environment

Chapter 2

Getting Started with Trend Micro™ IM Security

This chapter explains the IM Security product console and provides basic configuration information to get you up and running securely.

The topics discussed in this chapter include:

The Product Console

The IM Security product console is a Web-based console viewable using the Microsoft Internet Information Server (IIS) or Apache Web server. The product console allows administration of IM Security servers from any machine using a compatible Web browser.

During installation, Setup allows you to enable Secured Sockets Layer (SSL). Enable SSL to help ensure secure management between your Web browser and the IM Security server.

IM Security is compatible with the following Web browsers:

- Internet Explorer 6.0 SP1 or 7.0
- Mozilla Firefox 2.0 (or newer) with the latest Sun Java Virtual Machine (JVM)

Accessing the Product Console

There are two options for accessing the product console. You can access it locally from the IM Security server or remotely by using a computer with Internet access and an IM Security compatible browser.

Accessing the Product Console Locally

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

1. Click **Start** > **Programs** > **Trend Micro IM Security** > **IM Security Product Console**.
2. Type the user name and password in the fields provided.
3. Click **Log On**.

Accessing the Product Console Remotely

Setup enables a secure sockets layer (SSL) product 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 product console to the IM Security server. If Microsoft IIS Web server is selected during installation, IM Security supports HTTP or HTTPS. However, if Apache Web server is used during installation, IM Security only supports HTTP.

To access the product console using HTTPS:

- Type the URL for encrypted communication (HTTPS) in the following format:
  `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 used during an HTTPS session. If port 443 (default HTTPS port) is used, including the port number in the URL is not necessary.

  IMSecurity is the IM Security Web site name.

Note: If Apache HTTP Server is the Web server configured to host IM Security, ensure that you are using the exact virtual directory name when remotely accessing the product console. Otherwise, a missing page error appears.

When accessing a secure IM Security site, it automatically sends its certificate, and Internet Explorer displays a lock icon on the status bar.

To access the console remotely using HTTP:

1. Type the following in your browser's address field to open the log on screen:
   `http://{host name}/IMSecurity`

   Where:

   {host name} is the IM Security server's fully qualified domain name (FQDN), IP address, or server name. If HTTP port number is not the default value (80), you must include the port number in the URL.
2. Type the user name and password in the fields provided.
3. Click **Log On**.

The Summary Screen

The **Summary** screen allows you to view the following information:

Scan summary for today—Displays the scan types and statistics such as the number of security risks and unwanted content detected today.

Component Summary—Displays the components' current and available version and whether updates were successful.

The Component Summary table provides the following information:

- **Component**—Component name
- **Current Version**—Version number of the components available on the local IM Security server
- **Available**—Version number of the components available in the Update Source
- **Status**—Update status (successful or unsuccessful) and the time the update process was invoked.

In addition, the IM Security Summary screen allows you to perform the following tasks:

- View the product license information by clicking the **more info** link.
- Manually refresh the Summary screen by clicking the **Refresh** button.
- Manually update the selected components by clicking the **Update** button.

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

Configuring the Proxy Server

Most enterprises use proxy servers for added security and more efficient use of bandwidth. If your system uses a proxy server and you didn't configure it during the installation process, configure the proxy settings to ensure that the IM Security server can connect to the Internet and download components, perform product activation and registration, and participate in the World Virus Tracking program.

To configure the proxy server settings:

1. Click **Administration** > **Proxy** on the navigation menu.
2. Select **Use a proxy server for update and product license notification**.
3. Under Proxy Server, type the server name or IP address of the proxy server and the port used.
4. Select **Use SOCKS5** if SOCKS5 protocol is used.
5. Under **Proxy server authentication**, type the user name and password used to access the proxy server.

6. Click **Save** to apply settings.

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

Component Updates

To ensure that your instant messaging environment stays protected from the latest viruses/malware, spyware/grayware, and other potential security risks, regularly update your IM Security antivirus and content security components. Configure the IM Security server to download the latest program and component updates from the Trend Micro ActiveUpdate server. After the server downloads any available updates, it then applies and uses the latest components.

IM Security Updatable Components

IM Security uses the following components to keep your instant messaging environment protected:

- **Virus pattern—**Collection of telltale signatures used to detect viruses and malware
- **Spyware pattern**—Collection of telltale signatures used to detect spyware and other types of grayware
- **Virus scan engine**—Component used to perform multi-threaded real-time scanning
- **IntelliTrap pattern**—Component for detecting real-time compression files packed as executable files
- **IntelliTrap exception pattern**—Component containing a list of "approved" compression files
- **URL filtering engine**—The engine that facilitates communication between IM Security and the Trend Micro URL Filtering Service. The URL Filtering rates URLs and provides the rating information to IM Security

Update Methods

The IM Security product console **Update** menu provides these methods for updating your server:

- **Manual update**—Allows you to update components on-demand
- **Scheduled update**—Allows you to invoke manual downloads to implement scheduled downloads to automatically obtain update components

Update Sources

The IM Security product console **Updates** > **Source** tab allows you to select one of the following items as the source of the latest antivirus and content security components:

TABLE 2-1. Update sources and descriptions

ITEM	DESCRIPTION
Trend Micro ActiveUpdate server	This method allows you to download the latest components from the Trend Micro ActiveUpdate server. Select ActiveUpdate as a source for frequent and timely updates. The default Update Source is the Trend Micro ActiveUpdate server.
UNC path	This method allows you to download the latest components from an Intranet source that receives updated components. Type the Universal Naming Convention (UNC) path of another server on your network. For example, `\\fileserver\updates`. Setting one or more centralized source locations can greatly reduce network traffic and speed update time.

TABLE 2-1. Update sources and descriptions

ITEM	DESCRIPTION
Other update source	This method allows you to download components from the Internet or other source. For example, you may choose to receive updates from a special server during testing. More common scenarios might be if you need to download a special build of the virus pattern file upon instructions from support, or you replicate an ActiveUpdate server on your intranet to prevent multiple Trend Micro products from downloading.

Specify an Update Source

Use the Update Source screen to define the location where IM Security downloads the latest antivirus and content security components. The source specified in the screen applies to both manual and scheduled update screens.

To set the update source:

1. Select the location from which IM Security receives updates. The default location is the Trend Micro ActiveUpdate server.

   Tip: To ensure the latest component versions, set the ActiveUpdate server as the update source.

2. If the current server 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) onto the IM Security server `<root>:\Program Files\Trend Micro\IM Security\web\ActiveUpdate` folder.
3. Click **Save** to apply settings or **Reset** to restore the default settings.

Manually Update Components

Use the Manual Update screen to instruct IM Security to check for and download the latest component available from the update source. In addition, use this screen to view

the Component Summary table. The Component Summary table provides the component version that is present in the local IM Security server and available from the update source, and the status of the last update process. The Summary screen provides the identical Component Summary, and a direct link for manual update.

To update components manually:

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

   Tip: Trend Micro recommends checking for the latest version of all product components.

2. If necessary, set the **Update Source**.
3. Click the **Update** icon to invoke the manual update.

Clicking **Update** instructs IM Security to read the Manual Update screen settings, check for, and then download the latest components from the update source. IM Security will retry to connect to the update source three times if the connection request times out (exceeds 10 seconds). The update status can also be viewed from the **Summary** screen.

Schedule Component Updates

Configure IM Security to regularly check the update server and automatically download available components.

Note: During times of virus outbreaks, Trend Micro may update virus pattern files more than once a week. The scan engine is updated regularly, but less frequently than once a week. Trend Micro recommends updating daily (or even more frequently in times of virus outbreaks).

To set a schedule for component updates:

1. Click **Updates** > **Scheduled** on the navigation menu.
2. On the **Schedule** tab, set the **Start time** for the **hourly**, **daily**, or **weekly** frequency schedule by selecting the hour and minute. Each time the update occurs, the download begins at the specified **Start time** and follows the frequency schedule (for example, starting at 8:00PM every 2 days).

3. Click the **Components** tab to select the components that IM Security will download during each scheduled update.

Tip: Refer to the column **Available** to determine the availability of latest components.

4. If necessary, set the **Update Source**.
5. Click **Save** to apply settings or **Reset** to restore the default settings.

When scheduled update is enabled, IM Security checks for and downloads the latest components based on the Scheduled Update settings. IM Security will retry to connect to the update source three times if the connection request times out (exceeds 10 seconds). The update status can also be viewed from the Summary screen.

Product Registration and Activation

Register and activate IM Security to keep your antivirus and content security components current. IM Security has two types of Activation Code:

- **Evaluation**—Allows you to implement IM Security's full functionality for a limited evaluation period
- **Full**—Allows you to implement IM Security's full functionality

You must first register your product before you can activate it. Use your Registration Key, which is included in the IM Security package, to register your product on the Trend Micro Online Registration Web site. After registering your product, you are eligible to receive the latest security updates and other product maintenance services. After completing the registration, Trend Micro sends an email that includes an Activation Code, which you can then use to activate IM Security.

Obtaining the Product Activation Code

To activate your product, register online using the supplied Registration Key (RK) to obtain an Activation Code (AC), and then specify the AC on the Setup > Product Activation screen or product console > **Administration** > **Product License** screen.

- If you have purchased the full 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 a limited number of days, after which IM Security tasks will continue to load, but no virus scanning, message filtering, nor component update will occur.

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

The following table defines how IM Security behaves depending on the Activation Code activation and expiration.

TABLE 2-2. Product version behaviors

ACTION	FULL VERSION		EVALUATION VERSION	
	ACTIVATED	NOT ACTIVATED / EXPIRED	ACTIVATED	NOT ACTIVATED/ EXPIRED
File/IM scanning and filtering	Yes	Yes	Yes	No
Web Threat Protection	Yes	Yes	Yes	No
Disclaimer statements	Yes	Yes	Yes	No
ActiveUpdate	Yes	No	Yes	No
Product console access	Yes	Yes	Yes	Yes

Virus Scan for File Transfers

The Virus Scan feature is capable of providing real-time detection of viruses/malware, spyware/grayware, real-time compressed executable files (Packer viruses), and files containing malicious macro code. With the exception of macro scan, IM Security utilizes pattern files to detect threats. Macro scan supplements regular virus scans and employs heuristic scanning to detect macro viruses and other security risks.

