TREND MICRO™

1.6 IM Security for Microsoft™ Lync Server

Administrator's Guide

Instant Protection for Instant Messaging

Messaging Security

Document Part No.: TIEM16346/140311

Release Date: May 2014

Protected by U.S. Patent No.: Pending

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Chapter 8: Configuring Data Loss Prevention

Part III: Managing IM Security

Chapter 9: Monitoring IM Security

Chapter 10: Performing Administrative Tasks

Part IV: Getting Help

Appendix A: Performance Counters

Appendix B: IM Security and Control Manager Logs and Actions Comparison

Appendix C: Glossary

Index

Preface

Preface

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

This preface discusses the following topics:

IM Security Documentation

The product documentation consists of the following:

- **Online Help**: Web-based documentation that is accessible from the product console

  The Online Help contains explanations about IM Security features.

- **Installation and Deployment Guide**: PDF documentation that discusses requirements and procedures for installing and upgrading the product

- **Administrator's Guide**: PDF documentation that discusses getting started information and product management

- **Readme File**: Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

- **Knowledge Base**: Contains the latest information about all Trend Micro products. Other inquiries that were already answered area also posted and a dynamic list of the most frequently asked question is also displayed.

  http://esupport.trendmicro.com

Note

Trend Micro recommends checking the corresponding link from the Update Center (http://docs.trendmicro.com/en-us/enterprise/trend-micro-im-security.aspx) for updates to the documentation.

Audience

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

- Antivirus and content security protection

- Data Loss Prevention
- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Microsoft Lync Server administration
- Microsoft Lync Server 2010 and 2013 server role configurations

Document Conventions

The documentation uses the following conventions.

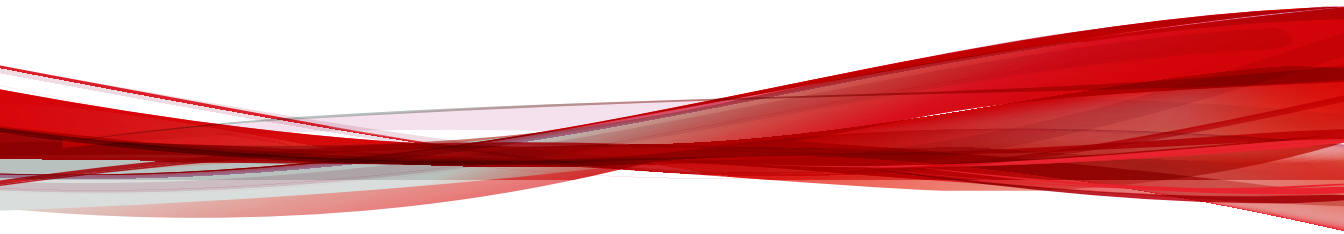
TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions

Convention	Description
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Part I

Introducing IM Security and Getting Started



Chapter 1

Introducing Trend Micro™ IM Security

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

Topics include:

IM Security Overview

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

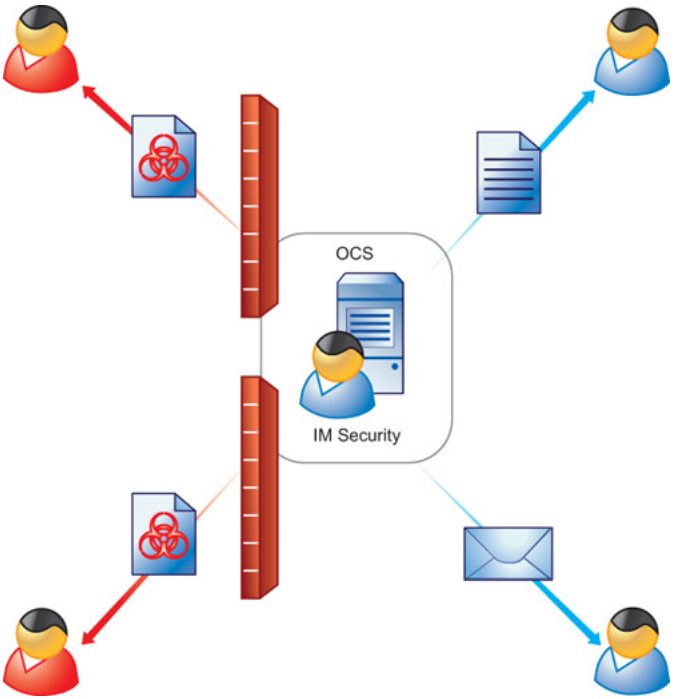


FIGURE 1-1. IM Security deployment

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

Features and Benefits

The following table outlines the IM Security features and benefits.

Feature	Benefit
Simple installation	IM Security provides the Setup installation program, which allows administrators to easily install the product on a single server or multiple servers with Lync Server 2010 or 2013.
Centralized product management	The IM Security web console allows administrators to configure IM Security anytime and from anywhere on the network.
Communication Control	Communication Control allows you to manage the Lync features granted to accounts at a company-wide or granular level, or allows you to limit the interactions between specific accounts.
File transfer scanning	IM Security protects Lync Server 2010 or 2013 and instant messaging (Lync Client) users from the following security risks associated with file transfers: • Virus/Malware and spyware/grayware • Sensitive or unwanted data transfers • Malicious URLs
Instant message scanning	IM Security protects Lync Server 2010 or 2013 and instant messaging (Lync Client) users from the following security risks associated with instant messages: • Sensitive or unwanted data transfers • Malicious URLs
Configurable disclaimer statements	IM Security supports configurable disclaimer statements for instant messaging sessions.

Feature	Benefit
Alerts and notifications	Set alerts to notify administrators or selected IT personnel whenever specific events related to IM Security or Lync Server occur. Inform administrators and contacts about IM Security actions using customizable notifications.
Reports and logs	Monitor IM Security activities using queried logs that detail security risk detections, content security events, and program update events. In addition, IM Security provides the option to send graphical reports using email.

File and Instant Messaging Protection

IM Security protects Lync Server users by providing the following scan filters.

Table 1-1. Security Scan Filters

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

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

TABLE 1-2. IM Security Order of Protection Precedence

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

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

Communication Control

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

For details, see *Configuring Communication Control on page 3-1*.

Virus Scan

File transfer scanning continually protects your Lync Server environment. Virus scan scans for viruses/malware, spyware/grayware, and other security risks that might be present in incoming and outgoing files.

For details, see *Configuring Virus Scans on page 4-1*.

FIGURE 1-2. How IM Security Virus Scan works

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

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

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

File Blocking

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

For details, see *Configuring File Blocking on page 5-1*.

FIGURE 1-3. How IM Security File Blocking works

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

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

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

2. Applies the File Blocking action.

3. Sends notifications to the administrator or contacts.

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

Content Filtering

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

For details, see *Configuring Content Filtering on page 6-1*.

FIGURE 1-4. How IM Security Content Filtering works

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

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

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

2. Applies the Content Filtering rule action.

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

3. Sends notifications to the administrator or contacts.

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

Web Reputation

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

For details, see *Configuring Web Reputation on page 7-1*.

IM Security performs the following tasks upon receiving a URL:

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

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

2. Applies the Web Reputation action.

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

3. Sends notifications to the administrator or contacts.

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

Note

The Web Reputation feature requires an active Internet connection.

Data Loss Prevention

Data Loss Prevention protects your Lync Server environment by evaluating the data that users send during messaging sessions and file transfers to determine if sensitive information (as defined by you) is present in the conversation or files.

For details, see *Configuring Data Loss Prevention on page 8-1*.

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

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

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

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

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

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

3. Sends notifications to the administrator or contacts.

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

Reports and Logs

To provide current information about the security of your Lync Server environment, IM Security is preconfigured to generate reports based on Virus Scan, File Blocking, Content Filtering (file transfers and instant messages), URL filtering (Web Reputation), Data Loss Prevention, and server traffic. Reports can be generated on demand or scheduled on a daily, weekly, or monthly basis.

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

Alerts and Notifications

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

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

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

Trend Micro Technology in IM Security

This section explains IM Security technology and how it protects your Lync Server 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 Lync Server. New pattern files are typically released at the rate of several per week.

- Virus 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 Reputation feature.

About ActiveUpdate

ActiveUpdate provides the latest downloads of all IM Security components over the Internet.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. IM Security can receive updates on a regularly scheduled interval or through manual updates.

Incremental Updates of the Pattern File

ActiveUpdate supports incremental updates of the pattern file. Rather than download the entire 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.

Configure IM Security to use ActiveUpdate and incremental updates to decrease the time spent updating.

The Trend Micro Virus Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. This engine has a long history in the industry and has proven to be one of the fastest.

Scan Engine Updates

Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- Trend Micro incorporates new detection technologies into the software
- A new, potentially harmful, virus/malware 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

To view the version of the scan engine that IM Security is currently using, open the product console and view **Summary**.

Tip

Trend Micro recommends frequently updating your scan engine. Scheduled updates can be used to conveniently and regularly update IM Security components.

The Trend Micro Pattern Files

The Trend Micro scan engine uses an external data file, called the virus pattern file, to identify the latest security risks.

You can view the most current version, release date, and a list of all the new definitions included in the file from the following website:

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

To view the version of the pattern file that IM Security is currently using on your IM Security server, open the product console and view **Summary**.

Tip

Trend Micro recommends frequently updating your pattern files. Scheduled updates can be used to conveniently and regularly update IM Security components.

Pattern File Numbering

To allow you to compare the current pattern file in your software products to the most current pattern file available from Trend Micro, pattern files have a version number.

The pattern file numbering system uses 7 digits, in the format xx.xxx.xx.

For the pattern file number 1.786.01:

- The first digit (1) indicates the new numbering system. (The second of two digits in this segment of the pattern file identifier will not be utilized until the number increases from 9 to 10.)
- The next three digits (786) represent the traditional pattern file number.
- The last two digits (01) provide additional information about the pattern file release.

Spyware Pattern

The Spyware Pattern identifies spyware/grayware in files and programs, modules in memory, Windows registry and URL shortcuts.

Trend Micro ActiveAction™

ActiveAction identifies virus/malware types and recommends actions based on how each type invades a computer system or environment. ActiveAction categorizes malicious code, replication, and payload types as viruses/malware. When a scan detects a virus or malware threat, it takes the recommended action on the virus/malware type to protect the environment's vulnerable points.

Tip

Trend Micro recommends using ActiveAction for users who are not familiar with the available scan actions or are not sure which scan action is suitable for a certain type of virus/malware.

Using ActiveAction provides the following benefits:

- **Time saving and easy to maintain**: ActiveAction uses scan actions recommended by Trend Micro. Users do not have to spend time configuring the scan actions.
- **Updateable scan actions**: Virus/malware writers constantly change the way viruses/malware attack computers. Trend Micro updates ActiveAction settings in each new pattern file to protect clients against the latest threats and the latest methods of virus/malware attacks.

IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files after enabling IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

IntelliScan™

IntelliScan optimizes scanning performance by examining file headers using true file type identification and scanning only file types associated with

malware risks. With true file type identification, IntelliScan identifies files disguised using false extension types.

IntelliScan provides the following benefits:

- **Performance optimization**: Using minimal system resources, IntelliScan does not affect the performance of crucial applications running on the host.
- **Shorter scanning period**: Using true file type identification, IntelliScan only scans files vulnerable to infection, significantly reducing scan times.

True File Type

Files can be easily renamed to disguise their actual type. Programs such as Microsoft Word are "extension independent". They will recognize and open "their" documents regardless of the file name. This poses a danger, for example, if a Word document containing a macro virus has been named "`benefits form.pdf`". Word will open the file, but the file may not have been scanned if IM Security is not set to check the true file type.

When set to IntelliScan, IM Security will confirm a file's true type by opening the file header and checking its internally registered data type.

Only files of that type that is actually capable being infected are scanned. For example, `.mid` files make up a large volume of all web traffic, but they are known not to be able to carry viruses. With true file type selected, once the true type has been determined, these inert file types are not scanned.

Protection Strategy

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

- What is the overall corporate IT security strategy?

- What are the available resources (processor, memory) on servers with Lync?
- Where and how can security risks and unwanted content enter the Lync Server environment (for example, file transfer, instant message)?

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

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

Note

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

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

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

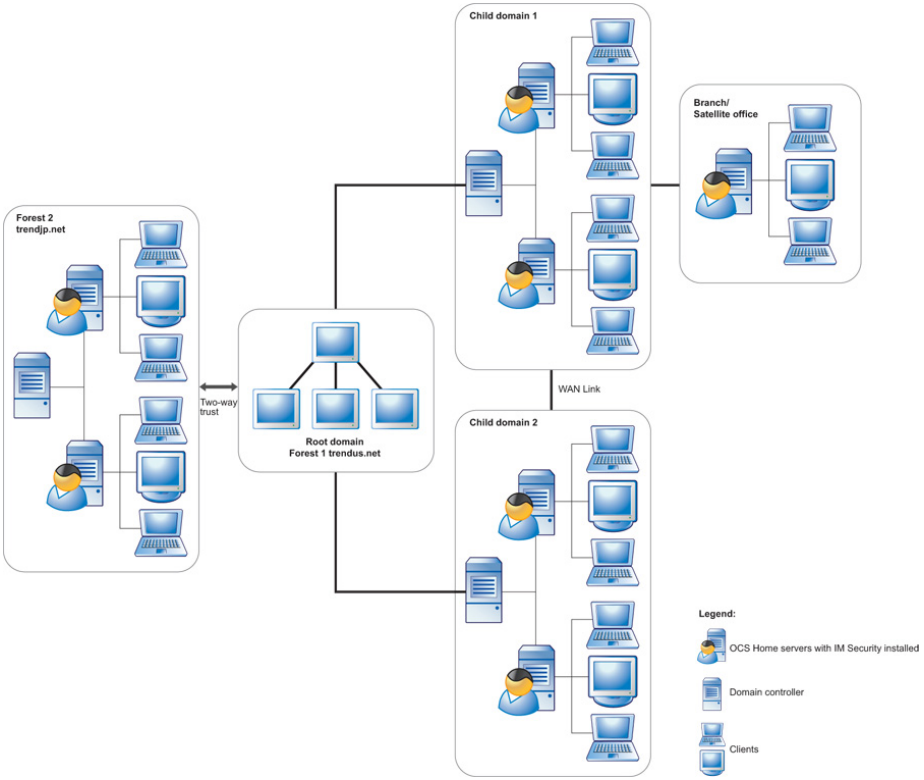


FIGURE 1-6. A sample protected Lync environment

Chapter 2

Getting Started with IM Security

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

Topics include:

The Product Console

The IM Security product console is a web-based console viewable using the Microsoft Internet Information Server (IIS). The product console allows administration of IM Security servers from any endpoint 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 later
- Mozilla Firefox 2.0 or later

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

Procedure

1. Click **Start** > **Programs** > **Trend Micro IM Security for Microsoft Lync Server** > **IM Security Product Console**.

   Note

   For Windows Server 2012 and later, an **IM Security Product Console** shortcut is created on the desktop.

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. SSL allows IM Security to encrypt the configuration data as it passes from the IM Security product console to the IM Security server. If the Microsoft IIS web server is selected during installation, IM Security supports HTTP or HTTPS.

Procedure

1. Access the web console using one of the following:

   - 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 16373 (default HTTPS port) is used, including the port number in the URL is not necessary.
     - `IMSecurity` is the IM Security website name.

     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:

     Type the following in your browser's address field to open the log on screen:

`http://{host name}:{port}/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 (16372), you must include the port number in the URL.

2. Type the user name and password in the fields provided.
3. Click **Log On**.

Server Management

Use the **Server Management** screen to complete the following tasks:

- Monitor server status

  The **Server Management** screen allows you to view the status of online IM Security servers available in a forest according to the following categories:

Category	Description
Pattern and engine version	Select **Pattern and engine version** to obtain information about the current virus pattern and virus scan engine. This category determines the servers with outdated components and prompts you to update components manually. For details, see *Configuring Manual Updates on page 2-12*.
Scan result	Select **Scan result** to obtain information about the total messages scanned and the scan results. Scan results also shows the number of blocked files, undesirable or sensitive content detections, and malicious URL detections.
Scan status	Select **Scan status** to determine whether IM Security features are enabled

CATEGORY	DESCRIPTION
Last replication	Select **Last replication** to view information about the replication process and results.

To view the server status:

On the **Server Management** screen, select the view category from the **Server Status For** list.

IM Security refreshes the window and displays the server information based on the category selected.

- Replicate server settings

  For details, see *Replicating Settings to Other Servers on page 2-5*.

Note

Disable your browser's pop-up blockers. Otherwise, the **Server Management** screen might not display.

IM Security populates the Server Management list by:

1. Querying the Global Catalog (GC) or local cache GC for the available Lync Servers in a forest
2. Determining whether the corresponding IM Security service per server has been installed

Note

If the service is not installed, IM Security does not include the server in the list.

Replicating Settings to Other Servers

If there are multiple IM Security servers in your environment, configure replication settings to copy settings from a source IM Security server to other servers with the same version and language.

Note

Ensure the compatibility of the source and target server(s).

Procedure

1. Click **Server Management** on the product console.

   The **Server Management** screen appears.

2. Click **Replicate**.

   The **Replication Settings** screen appears.

