



7.1 InterScan™ Messaging Security Suite

Administrator's Guide

Comprehensive threat protection at the Internet messaging gateway

for LINUX™ 7.1 SP2



Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<http://docs.trendmicro.com/en-us/enterprise/interscan-messaging-security-suite-for-linux.aspx>

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

© 2015. Trend Micro Incorporated. All Rights Reserved.

Document Part No.: MSEM76416_140429

Release Date: October 2015

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

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

About this Manual

About this Manual	ix
What's New	x
Audience	xiv
InterScan Messaging Security Suite Documentation	xv
Document Conventions	xv

Part I: Getting Started

Chapter 1: Introducing InterScan Messaging Security Suite

About InterScan Messaging Security Suite	1-2
IMSS Main Features and Benefits	1-2
About Spyware/Grayware	1-9
About Web Reputation	1-11
About Trend Micro Control Manager	1-11
About Trend Micro Smart Protection	1-14
About Marketing Email Message Scanning	1-16

Chapter 2: Getting Started

Opening the IMSS Management Console	2-2
Viewing the Management Console Using Secure Socket Layer	2-3
Changing the Management Console Password	2-4
Configuring Proxy Settings	2-5
IMSS Services	2-6
Opening the End-User Quarantine Console	2-7
Selecting a Scan Method	2-8

Chapter 3: Using the Configuration Wizard

Accessing the Configuration Wizard	3-2
Configuring Notification Settings	3-2
Configuring the Update Source	3-4
Configuring LDAP Settings	3-6
Configuring Internal Addresses	3-8
Configuring Control Manager Server Settings	3-10
Configuring Product Settings	3-11
Verifying Settings Summary	3-12

Chapter 4: Updating Components

Updating Engine and Pattern Files	4-2
Specifying an Update Source	4-3
Performing a Manual Update	4-4
Rolling Back a Component Update	4-6
Scheduled Component Updates	4-6

Part II: Configuring IMSS

Chapter 5: Configuring IP Filtering Settings

IP Filtering Service	5-2
Using Email Reputation	5-2
Configuring IP Filtering	5-8
Displaying Suspicious IP Addresses and Domains	5-21

Chapter 6: Scanning SMTP Messages

Message Transfer Agents	6-2
Enabling SMTP Connections	6-2

Configuring SMTP Routing	6-2
About Message Delivery	6-11

Chapter 7: Configuring POP3 Settings

Scanning POP3 Messages	7-2
Enabling POP3 Scanning	7-3
Configuring POP3 Settings	7-4

Part III: IMSS Policies

Chapter 8: Managing Policies

About Policies	8-2
How the Policy Manager Works	8-2

Chapter 9: Common Policy Objects

Policy Object Descriptions	9-2
Understanding Address Groups	9-2
Using the Keyword & Expression List	9-13
Using the Notifications List	9-27
Using Stamps	9-31
Using the DKIM Approved List	9-35
Using the Web Reputation Approved List	9-36

Chapter 10: Internal Addresses

Configuring Internal Addresses	10-2
Searching for Users or Groups	10-5
Searching for an LDAP User or Group	10-6

Chapter 11: Configuring Policies

Adding Policies	11-2
Specifying a Route	11-2
Specifying Scanning Conditions	11-10
Specifying Actions	11-30
Finalizing a Policy	11-37

Chapter 12: Scanning Exceptions

Setting Scan Exceptions	12-2
Configuring Exceptions for Security Settings Violations	12-3
Setting Scan Actions for Security Setting Violations	12-4
Setting Scan Actions for Malformed Messages	12-5

Chapter 13: Existing Policies

Modifying Existing Policies	13-2
Policy Example 1	13-5
Policy Example 2	13-9
Using the Asterisk Wildcard	13-14

Part IV: Monitoring the Network

Chapter 14: Monitoring the Network

Monitoring Your Network	14-2
Viewing System Status	14-2
Statistics Summary	14-3

Chapter 15: Reports

Generating Reports	15-2
--------------------------	------

Managing One-time Reports	15-4
Scheduled Reports	15-6

Chapter 16: Logs

About Logs	16-2
Configuring Log Settings	16-2
Querying Logs	16-4

Chapter 17: Mail Areas and Queues

Quarantine and Archive	17-2
Configuring Quarantine and Archive Settings	17-2
Managing Quarantine Areas	17-4
Managing Archive Areas	17-6
Querying Messages	17-9
Viewing Quarantined Messages	17-13
Viewing Archived Messages	17-14
Configuring User Quarantine Access	17-15
Adding an EUQ Database	17-17
Command-line Options for euqtrans Tool	17-18