When enabled, Virus Scan for file transfer scanning continually protects your instant messaging and Office Communications Server environments from security risks that might be present in incoming and outgoing files.

Specifying File Types to Scan

IM Security can scan all files that pass through it, or just a subset of those files as determined by true file type checking (IntelliScan) or the file extension. In addition, individual files contained within a compressed file can also be scanned.

Note: IM Security will not scan encrypted or password protected files.

To specify files to scan:

1. From the IM Security product console menu, select **File Transfer Scan > Virus Scan** and select the **Target** tab.
2. Select **Enable virus scan for file transfers**. Clear the check box to disable the feature.
3. Under Default Scanning, select from one of the following:
   - **All scannable files**—Scans all file types, regardless of file name extension. IM Security opens compressed files and scans all files within. This is the most secure, and recommended, configuration.
   - **IntelliScan**—Uses true file type identification to scan file types that are known to harbor viruses by checking the file's true-file type. Since checking the true file type is independent of the filename's extension, it prevents a potentially harmful file from having its extension changed to obscure its true file type.
   - **Specified file types**—You can explicitly configure the types of files to scan or skip based on their extensions. However, this configuration is not recommended, because the file extension is not a reliable means of determining its content. To scan only selected file types, click the **Show details** link to the right of the **Specified file types** option. The default list of extensions displays all file types that are known to potentially harbor viruses. This list is updated with each pattern file release. Select the file types that you want IM Security to scan. To specify additional file extensions, select **Specified file extensions**. Type a new file extension in the extension field and click **Add**.

Note: Type the extension to scan or exclude from scanning (typically three characters), without the period character. Do not precede an extension with a wildcard (*) character, and separate multiple entries with a semicolon.

4. Click **Save**.

Enabling IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of virus/malware entering your network by blocking files with real-time compressed executable files, or packer files.

To enable IntelliTrap, go to **File Transfer Scan > Virus Scan** and under the **IntelliTrap** section, select **Enable IntelliTrap**.

Specifying Additional Security Risks for Scans

IM Security Additional Security Risk Scanning provides protection from spyware and malware. The Additional Security Risk Scanning feature can be accessed from the Virus Scan screen (**File Transfer Scan > Virus Scan**).

To specify additional security risk scanning:

1. Under **Additional Security Risk Scanning**, select **Select all** to scan for all types of security risks listed or specify security risks that you want IM Security to scan for.
2. Click **Save** to keep new settings.

Configuring Compressed File Scan Restrictions

Setting compressed file scan restrictions criteria can enhance scanning performance and protect against Denial of Service attacks. IM Security opens and examines the contents of compressed files according to the criteria specified in the Compressed File Scan Restrictions section of the Virus Scan screen (**File Transfer Scan > Virus Scan**). IM Security decompresses the files according to the configurable limits (number of files in the compressed archive, size of the compressed file, number of compressed layers and the compression ratio).

To configure compressed file scan restrictions:

1. Under **Compressed File Scan Restrictions**, select from the following options:
   - **Decompressed file count exceeds**—Type a number in the field provided to set a limit for the number of decompressed files that IM Security will open and

scan. When IM Security encounters a file containing files whose number is equal to or greater than the limit, it will not scan the file.

- **Size of decompressed file exceeds**—Type a number in the field provided to set a limit for the Size of decompressed file exceeds. When IM Security encounters a compressed file that is equal to or greater than this size, it will not scan the file.
- **Number of layers of compression exceeds**—Type a number to set a limit for the Number of layers of compression exceeds field. When IM Security encounters a file of a compression layer equal to or greater than this number it will not scan the file.
- **Size of decompressed file is "x" times the size of compressed file**—Type a number to set a limit for the Size of decompressed file is "x" times the size of compressed file for which IM Security will scan. When IM Security encounters a file of a decompressed ratio equal to or greater than this number, it will not scan the file.

2. Click **Save** to keep new settings.

Specifying an Action for Security Risks in File Transfers

When IM Security detects a file that matches your scan configuration, it executes an action to protect your environment.

To specify an action:

1. Specify the scan action settings:
   - **ActiveAction**—If ActiveAction is selected, IM Security first attempts to clean the file. However, if IM Security is unable to perform the clean action, it performs a secondary action. If you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of security risk, Trend Micro recommends using ActiveAction.
   - **Customized action for detected threats**—Select this option if you are familiar with the different scan actions and if you know what action is suitable for different types of security risks. From this section, you can specify that one action be taken for all detected risks, or you can specify different actions for the different types of security risks.
   - **Back up infected files before action is taken**—In some instances a file may become unusable after the clean action is applied. If you are concerned that

important information may be made inaccessible after the clean action is taken, select this option.

- **Do not clean infected compressed files to optimize performance**—Select this option preserve resources on the OCS server.

2. Click **Save**.

Specifying Filter Settings and Actions for Macro Viruses

Advanced macro scanning analyzes Microsoft Office documents for evidence of macro code. If the advanced macro scan detects macro code in an Office document, criteria from the specified filtering level is applied to the code to determine if it is malicious. If the code is determined to be malicious, IM Security will take action on the file as specified in the Scan Action section of the Virus Scan screen. To specify filter settings and actions for Macros, go to **File Transfer Scan > Virus Scan > Action tab > Advanced Options**.

To specify filter settings and actions for Macros:

1. Select **Enable advanced macro scan**.
2. Specify a filtering level:
   - **1 - Lenient filtering**—Only very suspicious instances of macro code will be categorized as malicious. As a result, detections and false positives will be fewer.
   - **2 - Default filtering**—Trend Micro recommended filtering level. Optimized for the greatest degree of protection while minimizing false positives.
   - **3 - Sensitive filtering**—Provides a greater degree of protection against malicious macro code than the default level, but also increases the number of false positive detections.
   - **4 - Rigorous filtering**—Provides the greatest degree of protection against macro viruses. Most macro code, even small instances, will be categorized as malicious. As a result, detections and false positives will be greater than if a lesser filtering level is selected.
3. Select **Delete all macros detected by advanced macro scan**

   All macro code will be deleted even if a different action was specified in the Scan Actions section.
4. Click **Save**.

Specifying Actions for Unscannable Files

Unscannable files are files that are encrypted, password protected, or files that exceed specified scanning restrictions. If a user transfers an encrypted or password protected file and you specified **All Scannable files** from the **File Transfer Scan > Virus Scan > Target** tab, IM Security will not scan the file. Similarly if a user transfers a file that exceeds any of the limits specified in the **Compressed File Scan Restrictions** section of the **File Transfer Scan > Virus Scan > Target** tab, IM Security will not scan it. By default, IM Security delivers unscannable files. You can specify that IM Security cancel the file transfer if the file being transferred is unscannable. Specify an action for unscannable files from the **File Transfer Scan > Virus Scan > Action** tab.

Sending Notifications for Security Risk Detections

You can configure IM Security to send a notification when it takes action against detected security risks during Virus Scan, File Blocking, or Content Filtering. You can send notifications by email, instant messages, and SNMP. You can also automatically record Notifications in the Windows Event Log.

Notifications serve a number of purposes as follows:

- Warn the original recipients that their message was altered.
- Notify an administrator or other network security professional of a security risk.
- Display information to the recipient about security risks and the actions taken.

IM Security can send notifications to administrators, senders, and recipients. The notification feature can be configured from the **File Transfer Scan > Virus Scan > Notification** tab.

File Blocking for File Transfers

Using File Blocking rules, you can prevent the exchange of files between users based on specific file properties such as file name, extension, file size, or true file type. You can configure IM Security so that it applies rules to specific users or groups.

Note: Because the process for adding a rule varies only slightly from editing a rule, the details of both adding and editing a rule are displayed together.

To create a new File Blocking rule or edit an existing rule:

1. From the **File Blocking** screen, click the **Add** icon, or click the name of an existing rule.
2. **Contact**—Specify the user, users, group, or groups affected by the rule.
   - **Anyone**—This option applies the rule to all IM traffic (internal and external) passing through the Office Communications Server. User(s) or group(s) specified in the Exceptions list will not be affected by this rule.
   - **Specific user(s)/member(s) of a group**—Click to specify user(s) or group members affected by this rule.
     - **Search for users or group**—Type a name or part of a name and click **Search**.
     - **Type an address or domain**—Type an email address or domain and click **Add**.
   - **Session between user(s)/group(s)**—Click to specify user(s) or group members to whom this rule will apply.
     - **Search for users or group**—Type a name or part of a name and click **Search**.
     - **Type an address or domain**—Type an SIP address or domain and click **Add**.
3. **Block files based on**—Specify file properties
   - **Type**—IM Security will check file transfers for file types (extensions) that you specify in this section. This option uses true file type scanning to determine the actual file type.
   - **Name**—Select to have IM Security check for file names and file extensions that you specify. Specify extensions that do not appear in the Type section.
   - **File size**—Select to have IM Security check for files that exceed size limits that you specify.
4. **Delivery Option**—Specify an action for IM Security to take when it detects a file that violates the file blocking rule.
5. **Archive Option**—Specify whether IM Security will archive the file that violates the file blocking rule.
6. **Notification**—Specify whom to notify, the notification method, and the notification message.

7. **Log**—Specify whether IM Security should write the event to the Windows event log.
8. **Name**—Specify a new descriptive name for the rule to create a new rule.

IM Security displays and implements the file blocking rules in a linear fashion starting from the Default rule up to the last rule according to the Priority.

Content Filtering for File Transfers and Instant Messages

Content filtering when enabled and configured properly can prevent the delivery of messages and files that contain sexually explicit, racially offensive, or slanderous comments from one employee to another. Content filtering can also prevent sensitive corporate data from leaving a company's network.

Note: Because the process of adding a Content filtering rule for file transfers and instant messages varies only slightly from editing a rule, the details of both adding and editing a rule for file transfers and instant messages are displayed together.