3. Select to replicate **All settings** or **Specific settings**.

   When replicating **Specific settings**, select from the following:

   - Communication Control
   - Virus Scan
   - File Blocking
   - Content Filtering for File Transfer Scan
   - Web Reputation for File Transfer Scan
   - Data Loss Prevention for File Transfer Scan
   - Content Filtering for Instant Message Scan
   - Web Reputation for Instant Message Scan
   - Data Loss Prevention for Instant Message Scan
   - ActiveUpdate
   - Alerts
   - Logs
   - Administration (Proxy, Notification Settings, World Virus Tracking
   - Disclaimer Settings
   - Control Manager Settings

4. Select **Quarantine, backup, and archive directories** to copy the directory paths.

Note

If you selected **Specific settings**, IM Security only replicates the directories related to the settings selected.

For example, if you selected **Virus Scan** but not **Content Filtering for File Transfer Scan**, only the Virus Scan directories get replicated. IM Security does not replicate the Content Filtering directories.

5. Click **Deploy**.

   IM Security replicates the specified settings from the source to the target servers.

6. Click **Go Back to Server Status** to go back to the **Server Management** 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 website.

http://olr.trendmicro.com

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.

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 during installation on the **Product Activation** screen or through the product console's **Product License** (**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, 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 2-1. Product Version Behaviors

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

Registering IM Security

Note

These web screens and procedures are subject to change without notice.

Procedure

1. Using a Web browser, go to **Trend Micro Online Registration** (http://olr.trendmicro.com).

   The **Online Registration** page of the Trend Micro website opens.

2. Perform one of the following:

   - If you already have an account with the **Online Registration** website, log on using your logon ID and password.
   - If you are a new customer, select your location and click **Continue** under **Not registered**.

3. On the **Enter Registration Key** page, type or copy the IM Security Registration Key, and then click **Continue**.

4. On the **License Agreement** page, read the license agreement and then click **I accept**.

5. On the **Confirm Product Information** page, click **Continue Registration**.

6. Fill out the online registration form, and then click **Submit**.

7. Click **OK** twice.

   After completing the registration, Trend Micro sends an email containing the AC, which you can then use to activate IM Security. Choose one the following options to activate IM Security:

   - During installation
   - After installation using the product console

Activating IM Security

Procedure

1. Go to **Administration** > **Product License**.

   The **Product License** screen appears.

2. Click **Enter New AC**.

3. Type the full version AC in **New Activation Code**.

4. Click **Save**.

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

About IM Security Updates

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

IM Security components available for updating are:

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

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

Updating IM Security - Prerequisite Tasks

Procedure

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

Configuring Proxy Settings

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

Procedure

1. Click **Administration** > **Proxy**.
2. Select **Use a proxy server for Web Reputation, updates, and product license notifications**. Select this check box to use a proxy server for web reputation queries to Trend Micro reputation servers, updates, and product license notifications.
3. Type the proxy server name or IP address.
4. Type the **Port**.
5. (Optional) Select **Use SOCKS 5 proxy protocol**.

6. If the proxy server requires authentication, specify the user name and password.

Configuring Manual Updates

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

Procedure

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

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

Configuring Scheduled Update

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

Procedure

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

      The **Update Source** screen appears.

b. Select a download source.

c. Click **Save**.

2. Set up your schedule.

   a. Click **Updates** > **Scheduled**.

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

   c. Set the **Update Schedule**.

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

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

3. Select the components for downloading from the update source.

   a. Select the components that IM Security downloads during each scheduled update.

   Tip

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

   b. Click **Save**.

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

Configuring the Download Source

To keep IM Security updated, you need to download the latest components. Use this page to set the source where IM Security receives the latest components. The default location is the Trend Micro ActiveUpdate server.

During manual or scheduled downloads, IM Security checks the location you specify here, and downloads the latest components from that source.

Procedure

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

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

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

  Download components from an Intranet source that receives updated components.

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

  Note

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

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

  Download components from an Internet or other source.

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

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

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

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

About IM Security Accounts

IM Security uses the following types of accounts to perform specific processes:

- *Database Accounts on page 2-15*
- *Trusted Contacts on page 2-16*

Database Accounts

IM Security uses the following database account.

- For SQL server authentication, IM Security uses the SQL user account to access and query logs from the IM Security database.
- For Windows authentication, IM Security uses the Windows user account which started the IM Security services to access and query logs from the IM Security database.

Trusted Contacts

Trusted Contacts apply to all types of file and content protection. The Trusted Contacts list defines the contacts who IM Security trusts globally, regardless of the Selected or Exempted Contacts list. Users that belong to the Trusted Contacts list will be automatically exempted from virus scans, blocking, and content filtering.

The Trusted Contacts list is a configurable list. The IM Security agent notification account, which is automatically created during installation, is the default entry in this list. Delegate trusted contacts by adding their SIP addresses as `TrustyAccounts` values for the `TM_LCSHookSetting` instance in IM Security Windows Management Infrastructure (WMI) property.

- Install WMI CIM Studio to edit IM Security classes, properties, qualifiers, and instances.

By default, IM Security adds the agent notification account in the Trusted Contacts list (see *Configuring Administrator Notification Settings on page 10-7*). Plan and designate the users that will belong in a list according to organizational needs.

Defining Trusted Contacts

Use a WMI tool such as CIM Studio to define Trusted Contacts.

CIM Studio is part of Windows Management Instrumentation (WMI) SDK 1.5. The WMI SDK is available for download at:

http://go.microsoft.com/fwlink/?LinkId=16798.

Procedure

1. Launch the WMI CIM Studio console.
2. Connect to the `root\trendmicro\imsecurity namespace`.
3. Expand `TM_LCSHookSetting` to display `TrustyAccounts`.
4. Add trusted contacts as values for `TrustyAccounts`.

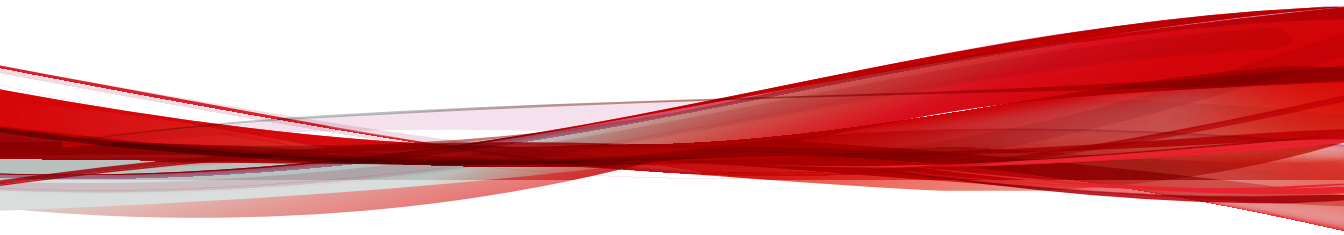
There is no limit to the number of trusted contacts that you can define. By default, IM Security adds the notification agent in the Trusted Contacts list.

WARNING!

Carefully consider the users in the Trusted Contacts list. Malicious users may relay unwanted content or propagate viruses/malware and spyware/grayware in your Lync Server environment through a trusted user.

Part II

Configuring Scans and Scan Filters



Chapter 3

Configuring Communication Control

This chapter explains how to configure the Communication Control feature for IM Security.

Topics include:

About Communication Control

The Communication Control feature allows you to manage the communication features granted to accounts at a company-wide or granular level, or you can limit the interactions between specific accounts. You may limit access to communication features during specified times when bandwidth or privacy is a concern.

Accounts that match a “Block” rule display an error message in the chat window and IM Security prevents any information sharing from occurring.

IM Security can control the following communication features:

- Instant message conversations
- File transfers
- Initiations of audio or video calls
- Sharing sessions (including Desktop, Program, Whiteboard, PowerPoint, Poll, and Q&A)

Enabling Communication Control Rules

Procedure

1. Go to **Communication Control**.

   The **Communication Control** screen appears.

2. Select **Enable Communication Control**.

3. Enable specific rules by changing the **Enabled** icon from disabled () to enabled ().

4. To change the order in which IM Security processes the rules:

   a. Select the check box beside a rule name and click **Change Priority**.

b. Under the **Priority** column, type the new priority for the rule in the text box that appears.

c. Click **Save** each time you want to change the priority for a rule.

5. Click **Save**.

Configuring a Communication Control Rule

Using Communication Control rules, you can manage the level of access that specific users or groups have when communicating through Lync. Configure granular or global permissions to communication features during specific times of the day.

Modify an existing rule by clicking the rule name.

Procedure

1. Go to the **Communication Control** > **Add** button.

   The **Communication Control > Add** screen appears.

2. Type the rule name.

3. Select the user, users, group, or groups affected by the rule.

   a. Select the type of contact to include in this rule.

      - **anyone**: This option applies the rule to all communication traffic (internal and external) passing through the Lync Server. The rule does not apply to user(s) or group(s) specified in the **Exceptions** list.

      - **in specific group**: Instructs IM Security to monitor triggered rules from users within a specific group (for example, the financial controller or Finance group).

      - **between groups**: Instructs IM Security to monitor rule matches when a user from one group communicates to a user from

another group (for example, users from “Security Group 1” and “Security Group 2”).

b. Beside any of the contact group headings (**Selected Contacts / Group1**, **Selected Contacts / Group2**, or **Exceptions**), click the **Edit** link.

The **Communication Control > Edit > Select Contact** screen appears.

For details on selecting Communication Control contacts and contact exceptions, see *Configuring Communication Control Contacts on page 3-6*.

4. Specify the **Time Settings** that apply to this rule.

- **From**: The date and time that the rule takes effect
- **No end date**: The rule does not expire
- **To**: The date and time that the rule expires

Note

After the rule expires, IM Security stops applying the rule to users. IM Security continues to apply any other lower priority rules to users as configured.

5. Under **Permissions**, specify whether to **Allow** or **Block** access to specific communication features during the specified times.

Feature	Description
Instant messaging	Specify if the selected accounts have permission to send and receive instant messages.
File transfers	Specify if the selected accounts have permission to send and receive files.
Audio/Video calls	Specify if the selected accounts have permission to send and receive audio/video.

Feature	Description
Desktop/App sharing	Specify if the selected accounts have permission to send and receive sharing sessions.

6. Select the person or people to send a notification to when IM Security detects a threat or policy detection (Administrator, Sender, or Recipient) and configure the notification options.

   - Specify any of the available notification methods (**Email**, **Instant message**, and **SNMP**).

     Note

     For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

     For details, see *Configuring Administrator Notification Settings on page 10-7*.

   - Modify the default message by clicking the **Settings** link.

     Note

     A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.

     Click **Save**.

7. Click **Save**.

Configuring Communication Control Contacts

Procedure

1. Go to the **Communication Control** > **Add** button.

   The **Communication Control > Add** screen appears.

2. Beside any of the contact group headings (**Selected Contacts / Group1**, **Selected Contacts / Group2**, or **Exceptions**), click the **Edit** link.

   The **Communication Control > Edit > Select Contact** screen appears.

3. Select specific users or groups to apply this rule to or exclude from this rule on the **Select Contact** screen.

   - To manually add a user or domain:
     a. Select **Type an address or domain** from the drop-down.
     b. Type the **sip** address or domain to add.
     c. Click **Add >**.
     d. Click **Save**.
   - To search for users or groups:
     a. Select **Search for users or groups** from the drop-down.
     b. Type the user or group you want to search for and click **Search**.
     c. Click a user or group in the search results list.
     d. Click **Add >**.
     e. Click **Save**.

Tip

To remove a user or group from the selected contacts list, click the remove icon.

Chapter 4

Configuring Virus Scans

This chapter explains how to configure the Virus Scan feature for File Transfer Scans.

Topics include:

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 transfers continually protects your instant messaging and Lync Server environments from potential security risks in incoming and outgoing files.

Enabling Virus Scan

Procedure

1. Go to **File Transfer Scan** > **Virus Scan**.
2. Select **Enable Virus Scan for File Transfer Scans**.
3. Click **Save**.

Configuring Virus Scan Targets

Procedure

1. Go to the **File Transfer Scan** > **Virus Scan** > **Target** tab.

   The **Target** tab displays.

2. Select one of the following for scanning:

   - **All scannable files**: IM Security scans for viruses/malware, worms, Trojans, and other malicious code in all files except unscannable

files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions. Other malicious code describes previously unknown threat types for which you want to configure a IM Security action.

- **IntelliScan**: IntelliScan uses Trend Micro recommended settings to perform an efficient scan.

  Note

  There is one key difference between using IntelliScan and performing other scans using IM Security true file type recognition. IM Security true file type recognition allows users to define their own selection of files to scan, while IntelliScan always uses the Trend Micro recommended selection of files to scan.

- **Specified file types**: Click the link to expand the list and select the files you want IM Security to scan. These files are "true file types". The scan engine examines the file header rather than the file name to ascertain the actual file type. Or, select to create a list of file extensions by selecting **Specified file extensions**.

  Note

  For example: If you click **Specified file types** and then click **Application and executables** > **Executable (.exe; .dll, .vxd)** then IM Security scans executable, DLL and VXD file types - even when the file has a false file extension name (is labeled `.txt` when it is actually an `.exe`). However, if you click **Specified file extensions** and type `.exe`, then IM Security scans only `.exe` type files. IM Security does not recognize falsely labeled file types.

3. To use IntelliTrap technology, select **Enable IntelliTrap**.

   For details on IntelliTrap scanning, see *IntelliTrap on page 1-15*.

4. To scan for spyware/grayware, select **Select all** for **Additional Virus Scanning** or select from the list.

5. Click **Compressed File Scan Restrictions** if performance improvement is required.

For details on compressed file restrictions, see *Virus Scan Compressed File Restrictions on page 4-6*.

Tip

Trend Micro recommends using scanning restrictions to protect against Denial-of-Service attacks. Denial-of-Service is an attack on a computer or network that causes a loss of 'service', namely a network connection. Typically, Denial-of-Service (DoS) attacks negatively affect network bandwidth or overload computer resources such as memory.

6. Click **Save**.

Configuring Virus Scan Actions

Procedure

1. Go to **File Transfer Scan** > **Virus Scan** > **Action**.

   The **Action** tab displays.

2. Select one of the following:

   - **ActiveAction**: Perform scan actions recommended by Trend Micro.
   - **Customized action for detected threats**: Select to perform an action over all security risks or specify an action for each threat.

TABLE 4-1. Virus Scan Actions

ACTION	DESCRIPTION
Quarantine	IM Security moves the file to a restricted access folder, removing it as a security risk. **Note** Trend Micro recommends using the default scan action "Quarantine" for viruses/malware.

Action	Description
Cancel file transfer	IM Security prevents the file transfer from occurring.
Deliver	IM Security delivers the file and records the detection.

3. To back up the infected file, select **Back up infected file before action is taken**.
4. Click the **Specify backup and quarantine directories** link to open the global **Directories** screen and then modify the folders where IM Security stores files.

   For details, see *Configuring Directories on page 10-3*.
5. Configure **Advanced Options** as necessary.
   a. Click the **Macros** heading to configure macro scan.
      i. Select **Enable advanced macro scan**.
      ii. Select one of the following:
         - **Heuristic level**
         - **Delete all macros detected by advanced macro scan**

   Note

   For details on configuring macro scanning, see *Configuring Macro Scanning on page 4-7*.

   b. Click the **Unscannable Message Parts** heading to specify actions for encrypted and password protected files and files not in the scan restriction criteria.
6. Click **Save**.

Compressed File Handling

Compressed files provide a number of special security concerns. Compressed files can be password-protected or encrypted, can harbor so-

called “zip-of-death” security risks, and can contain numerous layers of compression.

Compression Types

The IM Security scan engine can extract and scan files compressed using any of the most popular compression types (listed below). IM Security can also check for viruses/malware being "smuggled" within nested compressions, for example, an infected file that is zipped, ARJ-compressed, MS-compressed, and zipped again.

The maximum number of recursive scan layers is 20. You can configure this limit from **File Transfer Scan** > **Virus Scan** > **Target** > **Scan Restriction Criteria**.

TABLE 4-2. Supported Compression Types

- Archive created by LHA (`.lzh`)
- Archive created by Pkzip (`.zip`)
- Archive created by RAR (`.rar`)
- Archive created by Tar (`.tar`)
- ARJ Compressed archive (`.arj`)
- BINHEX (`.hqx`)
- GNU Zip (`.gz`; `.gzip`)
- LZW/Compressed 16bits (`.Z`)
- MacBinary (`.bin`)
- Microsoft Cabinet (`.cab`)
- Microsoft Compressed/MSCOMP
- MIME (`.eml`; `.mht`)
- Teledisk format (`.td0`)
- Unix BZ2 Bzip compressed file (`.bz2`)
- UUEncode (`.u`)
- WinAce (`.ace`)

Virus Scan Compressed File Restrictions

The following tables describes the compressed file restrictions available in IM Security.

TABLE 4-3. Virus Scan Compressed File Restrictions

SETTING	DESCRIPTION
Decompressed file count exceeds	Type a number to configure a restriction for the number of decompressed files that IM Security will scan. When the amount of decompressed files within the compressed file exceeds this number, then IM Security only scans files up to the limit set by this option.
Size of decompressed files exceeds	Type a number that represents the size limit in MB. IM Security only scans compressed files that are smaller or equal to this size after decompression.
Number of layers of compression exceeds	Type a number from 1-20. IM Security only scans compressed files that have less than or equal to the specified layers of compression. For example, if you set the limit to 5 layers of compression, then IM Security will scan the first 5 layers of compressed files, but not scan files compressed to 6 or more layers.
Size of decompressed file is "x" times the size of compressed file	IM Security only scans compressed files when the ratio of the size of the decompressed file compared to the size of the compressed file is less than or equal to this number. This function prevents IM Security from scanning a compressed file that might cause a Denial-of-Service (DoS) attack. A Denial-of-Service (DoS) attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing IM Security from scanning files that decompress into very large files helps prevent this problem from happening.