Chapter 18: Notifications

Event Notifications	18-2
Configuring Delivery Settings	18-2
Configuring Event Criteria and Notification Message	18-4
EUQ Digest	18-6
Configuring a Logon Notice	18-8
Editing Notifications	18-9

Part V: Administering IMSS

Chapter 19: Backing Up, Restoring, and Replicating Settings

Importing and Exporting Settings	19-2
Backing Up IMSS	19-4
Restoring IMSS	19-6
Replicating Settings	19-7

Chapter 20: Using End-User Quarantine

About EUQ	20-2
EUQ Authentication	20-2
Configuring End-User Quarantine (EUQ)	20-2
Disabling EUQ	20-13

Chapter 21: Performing Administrative Tasks

Managing Administrator Accounts	21-2
Configuring Connection Settings	21-6
Managing Product Licenses	21-15

Chapter 22: Troubleshooting, FAQ, and Support Information

Troubleshooting	22-2
Frequently Asked Questions	22-12
Support Information	22-33

Appendices

Appendix A: IMSS Scripts

Using IMSS Scripts	A-2
--------------------------	-----

Appendix B: Default Directory Locations

Default Mail Queues B-2
eManager, Virus, and Program Logs B-3
Temporary Folder B-3
Notification Pickup Folder B-4

Index

Index IN-1

Preface

About this Manual

Welcome to the Trend Micro™ InterScan™ Messaging Security Suite Administrator's Guide. This manual contains information about InterScan Messaging Security Suite (IMSS) features, system requirements, as well as instructions on configuring IMSS settings.

Refer to the *IMSS 7.1 SP2 Installation Guide* for information about installing and upgrading IMSS.

Topics include:

- *What's New on page x*
- *Audience on page xiv*
- *InterScan Messaging Security Suite Documentation on page xv*
- *Document Conventions on page xv*

What's New

The following tables provide an overview of new features available in IMSS 7.1 SP2.

TABLE 1. IMSS 7.1 SP2 New Features

NEW FEATURE	DESCRIPTION
Audit log enhancement	<p>Audit logs record various administrator operations and provide a way to query activities of specified administrator accounts.</p> <hr/> <p> Note As an enhanced log category of system events, Audit log replaces Admin activity on the IMSS management console.</p>
Attachment keyword expression enhancement	Keyword expressions configured for IMSS policies are enhanced to apply not only to attachment content but also to attachment names.
Attachment names supported by message tracking logs	Message tracking logs include attachment names as a new attribute. Multiple attachment names can be specified to query message tracking logs.
Logon notice support	Customizable logon notices are available both on the administrator logon page and End-User Quarantine logon page.

TABLE 2. IMSS 7.1 SP1 New Features

NEW FEATURE	DESCRIPTION
Marketing Email Management	Administrators can manage marketing messages separately from common spam. To allow end users to receive wanted marketings messages, email addresses and IP addresses specified in the marketing message exception list bypass scanning.

NEW FEATURE	DESCRIPTION
Smart Scan	Smart Scan facilitates a more efficient scanning process by offloading a large number of threat signatures previously stored on the IMSS server to the cloud.
IPv6 support	<p>IMSS supports the following IPv6 features in IPv6 networks and proxies:</p> <ul style="list-style-type: none"> • SMTP routing and POP3 connections • Trend Micro services: <ul style="list-style-type: none"> • Web Reputation Services • Product Registration • ActiveUpdate • Smart Feedback • Trend Micro Control Manager • IP address imports and exports in IPv6 format • Notifications • Logs and reports with relevant SMTP IPv6 information
Keyword & Expression enhancements	To improve visibility of triggered keywords and expressions, the entity name (where the keyword expression appears in a message) and the matched expressions now appear in the policy event log query details page. Administrators can also add a description to new keyword expressions for better tracking.
SMTP authentication support for End-User Quarantine	SMTP authentication provides users another option for enabling the End-User Quarantine feature.
Email alias support	The User Quarantine now has the option to allow end users to retrieve quarantined email messages with alias email addresses.

TABLE 3. IMSS 7.1 New Features

NEW FEATURE	DESCRIPTION
Common Policy Objects	<p>Several information objects that can be used by all policies have been removed from policy creation and given their own areas for configuration:</p> <ul style="list-style-type: none"> • Address Groups • Keywords & Expressions • Policy Notifications • Stamps • DKIM Approved List • Web Reputation Approved List
Web Reputation	Protect your clients from malicious URLs embedded in email messages with Web reputation.
NRS Terminology Change	Network Reputation Service (NRS) has been changed to Email Reputation Service (ERS).
Detection Capability Enhancement	Use DomainKeys Identified Mail (DKIM) enforcement, with the DKIM Approved List, in policies to assist in phishing protection and to reduce the number of false positives regarding domains.
X-Header Support	Insert X-Headers into email messages to track and catalog the messages.
Expanded File Scanning Support	Scanning support for Microsoft® Office 2007 and Adobe® Acrobat® 8 documents.
New Migration Tools	New tools provided to help customers migrating from previous product versions.