To create a new content filtering rule or edit an existing rule:

1. From the **Content Filtering** screen, click the **Add** icon, or click on the name of an existing rule.
2. **Contact**—Specify the user, users, group, or groups affected by the rule.
   - **Anyone**—This option applies the rule to all IM traffic (internal and external) passing through the Office Communications Server. User(s) or group(s) specified in the Exceptions list will not be affected by this rule.
   - **Specific user(s)/member(s) of a group**—Click to specify user(s) or group members affected by this rule.
     - **Search for users or group**—Type a name or part of a name and click **Search**.
     - **Type an address or domain**—Type an SIP (IM) address or domain and click **Add**.
   - **Session between user(s)/group(s)**—Click to specify user(s) or group members to whom this rule will apply.

- **Search for users or group**—Type a name or part of a name and click **Search**.
- **Type an address or domain**—Type an SIP (IM) address or domain and click **Add**.

3. **Specify Keyword**—Add a keyword to the list of keywords that IM Security uses when checking for unwanted content in file transfers and instant messages.
   - **Filter message that match Any specified keywords**—Creates a rule that performs an action when IM Security detects any of the specified keywords in a file or instant message.
   - **Filter messages that match All specified keywords**—Creates a rule that performs an action when IM Security detects all of the specified keywords in a file or instant message.
   - **Enable case sensitive matching**—Instructs IM Security to disregard words that do not match the keyword's case when filtering content.
   - **Match synonyms**—Instructs IM Security to consider the synonyms of the keywords in the list.

   Note: By default, IM Security filters content using the keywords list and their synonyms. To edit the synonyms that IM Security will use, select the synonym to include or exclude by clicking the right or left facing arrow buttons.

4. **Delivery Option**—Specify an action for IM Security to take when it detects a file or instant message that violates the content filtering rule.
5. **Archive Option**—Specify whether IM Security will archive the file or instant message that violates the rule.
6. **Notification**—Specify whom to notify, the notification method, and the notification message.
7. **Log**—Specify whether IM Security should write the event to the Windows event log.
8. **Name**—Specify a new descriptive name for the rule to create a new rule.

Web Threat Protection for Instant Messages

Web Threat Protection, when enabled, validates the authenticity of URLs that users send in instant messages. Users can sometimes fall victim to elaborately designed Web sites that use social engineering techniques to elicit confidential information (corporate and personal). Social engineering may be used to induce users to visit Web sites that automatically download malicious code or programs. The malicious code or program, once launched, then runs unknown to the user, in the background. These malicious programs, depending on their design, capture keyboard inputs and give unauthorized users access to and control of the infected computer. Web Threat Protection proactively protects users and network environments by warning users and preventing them from visiting dangerous Web sites.

Enabling Web Threat Protection

To enable Web Threat Protection, go to **Instant Message Scan > Web Threat Protection** and select **Enable Web Threat Protection**.

Specifying Security Levels and Action

To control access to malicious URLs, administrators specify a security level and an action. The Security Level setting works in conjunction with settings specified in the Action tab to control access to Web sites that may contain malicious code or programs (Web threats). Trend Micro uses proprietary metrics to calculate a URL's reputation score. The reputation score indicates the degree of certainty that a URL is or contains a Web Threat. IM Security uses the URL's reputation score to assign a risk level to the URL. The four risk levels that IM Security uses are "Dangerous", "Very suspicious", "Suspicious", and "Safe".

The three security levels that administrators can use to determine the overall protection level against Web Threats are:

- **High**—Takes administrator defined action on all URL addresses that are currently un-assessed, or that IM Security determines are Dangerous, Very suspicious, or Suspicious.
- **Medium**—Takes administrator defined action on all URL addresses that IM Security determines are Dangerous, or that are Very suspicious.

- **Low**—Takes administrator defined action on all URL addresses that IM Security determines are Dangerous.

The Web Threat Protection Security Level and Action settings can be accessed from the Web Threat Protection screen (**Instant Message Scan** > **Web Threat Protection**).

To specify a security level and action for Web Threat Protection:

1. From the **Web Threat Protection** screen, Target tab, select from one of the following Security Levels:
   - **High**
   - **Medium**
   - **Low**
2. Click the **Action** tab, and select from one of the following actions:
   - **Cancel instant message**—Prevents message from being delivered to recipient
   - **Replace all**—Replaces the entire contents of the message with:
   - **Tag and deliver**—Inserts a note in front of the message:
   - **Deliver**—Delivers the message including the malicious URL
3. Select an **Archive Option**:
   - **Archive**—This is the default setting
   - **Do not archive**
4. Specify **Advanced Options**:
   - **Take action on URLs that have not been assessed by Trend Micro**—Select this if you want IM Security to take the same action for URLs that have not yet been classified
5. Click **Save**.

Specifying Notifications for Web Threat Protection

To define administrator, sender, and recipient notifications:

1. From the **Web Threat Protection** screen, click the **Notification** tab.
2. Under **Administrator Notification**, specify one or more options for sending notifications to the administrator:
   - **Email**—Select and then type the administrator's email address
   - **Instant Message**—Select and then type the administrator's IM address

- **SNMP**

3. Specify content for the subject line and body of the notification.
   - Type the message subject that IM Security applies to email notifications. For example: [IM Security] Content Filter Notification
   - Modify the default message content by selecting from the available message variable.
4. Specify **Sender Notification** details.
5. Specify **Recipient Notification** details.
6. Click **Save** to apply settings.

Chapter 3

Managing Trend Micro™ IM Security

This chapter describes IM Security's administrative features and functionality.

The topics discussed in this chapter include:

Managing Alerts and Notifications

Alerts and notifications provide you with information about specific IM Security events.

Alerts—refer to messages that include IM Security service, update status, or Office Communications Server events. Send alerts to network/server administrators and IT employees to inform them of system status, which are critical to network operations.

Notifications—refer to messages generated by IM Security about virus scan and content filtering events. Send notifications to administrators and Office Communications Server users to inform them of scan, blocking, and filtering results.

IM Security sends alerts and notifications through one of the following methods:

- **Instant Messaging (IM)**—IM Security sends alerts or notifications using Session Initiation Protocol (SIP). A correct SIP address uses the following format:

  `sip:<SIP Communications Service name>`

  Where sip: is the address prefix followed by the actual SIP Communications Service name. For example, `sip:user1@domain.com`.

- **Email**—IM Security sends alerts or notifications using Simple Mail Transfer Protocol (SMTP).

  This method allows IM Security to send messages to mailboxes belonging to the organization's email system or POP3 accounts.

  For example, `user1@hotmail.com`.

  Note: Ensure the Internet Mail Service or Connector is set on the mail server when configuring IM Security to send notification to a POP3 account.

- **SNMP**—IM Security sends alerts or notifications using Simple Network Management Protocol (SNMP).

  This method allows IM Security to send SNMP traps to management consoles that support SNMP. SNMP allows a limited number of transferable strings. The maximum characters that an SNMP trap can handle are up to 213. Characters exceeding the said limit will be truncated.

  For example, set the **SNMP IP** address to `123.123.1.1` and **Community name** to public.

Note: SNMP only applies to notifications for administrators and alerts to specific recipients. Other methods apply to administrators, recipients, and senders.

- **Windows event log**—IM Security records alerts and notifications to Windows event log. View logs via **Start** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Event Viewer** > **Application Log**.

Setting Alerts

From the Alerts screen you can select the conditions that will trigger IM Security to send alerts, specify alert recipients and the methods IM Security uses to send the alert. You can also specify the subject line of the alert and select the information to be contained in the body of the alert message.

To set alerts:

1. Click **Alerts** on the navigation menu.
2. On the **Alerts** screen, click the **Conditions** tab to select from the list of IM Security and Office Communications Server conditions that will trigger IM Security to send an alert.

   IM Security sends the alert notification if one of the selected conditions occur.
3. Click the **Recipients** tab to select the method that IM Security will use to send the alert and then specify the recipients.
4. Click the **Message** tab to define the alert message.

   Tip: Trend Micro recommends specifying a descriptive subject header that is equal to or less than 255 characters

   IM Security will apply the subject you specified to its email notifications. For example, `[Alert] IM Security abnormal event encountered`.
5. Click **Save** to apply settings or **Reset** to restore the default settings.

Setting Notifications

From the Notifications screen, you can configure IM Security to send notifications when it takes actions against various security risks. Usually, notifications are sent to the administrator, using a global default for the administrator's email address.

Configure notification settings to define the generic administrator notification accounts. These accounts, which usually belong to your OCS server administrators, will:

- Receive IM Security alerts or notifications
- Send email-based notifications to contacts who match a rule

To configure administrator notification settings:

1. Click **Administration > Notification Settings** on the navigation menu.
2. Under **Notification Settings (Receiving)**, type the IM, email, and SNMP accounts that will receive notifications.

Tip: Click **Apply to All** to instruct IM Security to use the same **SIP** and **email addresse**s globally (Virus Scan, File Blocking, Content Filtering, Web Threat Protection, and Alerts screens). IM Security removes the settings you set per screen and applies the new SIP and email addresses.

---

3. Under **Email Account Settings**, type the **Display name**, **SMTP server**, **SMTP port**, and **SMTP authentication** used by the SMTP server that will send email notifications to contacts who match a rule.

   IM Security uses its own account when sending email-based notifications. Set a descriptive display name along with an informative notification message to create awareness about the organization's security policy.
4. Click **Save** to apply settings or **Reset** to restore the default settings.

Managing Reports

An IM Security report refers to 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 (HTML or PDF). IM Security can send the reports using email to a specified address.