Configuring Macro Scanning

IM Security uses the virus pattern file to identify known malicious macro codes during regular virus scanning. IM Security takes action against malicious macro code depending on the action that you configure from the **Virus Scan** screen. Use advanced macro scanning to gain additional protection against malicious macro code.

Advanced macro scanning supplements regular virus scanning. It uses heuristic scanning to detect macro viruses/malware or strips all detected macro codes. Heuristic scanning is an evaluative method of detecting viruses

that uses pattern recognition and rules-based technologies to search for malicious macro code. This method excels at detecting undiscovered viruses and security risks that do not have a known virus signature. When a malicious macro code is detected using heuristic scanning, IM Security takes action against the malicious code based on the action that you configured from the **Virus Scan** screen. When you select **Delete all macros detected by advanced macro scan**, then IM Security strips all macro code from the scanned files.

Procedure

1. Go to **File Transfer Scan** > **Virus Scan** > **Action**.
2. Click **Advanced Options** and then click **Macros**.
3. Select **Enable advanced macro scan**.
4. Select a detection type:
   a. Select **Heuristic level** and configure a level for the heuristic rules.
      - Level 1 uses the most specific criteria, but detects the least macro codes.
      - Level 4 detects the most macro codes, but uses the least specific criteria and may falsely identify safe macro code as harboring malicious macro code.

      Tip

      Trend Micro recommends a heuristic scan level of 2. This level provides a high detection level for unknown macro viruses, a fast scanning speed, and it uses only the necessary rules to check for macro virus/malware strings. Level 2 also has a low level of falsely identifying malicious code in safe macro code.

   b. Select **Delete all macros detected by advanced macro scan** to have IM Security delete all of the macro codes that it detects.
5. Click **Save**.

Configuring Virus Scan Notifications

Procedure

1. Go to the **File Transfer Scan** > **Virus Scan** > **Notification** tab.

   The **Notification** tab displays.

2. Select the person or people to send a notification to when IM Security detects a threat or policy detection (Administrator, Sender, or Recipient) and configure the notification options.

   - Specify any of the available notification methods (**Email**, **Instant message**, and **SNMP**).

     Note

     For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

     For details, see *Configuring Administrator Notification Settings on page 10-7*.

   - Modify the default message by clicking the **Show details** control beside **Specify the message content**.

     Note

     A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.

3. Select **Write to Windows event log** to have IM Security write the notification to a Windows event log.

4. Click **Save**.

Chapter 5

Configuring File Blocking

This chapter explains how to configure the File Blocking feature for File Transfer Scans.

Topics include:

About File Blocking

The File Blocking feature of IM Security allows you to:

- Prevent the exchange of files between users based on specified file properties (file size, file name, extension, true file type)
- Save network bandwidth by limiting the size of files being transferred across IM Security servers through the default invitation layer rule

Enable File Blocking to evaluate files based on Trend Micro or user-defined rules.

IM Security provides the following default rules.

Default Rules	Default Settings
Default file size rule	• Works at the “invitation layer” (before IM Security downloads the file) • Cannot be deleted • Filter files according to file size • Action = Cancel file transfer
Default file extension rule	• Works at the “transfer layer” (after IM Security downloads the file) • Can be deleted • Filter files according to file extension name • Action = Cancel file transfer • Depending on your Windows Messenger version and Service Pack installed, some extension names are automatically blocked at the invitation layer. Refer to Windows Messenger documentation for details.

File Blocking works by determining a file's properties (size, type, and name). Once it determines the file's properties, it then compares them with the values specified for each rule. If one of the file's properties matches a value specified in a rule, IM Security takes the administrator specified action on

the file. IM Security also sends notifications to administrator specified recipients whenever it takes action.

Enabling File Blocking and the Default Rule

The “Default” File Blocking rule applies to “Anyone” and IM Security takes the “Cancel file transfer” action on files that exceed the specified limit. The Default rule applies to the invitation layer.

Procedure

1. Go to **File Transfer Scan** > **File Blocking**.
2. Select **Enable file blocking**.
3. In the File Blocking rule list, set the **File size limit** for the **[Default rule]** and specify the file size in **MB** or **KB**.
4. Enable specific rules by changing the **Enabled** icon from disabled () to enabled ().
5. To change the order in which IM Security processes the rules:
   a. Select the check box beside a rule name and click **Change Priority**.
   b. Under the **Priority** column, type the new priority for the rule in the text box that appears.
   c. Click **Save** each time you want to change the priority for a rule.

   Note

   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**.
6. Click **Save**.

Configuring a File Blocking Rule

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.

Create a new rule by clicking the **File Transfer Scan** > **File Blocking** > **Add** button.

Modify an existing rule by clicking **File Transfer Scan** > **File Blocking** > **[Rule name]**.

Configure File Blocking rules through the following four step process:

- *Selecting Contacts on page 5-4*
- *Configuring File Blocking Targets on page 5-6*
- *Configuring File Blocking Actions and Notifications on page 5-7*
- *Configuring a File Blocking Rule Name on page 5-8*

Note

After configuring a File Blocking rule, ensure that you enable the rule in the File Blocking rule list.

For details, see *Enabling File Blocking and the Default Rule on page 5-3*.

Selecting Contacts

Procedure

1. Go to **File Transfer Scan** > **File Blocking** > **Add**.

   The **File Blocking > Add rule: Contact** screen appears.

2. Select 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 Lync Server. The rule does not apply to user(s) or group(s) specified in the **Exceptions** list.
- **Specific user(s)/member(s) of a group**: Instructs IM Security to monitor rule violation from users within a specific group (for example, the financial controller or "Finance" group).
- **Session between user(s)/group(s)**: Instructs IM Security to monitor rule matches when a user from one group communicates to a user from another group (for example, users from "Security Group 1" and "Security Group 2").
- **Exceptions**: Click to specify users or group members to exclude from this rule.

Note

Ensure that you configure the exceptions for the user, users, group, or groups affected by the rule. IM Security does not apply exception lists configured for the other contact types to the rule.

3. Select specific users or groups to apply this rule to or exclude from this rule on the **Select Contact** screen.
   - To manually add a user or domain:
     a. Select **Type an address or domain** from the drop-down.
     b. Type the **sip** address or domain to add.
     c. Click **Add >**.
     d. Click **Save**.
   - To search for users or groups:
     a. Select **Search for users or groups** from the drop-down.
     b. Type the user or group you want to search for and click **Search**.
     c. Click a user or group in the search results list.

d. Click **Add >**.

e. Click **Save**.

Tip

To remove a user or group from the selected contacts list, click the remove icon.

4. Click **Next >**.

Configuring File Blocking Targets

Procedure

1. Go to **File Transfer Scan** > **File Blocking** > **Add**.
2. Go to the **Block files based on** screen.
3. Select the check box(es) next to the characteristics on which to block files.
   - **Type**: Click to specify the file types to block.
     a. Select to include or exclude the selected file types during scanning.
     b. Click **Save**.
   - **Name**: Click to specify the file extensions or file names to block.
     a. Select to include or exclude the specified file extensions or file names during scanning.
     b. Select **Specified file extensions** and type a specific file extension to block or allow.

Note

Click **Load recommended list** to use the list of Trend Micro recommended file extensions to block.

c. Select **Specified file names** and type the full file name and extension of files to block or allow.

d. Click **Save**.

- **File size**: Specify the file size that is the maximum, minimum, or exact file size that IM Security uses to block files.

4. Click **Next >**.

Configuring File Blocking Actions and Notifications

Procedure

1. Go to **File Transfer Scan** > **File Blocking** > **Add**.
2. Go to the **Delivery Option and Notifications** screen.
3. Specify the actions that IM Security takes on detections that match the rule criteria.
   - **Delivery Option**: Select to **Cancel file transfer** or **Deliver** files.
   - **Archive Option**: Select to **Archive** or **Do not archive** files.
4. Select the person or people to send a notification to when IM Security detects a threat or policy detection (Administrator, Sender, or Recipient) and configure the notification options.
   - Specify any of the available notification methods (**Email**, **Instant message**, and **SNMP**).

Note

For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

For details, see *Configuring Administrator Notification Settings on page 10-7*.

- Modify the default message by clicking the **Settings** link.

Note

A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.

Click **Save**.

5. Select **Write to Windows event log** to have IM Security write the notification to a Windows event log.
6. Click **Next >**.

Configuring a File Blocking Rule Name

Procedure

1. Go to **File Transfer Scan** > **File Blocking** > **Add**.
2. Go to the **Type the rule name** screen.
3. Type the rule name.
4. Click **Save**.

Editing a File Blocking Rule

Procedure

1. Go to **File Transfer Scan** > **File Blocking** > **[Rule name]**.

   The **File Blocking > Edit** screen appears.
2. Edit the rule criteria as necessary.

- To edit the **Contacts**, click the **Edit** link on the top-right corner of the **Select Contacts/Group** and **Exceptions** sections.
- To edit the **Notification** settings, click the **Settings** link beside the person you want to notify.

3. Click **Save**.

Chapter 6

Configuring Content Filtering

This chapter explains how to configure the Content Filtering feature for File Transfer Scans and Instant Message Scans.

Topics include:

About Content Filtering

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.

Enabling Content Filtering Rules

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Content Filtering**
   - **Instant Message Scan** > **Content Filtering**

   The **Content Filtering** screen appears.
2. Select **Enable Content Filtering for File Transfer Scan** or **Enable Content Filtering for Instant Message Scan**.
3. Enable specific rules by changing the **Enabled** icon from disabled () to enabled ().
4. To change the order in which IM Security processes the rules:
   a. Select the check box beside a rule name and click **Change Priority**.
   b. Under the **Priority** column, type the new priority for the rule in the text box that appears.

c. Click **Save** each time you want to change the priority for a rule.

5. Click **Save**.

Configuring a Content Filtering Rule

Using Content Filtering rules, you can prevent the exchange of messages and files that contain sexually explicit, racially offensive, or slanderous comments from one employee to another.

Create a new File Transfer Scan rule by clicking the **File Transfer Scan** > **Content Filtering** > **Add** button.

Create a new Instant Message Scan rule by clicking the **Instant Message Scan** > **Content Filtering** > **Add** button.

Modify an existing rule by clicking the rule name.

Configure Content Filtering rules through the following four step process:

- *Selecting Contacts on page 6-4*
- *Configuring Content Filtering Keyword Lists on page 6-5*
- *Configuring Content Filtering Actions and Notifications on page 6-13*
- *Configuring a Content Filtering Rule Name on page 6-14*

Note

After configuring a Content Filtering rule, ensure that you enable the rule in the Content Filtering rule list.

For details, see *Enabling Content Filtering Rules on page 6-2*.

Selecting Contacts

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Content Filtering** > **Add**
   - **Instant Message Scan** > **Content Filtering** > **Add**

   The **Contact** screen appears.
2. Select 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 Lync Server. The rule does not apply to user(s) or group(s) specified in the **Exceptions** list.
   - **Specific user(s)/member(s) of a group**: Instructs IM Security to monitor rule violation from users within a specific group (for example, the financial controller or "Finance" group).
   - **Session between user(s)/group(s)**: Instructs IM Security to monitor rule matches when a user from one group communicates to a user from another group (for example, users from "Security Group 1" and "Security Group 2").
   - **Exceptions**: Click to specify users or group members to exclude from this rule.

     Note

     Ensure that you configure the exceptions for the user, users, group, or groups affected by the rule. IM Security does not apply exception lists configured for the other contact types to the rule.
3. Select specific users or groups to apply this rule to or exclude from this rule on the **Select Contact** screen.
   - To manually add a user or domain:

a. Select **Type an address or domain** from the drop-down.

b. Type the **sip** address or domain to add.

c. Click **Add >**.

d. Click **Save**.

- To search for users or groups:

a. Select **Search for users or groups** from the drop-down.

b. Type the user or group you want to search for and click **Search**.

c. Click a user or group in the search results list.

d. Click **Add >**.

e. Click **Save**.

Tip

To remove a user or group from the selected contacts list, click the remove icon.

4. Click **Next >**.

Configuring Content Filtering Keyword Lists

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Content Filtering** > **Add**
   - **Instant Message Scan** > **Content Filtering** > **Add**
2. Go to the **Specify Keyword** screen.
3. To specify keywords, use the following controls:

- **Match**: Select **All specified keywords** or **Any specified keywords**.
- **Enter keyword(s)**: Type a keyword to add to the list.
- **Add**: Click to add the keyword to the list.
- **Delete**: Click to delete the selected keyword from the list.
- **Export**: Click to export keywords to a file.
- **Import**: Click to import keywords from a file.
- **Enable case-sensitive matching**: Select to make scans for keywords case-sensitive.
- **Match synonyms**: Select to match synonyms.
- **Show details**: Click to manage synonyms.

4. Click **Next >**.

Advanced Regular Expressions

Content Filtering keywords support regular expression declarations. See the following tables for more in-depth examples of regular expressions.

There are a number of websites and tutorials available online. One such site is the PerlDoc site, which can be found at:

http://www.perl.com/doc/manual/html/pod/perlre.html

TABLE 6-1. Counting and Grouping

ELEMENT	MEANING	EXAMPLE
.	The dot or period character represents any character (except the new line character).	`do.` matches: doe, dog, don, dos, dot `d..r` matches: deer, door

Element	Meaning	Example
*	The asterisk character means zero or more instances of the preceding element.	`do*` matches: d, do, doo, dooo, doooo
+	The plus sign character means one or more instances of the preceding element.	`do+` matches: do, doo, dooo, doooo but not d
?	The question mark character means zero or one instances of the preceding element.	`do?` matches: d or do but not doo, dooo
( )	Parenthesis characters group whatever is between them to be considered as a single entity.	`d(eer)+` matches: deer or deereer or deereereer The + sign is applied to the substring within parentheses, so the regular expression looks for “d” followed by one or more of the grouping “eer”.
[ ]	Square bracket characters indicate a set or a range of characters.	`d[aeiouy]+` matches: da, de, di, do, du, dy, daa, dae, dai The “+” sign is applied to the set within brackets, so the regular expression looks for “d” followed by one or more of any of the characters in the set “[aeioy].” `d[A-Z]` matches: dA, dB, dC, and so on up to dZ. The set in square brackets represents the range of all upper-case letters between A and Z.
[^]	Caret characters within square brackets logically negate the set or range specified, meaning the regular expression will match any character that is not in the set or range.	`d[^aeiouy]` matches: db, dc or dd, d9, d#--d followed by any single character except a vowel

Element	Meaning	Example
{ }	Curly brace characters set a specific number of occurrences of the preceding element. A single value inside the braces means that only that many occurrences will match. A pair of numbers separated by a comma represents a set of valid counts of the preceding character. A single digit followed by a comma means there is no upper bound.	`da{3}` matches: daaa--d followed by 3 and only 3 occurrences of “a” `da{2,4}` matches: daa, daaa, daaaa, and daaaa (but not daaaaa)--d followed by 2, 3, or 4 occurrences of “a” `da{4,}` matches: daaaa, daaaaa, daaaaaa--d followed by 4 or more occurrences of “a”.

Table 6-2. Shorthand Classes

Element	Meaning	Example
\d	Any digit character; functionally equivalent to [0-9] or [[:digit:]]	`\d` matches: 1, 12, 123, but not 1b7--one or more of any digit characters.
\D	Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]	`\D` matches: a, ab, ab&, but not 1--one or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.
\w	Any "word" character--that is, any alphanumeric character; functionally equivalent to [A-Za-z0-9] or [[:alnum:]]	`\w` matches: a, ab, a1, but not !&--one or more upper- or lower-case letters or digits, but not punctuation or other special characters.
\W	Any non-alphanumeric character; functionally equivalent to [^A-Za-z0-9] or [^ [:alnum:]]	`\W` matches: *, &, but not ace or a1--one or more of any character but upper- or lower-case letters and digits.

Element	Meaning	Example
\s	Any white space character; space, new line, tab, non-breaking space, and others; functionally equivalent to [[:space]]	`vegetable\s` matches: "vegetable" followed by any white space character So the phrase "I like a vegetable in my soup" would trigger the regular expression, but "I like vegetables in my soup" would not.
\S	Any non-white space character; anything other than a space, new line, tab, non-breaking space, and others; functionally equivalent to [^[:space]]	`vegetable\S` matches: "vegetable" followed by any non-white space character So the phrase "I like vegetables in my soup" would trigger the regular expression, but "I like a vegetable in my soup" would not.

Table 6-3. Character Classes

Element	Meaning	Example
[:alpha:]	Any alphabetic characters	`.REG. [[:alpha:]]` matches: abc, def, xxx, but not 123, @#$.
[:digit:]	Any digit character; functionally equivalent to \d	`.REG. [[:digit:]]` matches: 1, 12, 123
[:alnum:]	Any "word" character--that is, any alphanumeric character; functionally equivalent to \w	`.REG. [[:alnum:]]` matches: abc, 123, but not ~!@.