TABLE 4. IMSS 7.0 New Features

NEW FEATURE	DESCRIPTION
Multiple Antivirus and Malware Policies	Multiple IMSS policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria.
Centralized Logging and Reporting	A consolidated, detailed report provides top usage statistics and key mail usage data. Centralized logging allows administrators to quickly audit message-related activities.
Centralized Archive and Quarantine Management	An easy way to search multiple IMSS quarantine and archive areas for messages.
Scalable Web End-User Quarantine (Web EUQ)	Multiple Web EUQ services offer end-users the ability to view quarantined email messages that IMSS detected as spam. Together with EUQ notification, IMSS will help lower the cost of helpdesk administrative tasks.
Multiple Spam Prevention Technologies	<p>Three layers of spam protection:</p> <ul style="list-style-type: none"> • Email Reputation Services filters connections from spam senders when establishing SMTP sessions. • IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS). • Trend Micro Anti-spam engine detects and takes action on spam.
IntelliTrap	IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus in a compressed file will enter your network through email.

NEW FEATURE	DESCRIPTION
Delegated Administration	LDAP-integrated account management allows users to assign administrative rights for different configuration tasks.
Easy Deployment with Configuration Wizard	An easy-to-use configuration wizard to get IMSS up and running.
Advance MTA Functions	Opportunistic TLS, domain based delivery, and other MTA functions help IMSS handle email efficiently and securely.
Migration	Easy upgrade process ensures that settings will be migrated with minimum effort during setup.
Mail Auditing and Tracking	Detailed logging for all messages tracks and identifies message flow related issues.
Integration with Trend Micro Control Manager	Perform log queries on Email Reputation Services from Control Manager, in addition to other supported features.

Audience

The IMSS documentation is written for IT administrators in medium and large enterprises. The documentation assumes that the reader has in-depth knowledge of email messaging networks., including details related to the following:

- SMTP and POP3 protocols
- Message transfer agents (MTAs), such as Postfix or Microsoft™ Exchange
- LDAP
- Database management

The documentation does not assume that the reader has any knowledge of antivirus or antispam technology.

InterScan Messaging Security Suite Documentation

The IMSS documentation consists of the following:

Administrator's Guide

Helps you get IMSS up and running with post-installation instructions on how to configure and administer IMSS.

Installation Guide

Contains introductions to IMSS features, system requirements, and provides instructions on how to deploy and upgrade IMSS in various network environments.

Online Help

Provides detailed instructions on each field and how to configure all features through the user interface. To access the online help, open the web management console, then click the help icon.

Readme File

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

The documentation is available at:

<http://docs.trendmicro.com>

Document Conventions

The documentation uses the following conventions:

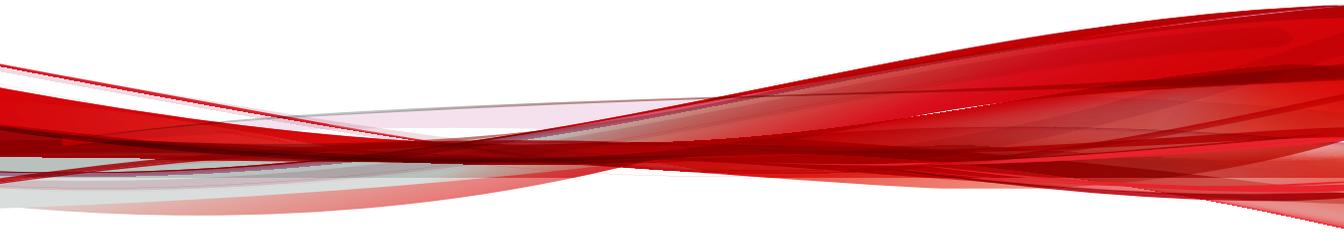
TABLE 5. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard

CONVENTION	DESCRIPTION
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

Part I

Getting Started



Chapter 1

Introducing InterScan™ Messaging Security Suite

This chapter introduces InterScan™ Messaging Security Suite (IMSS) features, capabilities, and technology, and provides basic information on other Trend Micro products that will enhance your anti-spam capabilities.