Generate a **One-time report** to obtain a quick overview of IM Security activities or create a **Scheduled report** to be regularly informed of IM Security activities. You can generate reports for any one of the following IM Security features:

TABLE 3-1. IM Security report contents

REPORT	DESCRIPTION
Virus Scan	Virus reports show detailed information about the numbers and types of viruses IM Security is detecting and the actions it is taking against them. It includes graphical features showing viruses detected versus time and proportions of the total viruses detected and uncleanable viruses.
File Blocking	File blocking reports show detailed information about the number of files IM Security is blocking. It shows the Top files blocked by type and extension name. It includes a graph showing files blocked versus time.
Content Filtering for files	Content filtering for files reports show information about the number of files IM Security is filtering. It shows the Top contacts of files that IM Security filtered out and shows how frequently your rules are filtering content. It includes a graph showing files filtered versus time.
Content Filtering for instant messages	Content filtering for instant message reports show information about the number of messages IM Security is filtering. It shows the Top contacts of messages that IM Security filtered out and shows how frequently your rules are filtering content. It includes a graph showing messages filtered versus time.

TABLE 3-1. IM Security report contents

REPORT	DESCRIPTION
Web Threat Protection	The Web threat protection for instant message report shows information about the number of URL addresses scanned and the number of malicious URL addresses detected. It also shows the top number of malicious URL addresses. The top number of malicious URL addresses is determined by the number of times IM security encounters a specific malicious URL. IM Security also provides the top URL senders.
Traffic	Traffic reports show the total number of instant messages and files delivered during a specific given period.

Generate a One-time Report

Configure IM Security to generate One-time reports to quickly obtain an overview of the latest IM Security processes and status. IM Security caches one-time reports and you can print, export, or email a report. Use the **Generate a report** screen to generate One-time reports.

To generate one-time reports:

1. On the **One-time Reports** screen, click the **Generate** button.
2. On the **One-time Reports** > **Generate** screen, type a name for the report.
3. Set the range by typing a date or clicking the calendar icon to select a date. IM Security follows the mm/dd/yyyy date and 24 hour time format.

Note: The maximum date range for one-time reports is one year.

4. Under **Content**, click the type of information that you want IM Security to gather for your report. Click the expand icon next to the report type to view detailed options for that report.
5. Under **Format**, select the output format of the report.

6. Under **Delivery**, click **Send to email** and then type the mailbox name that will receive the generated one-time report.
7. Click **Generate**.

IM Security gathers data to include in your report for the time range you specify and displays the report as soon as it is generated.

Create a Scheduled Report Template

Create scheduled report templates to define the content of reports, which IM Security uses to generate reports based on a schedule.

Use the **Scheduled Reports > Add** or **Edit Report Template** screen to create scheduled report templates.

To create a scheduled report template:

1. Click **Reports > Scheduled Reports** on the navigation menu.
2. On the **Scheduled Reports** screen, click **Add**.
3. On **Scheduled Reports > Add** or **Edit Report Template**, type a name for the report template.
4. Under **Schedule**, set the schedule that the template uses to generate individual reports:
   a. Set a schedule for when the template generates individual reports. It can generate reports on a **daily, weekly**, and **monthly** basis.
   b. Set the **Generate report at** time when the template generates the individual report.

      IM Security uses a 24-hour clock for all time settings.

      For example:

      If you set the schedule to be weekly every Sunday and set the time for report generation to be 02:00, then IM Security uses the template to generate an individual report every Sunday at 2:00AM.
5. Under **Content**, select the type of report that IM Security generates according to your schedule.
6. Under **Format**, select the output format of the report.

7. Under **Delivery**, click **Send to email** and then type the email address that will receive a report each time the template generates one.
8. Click **Save**.

The browser returns to the **Scheduled Reports** screen. The new template is added to the list of Report templates and begins generating reports. View the settings of the template by clicking the template name.

View Scheduled Reports

Configure IM Security to generate scheduled reports to obtain information about IM Security processes and status for a specific period. IM Security generates scheduled reports according to the schedule you set. Schedules are daily, weekly, or monthly. In addition, you can configure IM Security to deliver reports by email to an administrator or other recipient.

To view scheduled reports:

1. Click **Reports** > **Scheduled Reports** on the navigation menu.
2. On the **Scheduled Reports** screen, click the **List Reports** link.
3. Select from the list of generated reports, and then click **View**.

A new browser window opens that displays the contents of the scheduled report.

Delete Scheduled Report Templates

Perform scheduled report template deletion after confirming that the report is unused and expendable.

To delete scheduled report templates:

1. Click **Reports** > **Scheduled Reports** on the navigation menu.
2. Select the template name that you want to delete.
3. Click the **Delete** icon.

Review the contents of a scheduled report template before deleting it. IM Security permanently deletes the selected template. Reports based on the deleted template will no longer be generated.

Managing Logs

Logs are time-sequential records of IM Security events. These events refer to actions initiated by either a user or the IM Security server. IM Security allows you to query unformatted logs or display them through reports.

Logs are stored in the IM Security database. To avoid information loss, carefully review logs before deleting.

Tip: Saving logs means abundant available information about the IM Security server's performance. However, it also means more disk space usage. It is important to balance the need for information with the available system resources.

From the product console, you can query any of the following logs:

TABLE 3-2. IM Security logs

LOG TYPE	DESCRIPTION
Virus scan logs	Indicates the source of the infection or intrusion
File blocking logs	Enumerate blocked files with matching file blocking rules
Content filtering for files logs	Enumerate files with matching content filtering rules
Content filtering for IM logs	Enumerate messages with matching content filtering rules
Web threat protection for IM logs	Enumerate messages that contain web threats (malicious URL addresses)
Update logs	Indicate the types of update performed, including the result

Log Query

The Log Query screen allows you to setup, run, and view log queries. You can also export and print query results.

Query Logs

Set up and run a log query to immediately obtain information about virus/malware and content security events that occur in an IM Security network. The IM Security product console consolidates and lists logs in a descending order (with the latest log listed first).

Tip: More logs mean abundant available information about the IM Security system performance. However, it also means more occupied disk space. Balance the need for information with the available system resources.

To set up, run, and view log queries:

1. Click **Logs > Query** on the navigation menu.
2. Under **Criteria**, select the **date**.

   Select **All** or **Last 7 days** to query logs generated since IM Security has been installed or within the last 7 days. Alternatively, select **Range** and specify the date range by typing a date or clicking the calendar icon to select a date.
3. Select query type:
   - **Virus Scan**—Query information about the number of messages scanned and the viruses detected and cleaned
   - **File blocking—**Query information about the number of files scanned and blocked
   - **Content filtering for files—**Query information about the files IM Security filtered for undesirable content
   - **Content filtering for IM**—Query information about the instant messages IM Security filtered for undesirable content
   - **Web Threat Protection for IM**—Query information about the instant messages IM Security filtered for malicious URL addresses.
   - **Update**—Query information about component updates

     IM Security displays whether a component update was successful or unsuccessful (including the reason).
4. Specify whether you want to query information taken from **all** or **specific contacts** that violated the scanning and filtering rules.
5. Sort the logs into **ascending** or **descending** order.
6. Set the number of log queries to display per screen.

7. Click **Search**.

IM Security gathers data to include in your log query from the settings you specify. View the results on the lower portion of the **Log Query** screen.

Mouse-over the user name to determine the complete SIP address from log query results. IM Security will display the user's complete SIP address in exported logs and printed output.

Export and Print Query Results

IM Security provides options to export and print logs. These options allow you to review queried logs later.

To export queried logs:

1. Click **Logs > Query** on the navigation menu.
2. Query logs.
3. Click the **Export** icon to save the log query results in a CSV file format.
4. Use a spreadsheet application, such as Microsoft™ Office Excel, to open the `*.csv` file.

To print queried logs:

- Click the **Print** icon on the **Log Query** screen.

Note: A maximum total of 5,000 can be exported and printed.

Log Maintenance

From the **Log Maintenance** screen you can manually delete logs and set a schedule for automatic log deletion.

Delete Logs Manually

Configure manual log deletion to delete logs on-demand and free up additional disk space.

To delete logs manually:

1. Click **Logs > Maintenance** on the navigation menu.

2. Click the **Manual** tab to select the log **type** to delete.

   Select **All logs** or select **Specified logs** and then select the specific types of logs.

3. Under **Action**, type the **number of days** you want IM Security to retain logs.

   For example:

   If it is the tenth day and you type 3 days, then IM Security deletes all logs saved on the sixth day or before.

4. Click **Delete** Now.

IM Security deletes all logs older than the number of days you specified in step 3.

Note: If **Virus scan**, **File blocking**, **Content filtering for files**, **Content filtering for IM**, or **Web Threat Protection** log types are selected for log deletion, IM Security will also remove the corresponding quarantine, backup, and archive files.

Set a Schedule for Log Deletion

Configure automatic log deletion to prevent the consumption of vital hard disk space.

To delete logs automatically:

1. Click **Logs > Maintenance** on the navigation menu.
2. Click the **Automatic** tab and select **Enable automatic maintenance**.

   Maintenance runs everyday starting at 00:30.

3. Under **Type**, select the log **type** to delete.

   Select **All logs** or select **Specified logs** and then select the specific types of logs.

4. Under **Action**, type the **number of days** you want IM Security to retain logs.

   For example:

   If it is the tenth day and you type 3 days, then IM Security deletes all logs saved on the sixth day or before.

5. Click **Save** to apply settings.

IM Security begins to automatically delete all logs according to your settings.

Note: If **Virus scan**, **File blocking**, **Content filtering for files**, **Content filtering for IM**, and **Web Threat Protection** log types are selected for log deletion, IM Security will also remove the corresponding quarantine, backup, and archive files.

Managing Directories

IM Security uses the following directories per scan or filter action:

- **Quarantine Directory (Virus Scan)**—IM Security moves files to the Quarantine directory whenever it takes the quarantine action after detecting an infected file

  `<root>:\Program Files\Trend Micro\IM Security\quarantine` is the default Quarantine directory. IM Security can send messages to the Quarantine directory during a virus scan.

- **Backup Directory (Virus Scan)**—IM Security saves a copy of a file to the Backup directory before taking action on it

  The Backup directory is a safety precaution designed to protect the original file from damage. `<root>:\Program Files\Trend Micro\IM Security\backup` is the default Backup directory. IM Security can send files to the Backup directory during a virus scan.