Element	Meaning	Example
[:space:]	Any white space character; space, new line, tab, non-breaking space; functionally equivalent to \s	`.REG. (vegetable)[[:space:]]` matches: "vegetable" followed by any white space character So the phrase "I like a vegetable in my soup" would trigger the regular expression, but "I like vegetables in my soup" would not.
[:graph:]	Any characters except space, control characters, or other similar characters	`.REG. [[:graph:]]` matches: 123, abc, xxx, ><", but not space or control characters.
[:print:]	Any characters (similar with [:graph:]) but includes the space character	`.REG. [[:print:]]` matches: 123, abc, xxx, ><", and space characters.
[:cntrl:]	Any control character (for example, CTRL + C, CTRL + X)	`.REG. [[:cntrl:]]` matches: 0x03, 0x08, but not abc, 123, !@#.
[:blank:]	Space and tab characters	`.REG. [[:blank:]]` matches: space and tab characters, but not 123, abc, !@#
[:punct:]	Punctuation characters	`.REG. [[:punct:]]` matches: ; : ? ! ~ @ # $ % & * ‘ “ , but not 123, abc
[:lower:]	Any lowercase alphabetic character **Note** **Enable case sensitive** matching must be enabled or else it will function as [:alnum:])	`.REG. [[:lower:]]` matches: abc, Def, sTress, Do, but not ABC, DEF, STRESS, DO, 123, !@#.

Element	Meaning	Example
[:upper:]	Any uppercase alphabetic character **Note** **Enable case sensitive** matching must be enabled or else it will function as [:alnum:])	`.REG. [[:upper:]]` matches: ABC, DEF, STRESS, DO, but not abc, Def, Stress, Do, 123, !@#.
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)	`.REG. [[:xdigit:]]` matches: 0a, 7E, 0f

Table 6-4. Pattern Anchor Regular Expressions

Element	Meaning	Example
^	Indicates the beginning of a string	`^(notwithstanding)` matches: Any block of text that begins with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would trigger the regular expression, but "The fact that I like vegetables in my soup notwithstanding" would not.
$	Indicates the end of a string	`(notwithstanding)$` matches: Any block of text that ends with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would not trigger the regular expression, but "The fact that I like vegetables in my soup notwithstanding" would.

TABLE 6-5. Escape Sequences and Literal Strings

ELEMENT	MEANING	EXAMPLE
\	"matches" Indicates that some characters match a special meaning in a regular expression (for example, +)	`.REG. C\/C\+\+` matches: 'C\C++' `.REG. \*` matches: * `.REG. \?` matches: ?
\t	Indicates a tab character (ASCII 0x09 character)	`(stress)\t` matches: Any block of text that contained the substring "stress" immediately followed by a tab.
\n	Indicates a new line character (ASCII 0x0A character) **Note** Different platforms represent a new line character differently. On Windows, a new line is a pair of characters, a carriage return followed by a line feed. On UNIX and Linux, a new line is just a line feed, and on Macintosh a new line is just a carriage return.	`(stress)\n\n` matches: Any block of text that contained the substring "stress" followed immediately by two new line characters.
\r	Indicates a carriage return character (ASCII 0x0D character)	`(stress)\r` matches: Any block of text that contained the substring "stress" followed immediately by one carriage return.

Element	Meaning	Example
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value)	`\x7E(\w){6}` matches: Any block of text containing a "word" of exactly six alphanumeric characters preceded with a ~ (tilde) character. Additional examples that will trigger a match: ~ab12cd and ~Pa3499.
\b	Indicates a backspace character	`(stress)\b` matches: Any block of text that contained the substring “stress” followed immediately by one backspace (ASCII 0x08) character

Configuring Content Filtering Actions and Notifications

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Content Filtering** > **Add**
   - **Instant Message Scan** > **Content Filtering** > **Add**
2. Go to the **Delivery Option and Notifications** screen.
3. Specify the actions that IM Security takes on detections that match the rule criteria.
   - **Delivery Option**:
     - **Cancel** the instant message or file transfer.
     - **Replace all** the content of an instant message.
     - **Deliver** the instant message or file transfer.
   - **Archive Option**: Select to **Archive** or **Do not archive** files.

4. Select the person or people to send a notification to when IM Security detects a threat or policy detection (Administrator, Sender, or Recipient) and configure the notification options.

   - Specify any of the available notification methods (**Email**, **Instant message**, and **SNMP**).

     Note

     For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

     For details, see *Configuring Administrator Notification Settings on page 10-7*.

   - Modify the default message by clicking the **Settings** link.

     Note

     A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.

     Click **Save**.

5. Select **Write to Windows event log** to have IM Security write the notification to a Windows event log.

6. Click **Next >**.

Configuring a Content Filtering Rule Name

Procedure

1. Go to one of the following:

- **File Transfer Scan** > **Content Filtering** > **Add**
- **Instant Message Scan** > **Content Filtering** > **Add**

2. Go to the **Type the rule name** screen.
3. Type the rule name.
4. Click **Save**.

Editing a Content Filtering Rule

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Content Filtering** > **[Rule name]**
   - **Instant Message Scan** > **Content Filtering** > **[Rule name]**
2. Edit the rule criteria as necessary.
   - To edit the **Contacts**, click the **Edit** link on the top-right corner of the **Select Contacts/Group** and **Exceptions** sections.
   - To edit the **Notification** settings, click the **Settings** link beside the person you want to notify.
3. Click **Save**.

Chapter 7

Configuring Web Reputation

This chapter explains how to configure the Web Reputation feature for File Transfer Scans and Instant Message Scans.

Topics include:

About Web Reputation Services

Web Reputation Services tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones.

Note

Because the process of configuring Web Reputation for file transfers and instant messages is the same, the configuration details for file transfers and instant messages are displayed together.

Connecting to Smart Protection Servers

By default, IM Security connects to the global Trend Micro Smart Protection Network when performing URL filtering. You can configure Web Reputation to query a local Smart Protection Server when performing URL filtering. Querying a local Smart Protection Server reduces the bandwidth required by Web Reputation compared to querying the Trend Micro Smart Protection Network.

Procedure

1. Install a Smart Protection Server on your network.
2. Add the following registry keys to the IM Security server using a registry editing program (for example, `regedit.exe`).

TABLE 7-1. Registry Keys that Support the Local Smart Protection Server

PARAMETER	TYPE	DESCRIPTION
`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security\CurrentVersion`		

PARAMETER	TYPE	DESCRIPTION
LwcsServerAddress	String	Server name or IP address of the local Smart Protection Server **Note** IM Security uses the provided server name or IP address when performing Web Reputation queries. If the registry key does not exist, Web Reputation queries the Trend Micro Smart Protection Network.
LwcsServerPort	DWORD	Port number of the local Smart Protection Server **Note** IM Security uses the default port number of 5274 if the registry key does not exist.

3. Restart the IM Security Server service.

Enabling Web Reputation

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Web Reputation**
   - **Instant Message Scan** > **Web Reputation**

   The **Web Reputation** screen displays.
2. Select **Enable Web Reputation for File Transfer Scan** or **Enable Web Reputation for Instant Message Scan**.
3. Click **Save**.

Configuring Web Reputation Targets

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Web Reputation**
   - **Instant Message Scan** > **Web Reputation**

   The **Web Reputation** screen displays.
2. Click the **Target** tab.
3. Select one of the following security levels:
   - **High**: Blocks a greater number of web threats but increases the risk of false positives.
   - **Medium**: Blocks most web threats while keeping the false positive count low.
   - **Low**: Blocks fewer web threats but reduces the risk of false positives.
4. Select **Enable approved URL list** to avoid scanning URLs deemed safe under your security policy.

   Note

   IM Security applies the same approved URL list to both File Transfer Scan and Instant Message Scan. A URL added to the list from Web Reputation for File Transfer Scan also applies to Web Reputation for Instant Message Scan.
5. Add approved URLs to the list.
6. Click **Save**.

Configuring Web Reputation Actions

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Web Reputation**
   - **Instant Message Scan** > **Web Reputation**

   The **Web Reputation** screen displays.
2. Click the **Action** tab.
3. Select from the following **Delivery Actions**:
   - Cancel the transmission:
     - **Cancel file transfer**: IM Security cancels the file transfer.
     - **Cancel instant message**: IM Security does not send the instant message.
   - **Replace all** (Instant Message Scan): The entire message will be replaced by the Trend Micro default message or a message that you define.
   - **Tag and deliver** (Instant Message Scan): The Trend Micro default message or a message that you define will be added to the beginning of the original message.
   - **Deliver**: Selecting this option allows the receiver to view the file or message and access the malicious URL.
4. Select to **Archive** or **Do not archive** files or instant messages.
5. Select **Take action on URLs that have not been assessed by Trend Micro** to treat URLs that have not been classified as suspicious URLs and perform the specified action.
6. Click **Save**.

Configuring Web Reputation Notifications

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **Web Reputation**
   - **Instant Message Scan** > **Web Reputation**

   The **Web Reputation** screen displays.
2. Click the **Notification** tab.
3. Select the person or people to send a notification to when IM Security detects a threat or policy detection (Administrator, Sender, or Recipient) and configure the notification options.
   - Specify any of the available notification methods (**Email**, **Instant message**, and **SNMP**).

     Note

     For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

     For details, see *Configuring Administrator Notification Settings on page 10-7*.
   - Modify the default message by clicking the **Show details** control beside **Specify the message content**.

     Note

     A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.
4. Select **Write to Windows event log** to have IM Security write the notification to a Windows event log.

5. Click **Save**.

Chapter 8

Configuring Data Loss Prevention

This chapter explains how to configure Data Loss Prevention data identifiers, templates, and policies for File Transfer Scans and Instant Message Scans.

Topics include:

About Data Loss Prevention (DLP)

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure.

Data Loss Prevention safeguards an organization's sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as file transfers and instant messages
- Enforce compliance to established privacy standards

Before you can monitor sensitive information for potential loss, you must be able to answer the following questions:

- What data needs protection from unauthorized users?
- Where does the sensitive data reside?
- How is the sensitive data transmitted?
- What users are authorized to access or transmit the sensitive data?
- What action should be taken if a security violation occurs?

This important audit typically involves multiple departments and personnel familiar with the sensitive information in your organization.

If you already defined your sensitive information and security policies, you can begin to define data identifiers and company policies.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure.

  For details, see *Expressions on page 8-3*.

- **Keyword lists**: A list of special words or phrases.

  For details, see *Keywords on page 8-8*.

Note

Administrators cannot delete a data identifier that a DLP template is using. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

Administrators can use predefined and customized expressions.

For details, see *Predefined Expressions on page 8-3* and *Customized Expressions on page 8-4*.

Predefined Expressions

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted.

Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/

  Note

  You can define regular expressions used in customized DLP expressions the same way as Content Filtering keyword lists. For details, see *Advanced Regular Expressions on page 6-6*.

- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expressions on page 8-5*.

Criteria for Customized Expressions

TABLE 8-1. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau • Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number • Expression: [^\d]([0123678]\d{8})[^\d] • Characters: 0123456789 • Minimum characters: 9 • Maximum characters: 9
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address • Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • Suffix characters: 0123456789- • Number of characters: 5 • Minimum characters in the expression: 25 • Maximum characters in the expression: 80

CRITERIA	RULE	EXAMPLE
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address • Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimum characters to the left: 3 • Maximum characters to the left: 15 • Maximum characters to the right: 30

Adding and Editing Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Expressions** tab.

3. Click **Add** or edit an expression by clicking the expression's name.

   A new screen displays.

4. Type a name for the expression.

   The name must not exceed 512 bytes in length.

5. Type a description that does not exceed 2048 bytes in length.

6. Type the expression and specify whether it is case-sensitive.

7. Type the displayed data.

For example, when creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and does not appear elsewhere in the product.

8. Choose one of the following criteria and configure additional settings for the chosen criteria:

   - **None**
   - **Specific characters**
   - **Suffix**
   - **Single-character separator**

9. Select an additional validation method if necessary.

   These additional validators were specifically designed to detect highly specialized digital assets.

10. Test the expression against an actual data.

    For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.

11. Click **Save**.

Tip

Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

Importing Expressions

Administrators with a properly-formatted `.dat` file containing the expressions can use this option. Generate the file by exporting the expressions from either the IM Security server on the current server or from another IM Security server.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Expressions** tab.

3. Click **Import** and then locate the `.dat` file containing the expressions.

4. Click **Open**.

   A message appears, indicating the status of the import.

Note

Each expression contains a unique ID value. If an expression with the same ID already exists, IM Security overwrites the existing expression.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure Data Loss Prevention to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 8-9* and *Customized Keyword Lists on page 8-9*.

Predefined Keyword Lists

Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meet your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before Data Loss Prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see *Customized Keyword List Criteria on page 8-9*.

Customized Keyword List Criteria

TABLE 8-2. Criteria for a Keyword List

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.
All keywords	A file must contain all the keywords in the keyword list.

CRITERIA	RULE
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If Data Loss Prevention detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK******************WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, usually results in a faster scanning time but only covers a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Adding and Editing Keyword Lists

Keywords are special words or phrases. Add related keywords to a keyword list to identify specific types of data. Create customized keyword lists if none of the predefined keyword lists meet the company's requirements.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Keyword Lists** tab.

3. Click **Add** or edit a keyword list by clicking the keyword list's name.

   A new screen displays.

4. Type a name for the keyword list.

   The name must not exceed 512 bytes in length.

5. Type a description that does not exceed 2048 bytes in length.

6. Choose one of the following criteria and configure additional settings for the chosen criteria:

   - **Any keyword**
   - **All keywords**
   - **All keywords within <x> characters**
   - **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:

   a. Type a keyword that is 3 to 512 bytes in length and specify whether it is case-sensitive.

   b. Click **Add**.

8. To delete keywords, select the keywords and click **Delete**.

9. Click **Save**.

Importing Keyword Lists

Use this option if you have a properly-formatted `.dat` file containing the keyword lists. You can generate the file by exporting the keyword lists from

either the IM Security server you are currently accessing or from another IM Security server.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Keyword Lists** tab.

3. Click **Import** and then locate the `.dat` file containing the keyword lists.

4. Click **Open**.

   A message appears, informing you if the import was successful.

   Note

   Each keyword list contains a unique ID value. If a keyword list with the same ID already exists, IM Security overwrites the existing keyword list.

About Data Loss Prevention Templates

Use Data Loss Prevention templates to tag and detect sensitive content by a set combination of data identifiers. A template combines data identifiers and operators (And, Or) in condition statements. When a set of data matches the criteria of a condition, Data Loss Prevention triggers a policy action. For example, a file containing data matching the All: Names from US Census Bureau AND US: HICN (Health Insurance Claim Number) templates, triggers the HIPAA policy.

Use Data Loss Prevention out-of-the-box templates for regulatory compliance initiatives, such as GLBA, PCI-DSS, SB-1386, US PII, and HIPAA. Companies can also create custom templates or modify existing templates to suit their business requirements. Companies that have preexisting, user-defined templates can import and export templates to maintain policy consistency throughout their organization.

Create company-specific templates after configuring DLP data identifiers or use the predefined templates.

Predefined DLP Templates

Data Loss Prevention comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA**: Gramm-Leach-Billey Act
- **HIPAA**: Health Insurance Portability and Accountability Act
- **PCI-DSS**: Payment Card Industry Data Security Standard
- **SB-1386**: US Senate Bill 1386
- **US PII**: United States Personally Identifiable Information

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Defining a Data Loss Prevention Template

Data Loss Prevention templates define an organization's sensitive data using keyword lists and expressions. Define templates to use in Data Loss Prevention policies and protect sensitive information that is company-specific. For more information on Data Loss Prevention Templates, see *About Data Loss Prevention Templates on page 8-12*.

Note

Administrators cannot modify a pre-packaged template. To use a pre-packaged template as the basis for a new template, select the check box beside the template name and click **Copy** in the Data Loss Prevention Template toolbar. This creates a new template with the suffix "Copy" at the end.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. Choose to create or modify a Data Loss Prevention Template.

   - To create a template, on the Data Loss Prevention Templates toolbar, click **Add**.
   - To modify a template, click the template name.

3. Type the **Name** of the template.

4. (Optional) Type a **Description** of the template.

5. From the drop-down box under **Condition Statement**, beside the (+) control, select the criteria **Expressions** or **Keyword Lists**.

6. Select an expression or keyword list from the drop-down box beside the selected criteria.

7. When adding **Expressions** criteria, type the number of **Occurrences** necessary for the template to trigger. This value designates the number of times an expression must be present in an email message before IM Security triggers an action.

   Note

   The **Occurrences** amount is a required value. The value cannot be zero (0) or blank.

8. Add additional criteria by clicking the (+) control. Remove criteria by clicking the (−) control.

9. When adding more than one template definition, select the **And** or **Or** operator from the drop-down box beside the condition in the **Condition Statement** list.

10. Click **Add** to add the condition to the **Template Definition** list or click **Clear** to clear the condition statement.

11. When adding more than one condition, select the **And** or **Or** operator from the drop-down box beside the template definition in the **Template Definition** list.

12. To remove a definition from the **Template Definition** list, click the delete icon ( ) to the right of the definition.

13. Click **Save**.

    The **Data Loss Prevention Templates** screen appears with the new template at the bottom of the Data Loss Prevention templates list.

Deleting a Data Loss Prevention Template

Note

Administrators cannot delete a pre-packaged DLP template or any templates associated with a company policy. Remove the template from all policies before deleting the template.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. Select the check box beside the template that you want to delete.