Topics include:

- *About InterScan Messaging Security Suite on page 1-2*
- *IMSS Main Features and Benefits on page 1-2*
- *About Spyware/Grayware on page 1-9*
- *About Trend Micro Control Manager on page 1-11*
- *About Trend Micro Smart Protection on page 1-14*

About InterScan Messaging Security Suite

InterScan Messaging Security Suite (IMSS) 7.1 SP2 integrates antivirus, anti-spam, anti-phishing, and content filtering technology for complete email protection. This flexible software solution features award-winning antivirus and zero-day protection to block known and potential viruses.

Multi-layered anti-spam combines the first level of defense in Email reputation technology with customizable traffic management through IP Profiler and the blended techniques of a powerful composite engine. Multi-lingual anti-spam provides additional support to global companies. Advanced content filtering helps to achieve regulatory compliance and corporate governance, and protects confidential information. IMSS delivers protection on a single, highly scalable platform with centralized management for comprehensive email security at the gateway.

IMSS Main Features and Benefits

The following table outlines the main features and benefits that IMSS can provide to your network.

TABLE 1-1. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
Data and system protection		
Antivirus protection	IMSS performs virus detection using Trend Micro scan engine and a technology called pattern matching. The scan engine compares code in files traveling through your gateway with binary patterns of known viruses that reside in the pattern file. If the scan engine detects a match, it performs the actions as configured in the policy rules.	Enhanced virus/content scanner keeps your messaging system working at top efficiency.

FEATURE	DESCRIPTIONS	BENEFITS
Smart Scan	<p>Smart Scan facilitates a more efficient scanning process by off-loading a large number of threat signatures previously stored on the IMSS server to the cloud.</p>	<p>Smart Scan leverages the Smart Protection Network to:</p> <ul style="list-style-type: none"> • Enable fast, real-time security status lookup capabilities in the cloud • Reduce the time necessary to deliver protection against emerging threats • Lower memory consumption on the server
IntelliTrap	<p>Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files.</p> <p>Because there is the possibility that IntelliTrap may identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature.</p> <p>By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be classified as security risks.</p>	<p>IntelliTrap helps reduce the risk that a virus compressed using different file compression schemes will enter your network through email.</p>

FEATURE	DESCRIPTIONS	BENEFITS
Content management	IMSS analyzes email messages and their attachments, traveling to and from your network, for appropriate content.	Content that you deem inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using IMSS.
Protection against other email threats		
DoS attacks	By flooding a mail server with large attachments, or sending messages that contain multiple viruses or recursively compressed files, individuals with malicious intent can disrupt mail processing.	IMSS allows you to configure the characteristics of messages that you want to stop at the SMTP gateway, thus reducing the chances of a DoS attack.
Malicious email content	Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions.	IMSS allows you to configure the types of messages that are allowed to pass through the SMTP gateway.
Degradation of services	Non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours.	Most companies have acceptable usage policies for their messaging system—IMSS provides tools to enforce and ensure compliance with existing policies.

FEATURE	DESCRIPTIONS	BENEFITS
Legal liability and business integrity	<p>Improper use of email can also put a company at risk of legal liability. Employees may engage in sexual or racial harassment, or other illegal activity. Dishonest employees can use a company messaging system to leak confidential information. Inappropriate messages that originate from a company's mail server damage the company's reputation, even if the opinions expressed in the message are not those of the company.</p>	<p>IMSS provides tools for monitoring and blocking content to help reduce the risk that messages containing inappropriate or confidential material will be allowed through your gateway.</p>
Mass mailing virus containment	<p>Email-borne viruses that may automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users.</p> <p>When IMSS detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses.</p> <p>For example, if IMSS detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if IMSS detects a mass-mailing virus, the program can automatically delete the entire message.</p>	<p>By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value.</p> <p>The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabsSM ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.</p>
Protection from spyware and other types of grayware		

FEATURE	DESCRIPTIONS	BENEFITS
Spyware and other types of grayware	Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see About Spyware/Grayware on page 1-9 .	IMSS's ability to protect your environment against spyware and other types of grayware enables you to significantly reduce security, confidentiality, and legal risks to your organization.
Integrated anti-spam features		
Spam Prevention Solution (SPS)	<p>Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam detection services to other Trend Micro products. To use SPS, obtain an SPS Activation Code. For more information, contact your sales representative.</p> <p>SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license.</p>	The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real-time detection that is highly adaptable, even as spam senders change their techniques.
Spam Filtering with IP Profiler and Email reputation	<p>IP Profiler is a self-learning, fully configurable feature that proactively blocks IP addresses of computers that send spam and other types of potential threats. Email reputation blocks IP addresses of known spam senders that Trend Micro maintains in a central database.</p> <hr/> <p> Note Activate SPS before you configure IP Profiler and Email reputation.</p>	With the integration of IP Filtering, which includes IP Profiler and Email reputation, IMSS can block spammers at the IP level.
Administration and integration		