- **Archive**—IM Security moves the file in the specified archive directory

  `<root>:\Program Files\Trend Micro\IM Security\archive` is the default Archive directory. IM Security can send files to the Archive directory during file blocking and file content filtering, and URL filtering.

The Archive directory is available for file blocking and file content filtering.

Specify Quarantine, Backup, and Archive Directories

From the Directories screen you can specify locations for the **Virus Scan Quarantine** and **Backup directories** and the **File Blocking** and **File Transfer Content Filtering Archive directories**.

To specify the Quarantine, backup, and archive directories:

1. Under the specific directory section, type the directory's full Windows path.

   For example, type `c:\Program Files\Trend Micro\IMSecurity\quarantine` for the quarantine directory.

2. Click **Save**.

Consider the following points when setting the IM Security directories:

- Allocate a directory with sufficient disk space that is not less than 100MB.
- Exclude the directory paths from local server virus scans.
- When performing a manual scan of the server using a file server-based antivirus application, exclude the Archive, Quarantine, and Backup directories

IM Security stores infected files or messages in the Quarantine and Backup directories.

Managing Disclaimer Statements

Disclaimer statements are used to notify individuals that their instant messaging sessions are being monitored for corporate security reasons. IM Security inserts the disclaimer statement into the instant messaging window when a user initiates a new instant message session, or when a new user joins a current session. IM Security sends disclaimers to all persons (internal and external) involved in the instant message session.

Internal/External user definitions

IM Security supports disclaimers for both internal and external users. IM Security defines internal users as those users that have been added to the **Selected Internal Users** list in the Disclaimer Settings screen. IM Security considers all other users external.

Internal/External sessions

IM Security categorizes instant messaging sessions as being either internal or external. IM Security considers an instant messaging session to be internal when all of the users participating in the session belong to the **Selected Internal Users** list. If one or more of the users is not on the Selected Internal Users list, IM Security categorizes the session as external. IM Security will re-categorize the session as new users join the session or old users leave the session. One exception is that if there are three users, two of which are

internal and one external. If the external user leaves the conversation, IM Security will not re-categorize the session to internal.

Note: As a rule, if one or more of the users are not on the **Selected Internal Users** list, IM Security categorizes the session as external.

Configure Disclaimer for Internal and External Chat Sessions

Use the **Disclaimer Settings** screen to enable and customize IM Security Disclaimer messages for internal and external users.

To enable and customize internal and external disclaimer statements:

1. Select the **Enable insertion of disclaimer into the initiation of an IM session** check box.
2. Click the **External Disclaimer** tab.
3. Type a disclaimer statement for external users or use the default statement.
4. Click the **Internal Disclaimer** tab.
5. Add internal users to the **Selected Internal Users** list.
6. Type a disclaimer statement for internal users or use the default statement.

Managing the Product License

The **Product License** screen displays details about your license. Depending on the options you chose during installation, you might have a fully licensed version of IM Security or an evaluation version. In either case, your license will expire after a period of time as specified in your maintenance agreement. You can use the Product License screen to find out in advance when you license will expire.

Standard Maintenance Agreement

The standard Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. A license to the Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support ("Maintenance") for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro's then-current Maintenance fees. The Maintenance Agreement expires. Your License Agreement does not.

When your license expires

When your license expires, IM Security continues to protect your Office Communications servers in a very limited manner. Trend Micro recommends that you keep your license agreement activated at all times. If your license expires, obtain a new Activation Code or renew your expired license immediately.

Renewing your product license

To renew the product license:

1. Contact your Trend Micro sales representative or corporate reseller to renew your license agreement.
2. The representative will update your IM Security registration information using Trend Micro Product Registration.
3. IM Security polls the Product Registration and receives the new expiration date directly from the Product Registration server. You are not required to manually enter a new Activation Code when renewing your license.

Note: Click **Update License** to have IM Security update the license information immediately based on its latest poll of the Product Registration server.

View Product License

Open the **Product License** screen to view the current license information for IM Security. You can also update your license or enter a new Activation Code.

To view product license information:

- Click **Administration > Product License** on the navigation menu.

Tip: The Summary screen, which is the first screen that displays when you open the IM Security product console, displays information about your maintenance expiration. Click the **more info** link to open the Product License screen.

The Product License screen provides the following details:

- **Product name**
- **Expiration date**—Date when IM Security license expires
- **License status**—Activated, expired, or grace period

Tip: Ensure that your license agreement is activated at all times. Otherwise, an expired license causes IM Security to apply limited scanning and filtering features.

- **License version**—Activation Code type (Full or Evaluation/Trial)
- **License last updated**—Date when IM Security license has been updated (for example, when the maintenance is renewed)
- **Activation Code**

To view more detailed product license information, from the Product License screen, click the **View detailed license online** link.

Participating in World Virus Tracking

The World Virus Tracking Program screen allows IM Security to send virus scan results to the Trend Micro World Virus Tracking Program to better track trends in virus outbreaks. Your participation in this program can benefit the attempt to better understand the development and spread of virus infections. The IM Security Setup prompts you whether you want to participate in the World Virus Tracking Program. You can change the setting at a later time from the **Administration > World Virus Tracking** menu.

To participate in World Virus Tracking Program:

1. Click **Administration > World Virus Tracking** on the navigation menu.
2. On the **World Virus Tracking Program** screen, read the disclaimer and click **Yes** to participate. Otherwise, click **No** to decline participation.
3. Click **Save**.

To view the current Trend Micro virus map, click **Virus Map** or enter the following address in your Web browser: http://wtc.trendmicro.com/wtc/default.asp

Chapter 4

Trend Micro™ IM Security Tools

This chapter describes features and capabilities for other Trend Micro IM Security tools.

The topics discussed in this chapter include:

Trend Micro™ IM Security Migration Tool

The IM Security Migration Tool (`toolMigrationTool.exe`) is a command line tool, which allows you to easily migrate settings from IM Security 1.0 running on Microsoft Live Communications Server (LCS) to IM Security 1.5 running on Office Communications Server (OCS) 2007. The tool also allows for migration of settings between two different servers running IM Security 1.5 on OCS 2007.

To run the Migration Tool:

1. Click **Start > Run**.
2. Type **cmd**, and then click **OK** to open the Windows Command Interpreter.
3. On the Windows Command Interpreter, go to the folder where the Migration Tool program (`toolMigrationTool.exe`) is located.
4. Type the appropriate command.

   Usage:

   ```
   toolMigrationTool.exe /Action:<"import" or "export"> /Location:
   <full path to file> /Server:<IM Security server domain name or
   IP> /User:<username for server> /Password:<password for server>
   ```

Command:

TABLE 4-1. Migration Tool Commands

PARAMETER	DESCRIPTION
`/Action <action>`	Import or Export settings
`/Location <full path to file>`	Where to place the migration settings file (export) or where to get the migration settings file (import)
`/Server <IM Security Server>`	Server name or IP address of the remote server
`/User <user name>`	The user account used to log on to the remote server
`/Password <password>`	The password for the user account
`/Help or /?`	Quick help

Example:

When running the tool remotely:

```
toolMigrationTool.exe /Action:export
/Location:target_settings_file /Server:target_server_name
/User:username /Password:password
toolMigrationTool.exe /Action:import
/Location:location_settings_file /Server:target_server_name
/User:username /Password:password
```

When running the tool locally:

```
toolMigrationTool.exe /action:import
/Location:location_settings_file
toolMigrationTool.exe /action:export
/Location:location_settings_file
```

IM Security Server Management Tool

The IM Security Server Management Tool (`toolSrvMgmt.exe`) is a command line tool, which allows you to easily add and register other IM Security servers in the **Server Management** list. Registering servers provides you the ability to replicate scan, filter, and update settings to multiple IM Security servers at the same time.

The Server Management Tool automates the target servers' registration onto a source server. Adding the source server's **IM Security Admins** group to the Access Control List (ACL) of the target server's `root\TrendMicro\IMSecurity` WMI instance completes the registration process.

Tip: Run the Server Management Tool from the target or source IM Security server (typically under `<root>\Program Files\Trend Micro\IM Security\`).

Before using this tool, gather and ensure the correctness of the following information:

- Source server's domain name
- Target server's host name or IP address
- User name and password of the Windows account that has Domain Administrator privileges

To run the Management Tool:

1. Click **Start > Run**.
2. Type **cmd**, and then click **OK** to open the Windows Command Interpreter.
3. On the Windows Command Interpreter, go to the folder where the Server Management Tool program (toolSrvMgmt.exe) is located.
4. Type the appropriate command.

   Usage:

   ```
   toolSrvMgmt.exe /u <domain name\user name> /p <password> /s
   <source server domain name> /t <target server name> /o
   <operation> /a <IMSecurity notification account> /?
   ```

Command:

TABLE 4-2. Server Management Tool Commands

PARAMETER	DESCRIPTION
/u <user name>	The user account that has local administrator privilege on the target server
/p <password>	The password of the user account
/s <domain name>	Domain name of the source server
/t <server name>	Host name or IP address of the target server
/a	IM Security notification account
/o <operation type>	Operation to execute–"add" or "remove"
/h	Quick help

Example:

When running the tool remotely:

```
toolSrvMgmt.exe /u domain_name\user_name /p password /s
source_server_domain_name/t target_server_name /a
IMSecurity_notification_account /o add
```

When running the tool locally:

```
toolSrvMgmt.exe /s source_server_domain_name /a
IMSecurity_notification_account /o add
```

IM Security Agent Account Tool

The IM Security Agent Account Tool (`toolImAgentCfg.exe`) is a command line tool, which allows you to specify another Windows account as the new IM Security notification account.

- Run the Agent Account Tool locally on the IM Security server (typically under `<root>\Program Files\Trend Micro\IM Security\`).