3. On the Data Loss Prevention Templates toolbar, click **Delete**.

Importing a Data Loss Prevention Template

Administrators can import Data Loss Prevention templates from other IM Security servers or other Trend Micro products to keep predefined rules consistent throughout the organization.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. On the Data Loss Prevention Templates toolbar, click **Import**.

   Note

   Each template contains a unique ID value. If a template with the same ID already exists, IM Security overwrites the existing template.

   The **Data Loss Prevention Import Template** screen appears.

3. Click the **Browse...** button, locate, and select the template file to import. Click **Open**.

4. Click **Import** to import the template file.

Exporting a Data Loss Prevention Template

You can export templates to other IM Security servers or other Trend Micro products to keep predefined rules consistent throughout your organization.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. Select the check box(es) next to the template name(s) that you want to export.

3. On the Data Loss Prevention Templates toolbar, click **Export**.

   A **File Download** dialog appears.

4. Click **Save**.

A **Save As** dialog appears.

5. Select a name and location for the export file. Click **Save**.

Note

Template files save in DAT format.

About Data Loss Prevention Policies

Data Loss Prevention policies allow companies to monitor the flow of sensitive information over the network. Policy rules, through use of Data Loss Prevention templates, help to manage the distribution of sensitive data across the network. Administrators can scale policies to apply to the entire company, groups, or specific endpoints.

Enabling Data Loss Prevention Policies

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **DLP Policies**
   - **Instant Message Scan** > **DLP Policies**

   The **DLP Policies** screen appears.
2. Select **Enable Data Loss Prevention for File Transfer Scan** or **Enable Data Loss Prevention for Instant Message Scan**.
3. Enable specific rules by changing the **Enabled** icon from disabled ( ) to enabled ( ).
4. To change the order in which IM Security processes the rules:
   a. Select the check box beside a rule name and click **Change Priority**.

b. Under the **Priority** column, type the new priority for the rule in the text box that appears.

c. Click **Save** each time you want to change the priority for a rule.

5. Click **Save**.

Configuring a Data Loss Prevention Policy

Using Data Loss Prevention policies, you can prevent the exchange of sensitive data in messages and files from transferring to destinations that may be security risks.

Create a new File Transfer Scan policy by clicking the **File Transfer Scan** > **DLP Policies** > **Add** button.

Create a new Instant Message Scan policy by clicking the **Instant Message Scan** > **DLP Policies** > **Add** button.

Modify an existing policy by clicking the policy name.

Configure Data Loss Prevention policies through the following four step process:

- *Selecting Contacts on page 8-18*
- *Configuring DLP Targets on page 8-20*
- *Configuring DLP Actions and Notifications on page 8-21*
- *Configuring a DLP Policy Name on page 8-22*

Selecting Contacts

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **DLP Policies** > **Add**

- **Instant Message Scan** > **DLP Policies** > **Add**

The **Contact** screen appears.

2. Select 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 Lync Server. The rule does not apply to user(s) or group(s) specified in the **Exceptions** list.
   - **Specific user(s)/member(s) of a group**: Instructs IM Security to monitor rule violation from users within a specific group (for example, the financial controller or "Finance" group).
   - **Session between user(s)/group(s)**: Instructs IM Security to monitor rule matches when a user from one group communicates to a user from another group (for example, users from "Security Group 1" and "Security Group 2").
   - **Exceptions**: Click to specify users or group members to exclude from this rule.

   Note

   Ensure that you configure the exceptions for the user, users, group, or groups affected by the rule. IM Security does not apply exception lists configured for the other contact types to the rule.

3. Select specific users or groups to apply this rule to or exclude from this rule on the **Select Contact** screen.

   - To manually add a user or domain:

     a. Select **Type an address or domain** from the drop-down.

     b. Type the **sip** address or domain to add.

     c. Click **Add >**.

     d. Click **Save**.

   - To search for users or groups:

a. Select **Search for users or groups** from the drop-down.

b. Type the user or group you want to search for and click **Search**.

c. Click a user or group in the search results list.

d. Click **Add >**.

e. Click **Save**.

Tip

To remove a user or group from the selected contacts list, click the remove icon.

4. Click **Next >**.

Configuring DLP Targets

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **DLP Policies** > **Add**
   - **Instant Message Scan** > **DLP Policies** > **Add**
2. Go to the **Templates** screen.
3. Select templates from the list of available templates and click **Add >>** to apply the templates to the policy.

Note

A Data Loss Prevention policy requires selecting at least one template before activation.

4. In the Available DLP Template(s) toolbar, click **Add** to create a new template or click **Import** to import a template file.

For details on adding templates, see *Defining a Data Loss Prevention Template on page 8-13*.

For details on importing templates, see *Importing a Data Loss Prevention Template on page 8-15*.

5. Click **Next >**.

Configuring DLP Actions and Notifications

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **DLP Policies** > **Add**
   - **Instant Message Scan** > **DLP Policies** > **Add**
2. Go to the **Delivery Option and Notifications** screen.
3. Specify the actions that IM Security takes on detections that match the rule criteria.
   - **Delivery Option**:
     - For File Transfer Scan, select **Cancel file transfer** or **Deliver**.
     - For Instant Message Scan, select **Cancel instant message**, **Replace all**, or **Deliver**.
   - **Archive Option**: Select to **Archive** or **Do not archive** files.
4. Select the person or people to send a notification to when IM Security detects a threat or policy detection (Administrator, Sender, or Recipient) and configure the notification options.
   - Specify any of the available notification methods (**Email**, **Instant message**, and **SNMP**).

Note

For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

For details, see *Configuring Administrator Notification Settings on page 10-7*.

- Modify the default message by clicking the **Settings** link.

Note

A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.

Click **Save**.

5. Select **Write to Windows event log** to have IM Security write the notification to a Windows event log.
6. Click **Next >**.

Configuring a DLP Policy Name

Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **DLP Policies** > **Add**
   - **Instant Message Scan** > **DLP Policies** > **Add**
2. Go to the **Type the rule name** screen.
3. Type the rule name.

4. Click **Save**.

Editing a DLP Policy

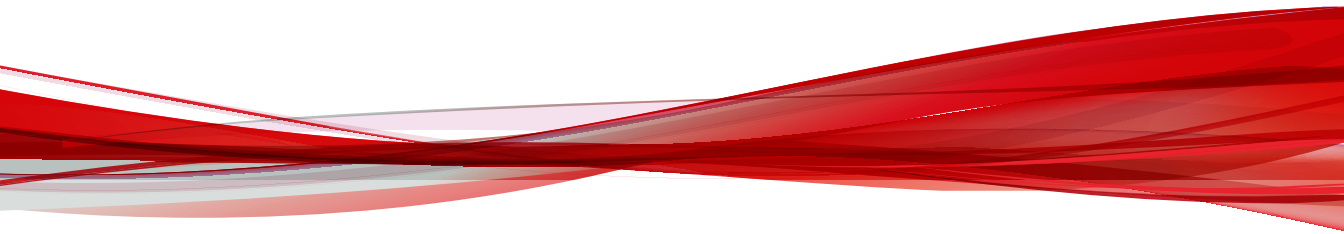
Procedure

1. Go to one of the following:
   - **File Transfer Scan** > **DLP Policies** > **[Policy name]**
   - **Instant Message Scan** > **DLP Policies** > **[Policy name]**
2. Edit the rule criteria as necessary.
   - To edit the **Contacts**, click the **Edit** link on the top-right corner of the **Select Contacts/Group** and **Exceptions** sections.
   - To edit the **Templates**, click the template name and **Add >>** to the **Selected DLP template(s)** list or **<< Remove** templates from the list.

     In the Available DLP Template(s) toolbar, click **Add** to create a new template (see *Defining a Data Loss Prevention Template on page 8-13*) or click **Import** to import a template file (see *Importing a Data Loss Prevention Template on page 8-15*).
   - To edit the **Notification** settings, click the **Settings** link beside the person you want to notify.
3. Click **Save**.

Part III

Managing IM Security



Chapter 9

Monitoring IM Security

This chapter describes notifications, reports, and logs to help you monitor your network.

Topics include:

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 **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.

Note

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.

Understanding Real-time Monitor

The Real-time Monitor displays information about one Lync Server in real time. Administrators can view IM Security scanning messages and the current count of any security risks detected on the server.

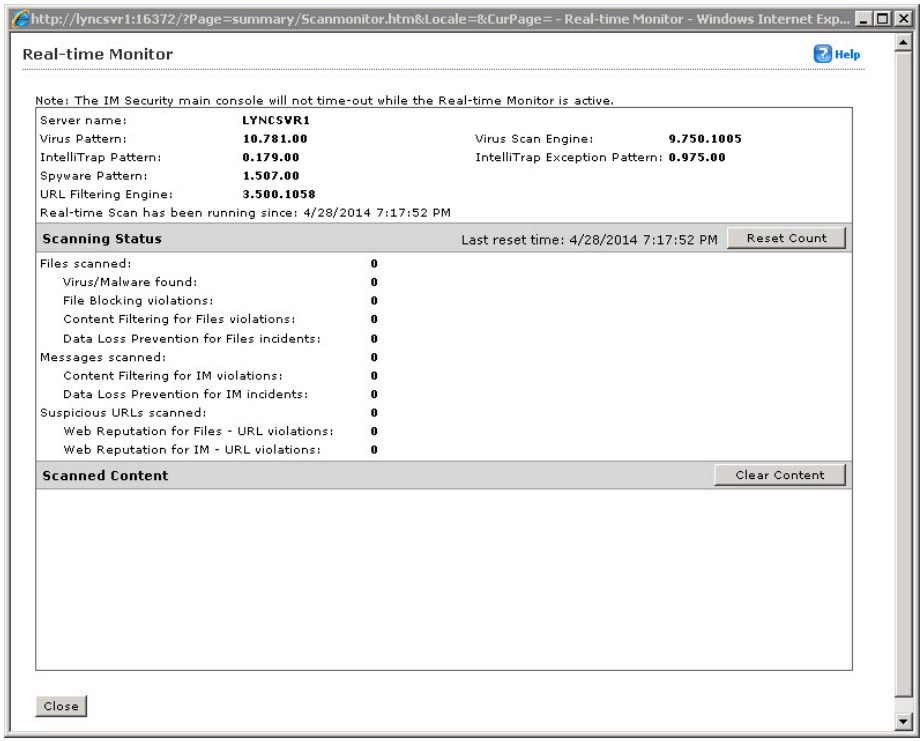


FIGURE 9-1. Real-time Monitor

A brief description of the options is available below.

- **Reset Count**: Resets all **Scanning Status** counts and messages scanned to zero and clears **Message Scanned** information
- **Clear Content**: Clears **Scanned Messages** information

- **Close**: Closes the screen

Viewing Real-time Monitor

Procedure

1. Access the server using the product console.
2. Click **Real-time monitor**.

   The **Real-time Monitor** screen opens.

Alerts

Alerts are messages regarding IM Security services, update status, or Lync Server events. Send alerts to network/server administrators and IT employees to inform them of system status, which are critical to network operations.

IM Security provides alerts for the following events.

TABLE 9-1. IM Security Alerts

ALERT	DESCRIPTION
IM Security services	
Services started unsuccessfully	Select to receive an alert each time the IM Security service was not started successfully.
Services stopped	Select to receive an alert each time the IM Security service stopped unexpectedly.
Component update is unsuccessful	Select to receive an alert each time an update is unsuccessful.
Excess session timeouts or scanning time	Select to receive an alert when the IM Security server is unable to manage an excessive amount of IM activity.

Alert	Description
Lync Server services	
Services stopped	Select to receive an alert each time the Lync Server services stopped unexpectedly.
Performance counter reaches high watermark	Select to receive an alert each time the Lync Server reported that the amount of IM activity reached the “high watermark” level as configured on the server.

Configuring Alerts

Note

To use System Center Operations Manager (SCOM), install the management pack found in the IM Security installation package and select **Write to Windows event log** in the **Recipients** tab for the alert settings.

Procedure

1. Go to **Alerts**.

   The **Alerts** screen appears.

2. On the **Conditions** tab, select the conditions that trigger IM Security to send an alert.

   For details on the conditions available, see *Alerts on page 9-4*.

3. On the **Recipients** tab, configure the recipients to whom IM Security send alerts.

   - **IM**: Specify the Instant Messaging address that IM Security notifies.

     Note

     IM Security is unable to send the notification to the recipient if the IM account is offline or the IM Security service is not running. To ensure that the intended recipient receives the alert, select the **Email** notification method instead.

- **Email**: Specify the email address that IM Security notifies.
- **SNMP**: Select to use the SNMP administrator settings.
- **Write to Windows event log**: IM Security writes the notification to a Windows event log.

Note

For Administrators, specify the administrator email address and instant messaging address in the text boxes provided, or configure the global administrator notification settings on the **Administrator Notification** screen.

For details, see *Configuring Administrator Notification Settings on page 10-7*.

4. On the **Message** tab, specify the message that the recipient receives whenever a condition is met.

Tip

A list of available message variable tokens displays to the left of the message body details. To insert a variable token in the message body, select the variable token and click the arrow button.

About Reports

IM Security reports refer to a collection of logs about virus and content security events that occur in the 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.

TABLE 9-2. Report Contents

REPORT	DESCRIPTION
Virus Scan	Virus Scan 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.
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.
Web Reputation for files	The Web Reputation for files 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.
Web Reputation for instant messages	The Web Reputation 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.
Data Loss Prevention for files	The Data Loss Prevention for files report shows information about the number of files detected that contained sensitive information. It shows the top violated rules, top rule violators, and the top violated templates for the specified time period.

Report	Description
Data Loss Prevention for instant messages	The Data Loss Prevention for instant messages report shows information about the number of instant messages detected that contained sensitive information. It shows the top violated rules, top rule violators, and the top violated templates for the specified time period.
Traffic	Traffic reports show the total number of instant messages and files delivered during a specific given period.

One-time Reports

Generate a one-time report to get a quick summary of IM Security information. The web console displays the report as soon as it is generated. Administrators can then print or send an email message of the one-time report.

IM Security saves generated reports in a cache for quick viewing at a later time. IM Security retains reports until the administrator manually deletes the report or IM Security deletes them by following the report maintenance settings.

Generating One-time Reports

Procedure

1. Click **Reports** > **One-time Reports** to open the **One-time Reports** screen.
2. Click **Generate report**.
3. Type a **Report name**.
4. Set the time range by typing a date or clicking the calendar icon to select a date.

   IM Security gathers data to include in the report for the specified time range.

Note

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

5. Click the type of information that IM Security includes in the report.

   Click the plus icon (+) next to the report type to view detailed options for that report.

6. Under **Format**, select the output format of the report.

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

8. Click **Generate**.

Scheduled Reports

IM Security generates scheduled reports according to the specified day and time. Administrators can configure IM Security to deliver reports by email message to an administrator or other recipient.

Scheduled reports follow a template. To generate individual scheduled reports, define the template and then IM Security generates reports according to that template. Specify the schedule and content included in each individual report for the report template. IM Security generates a report at the time specified in the template. Each template can have many individual reports that administrators can view by clicking **List Reports** from the **Scheduled Reports** screen. View the content of the template by clicking the template name.

Generating Scheduled Reports

Procedure

1. Click **Reports** > **Scheduled Reports** to open the **Scheduled Reports** screen.

2. Click **Add**.

   The **Schedule Reports > Add Report Template** screen opens to let you set up your report.

3. Type a name for the report template.

4. Specify the schedule that the template uses to generate individual reports.

   IM Security can generate reports on a daily, weekly, and monthly basis.

5. Specify the **Generate report at** time when the template generates the individual report.

   Note

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

   For example: After specifying the schedule to be weekly every Sunday and configuring the time for report generation to be 02:00, then IM Security uses the template to generate an individual report every Sunday at 02:00.

6. Select the type of report that IM Security generates according to the schedule.

7. Under **Format**, select the output format of the report.

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

9. Click **Add**.

   The browser returns to the **Scheduled Reports** screen. The new template is added to the list of report templates.

Report Maintenance

Configure the **Report Maintenance** screen to specify the number of reports that IM Security saves. For one-time reports and scheduled reports, type a

number. When the number of reports exceeds the specified limit, IM Security deletes excess reports, beginning with the oldest report. For scheduled reports saved in each template, the number specified limits the amount of saved reports for each template.

For example, there are five saved report templates. The limit for Scheduled reports saved in templates is 4. This means that each template can generate four individual reports, for a total of 20 reports (5 templates x 4 reports each). If a template generates another report, then IM Security deletes the oldest generated report for that template, keeping the total number of reports at 20.

A brief description of the options available on the **Report Maintenance** (**Reports** > **Maintenance**) screen is available below.

- **One-time reports**: Specify the maximum number of reports to save.
- **Scheduled reports saved in each template**: Specify the maximum number of reports to save.
- **Scheduled report template**: Specify the maximum number of report templates to save.

About 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 9-3. Log Types

LOG TYPE	DESCRIPTION
Virus Scan	Indicates the source of the infection or intrusion
File Blocking	Enumerates blocked files with matching File Blocking rules
Content Filtering for files logs	Enumerates files with matching Content Filtering rules
Content Filtering for IM logs	Enumerates messages with matching Content Filtering rules
Data Loss Prevention for files	Enumerates files that triggered Data Loss Prevention policies
Data Loss Prevention for IM	Enumerates messages that triggered Data Loss Prevention policies
Web Reputation for IM	Enumerates messages that contain web threats (malicious URL addresses)
Web Reputation for file	Enumerates files that contain web threats (malicious URL addresses)
Communication Control	Displays the contacts that triggered the “Block” action of a Communication Control policy
Update	Indicates the types of updates performed, including the result
Event tracking	Provides information about all console operations

Querying Logs

Procedure

1. Click **Logs** > **Query**.

   The **Log Query** screen displays.

2. Select the date range.

3. Select the type of entry.

4. (Optional) Specify any of the following criteria:

- **Contacts**: Type the specific contact names to display logs for and whether to **Search all contacts** or **Search matching sender**.
- **File name**: Specify the file name that triggered a File Transfer Scan policy.

5. Specify the option for **Sort by**.
6. Specify the number of items to display per page.
7. Click **Display Logs**.

Performing Manual Log Maintenance

WARNING!

IM Security also removes any corresponding quarantine, backup, and archive files related to the logs selected for deletion.

Procedure

1. Click **Logs** > **Maintenance**.

   The **Log Maintenance** screen displays.
2. Click the **Manual** tab.
3. Select the log types to delete.
4. Specify the number of days to keep logs before deleting.
5. Click **Delete Now** to delete logs and events.

Performing Scheduled Log Maintenance

WARNING!

IM Security also removes any corresponding quarantine, backup, and archive files related to the logs selected for deletion.

Procedure

1. Click **Logs** > **Maintenance**.

   The **Log Maintenance** screen displays.

2. Click the **Automatic** tab.
3. Select **Enable automatic maintenance**.
4. Select the log types to delete.
5. Specify the number of days to keep logs before deleting.
6. Click **Save**.

Chapter 10

Performing Administrative Tasks

This chapter describes administrative tasks.

Topics include:

Configuring Proxy Settings

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

Procedure

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

IM Security 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.

  Default directory: `<root>:\Program Files\Trend Micro\IM Security\quarantine\`

- **Backup Directory (Virus Scan)**: IM Security saves a copy of a file as a safety precaution designed to protect the original file from damage to the Backup directory before taking action on it.

  Default directory: `<root>:\Program Files\Trend Micro\IM Security\backup\`

- **Archive Directory (File Blocking)**: IM Security moves the file to the specified archive directory.

  Default directory: `<root>:\Program Files\Trend Micro\IM Security\archive\`

- **Archive Directory (File Transfer Content Filtering)**: IM Security moves the file to the specified archive directory.

  Default directory: `<root>:\Program Files\Trend Micro\IM Security\archive\`

- **Archive Directory (File Transfer Web Reputation)**: IM Security moves the file to the specified archive directory.

  Default directory: `<root>:\Program Files\Trend Micro\IM Security\archive\`

- **Archive Directory (File Transfer Data Loss Prevention)**: IM Security moves the file to the specified archive directory.

  Default directory: `<root>:\Program Files\Trend Micro\IM Security\archive\`

Configuring Directories

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 in the Quarantine and Backup directories.

Procedure

1. Go to **Administration** > **Directories**.

   The **Directories** screen appears.

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

   For example, for the quarantine directory type:

   ```
   c:\Program Files\Trend Micro\IMSecurity\quarantine
   ```

3. Click **Save**.

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 recategorize 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 recategorize 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.

Configuring Disclaimers for Internal and External Chat Sessions

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

Procedure

1. Go to **Administration** > **Disclaimer Settings**.

   The **Disclaimer Settings** screen appears.

2. Select the **Enable insertion of disclaimer into the initiation of an IM session** check box.

3. Click the **External Disclaimer** tab.

4. Type a disclaimer statement for external users or use the default statement.

5. Click the **Internal Disclaimer** tab.

6. Add internal users to the **Selected Internal Users** list.

7. Type a disclaimer statement for internal users or use the default statement.

Notification Settings

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

Alerts refer to messages that include IM Security service, update status, or Lync 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 scan events. Send notifications to administrators and Lync Server users to inform them of the scan, blocking, and filtering results.

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

TABLE 10-1. Alert and Notification Methods

METHOD	DESCRIPTION
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`.

Method	Description
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`. **Tip** Ensure the Internet Mail Service or Connector is set on the mail server when configuring IM Security to send notification to a POP3 account. For details, see *Email Notifications on page 13-9*.
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. 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 in the Windows event log. View logs by accessing **Start** > **Administrative Tools** > **Event Viewer** > **Application**

Configuring Administrator Notification Settings

From the **Administrator 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 Lync Server administrators, receive IM Security alerts or notifications and send email notifications to contacts who trigger a rule.

Procedure

1. Go to **Administration** > **Notification Settings**.

   The **Administrator Notification** screen appears.

2. Under **Notification Settings (Receiving)**, type the IM, email, and SNMP accounts that will receive notifications.

   Note

   Click **Apply to All** to instruct IM Security to use the same SIP and email addresses globally. IM Security removes the settings you set per screen and applies the new SIP and email addresses.

3. Under **Sender Settings**, type the email address that displays as the sender of the notification.

4. 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.

   Note

   IM Security uses its own account when sending email notifications. Set a descriptive display name along with an informative notification message to create awareness about the organization's security policy.

5. Click **Save**.

About Access Control

Use the role based administration feature to grant and control access to IM Security product console menu and submenu items. If there are multiple IM

Security administrators in the organization, this feature can help delegate management tasks to administrators and manage the menu items accessible to each administrator. Administrators can also grant non-administrators "view only" access to the product console.

Access Control Permissions

A brief description of the access control permissions (**Administration** > **Access Control** > **Permissions**) is available below.

- **Full**: Select to allow users in this group to enable, disable, and configure this feature.
- **Read**: Select to allow users in this group to view this feature and perform the following:

TABLE 10-2. Read Permissions

PERMISSION	DESCRIPTION
Updates	Operators can configure manual updates.
Logs	Operators can query logs.
Reports	Operators can generate logs.

- **None**: Select to hide this feature from users in this group.

Enabling Access Control

Procedure

1. Click **Administration** > **Access Control**.

   The **Access Control** screen displays.

2. Click the icon under **Status** to display a green check icon () which indicates that the access role is enabled. A red x icon () indicates the policy is disabled.

3. Select **Enable Single Sign-On** to allow log on with Microsoft™ Windows™ authentication.

   This feature is only supported with Microsoft™ Internet Explorer™. If Internet Explorer Enhanced Security is enabled, add the IM Security product console site to the Local intranet zone to use this feature.

4. Click **Save**.

Configuring Access Control

Procedure

1. Click **Administration** > **Access Control**.

   The **Access Control** screen displays.

2. Click one of the following access control roles:

   - **Administrator**
   - **Operator**

3. Click the **Authentication** tab.
4. Specify the description for the group.
5. Add accounts from Active Directory using **Search**.
6. Click **Save**.
7. Click the **Permissions** tab.
8. Select the permissions for this group.
9. Click **Save**.

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.

Renewing the Product License

When your license expires, IM Security continues to protect your Lync 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.

Procedure

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.
4. If you have received an Activation Code and want to manually renew the product license:
   a. Go to **Administration** > **Product License**.

      The **Product License** screen appears.

   b. Click **Enter New AC**.
   c. Type the Activation Code in the **New activation code** field.
   d. Click **Save**.

World Virus Tracking Program

Trend Micro World Virus Tracking Program provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. Each new threat identified through a single customer's routine reputation check automatically updates all of Trend Micro's threat databases, blocking any subsequent customer encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security. This is much like an automated neighborhood watch that involves the community in the protection of others. The privacy of a customer's personal or business information is always protected because the threat information gathered is based on the reputation of the communication source.

Trend Micro World Virus Tracking Program collects and transfers relevant data from Trend Micro products to the Smart Protection Network for further analysis, and consequently, advanced solutions evolve. These advanced solutions further enhance the protection for clients.

Some samples of information sent to Trend Micro:

- File checksums
- Websites accessed
- File information, including sizes and paths
- Names of executable files

You can terminate your participation to the program anytime from the web console.

Tip

You do not need to participate in World Virus Tracking Program to protect your computers. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in World Virus Tracking Program to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Joining the World Virus Tracking Program

Procedure

1. Click **Administration** > **World Virus Tracking**.
2. Click the **Virus Map** to view worldwide scanning results and statistics.
3. Select **Yes**.
4. Click **Save**.

About Trend Micro Control Manager

Trend Micro™ Control Manager™ is a software management solution that provides the capability to control antivirus and content security programs from a central location-regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus/malware and content security policy.

- **Control Manager server**: The Control Manager server is the machine upon which the Control Manager application is installed. The web-based Control Manager management console is generated on this server.
- **Agent**: The agent is an application installed on a product-server that allows Control Manager to manage the product. It receives commands from the Control Manager server, and then applies them to the managed product. It also collects logs from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.
- **Communicator**: The Communicator is the communications backbone of the Control Manager system; it is part of the Trend Micro Management Infrastructure. Commands from the Control Manager server to the managed products, and status reports from the products to the Control Manager server all pass through this component. Only one Communicator is installed on each product server; the Communicator then handles the needs of all the agents on the aforementioned server.
- **Entity**: An entity is a representation of a managed product on the Product Directory link. You see these icons in the directory tree of the Entity section. The directory tree is a composition of all managed entities, residing on the Control Manager console.

About Trend Micro Management Communication Protocol

Trend Micro™ Management Communication Protocol (MCP) is the next generation agent for Trend Micro managed products. Management Communication Protocol (MCP) replaces Trend Micro Infrastructure (TMI)

as the way Control Manager communicates with Trend Micro IM Security. MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and Two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Using IM Security with Control Manager

- Multiple IM Security servers can share the same configurations by using Trend Micro Control Manager (TMCM).
- Control Manager 6.0 SP1 permits administrators to configure and deploy Data Loss Prevention policies (rules) directly to IM Security servers from the Control Manager web console.
- Administrators can also use Control Manager to synchronize virus pattern file and other downloads (Control Manager contacts Trend Micro through the Internet; Control Manager then distributes the updates to the various instances of IM Security through the Intranet).
- Unless included as part of a Control Manager domain, each instance of IM Security on the network updates its own virus pattern file and other updates.

For more information, see the Control Manager documentation.

Registering to Control Manager

Administrators can manage IM Security using the Trend Micro Control Manager management console. However, administrators must first install a Control Manager agent on the IM Security server (during IM Security

installation or using the web console) and then register the agent with the Control Manager server.

Procedure

1. Click **Administration** > **Control Manager Settings**.

   The **Control Manager Settings** screen displays.

2. Under **Connection Settings**, type the name of the IM Security server in the **Entity display name** field.

3. Under **Control Manager Server Settings** specify the following:

   a. Type the Control Manager server IP address or host name in the **Server FQDN or IP address** field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

   c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products), select **Connect through HTTPS**.

   d. If the network requires authentication, type the user name and password for the IIS server in the **Username** and **Password** fields.

   e. If using a NAT device, select **Enable two-way communication port forwarding** and type the NAT device's IP address and port number in **IP address** and **port number**.

   Refer to the *Trend Micro Control Manager Administrator's Guide* for more information about managing products in Control Manager.

Unregistering IM Security from Control Manager

Note

During Outbreak Prevention, administrators cannot unregister from Control Manager or disable communication between the IM Security MCP agent and the Control Manager server.

Procedure

1. Click **Administration** > **Control Manager Settings**.

   The **Control Manager Settings** screen displays.

2. Under **Connection Status**, click **Unregister**.

   A progress screen displays.

Using the Debug Logs

IM Security Debugger can assist you in debugging or reporting the status of the IM Security processes. When you are having unexpected difficulties, you can use the debugger to create debugger reports and send them to Trend Micro technical support for analysis.

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

- For the IM Security server: `servIMSHost.log` or `servIMSHost.log.#`
- **Trend Micro IM Security System Attendant service**
- For Control Manager Agent: `servCmAgentHost.log` or `servCmAgentHost.log.#`

Note

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:

```
<root>:\Program Files\Trend Micro\IM Security\Debug
```

Procedure

1. Go to **Administration** > **Debug Logs**.

   The **Debug Logs** screen appears.

2. Select the modules to debug:

   - **Trend Micro IM Security Server**
   - **Trend Micro IM Security System Attendant service**
   - **Trend Micro Control Manager Agent**

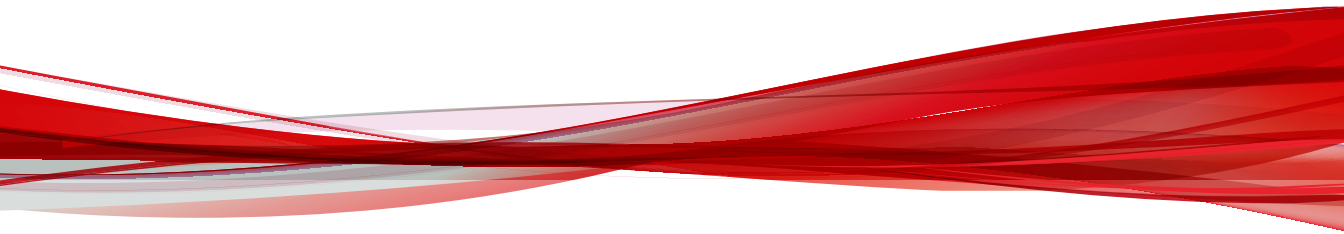
3. Click **Apply**.

   Note

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

Part IV

Getting Help



Chapter 11

Understanding Security Risks

This chapter describes security risks to help you understand possible risks to your network.

Topics include:

Understanding the Terms

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a list of these terms and their meanings as used in this document.

Some of these terms refer to real security risks and some refer to annoying or unsolicited incidents. Trojans, viruses/malware, and worms are examples of terms used to describe real security risks. Joke programs, spyware/grayware are terms used to describe incidents that might be harmful, but are sometimes simply annoying and unsolicited. IM Security can protect against all of the incidents described in this chapter.

About Internet Security Risks

Thousands of viruses/malware are known to exist, with more being created each day. In addition to viruses/malware, new security risks designed to exploit vulnerabilities in corporate email systems and websites continue to emerge. These include spyware/grayware, phish sites, network viruses/malware, Trojans, and worms.

Collectively, these threats are known as security risks. Here is a summary of the major security risk types:

TABLE 11-1. Internet Security Risks

THREAT TYPE	CHARACTERISTICS
Advanced threats	Advanced threats use less conventional means to attack or infect a system. Heuristic scanning can detect advanced threats to mitigate the damage to company systems. Some types of advanced threats that ATSE detects include: • Advanced Persistent Threats (APT): Advanced persistent threats are attacks against targeted companies and resources. Typically, a social engineering attack on an employee triggers a series of activities that open up the company to serious risks. • Targeted attacks: Targeted attacks refer to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. These attacks seek to maintain a persistent presence within the target's network so that the attackers can move laterally and extract sensitive information. • Exploits: Exploits are code purposely created by attackers to abuse or target a software vulnerability. This code is typically incorporated into malware. • Zero-day attacks: Zero-day attacks exploit previously unknown vulnerabilities in software.
Denial-of-Service (DoS) attack	A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing IM Security from scanning files that decompress into very large files helps prevent this problem from happening.
Phish	Unsolicited email requesting user verification of private information, such as credit card or bank account numbers, with the intent to commit fraud.
Spyware/Grayware	Technology that aids in gathering information about a person or organization without their knowledge.

Threat Type	Characteristics
Trojan Horse program	Malware that performs unexpected or unauthorized, often malicious, actions. Trojans cause damage, unexpected system behavior, and compromise system security, but unlike viruses/malware, they do not replicate.
Virus/Malware	A program that carries a destructive payload, and replicates - spreading quickly to infect other systems. By far, viruses/malware remain the most prevalent threat to computing.
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, typically through network connections or email attachments.
Other malicious codes	IM Security detects some malicious code that is difficult to categorize, but pose a significant threat to Exchange. This category is useful when you want IM Security to perform an action against a previously unknown threat type.
Packed files	Potentially malicious code in real-time compressed executable files that arrive as email attachments. IntelliTrap scans for packing algorithms to detected packed files. Enabling IntelliTrap allows IM Security to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Viruses/Malware

A computer virus/malware is a segment of code that has the ability to replicate by infecting files. When a virus/malware infects a file, it attaches a copy of itself to the file in such a way that when the former executes, the virus/malware also runs. When this happens, the infected file also becomes capable of infecting other files. Like biological viruses, computer viruses/malware can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses/malware share another commonality: a damage routine that delivers a 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.

Generally, there are three kinds of viruses/malware:

TABLE 11-2. Types of Virus/Malware

TYPE	DESCRIPTION
File	File viruses/malware may come in different types—there are DOS viruses/malware, Windows viruses/malware, macro viruses/malware, and script viruses/malware. All of these share the same characteristics of viruses/malware except that they infect different types of host files or programs.
Boot	Boot viruses/malware infect the partition table of hard disks and boot sector of hard disks and floppy disks.
Script	Script viruses/malware are viruses/malware written in script programming languages, such as Visual Basic Script and JavaScript and are usually embedded in HTML documents. VBScript (Visual Basic Script) and Jscript (JavaScript) viruses/malware make use of Microsoft's Windows Scripting Host to activate themselves and infect other files. Since Windows Scripting Host is available on Windows 98, Windows 2000 and other Windows operating systems, the viruses/malware can be activated simply by double-clicking a `*.vbs` or `*.js` file from Windows Explorer. What is so special about script viruses/malware? Unlike programming binary viruses/malware, which requires assembly-type programming knowledge, virus/malware authors program script viruses/malware as text. A script virus can achieve functionality without low-level programming and with code as compact as possible. It can also use predefined objects in Windows to make accessing many parts of the infected system easier (for example, for file infection, for mass-mailing). Furthermore, since the code is text, it is easy for others to read and imitate the coding paradigm. Because of this, many script viruses/malware have several modified variants. For example, shortly after the "I love you" virus appeared, antivirus vendors found modified copies of the original code, which spread themselves with different subject lines, or message bodies.