Before using this tool, gather and ensure the correctness of the following information:

- The new notification account's user name and password
- Transport type (communications service setting): TCP, TLS, or MTLS

To run the Agent Account Tool:

1. Obtain the necessary values for the Agent Account Tool parameter.
2. Stop **Trend Micro IM Security server** from the Windows Service panel.
3. Click **Start > Run**.
4. Type **cmd**, and then click **OK** to open the Windows Command Interpreter.
5. On the Windows Command Interpreter, go to the folder where the Agent Account Tool program (toolImAgentCfg.exe) is located.
6. Type the appropriate command.

   Usage:

   ```
   toolImAgentCfg.exe /u <user name> /p <password> /t
   <transport type> /h
   ```

   Command:

   TABLE 4-3. Agent Account Tool Commands

PARAMETER	DESCRIPTION
`/u <user name>`	User name of the IM Security Administrator account
`/p <password>`	Password of the IM Security Administrator account
`/t <transport type>`	Transport type / Communications service setting: TCP or TLS
`/h`	Quick help

   Example:

   ```
   toolImAgentCfg.exe /u new_agent /p new_agent_password /t TCP
   ```

Running Tools From a Different Location

IM Security requires the following files when running a tool from a location other than the default IM Security installation folder. For example, to run the Agent Account tool from `d:\temp`, ensure that the corresponding required files are present in `d:\temp`

Commands:.

TABLE 4-4. IM Security Tools

TOOL	REQUIRED IM SECURITY FILES

Agent Account Tool (`toolImA-gentCfg.exe`)	`UTILCOMMON.DLL`
	`UTILMANAGEMENT.DLL`
	`UTILADUSERGROUPMGMT.DLL`
	`UTILMSSIPINFO.DLL`
	`MSVCP71.DLL`
	`MSVCR71.DLL`
	`ICUU18.DLL`
	`UTILDEBUG.DLL`

Server Management Tool (`toolSrvMgmt.exe`)	`MSVCP71.DLL` `MSVCR71.DLL`

For example, if you are running the Server Management Tool from a target server's `c:\temp\ims directory`, ensure that `MSVCP71.DLL` and `MSVCR71.DLL` are available in the same directory.

Chapter 5

Troubleshooting and FAQ

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

The topics discussed in this chapter include:

Determine Product Version

Perform the following to determine the product version and build:

- Click About from the header menu to determine the product version and build

Check the product version and build to verify whether you need to update to the latest IM Security patch, if a patch is available.

Generate Debug Logs

Use **Debug Logs** to analyze unexpected IM Security errors. IM Security Debugger can assist you in reporting the status of IM Security processes on the local IM Security server.

System Debugger works by instructing each IM Security module to insert messages into the program, and then records the action into log files upon execution. Forward the logs to Trend Micro technical support staff to help them debug the actual program flow in your environment. The log files are text files, and you can use any text editor to view them.

To generate debug logs using the System Debugger:

1. Access the product console.
2. Click **Administration > Debug Logs**.
3. Select the check boxes of the modules that you want to debug.

Tip: All of the modules produce text files that you can view with any text editor. By default, IM Security keeps the logs in the directory: `c:\Program Files\Trend Micro\IM Security\Debug`

---

4. Click **Apply** to start collecting data for the module(s) that you have selected.

Note: IM Security continues to collect debug data until you clear all items you were debugging and click **Apply**.

IM Security starts to collect debug data and saves them in a corresponding log file. Once a debug file's size reaches 10MB, IM Security creates a new file and implements the following file naming convention:

`servIMSHost-yy-mm-dd-#####.log`

Where ***#####*** is the instance number of the debug file. For example, `servIMSHost-05-01-25-00001.log` and `servIMSHost-05-01-25-00002.log`.

Alert Issues

Use the Windows **Services** Panel to check whether the **Trend Micro IM Security System Attendant Service** status is started. Restart the service if its status is stopped.

Component Update Issues

IM Security displays the result of an automatic or manual update through the following screens:

- Summary
- Log Query

Use one of the above methods to determine whether component update was successful. Otherwise, refer to the following section to troubleshoot update issues.

To troubleshoot update issues:

1. Check the Summary screen or query update logs to verify whether there are component update errors. If there are, try to follow the suggestions provided by the error messages or logs.

2. Select the location from which IM Security receives updates. The default location is **Trend Micro's ActiveUpdate server**.

   If **Intranet location containing a copy of the current file** or **Other Update Source** is enabled as the update source, check whether the folder contains the latest components.

3. If **Trend Micro ActiveUpdate** is enabled as the update source, check the connection from the IM Security server to the ActiveUpdate server.

   a. Run nslookup to make sure the IM Security server can resolve the ActiveUpdate server's FQDN.

   b. `Ping http://imsecurity15-p.activeupdate.trendmicro.com/activeupdate/` from the IM Security server.

   c. Telnet the ActiveUpdate server at port 80 to make sure the IM Security server can connect using HTTP.

Log Issues

One of the following issues may occur:

- An error occurs trying to query and display logs
- Unable to export logs

To troubleshoot log generation issues:

1. Use the Windows **Services** panel to verify whether the IM Security SQL or the Microsoft SQL Server 2005 instance is running.
2. Ensure that there is at least 128MB free disk space available on the IM Security database folder. Otherwise, delete older log entries.
3. Check the database connection by opening the IM Security database through Microsoft Access or a SQL utility.
4. If any of the above tasks do not solve the issue, contact Trend Micro support.

Product Console Access Issues

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

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

To troubleshoot product console access issues:

1. Check whether the following settings are true:
   - Both IM Security and Microsoft SharePoint Portal Server are installed on the same server
   - The IM Security product console belongs to the Microsoft Internet Information Services (IIS) Default Web site

     If all of the above conditions are true, the product console will be inaccessible. SharePoint prevents access to other Web sites by default. To exclude the IM Security Web site (allow access), refer to **Product Console Access Issues** in the *IM Security Online Help*.
2. Check whether the account used to access the product console belongs to the **IM Security Admins** Active Directory group.
3. Verify whether the latest Sun Java Virtual Machine (JVM) is available on the IM Security server. Otherwise, the User name and Password field will appear with an "x" mark on the product console.

Note: IM Security supports Sun JVM version 1.5.0 or 6.0.

---

4. Use Windows **Services** panel to verify whether **Trend Micro IM Security Server** is started.
5. Ensure that the Web service is started.
6. Verify whether the IM Security administrator account has not been changed. Otherwise, obtain the latest account user name and password.
7. Check the network connection and HTTP port being used.

Notification Issues

You configured IM Security to send notification to a POP3 account (for example, `my_email@yahoo.com`). However, IM Security encountered an error and was unable to send notifications to `my_email@yahoo.com`.

Email Notification

To troubleshoot Email notification issues:

1. Verify and ensure the correctness of the administrator's SMTP notification settings. IM Security uses the notification settings to send email notification.
2. Contact your mail administrator to verify whether SMTP server authentication is enabled. If so, verify that the credentials used are valid.
3. Ping the SMTP server to ensure that the server can be resolved (through host name or IP address).
4. Verify IM Security's SMTP port setting is matching the SMTP port being used (the default SMTP port is 25).
5. Check if the Exchange Server is an internal or a production Exchange Server.

   If the Exchange server is an internal server, meaning the Internet Mail Service has not been installed, and then the Exchange Server will not be able to send a message outside of the Exchange Server.
6. Check if the Internet Mail Service (Microsoft Exchange™ 5.5) or Connector for SMTP Connector (Microsoft Exchange 200x) is installed on the Exchange Server.
7. Verify if the Exchange server is able to send messages to an account not belonging to the organization:
   a. From the IM Security server, open an email client (for example, Outlook Express™).
   b. Create a new message and send it to a POP3 account.
   c. Using Windows Explorer™, open the POP3 account Inbox and check if it receives the message from the IM Security server.
8. Check whether the POP3 account receives the message.
   - If the POP3 account receives the message, the Exchange server has the Internet Mail Service or Connector already configured.
     i. Access the IM Security product console.
     ii. Configure virus scan, file blocking, file content filtering, instant message URL filtering, or instant message content filtering.
     iii. Define the administrator or contact notification.

- If the POP3 account did not receive the message, the Exchange server has no Internet Mail Service or Connector configured, install the Exchange server Internet Mail Service to send email notification to a POP3 account.

SNMP Trap Notification

To troubleshoot SNMP trap notification issues:

1. Verify whether the administrator's SNMP notification settings that IM Security uses to send SNMP trap notifications exist.
2. Ping the SNMP server using its IP address to ensure that IM Security can resolve the server.
3. Verify the **community name** validity.
4. Ensure your SNMP community name can listen to the SNMP trap settings set.

Instant Message Notification

To troubleshoot instant message notification issues:

1. If you enabled administrator notification, verify and ensure the correctness of the administrator's SIP address.
2. Test whether the IM Security agent notification account has the correct attributes
    i. Run "dsa.msc" or "dsa.msc -32" to open "Active Directory users and computers" on the OCS server.
    ii. Select IM Security agent notification account properties > communications > configure button.
    iii. Check whether "Enable enhanced presence" is enabled , if it is not enabled, enable it.
3. Test whether the IM Security agent notification account can send instant messages to another user by using the agent's SIP address to log on to Office Communicator and establish a conversation with another user.
4. Verify whether the agent notification account is present on the local or another remote server.
5. Verify the validity of the SIP address and password used. Check whether the SIP address is enabled. Alternatively, verify whether the password was modified.

6. Check whether the listening ports for TCP or TLS transport is not reconfigured after IM Security is installed.
7. To specify another agent notification account, use the Agent Account Tool.

Product Activation Issues

One of the following issues may occur:

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

To troubleshoot product activation issues:

1. Register IM Security to obtain an Activation Code.

Note: Do not use the Registration Key when activating IM Security. Otherwise, product activation will not work.

---

2. Verify the Activation Code used. Be sure to use the following format (excluding dashes) 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.

Report Issues

One of the following issues occurs:

- Unable to generate scheduled reports
- Unable to view generated scheduled reports
- PDF or HTML reports cannot be opened nor read

To troubleshoot report generation issues:

1. If there are messages or logs related to the report issue, check for the possible solutions offered by the logs or messages.

2. Ensure that there is at least 128MB free disk space available on the IM Security program folder. Otherwise, the report module cannot run and generate reports.
3. Use the Windows Services panel to verify whether the IM Security SQL or the Microsoft SQL Server 2005 Express instance is running.
4. Check the database connection by opening the IM Security database through Microsoft Access or a SQL utility.
5. Generate a one-time report with a limited date range (for example, `from 05.01.2005 to 05.09.2005`).
6. If IM Security is unable to generate a one-time report, send `<root>:\Program Files\Trend Micro\IM Security\TMreportEX.log` to Trend Micro support.

To troubleshoot PDF or HTML report display issues:

- Check whether the following settings are enabled:
  - HTTPS product console
  - Internet Explorer > **Options > Advanced > Do not save encrypted pages to disk**

  If the above options are enabled, PDF reports cannot be displayed. As a workaround, disable **Do not save encrypted pages to disk**.
- Verify whether the **Internet Explorer Enhanced Security Configuration** Windows component is installed.

  If so, reports sent as email attachments cannot be opened directly from the message. As a workaround, remove **Internet Explorer Enhanced Security Configuration** or save the attached `*.MHT` file to a local folder before opening the report.

Frequently Asked Questions

This section answers the following common questions about IM Security:

- General Product Knowledge.
- Installation, Registration, and Activation

General Product Knowledge

- What is IM Security?
- How does IM Security protect my OCS server?

- Can IM Security scan files or filter messages transmitted using non-OCS IM chats using 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 an RK or AC?

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 OCS environments.

How does IM Security protect my OCS server?

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

Can IM Security scan files or filter messages transmitted by non-OCS IM chats such as MSN/Windows Messenger?

IM Security can only scan files or filter messages transmitted through Microsoft OCS.

Can IM Security filter content of all file types?

No. IM Security is able to filter content of Microsoft Office files (`*.ppt, *.doc, *.xls`), Microsoft Office 2007 file (*.pptx, *.docx, *.xlsx), 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 OCS is installed.

What are the instant messaging clients that IM Security supports?

IM Security only supports Office Communicator 2005 and 2007.

Where can I get an RK or AC?

Refer to the Trend Micro Web site (`http://esupport.trendmicro.com/support`).

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 topics discussed in this chapter include:

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 *Installation and Deployment 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://esupport.trendmicro.com/support`

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:

`http://subwiz.trendmicro.com/SubWiz/Default.asp`

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

Appendix A

Performance Counters

This chapter contains information about the performance counters available for Trend Micro™ IM Security.

The IM Security performance counters (by feature):

Real-Time Scan Performance Counters

The following table provides a brief description of the Instant Message and File Transfer Scan performance counters for real-time scan

TABLE A-1. Instant Message and File Transfer Scan counters

COUNTER NAME	DESCRIPTION
Instant Message Scan - 001 - Total scanned instant messages	Total number of scanned instant messages
Instant Message Scan - 002 - Total scanning time	The total scanning time of all scanned instant messages
Instant Message Scan - 003 - Scanned messages / sec	Rate of instant messages passing through the real-time scan modules (Content Filtering + Web Threat Protection) (= 001 / 002)
File Transfer Scan - 004 - Total scanned files	The total number of scanned files
File Transfer Scan - 005 - Total scanning time	The total scanning time of all files scanned
File Transfer Scan - 006 - Scanned files / sec	Rate of files passing through the real-time scan modules (File Blocking, Content Filtering & Virus Scan) (= 004 / 005)

Virus Scan Performance Counters

The following table provides a brief description of the Virus Scan performance counters

TABLE A-2. Virus Scan counters

COUNTER NAME	DESCRIPTION
VScan - 001 - Total scanned items	The number of files scanned by Virus Scan
VScan - 002 - Total scanning time	The total scanning time for all files scanned by Virus Scan

TABLE A-2. Virus Scan counters

COUNTER NAME	DESCRIPTION
VScan - 003 - Total matching files	The number of files that match virus scan settings, including : • virus or spyware detected • over restriction (compressed file) • unscannable files (password-protected or encrypted files)
VScan - 004 - Scanned items / sec	Rate of files passing through the Virus Scan filter (= 001 / 002)

File Blocking Performance Counters

The following table provides a brief description of the File Blocking performance counters.

TABLE A-3. File Blocking counters

COUNTER NAME	DESCRIPTION
File Blocking - 001 - Total scanned items	The number of files scanned by File Blocking
File Blocking - 002 - Total scanning time	The total scanning time of all scanned files by File Blocking
File Blocking - 003 - Total matching files	The number of files that match File Blocking rules, including : • matches the specific file size • matches the specific file name • matches the specific file type
File Blocking - 004 - Scanned items / sec	Rate of files passing through the File Blocking filter (= File Blocking counter 001 / File Blocking counter 002)

Content Filtering Performance Counters

The following table provides a brief description of the Content Filtering performance counters

TABLE A-4. Content Filtering Counters

COUNTER NAME	DESCRIPTION
CFilter -001 - IM: Total scanned items	The number of messages scanned by Content Filtering
CFilter -002- IM : Total scanning time	The total scanning time of all instant messages scanned for Content Filtering violations
CFilter -003- IM : Total matching items	The number of instant messages that violated Content Filtering rules
CFilter - 004 -FT : Total scanned items	The number of files scanned for Content Filtering violations
CFilter - 005 -FT : Total scanning time	The total scanning time of all files scanned for Content Filtering violations
CFilter - 006 -FT : Total matching items	The number of files that violated Content Filtering rules
CFilter - 007 -IM : Filtered messages / sec	Rate of instant messages passing through Content Filtering (= 001 / 002)
CFilter - 008 -FT : Filtered files / sec	Rate of files passing through Content Filtering (= 004 / 005)

Directory Service Access Performance Counters

The following table provides a brief description of the Directory Service Access (DSAccess) performance counters

TABLE A-5. DSAccess Counters

COUNTER NAME	DESCRIPTION
DSAccess - 001 - Total directory accesses	Total amount of data queried from the Global Catalog (GC) (= 005 + 009 + 013)
DSAccess - 002 - Total directory access time	Total time spent querying data from GC (= 006 + 010 + 014)
DSAccess - 003 - Total local cache accesses	Total amount of data queried from caches (= 007 + 011 + 015)
DSAccess - 004 - Total local cache access time	Total time spent querying data from caches (= 008 + 012 + 016)
DSAccess - 005 - [User Identity] directory accesses	Total amount of user data queried from GC
DSAccess - 006 - [User Identity] directory access time	Total time spent querying user data from GC
DSAccess - 007 - [User Identity] cache accesses	Total amount of user data queried from user cache
DSAccess - 008 - [User Identity] cache access time	Total time spent querying user data from user cache
DSAccess - 009 - [Primary Group] directory accesses	Total amount of primary group data queried from GC
DSAccess - 010 - [Primary Group] directory access time	Total time spent querying primary group data from GC
DSAccess - 011 - [Primary Group] cache accesses	Total amount of primary group data queried from Primary Group cache

TABLE A-5. DSAccess Counters

COUNTER NAME	DESCRIPTION
DSAccess - 012 - [Primary Group] cache access time	Total time spent querying primary group data from the Primary Group cache
DSAccess - 013 - [Nested Group] directory accesses	Total amount of nested group data queried from the GC
DSAccess - 014 - [Nested Group] directory access time	Total time spent querying nested group data from the GC
DSAccess - 015 - [Nested Group] cache accesses	Total amount of nested group data queried from the Nested Group cache
DSAccess - 016 - [Nested Group] cache access time	Total time spent querying nested group data from the Nested Group cache

Instant Messaging Hook Module Performance Counters

The following table describes the Instant Messaging Hook (IMHook) module performance counters

TABLE A-6. IMHook counters

COUNTER NAME	DESCRIPTION
IMHook - 001 - Total number of requests from LCS	Total number of requests coming from the LCS / OCS server (The first instant message to a recipient increments the counter by 2. The INVITE establishes the session and the MESSAGE delivers the message content.)
IMHook - 002 - Total number of responses from LCS	Total number of responses coming from the LCS / OCS server

TABLE A-6. IMHook counters

COUNTER NAME	DESCRIPTION
IMHook - 003 - Total messages passing to the scan modules	Total number of instant messages scanned by the IM Security scan modules
IMHook - 004 - File transfer monitoring map size	Map size of the file transfer monitor (Total number of FT invitation monitoring tasks in the Monitor Queue at present. The number will become 0 when there is no file transfer taking place)
IMHook - 005 - Total number of requests from trusted users	Total number of requests coming from trusted users (Total number of SIP requests sent from trusted users - by default, it should be the IM Agent. This number usually increases when the IM Agent sends IM notifications to the intended recipients)
IMHook - 006 - Total number of requests from trusted servers	Total number of requests coming from trusted servers (Total number of SIP requests that have been scanned by another IM Security server)
IMHook - 007 - LCS requests / sec	Rate of LCS / OCS requests (Number of SIP request 'MESSAGE' or 'INVITE' sent from LCS / OCS per second)
IMHook - 008 - LCS responses / sec	Rate of LCS / OCS responses (Number of SIP responses sent from LCS / OCS per second)

TABLE A-6. IMHook counters

COUNTER NAME	DESCRIPTION
IMHook - 009 - Passing messages / sec	Rate of messages passing to the scan module (Number of instant messages being passed to the IM Security scan module per second)

File Transfer Hook Module Performance Counters

The following table describes the File Transfer Hook (FTHook) module performance counters

TABLE A-7. FTHook counters

COUNTER NAME	DESCRIPTION
FTHook - 001 - Unhandled task queue size	The number of unhandled file transfer tasks (Not available, reserved counter for future use)
FTHook - 002 - Total passing files	Total number of files have been passed to IM Security scan modules
FTHook - 003 - Current processing file transfer sessions	The number of processing file transfer tasks / sessions (Not available, reserved counter for future use)