Whatever their type is, the basic mechanism remains the same. A virus contains code that explicitly copies itself. In the case of file viruses/malware, this usually entails making modifications to gain control when a user accidentally executes the infected program. After the virus code has finished

execution, in most cases, it passes back the control to the original host program to give the user an impression that nothing is wrong with the infected file.

Take note that there are also cross-platform viruses/malware. These types of viruses/malware can infect files belonging to different platforms (for example, Windows and Linux). However, such viruses/malware are very rare and seldom achieve 100% functionality.

Virus/Malware Writers

In the traditional scenario, it was an individual, highly technical and working alone, who would write a virus/malware program and then introduce it onto a computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations.

Now, however, it takes no special skill to create a macro virus/malware, a mass mailer, or other virus/malware with highly disruptive potential. In fact, "virus kits" proliferate on the Internet and are free for the taking for anyone who wants to try their hand at disrupting the Internet or corporate communications.

And increasingly, organized crime from remote countries is getting into the act by creating sophisticated spyware/grayware programs and phish sites. Distributed through a million spam messages, these exploits are low effort but with a high potential for yielding personal information such as passwords, social security numbers, and credit card numbers.

Malware Naming

Malware, with the exception of boot sector viruses and some file infectors, is named according to the following format:

```
PREFIX_THREATNAME.SUFFIX
```

The suffix used in the naming convention indicates the variant of the threat. The suffix assigned to a new threat (meaning the binary code for the threat is not similar to any existing security risks) is the alpha character "A." Subsequent strains are given subsequent suffixes, for example, "B", "C", "D".

Occasionally a threat is assigned a special suffix, (`.GEN`, for generic detection or `.DAM` if the variant is damaged or malformed).

Prefix	Description
No prefix	Boot sector viruses or file infector
1OH	File infector
ADW	Adware
ALS	Auto-LISP script malware
ATVX	ActiveX malicious code
BAT	Batch file virus
BHO	Browser Helper Object - A non-destructive toolbar application
BKDR	Backdoor virus
CHM	Compiled HTML file found on malicious websites
COOKIE	Cookie used to track a user's web habits for the purpose of data mining
COPY	Worm that copies itself
DI	File infector
DIAL	Dialer program
"DOS, DDOS"	Virus that prevents a user from accessing security and antivirus company websites
ELF	Executable and Link format viruses
EXPL	Exploit that does not fit other categories
FLOODER	Tool that allows remote malicious hackers to flood data on a specified IP, causing the target system to hang
FONO	File infector
GCAE	File infector

Prefix	Description
GENERIC	Memory-resident boot virus
HKTL	Hacking tool
HTML	HTML virus
IRC	Internet Relay Chat malware
JAVA	Java malicious code
JOKE	Joke program
JS	JavaScript virus
NE	File infector
NET	Network virus
PALM	Palm PDA-based malware
PARITY	Boot virus
PE	File infector
PERL	Malware, such as a file infector, created in PERL
RAP	Remote access program
REG	Threat that modifies the system registry
SPYW	Spyware
SYMBOS	Trojan that affects telephones using the Symbian operating system
TROJ	Trojan
UNIX	Linux/UNIX script malware
VBS	VBScript virus
WORM	Worm
W2KM, W97M, X97M, P97M, A97M, O97M, WM, XF, XM, V5M	Macro virus

Compressed Files

Compression and archiving are among the most common methods of file storage, especially for file transfers - such as email attachments, FTP, and HTTP. Before any virus/malware detection can occur on a compressed file, however, you must first decompress it. For other compression file types, IM Security performs scan actions on the whole compressed file, rather than individual files within the compressed file.

IM Security currently supports the following compression types:

- Extraction: used when multiple files have been compressed or archived into a single file: PKZIP, LHA, LZH, ARJ, MIME, MSCF, TAR, GZIP, BZIP2, RAR, and ACE.
- Expansion: used when only a single file has been compressed or archived into a single file: PKLITE, PKLITE32, LZEXE, DIET, ASPACK, UPX, MSCOMP, LZW, MACBIN, and Petite.
- Decoding: used when a file has been converted from binary to ASCII, a method that is widely employed by email systems: UUENCODE and BINHEX.

Note

When IM Security does not support the compression type, then it cannot detect viruses/malware in compression layers beyond the first compression layer.

When IM Security encounters a compressed file it does the following:

1. IM Security extracts the compressed files and scans them.

   IM Security begins by extracting the first compression layer. After extracting the first layer, IM Security proceeds to the second layer and so on until it has scanned all of the compression layers that the user configured it to scan, up to a maximum of 20.

2. IM Security performs a user-configured action on infected files.

   IM Security performs the same action against infected files detected in compressed formats as for other infected files. For example, if you select

Quarantine as the action for infected files, then IM Security quarantines entire files in which it detects the threat.

Joke Programs

A joke program is an ordinary executable program with normally no malicious intent. Virus authors create joke programs for making fun of computer users. They do not intend to destroy data but some inexperienced users may inadvertently perform actions that can lead to data loss (such as restoring files from an older backup, formatting the drive, or deleting files).

Since joke programs are ordinary executable programs, they will not infect other programs, nor will they do any damage to the computer system or its data. Sometimes, joke programs may temporarily reconfigure the mouse, keyboard, or other devices. However, after a joke program finishes its execution or the user reboots the machine, the computer returns to its original state. Joke programs, while normally harmless, can be costly to an organization.

Macro Viruses/Malware

Macro viruses/malware are application-specific. They infect macro utilities that accompany such applications as Microsoft Word (`.doc`) and Microsoft Excel (`.xls`). Therefore, they can be detected in files with extensions common to macro capable applications, such as `.doc`, `.xls`, and `.ppt`. Macro viruses/malware travel between data files in the application and can eventually infect hundreds of files if undeterred.

As these file types are often attached to email messages, macro viruses/malware spread readily by means of the Internet in email attachments.

IM Security prevents macro viruses/malware from infecting your server in the following ways:

- Detects malicious macro code using heuristic scanning

  Heuristic scanning is an evaluative method of detecting viruses/malware. This method excels at detecting undiscovered viruses/malware and threats that do not have a known virus signature.

- Strips all macro code from scanned files

Trojan Horse Programs

A Trojan is a type of threat named after the Trojan Horse of Greek mythology. Like the Greek Trojan Horse, a Trojan network threat has malicious intent, hidden within its code. While a Trojan may appear innocent, executing a Trojan can cause unwanted system problems in operation, lost data, and loss of privacy.

For example, a Trojan called "happy birthday" might play a song and display an animated dance on your screen, while at the same time opening a port in the background and dropping files that lets malicious hackers take control of the computer for whatever scheme or exploit he or she may have in mind. One common scheme is to hijack the computer for distributing spam. Another is to collect keystrokes and send them, along with all the data they contain, to the malicious hacker.

Trojans are not viruses/malware. Unlike viruses/malware, they do not infect files, and they do not replicate. The scan engine detects and logs these threats and can take whatever action you specify.

With Trojans, however, simply deleting or quarantining is often not enough to rid your system of the Trojan's effects. You must also clean up after it; that is, remove any programs that may have been copied to the machine, close ports, and remove registry entries.

Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Unlike viruses/malware, worms do not need to attach themselves to host programs. Worms often use email and applications, such as Microsoft™ Outlook™, to propagate. They may also drop copies of themselves into shared folders or utilize file-sharing systems, such as Kazaa, under the assumption that users will likely download them, thus letting the

worm propagate. In some cases, worms use chat applications such as ICQ, AIM, mIRC, or other Peer-to-Peer (P2P) programs to spread copies of themselves.

Zip of Death

"Zip-of-death" describes a subterfuge designed to bring down a network by overwhelming the antivirus software and/or network traffic checking security applications.

Using special techniques, a hacker can compress a file down to as little as 500 KB, that, when decompressed, may reach 15 GB or more in size. Another version of the exploit involves compressing such a large number of files, that, when decompressed, it can crash the system.

IM Security allows you to set limits on the size, as well as the number of files it will extract from a compressed archive. When the limit is reached, IM Security stops decompressing and takes the action specified for files outside of the scan restriction criteria.

About Spyware/Grayware

Your clients are at risk from potential threats other than viruses/malware. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization.

TABLE 11-3. Types of Grayware

TYPE	DESCRIPTION
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties
Adware	Displays advertisements and gathers data, such as user web surfing preferences, to target advertisements at the user through a web browser

Type	Description
Dialers	Change computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Programs	Cause abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Help hackers enter computers
Remote Access Tools	Help hackers remotely access and control computers
Password Cracking Applications	Help hackers decipher account user names and passwords
Other	Other types not covered above

Potential Risks and Threats

The existence of spyware/grayware on your network has the potential to introduce the following:

Table 11-4. Types of Risks

Type	Description
Reduced computer performance	To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
Increased web browser-related crashes	Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.
Reduced user efficiency	By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users can be unnecessarily distracted from their main tasks.
Degradation of network bandwidth	Spyware/grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network.

Type	Description
Loss of personal and corporate information	Not all data that spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network.
Higher risk of legal liability	If hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties.

How Spyware/Grayware Gets into your Network

Spyware/grayware often gets into a corporate network when users download legitimate software that has grayware applications included in the installation package.

Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

True File Type

Files can be easily renamed to disguise their actual type. Programs such as Microsoft Word are "extension independent". They will recognize and open "their" documents regardless of the file name. This poses a danger, for example, if a Word document containing a macro virus has been named "`benefits form.pdf`". Word will open the file, but the file may not have been scanned if IM Security is not set to check the true file type.

When set to IntelliScan, IM Security will confirm a file's true type by opening the file header and checking its internally registered data type.

Only files of that type that is actually capable being infected are scanned. For example, `.mid` files make up a large volume of all web traffic, but they are known not to be able to carry viruses. With true file type selected, once the true type has been determined, these inert file types are not scanned.

Disease Vector

A "disease vector" is a website or URL known to distribute Internet security risks including spyware/grayware, password-cracking applications, key-stroke trackers, and virus/malware kit downloads.

Another category of disease vectors are sites made to look legitimate, but below the surface the hacker directs all the "back-end" functionality such as links and data posts to his or her own locations.

Trend Micro quickly adds confirmed malicious sites to the phish and spyware pattern file so you can prevent LAN clients from downloading the virus/malware, or from being duped by the look-alike sites.

Phish

Phish, or Phishing, is a rapidly growing form of fraud that seeks to fool web users into divulging private information by mimicking a legitimate website.

In a typical scenario, an unsuspecting user gets an urgent sounding (and authentic looking) email telling him or her there is a problem with their account that they must immediately fix, or the account will be closed. The email will include a URL to a website that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate website but then change the so-called back-end—where the collected data is actually sent.

The email tells the user to log on to the site and confirm some account information. Any data entered at the site is directed to a malicious hacker who steals the log on name, password, credit card number, social security number, or whatever data s/he requests.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even

computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Chapter 12

Trend Micro IM Security Tools

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

Topics include:

IM Security Server Management Tool

The IM Security Server Management Tool (`toolSrvMgmt.exe`) is a command line tool that allows you to easily add and register other IM Security servers in the **Server Management** list. Register servers 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 user who started the IM Security services on the source server to the Access Control List (ACL) of the target server (`<root>\TrendMicro\IMSecurity WMI instance`) completes the registration process.

Tip

Run the Server Management Tool from the target or source IM Security server (typically `<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 Local Administrator privileges on the target server

Running the Server Management Tool

Important

To run the Server Management Tool, you must be a member of the “Local admin” group. The Server Management Tool does not display servers to which you do not have the privilege to view.

Procedure

1. Click **Start** > **Run**.
2. Type `cmd`, and then click **OK** to open a command line prompt.
3. On the command line prompt, 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 IM Security logon account> /t <target server
   name> /o <operation>
   ```

   TABLE 12-1. 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 <source server IM Security logon account>`	The IM Security services logon account on the source server
`/t <server name>`	Host name or IP address of the target server
`/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 domain_name\user_name /t target_server_name /o add`

   When running the tool locally:

- `toolSrvMgmt.exe /s domain_name\user_name /o add`

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 Server Management Tool from `d:\temp`, ensure that the corresponding required files are present in `d:\temp`.

- `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 13

Troubleshooting and FAQs

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

Topics include:

Determining the Product Version

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

Procedure

1. Click **About** from the header menu to determine the product version and build.

2. Verify that the **Version** and **Build** values are up-to-date.

   To find out if an updated version, service pack, or patch is available for IM Security, go to the Trend Micro Download Center:

   http://downloadcenter.trendmicro.com/

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

Procedure

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.

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**

Procedure

1. Check whether the account used to access the product console belongs to the local **Administrators** group.
2. Use Windows Services Panel to verify whether "Trend Micro IM Security Server" is started.
3. Ensure that the web service is started.
4. Verify whether the IM Security administrator account has not been changed. Otherwise, obtain the latest account user name and password.

5. Check the network connection and HTTP port being used.

6. Check that the IM Security website has been added to the browser's **Trusted Sites**.

Note

Trend Micro recommends operating Internet Explorer 10 or later in compatibility view.

Adding the IM Security Website from SharePoint's Exclusion List

Procedure

1. On the server where IM Security and SharePoint are installed, click **Start** > **All Programs** > **Administrative Tools** > **SharePoint Central Administration**.

2. On the **Central Administration** screen, under **Virtual Server Configuration**, click **Configure virtual server settings**.

3. On the **Virtual Server List** screen, select the virtual server you want to configure.

4. On the **Virtual Server Settings** screen, under **Virtual Server Management**, click **Define managed paths**.

5. In the **Add a New Path** section, in the **Path** box, type the path `IMSecurity`.

6. Select **Excluded path**.

7. Click **OK**.

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.

Procedure

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 ActiveUpdate Server**.

   If **Intranet location containing a copy of the current file** or **Other update source** is enabled as the update source (**Updates** > **Source**), check whether the folder contains the latest components.
3. If **Trend Micro ActiveUpdate Server** 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 the following address from the IM Security server:

   ```
   http://imsecurity16-p.activeupdate.trendmicro.com/
   activeupdate
   ```

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

Using the Debug Logs

IM Security Debugger can assist you in debugging or reporting the status of the IM Security processes. When you are having unexpected difficulties, you can use the debugger to create debugger reports and send them to Trend Micro technical support for analysis.

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

- For the IM Security server: `servIMSHost.log` or `servIMSHost.log.#`
- **Trend Micro IM Security System Attendant service**
- For Control Manager Agent: `servCmAgentHost.log` or `servCmAgentHost.log.#`

Note

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:

```
<root>:\Program Files\Trend Micro\IM Security\Debug
```

Procedure

1. Go to **Administration** > **Debug Logs**.

   The **Debug Logs** screen appears.

2. Select the modules to debug:
   - **Trend Micro IM Security Server**
   - **Trend Micro IM Security System Attendant service**
   - **Trend Micro Control Manager Agent**
3. Click **Apply**.

Note

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

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.

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

Report Generation Issues

Procedure

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 128 MB free disk space available on the IM Security program folder or the report module cannot run and generate reports.
3. Check the database connection by opening the IM Security database through Microsoft SQL Server Management Studio.

4. Enable report debug logging.

   a. Open the file `TMReportExCfg.xml`.

      The default location is: `C:\Program Files\Trend Micro\IM Security\`

   b. Change the value of `DebugLogLevel` from `0` to `3`.

5. Generate a one-time report with a limited date range (for example, from "05.01.2014" to "05.09.2014").

6. If IM Security is unable to generate a one-time report, send `<root>:\Program Files\Trend Micro\IM Security\debug\TMreportEX.log` to Trend Micro support.

PDF or HTML Report Display Issues

Procedure

- 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.

Log Issues

One of the following issues may occur:

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

Procedure

1. Ensure that there is at least 128MB free disk space available on the IM Security database folder. Otherwise, delete older log entries.
2. Check the database connection by opening the IM Security database using Microsoft SQL Server Management Studio.
3. If any of the above tasks do not solve the issue, contact Trend Micro support.

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 Notifications

Procedure

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).

SNMP Trap Notification

Procedure

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.

Frequently Asked Questions (FAQ)

General Product Knowledge

What is IM Security?

Trend Micro IM Security is an antivirus application that provides antivirus and content security protection to Microsoft Lync Servers.

How does IM Security protect my Lync Server?

IM Security provides real-time virus/malware, spyware/grayware, File Blocking, URL filtering, Content Filtering, Communication Control, and Data Loss Prevention.

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

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

What are the instant messaging applications that IM Security supports?

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

What are the instant messaging clients that IM Security supports?

IM Security only supports the instant messaging clients supported by Microsoft Lync Server.

Can Communication Control block PSTN calls?

Communication Control does not block PSTN calls for local or external users.

What is the IM Security "System Attendant Service"?

The IM Security System Attendant Service is one of the IM Security services. It monitors the service status of Microsoft Lync Server and IM Security Server services.

Which account is used to start the "Trend Micro IM Security Server" and "Trend Micro IM Security System Attendant" services?

IM Security uses the account configured during installation to start the "Trend Micro IM Security Server" and "Trend Micro IM Security System Attendant" services.

What do I do if the "Trend Micro IM Security Server" service is unable to start successfully?

Procedure

1. Ensure that the Lync Front-End server is functioning correctly.
2. Verify that the password of the account configured during installation has not expired. If the password has expired, perform the following:
   a. Open Windows Services Panel.
   b. Locate the following IM Security services:
      - Trend Micro IM Security Server
      - Trend Micro IM Security System Attendant
   c. Manually stop the services.
   d. Select each service individually, right-click and click **Properties** > **Log on**.
   e. Clear the log on password and type the updated password.
   f. Click **OK**.
   g. Manually restart the service.

How do I change the account used to start the IM Security services?

Procedure

1. Prepare a user account that IM Security uses to start the services.

   The account must be a member of the following groups:

   - "RTCUniversalServerReadOnlyGroup" of the Domain Controller
   - "RTC Server Applications"
   - "RTC Local Administrators"
   - "Local Administrator" of the IM Security server

2. Update the account and password information for the IM Security services:

   a. Open Windows Services Panel.

   b. Locate the following IM Security services:

      - Trend Micro IM Security Server
      - Trend Micro IM Security System Attendant

   c. Manually stop the services.

   d. Select each service individually, right-click and click **Properties** > **Log on**.

   e. Clear the log on password and type the updated password.

   f. Click **OK**.

   g. Manually restart the service.

Important

IM Security does not support the use of built-in accounts including the local system account, local service account, or the network service account to start the IM Security services.

Registration and Activation

Where can I get a Registration Key or Activation Code?

Refer to the Trend Micro website:

http://esupport.trendmicro.com/en-us/default.aspx

Contacts

What is the "Selected List"?

The **Selected List** is a list that stores the users, groups, or domains to which IM Security applies enabled rules. The **Selected List** is not a global list—it varies per rule. Add users, groups, or domains in a Selected Contacts list when creating a rule.

What is the "Exempted List"?

The **Exempted List** is a list that stores the users, groups, or domains that are exempted from IM Security enabled rules matching. Use this list to define the persons or groups in your organization that IM Security exempts from File Blocking, Content Filtering, and Data Loss Prevention. Similar to the **Selected List**, the **Exempted List** is not a global list—it varies per rule. Add users, groups, or domains in an Exempted Contacts list when creating a rule.

Administration

How does IM Security send notifications to network/mail administrators and contacts?

IM Security can send notifications using email, instant messaging, or SNMP trap protocols. In addition, it provides an option to save logs to Windows Event logs.

For details, see *Notification Settings on page 10-6*.

How does IM Security populate the Server Management list?

IM Security populates the **Server Management** list by:

- Querying the Global Catalog (GC) or local cache GC for the available Lync Servers in a forest
- Using the currently logged on user account to connect the servers in a forest
- Checking the user account's permission to access remote servers

  If the user account is allowed to access a remote server, IM Security then verifies whether the `WMI namespaceroot\TrendMicro\IMSecurity` exists on that server. If the namespace exists, IM Security concludes that the remote server has Lync Server and IM Security installed.

If all of the above conditions are satisfied, IM Security includes the server in the **Server Management** list.

Can I replicate my local IM Security server settings to another server(s)? If so, how?

IM Security allows you to replicate settings to additional IM Security servers from a single product console.

To register a server, use the Server Management Tool.

For details, see *IM Security Server Management Tool on page 12-2*.

To replicate settings to another server, use the product console's **Server Management** window.

For details, see *Replicating Settings to Other Servers on page 2-5*.

What are the web protocols that IM Security supports?

IM Security supports HTTP and HTTPS.

In which folder can I locate IM Security after registering to the Trend Micro Control Manager server?

If you performed a fresh installation of IM Security and registered to the Control Manager server, IM Security is located in the "IM Security for Lync" folder on the Control Manager server.

If you performed an upgrade from a previous IM Security version that was registered to the Control Manager server, IM Security is located in the previously configured "IM Security for OCS" folder on the Control Manager server.

Chapter 14

Contacting Trend Micro

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

Topics include:

Contacting Technical Support

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

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

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

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

TrendLabs

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

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

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

believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

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

Speeding Up Your Support Call

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

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

Using the Support Portal

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

Procedure

1. Go to http://esupport.trendmicro.com.

2. Select a product or service, or click a button to find more products or services.
3. Use the **Search Support** field to search for available solutions.
4. If no solution is found, click **Contact Support** or submit a support case here:

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

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

Security Information Site

Comprehensive security information is available at the Trend Micro website:

http://about-threats.trendmicro.com

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

Information available:

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

Appendices

Appendices

Appendix A

Performance Counters

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

Topics include:

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	The rate of instant messages passing through the real-time scan modules (Content Filtering + Web Reputation + Data Loss Prevention)(= 002 / 003)
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	The rate of files passing through the real-time scan modules (File Blocking, Content Filtering, Virus Scan, Web Reputation, and Data Loss Prevention) (= 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

Counter Name	Description
VScan - 002 - Total scanning time	The total scanning time for all files scanned by Virus Scan
VScan - 003 - Total matching files	The number of files that match virus scan settings, including: • Virus or spyware detected • Compressed file restrictions • Unscannable files (password-protected or encrypted files)
VScan - 004 - Scanned items / sec	The 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

Counter Name	Description
File Blocking - 004 - Scanned items / sec	The rate of files passing through the File Blocking filter (= 001 / 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 detections
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 detections
CFilter - 005 - FT : Total scanning time	The total scanning time of all files scanned for Content Filtering detections
CFilter - 006 - FT : Total matching items	The number of files that violated Content Filtering rules
CFilter - 007 - IM : Filtered messages / sec	The rate of instant messages passing through Content Filtering (= 001 / 002)

Counter Name	Description
CFilter - 008 - FT : Filtered files / sec	The rate of files passing through Content Filtering (= 004 / 005)

Web Reputation Performance Counters

The following table describes the Web Reputation performance counters.

Table A-5. 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 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)

Counter Name	Description
UFilter - 009 - IM : Total scanned items containing URLs	The number of instant messages scanned by the URL filter that contained URL addresses
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
UFilter - 011 - FT : Total items scanned	The number of files scanned by the URL filter
UFilter - 012 - FT : Total scanning time	The total scanning time of all files
UFilter - 013 - FT : Total scanned items containing URLs	The number of files scanned by the URL filter that contained URL addresses
UFilter - 014 - FT : Total scanned items containing malicious URLs	The number of files containing malicious URL addresses that were scanned by the URL filter
UFilter - 015 - FT : Files scanned per second	Rate of files passing through the URL filter module (= 011 / 012)
UFilter - 016 - IM : Total malicious URLs for IM	The total number of malicious URLs detected in instant messages
UFilter - 017 - FT : Total malicious URLs for file	The total number of malicious URLs detected in files

Data Loss Prevention 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-6. Instant Message and File Transfer Scan Counters

Counter Name	Description
DLPFilter- 001 - IM: Total scanned items	The number of messages scanned by Data Loss Prevention

Counter Name	Description
DLPFilter- 002 - IM : Total scanning time	The total scanning time of all instant messages scanned for Data Loss Prevention detections
DLPFilter- 003 - IM : Total matching items	The number of instant messages that violated Data Loss Prevention rules
DLPFilter- 004 - FT : Total scanned items	The number of files scanned for Data Loss Prevention detections
DLPFilter- 005 - FT : Total scanning time	The total scanning time of all files scanned for Data Loss Prevention detections
DLPFilter- 006 - FT : Total matching items	The number of files that violated Data Loss Prevention rules
DLPFilter- 007 - IM : Filtered messages/sec	The rate of instant messages passing through Data Loss Prevention (= 001 / 002)
DLPFilter- 008 - FT : Filtered files/sec	The rate of files passing through Data Loss Prevention (= 004 / 005)

Directory Service Access Performance Counters

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

Table A-7. DSAccess Counters

Counter Name	Description
DSAccess - 001 - Total directory accesses	The total amount of data queried from the Global Catalog (GC) (= 005 + 009 + 013)

Counter Name	Description
DSAccess - 002 - Total directory access time	The total time spent querying data from GC (= 006 + 010 + 014)
DSAccess - 003 - Total local cache accesses	The total amount of data queried from caches (= 007 + 011 + 015)
DSAccess - 004 - Total local cache access time	The total time spent querying data from caches (= 008 + 012 + 016)
DSAccess - 005 - [User Identity] directory accesses	The total amount of user data queried from GC
DSAccess - 006 - [User Identity] directory access time	The total time spent querying user data from GC
DSAccess - 007 - [User Identity] cache accesses	The total amount of user data queried from user cache
DSAccess - 008 - [User Identity] cache access time	The 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	The total time spent querying primary group data from GC
DSAccess - 011 - [Primary Group] cache accesses	The total amount of primary group data queried from Primary Group cache
DSAccess - 012 - [Primary Group] cache access time	The total time spent querying primary group data from the Primary Group cache
DSAccess - 013 - [Nested Group] directory accesses	The total amount of nested group data queried from the GC
DSAccess - 014 - [Nested Group] directory access time	The total time spent querying nested group data from the GC
DSAccess - 015 - [Nested Group] cache accesses	The total amount of nested group data queried from the Nested Group cache

Counter Name	Description
DSAccess - 016 - [Nested Group] cache access time	The 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-8. IMHook Counters

Counter Name	Description
IMHook - 001 - Total number of requests from LCS	The total number of requests coming from the LCS / Lync 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	The total number of responses coming from the LCS / Lync Server
IMHook - 003 - Total messages passing to the scan modules	The total number of instant messages scanned by the IM Security scan modules
IMHook - 004 - File transfer monitoring map size	The 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)

Counter Name	Description
IMHook - 005 - Total number of requests from trusted users	The 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	The 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	The rate of LCS / Lync requests (Number of SIP request 'MESSAGE' or 'INVITE' sent from LCS / Lync Server per second)
IMHook - 008 - LCS responses / sec	The rate of LCS / Lync responses (Number of SIP responses sent from LCS / Lync Server per second)
IMHook - 009 - Passing messages / sec	The 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-9. 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	The 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)
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	The total number of held scan tasks (Total number of files to be scanned after downloading)
FTHook - 007 - Total pending scan tasks	The total number of pending scan tasks (Total number of files waiting for scanning)

Counter Name	Description
FTHook - 008 - Total scan tasks in progress	The total number of scan tasks in progress (Total number of files being scanned)
FTHook - 009 - Passing files / sec	The rate of files being passed to the scan module

Session Management Performance Counters

The following table describes the Session Management performance counters.

Table A-10. 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-11. Disclaimer Counters

COUNTER NAME	DESCRIPTION
Disclaimer - 001 - Total disclaimer records	The number of disclaimer records which 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 Control Manager Logs and Actions Comparison

This chapter contains information about comparisons between the IM Security and Control Manager logs and actions.

Topics include:

IM Security and Control Manager Logs and Actions

Virus Scan and Additional Threats

IM Security - Logs and Actions	Mapped to Control Manager 5.5 (and later)
Virus Scan	Security Threat Information => Virus/Malware Information
Virus Scan (additional threats)	Security Threat Information => Spyware/Grayware Information
Quarantine	File quarantined
Cancel Transfer	File deleted
Deliver	File passed

File Blocking, Content Filtering, and Data Loss Prevention for File Transfers and Instant Messages

IM Security - Logs and Actions		Mapped to Control Manager 5.5 (and later)
File Blocking		Security Threat Information => Content Violation Information
	Cancel + Archive	Quarantine
	Deliver + Archive	Deliver
	Cancel	Delete

IM Security - Logs and Actions		Mapped to Control Manager 5.5 (and later)
	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

IM Security - Logs and Actions		Mapped to Control Manager 5.5 (and later)
Data Loss Prevention: File Transfers		For Control Manager 5.5: • Security Threat Information => Content Violation Information For Control Manager 6.0: • Data Protection Information => Data Loss Prevention Information
	Cancel + Archive	Quarantine
	Deliver + Archive	Deliver
	Cancel	Delete
	Deliver	Deliver
Data Loss Prevention: Instant Messages		For Control Manager 5.5: • Security Threat Information => Content Violation Information For Control Manager 6.0: • Data Protection Information => Data Loss Prevention Information
	Cancel + Archive	Quarantine
	Replace all + Archive	Replace
	Deliver + Archive	Deliver
	Cancel	Delete

IM Security - Logs and Actions		Mapped to Control Manager 5.5 (and later)
	Replace all	Replace
	Deliver	Deliver

Web Reputation

IM Security - Logs and Actions	Mapped to Control Manager 5.5 (and later)
Web Reputation	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

Appendix C

Glossary

Term	Explanation
100BaseT	An alternate term for “fast Ethernet”, an upgraded standard for connecting computers into a local area network (LAN). 100BaseT Ethernet can transfer data at a peak rate of 100 Mbps. It is also more expensive and less common than 10BaseT. 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.

TERM	EXPLANATION
action	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 • file blocking has been triggered, or • senstive data is detected. 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. Also see target and notification.
activate	To enable your software after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the **Product License** screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: `SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4` Also see Registration Key.
active FTP	Configuration of FTP protocol that allows the client to initiate "handshaking" signals for the command session, but the host initiates the data session.
ActiveUpdate	A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, as well as the anti-spam rules database and anti-spam engine. ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update website, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.

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

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

TERM	EXPLANATION
case-matching	Scanning for text that matches both words and case. For example, if dog is added to the content-filter, with case-matching enabled, messages containing Dog will pass through the filter; messages containing dog will not.
cause	The reason a protective action, such as URL-blocking or file-blocking, was triggered. This information appears in log files.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a server) using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
client-server environment	A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the Content Filtering policy.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your web browser for later use. The next time you access a website for which your browser has a cookie, your browser sends the cookie to the web server, which the web server can then use to present you with customized web pages. For example, you might enter a website that welcomes you by name.

TERM	EXPLANATION
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
damage routine	The destructive portion of virus code, also called the payload.
Data Loss Prevention (DLP)	A scan filter that determines if data being transferred contains sensitive information as defined by the administrator using templates, expressions, and keyword lists.
default	A value that pre-populates a field in the management console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.
Denial of Service (DoS) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. 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`

Term	Explanation
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message.
domain (administrative)	A group of computers sharing a common database and security policy.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called name resolution, uses the Domain Name System (DNS).
Domain Name System (DNS)	A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
Domain Name System (DNS) resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
DOS virus	Also referred to as “COM” and “EXE file infectors”. DOS viruses infect DOS executable programs- files that have the extensions `*.COM` or `*.EXE`. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.
download (noun)	Data that has been downloaded, for example, from a website via HTTP.
download (verb)	To transfer data or code from one computer to another. Downloading often refers to transfer from a larger host system (especially a server or mainframe) to a smaller client system.
dropper	Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.

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

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

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

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

TERM	EXPLANATION
installation script	The installation screens used to install Unix versions of Trend Micro products.
IntelliScan	IntelliScan is a Trend Micro scanning technology that optimizes performance by examining file headers using true-file type recognition, and scanning only file types known to potentially harbor malicious code. True-file type recognition helps identify malicious code that can be disguised by a harmless extension name.
Internet	A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.
interrupt	An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an interrupt handler routine.
“in the wild”	Describes known viruses that are actively circulating. 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`.

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

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

TERM	EXPLANATION
Local Area Network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
log storage directory	Directory on your server that stores log files.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
macro	A command used to automate certain functions within an application.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Macro viruses are often encoded as an application macro and included in a document. Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, web downloads, file transfers, and cooperative applications.
Mail Transfer Agent (MTA)	The program responsible for delivering email messages. Also see SMTP server.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
management console	The user interface for your Trend Micro product.

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

Term	Explanation
notification (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.
purge	To delete all, as in getting rid of old entries in the logs.

TERM	EXPLANATION
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. 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.
router	This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
scan	To examine items in a file in sequence to find those that meet a particular criteria.

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

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

TERM	EXPLANATION
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of `255.255.255.0` specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of `255.255.0.0`. 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	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. (Also see action and notification)
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.
top-level domain	The last and most significant component of an Internet fully qualified domain name, the part after the last .. For example, host `wombat.doc.ic.ac.uk` is in top-level domain uk (for United Kingdom).
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.

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

TERM	EXPLANATION
tunneling	A method of sending data that enables one network to send data via another network's connections. Tunneling is used to get data between administrative domains which use a protocol that is not supported by the internet connecting those domains. 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.
Universal Resource Locator (URL)	A standard way of specifying the location of an object, typically a web page, on the Internet, for example, `www.trendmicro.com`. The URL maps to an IP address using DNS.

TERM	EXPLANATION
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a **Click Here for More Information** button on a web page. 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 website which sends out web pages in response to HTTP requests from remote browsers.
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a wildcard, can be used for any number or suit in the card deck.
working directory	The destination directory in which the main application files are stored, such as `/etc/iscan/iwss`.

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

Index

TREND MICRO INCORPORATED

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

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

www.trendmicro.com

Item Code: TIEM16346/140311