TABLE A-7. FTHook counters

COUNTER NAME	DESCRIPTION
FTHook - 004 - Current server agent connections	The current number of server agent connections (Total number of server agent connections established between recipient(s). After the file is scanned, IM Security will act as the sender and the server agent will be in charge of delivering the scanned file to the recipient. And the delivery, the count will become 0)
FTHook - 005 - Current client agent connections	The current number of client agent connections (Total number of client agent connections established between sender(s). After the file transfer invitation is completed, IM Security will act as the recipient and the client agent will be in charge of downloading the file from the sender. After downloaded, the count will become 0)
FTHook - 006 - Total held scan tasks	Total number of held scan tasks (Total number of files to be scanned after downloading)
FTHook - 007 - Total pending scan tasks	Total number of pending scan tasks (Total number of files waiting for scanning)
FTHook - 008 - Total scan tasks in progress	Total number of scan tasks in progress (Total numberof files being scanned)

TABLE A-7. FTHook counters

COUNTER NAME	DESCRIPTION
FTHook - 009 - Passing files / sec	Rate of files being passed to the scan module

URL Filtering Performance Counters

The following table describes the URL Filtering performance counters

TABLE A-8. URL Filtering counters

COUNTER NAME	DESCRIPTION
UFilter - 001 - URL : Total items scanned	The number of URL addresses scanned by the URL filter
UFilter - 002 - URL : Total scanning time	The total scanning time of all URL addresses
UFilter - 003 - URL : Total malicious URLs	The number of URL addresses that were rated as unsafe
UFilter - 004 - URL : URLs scanned per sec	Rate of URL addresses passing through the URL filter module (= 001 / 002)
UFilter - 005 - URL : Total approved items	The number of URL addresses in the white (approved) list
UFilter - 006 - IM : Total scanned items	The number of instant messages scanned by the URL filter
UFilter - 007 - IM : Total scanning time	The total scanning time of all instant messages
UFilter - 008 - Messages scanned per second	Rate of instant messages passing through the URL filter module (= 006 / 007)
UFilter - 009 - IM : Total scanned items containing URLs	The number of instant messages scanned by the URL filter that contained URL addresses

TABLE A-8. URL Filtering counters

COUNTER NAME	DESCRIPTION
UFilter - 010 - IM : Total scanned items containing malicious URLs	The number of instant messages containing malicious URL addresses that were scanned by the URL filter

Session Management Performance Counters

The following table describes the Session Management performance counters

TABLE A-9. Session Management counters

COUNTER NAME	DESCRIPTION
Session Management - 001 - Total active sessions	The number of active sessions monitored by Session Management
Session Management - 002 - Total active dialogs	The number of active dialogs which have a unique call-id value
Session Management - 003 - Total active conferences	The number of active conferences associated with a unique sip-focus
Session Management - 004 - Total expired sessions	The number of sessions that are unresponsive in session-expired time or exceeds maximum idle time

Disclaimer Performance Counters

The following table describes the Disclaimer performance counters

TABLE A-10. Disclaimer counters

COUNTER NAME	DESCRIPTION
Disclaimer - 001 - Total disclaimer records	The number of disclaimer records. disclaimer records maintain the disclaimer status (the number of messages with a disclaimer inserted) (= 002 + 003)
Disclaimer - 002 - Total internal disclaimer messages	The number of messages that have the internal disclaimer inserted
Disclaimer - 003 - Total external disclaimer messages	The number of messages that have the external disclaimer inserted

Appendix B

IM Security and TMCM Logs and Actions Comparison

This topics discussed in this appendix include:

IM Security and TMCM 5.0 Logs and Actions

Virus Scan and Additional Threats

TABLE B-1. Virus scan and additional threats logs and actions

IM SECURITY - LOGS AND ACTIONS	MAPPED TO CM 5.0
Virus Scan	**Security Threat Information => Virus/Malware Information**
Virus Scan (additional threats)	**Security Threat Information => Spyware/Grayware Information**
Clean	File cleaned
Quarantine	File quarantined
Cancel Transfer	File deleted
Deliver	File passed

File Blocking and Content Filtering for File Transfers and Instant Messages

TABLE B-2. File blocking and content filtering logs and actions

IM SECURITY LOGS AND ACTIONS	MAPPED TO CM 5.0
File Blocking	**Security Threat Information => Content Violation Information**
Cancel + Archive	Quarantine
Deliver + Archive	Deliver
Cancel	Delete
Deliver	Deliver
Content Filtering: File Transfers	**Security Threat Information => Content Violation Information**
Cancel + Archive	Quarantine
Deliver + Archive	Deliver
Cancel	Delete
Deliver	Deliver
Content Filtering: Instant Messages	**Security Threat Information => Content Violation Information**
Cancel + Archive	Quarantine
Replace all + Archive	Replace
Deliver + Archive	Deliver
Cancel	Delete
Replace all	Replace
Deliver	Deliver

Web Threat Protection

TABLE B-3. Web threat protection logs and actions

IM SECURITY LOGS AND ACTIONS	MAPPED TO CM 5.0
File Blocking	**Security Threat Information => Web Violation Information**
Cancel + Archive	Block
Replace + Archive	Block
Tag/Deliver + Archive	Pass
Deliver + Archive	Pass
Cancel	Block
Replace	Block
Tag/Deliver	Pass
Deliver	Pass

IM Security Log and TMCM 3.5 Logs and Actions

Virus Scan and Additional Threats

TABLE B-4. Virus scan and additional threats logs and actions

IM SECURITY - LOGS AND ACTIONS	MAPPED TO CM 3.5
Virus Scan	**Security logs => All virus log incidents**
Virus Scan (additional threats)	**Security logs => All spyware/grayware log incidents**
Clean	File cleaned
Quarantine	File quarantined
Cancel Transfer	File deleted
Deliver	File passed

File Blocking and Content Filtering for File Transfers and Instant Messages

TABLE B-5. File blocking and content filtering logs and actions

IM SECURITY LOGS AND ACTIONS	MAPPED TO CM 3.5
File Blocking	**Security logs => (or Content security violations: Attachment blocking)**
Cancel + Archive	Quarantine
Deliver + Archive	Deliver
Cancel	Delete
Deliver	Deliver
Content Filtering: File Transfers	**Security logs => Content security violations**
Cancel + Archive	Quarantine
Deliver + Archive	Deliver
Cancel	Delete
Deliver	Deliver
Content Filtering: Instant Messages	**Security logs => Content security violations**
Cancel + Archive	Quarantine
Replace all + Archive	Replace
Deliver + Archive	Deliver
Cancel	Delete
Replace all	Replace
Deliver	Deliver

Web Threat Protection

TABLE B-6. Web threat protection logs and actions

IM SECURITY LOGS AND ACTIONS	MAPPED TO CM 3.5
File Blocking	**Security logs => Web security violations**
Cancel + Archive	n/a
Replace + Archive	n/a
Tag/Deliver + Archive	n/a
Deliver + Archive	n/a
Cancel	n/a
Replace	n/a
Tag/Deliver	n/a
Deliver	n/a

Glossary

This glossary describes special terms used in this document or the online help.

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. *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. *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.
action (*Also see* target and notification)	The operation to be performed when: - a virus has been detected - spam has been detected - a content violation has occurred - an attempt was made to access a blocked URL, or - file blocking has been triggered. 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.

TERM	EXPLANATION
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 *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	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, 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.
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. 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."
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.

TERM	EXPLANATION
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.
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.

TERM	EXPLANATION
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). 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 pub-lic-key systems using digital signatures. *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.
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.

TERM	EXPLANATION
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 Web site 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 Web site 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.
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.
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. *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: *C:\Programs\Trend Micro\ISVW\Quarantine*
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.

TERM	EXPLANATION
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
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.
(administrative) domain	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).
DoS (Denial of Service) 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.
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 Web site 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
ELF	Executable and Linkable Format—An executable file format for Unix and Linux platforms.
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. 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.
executable file	A binary file containing a program in machine language which is ready to be executed (run).

TERM	EXPLANATION
EXE file infector	An executable program with a .exe file extension. *Also see* DOS virus.
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.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.
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 pre-determined time or perform some other malicious action. 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 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 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.

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.
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.
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: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office
GUI	Graphical User Interface—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.

TERM	EXPLANATION
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.
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.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
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.

TERM	EXPLANATION
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.
installation script	The installation screens used to install Unix versions of Trend Micro products.
integrity checking	*See* checksumming.
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.

TERM	EXPLANATION
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. *Also see* “in the zoo.”
“in the zoo”	Describes known viruses that are currently controlled by antivirus products. *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.
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. 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."

TERM	EXPLANATION
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. *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. 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. *Also see* VBscript virus.
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.
KB	Kilobyte—1024 bytes of memory.
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.
LAN (Local Area Network)	A data communications network which is geographically limited, allowing easy interconnection of computers within the same building.

TERM	EXPLANATION
LDAP (Lightweight Directory Access Protocol)	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.
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.
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.
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.

TERM	EXPLANATION
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.
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.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.
MB	Megabyte—1024 kilobytes of data.

TERM	EXPLANATION
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.
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
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.
MTA (Mail Transfer Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
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 (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer 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. (*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. *Also see* authentication *and* digital signature.

TERM	EXPLANATION
purge	To delete all, as in getting rid of old entries in the logs.
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. *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 *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.

TERM	EXPLANATION
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.
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. (*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.

TERM	EXPLANATION
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	*See* virus signature.
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. *Also see* rule-based spam detection. *Also see* false positive.
SMTP	Simple Mail Transfer Protocol—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.
SMTP server	A server that relays email messages to their destinations.
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
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. *See* SNMP.
spam	Unsolicited email messages meant to promote a product or service.

TERM	EXPLANATION
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.
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. 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. *Also see* IP address.
target (*Also see* action and notification)	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.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
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).

TERM	EXPLANATION
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.
Transmission Control Protocol/Internet Protocol (TCP/IP)	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. 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. 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. *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.
URL	Universal Resource Locator—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. 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. *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. 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 Web site which sends out Web pages in response to HTTP requests from remote browsers.

TERM	EXPLANATION
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.
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).

Note:

Index

S

U

V

W