FEATURE	DESCRIPTIONS	BENEFITS
LDAP and domain-based policies	You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™ or Microsoft™ Active Directory™ for user-group definition and administrator privileges.	Using LDAP, you can define multiple rules to enforce your company's email usage guidelines. You can define rules for individuals or groups, based on the sender and recipient addresses.
Web-based management console	The management console allows you to conveniently configure IMSS policies and settings.	The management console is SSL-compatible. Being SSL-compatible means access to IMSS is more secure.
End-User Quarantine (EUQ)	IMSS provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Spam Prevention Solution (SPS) quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete, or approve for delivery.	With the web-based EUQ management console, end-users can manage messages that IMSS quarantines.
Delegated administration	IMSS offers the ability to create different access rights to the management console. You can choose which sections of the console are accessible for different administrator logon accounts.	By delegating administrative roles to different employees, you can promote the sharing of administrative duties.

FEATURE	DESCRIPTIONS	BENEFITS
Centralized reporting	Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports.	Helps you analyze how IMSS is performing. One time (on demand) reports allow you to specify the type of report content as and when required. Alternatively, you can configure IMSS to automatically generate reports daily, weekly, and monthly.
System availability monitor	A built-in agent monitors the health of your IMSS server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow.	Email and SNMP notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.
POP3 scanning	You can choose to enable or disable POP3 scanning from the management console.	In addition to SMTP traffic, IMSS can also scan POP3 messages at the gateway as messaging clients in your network retrieve them.
Clustered architecture	The current version of IMSS has been designed to make distributed deployment possible.	You can install the various IMSS components on different computers, and some components can exist in multiples. For example, if your messaging volume demands, you can install additional IMSS scanner components on additional servers, all using the same policy services.

FEATURE	DESCRIPTIONS	BENEFITS
Integration with Trend Micro Control Manager™	Trend Micro Control Manager™ (TMC) is a software management solution that gives you the ability 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 and content security policy.	Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available.

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 1-2. 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
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

TYPE	DESCRIPTION
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

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.

Potential Risks and Threats

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

TABLE 1-3. 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.

TYPE	DESCRIPTION
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.
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.

About Web Reputation

Trend Micro web reputation technology helps break the infection chain by assigning websites a “reputation” based on an assessment of the trustworthiness of an URL, derived from an analysis of the domain. Web reputation protects against web-based threats including zero-day attacks, before they reach the network. Trend Micro web reputation technology tracks the lifecycle of hundreds of millions of web domains, extending proven Trend Micro anti-spam protection to the Internet.

About Trend Micro Control Manager

Trend Micro™ Control Manager™ is a software management solution that gives you the ability 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 hosted from this server.
- **Agent:** The agent is an application installed on a managed product that allows Control Manager to manage the product. The agent receives commands from the Control Manager server, and then applies them to the managed product. The agent collects logs from the product, and sends them to Control Manager.
- **Entity:** An entity is a representation of a managed product on the Product Directory link. Each entity has an icon in the directory tree. The directory tree displays all managed entities residing on the Control Manager console.

Control Manager Support

The following table shows a list of Control Manager features that IMSS supports.

TABLE 1-4. Supported Control Manager Features

FEATURE	DESCRIPTION	SUPPORTED?
Two-way communication	Using 2-way communication, either IMSS or Control Manager may initiate the communication process.	No. Only IMSS can initiate a communication process with Control Manager.
Outbreak Prevention Policy	The Outbreak Prevention Policy (OPP) is a quick response to an outbreak developed by TrendLabs that contains a list of actions IMSS should perform to reduce the likelihood of the IMSS server or its clients from becoming infected. Trend Micro ActiveUpdate Server deploys this policy to IMSS through Control Manager.	Yes

FEATURE	DESCRIPTION	SUPPORTED?
Log upload for query	Uploads IMSS virus logs, Content Security logs, and Email reputation logs to Control Manager for query purposes.	Yes
Single Sign-on	Manage IMSS from Control Manager directly without first logging on to the IMSS management console.	No. You need to first log on to the IMSS management console before you can manage IMSS from Control Manager.
Configuration replication	Replicate configuration settings from an existing IMSS server to a new IMSS server from Control Manager.	Yes
Pattern update	Update pattern files used by IMSS from Control Manager	Yes
Engine update	Update engines used by IMSS from Control Manager.	Yes
Product component update	Update IMSS product components such as patches and hot fixes from Control Manager.	No. Refer to the specific patch or hot fix readme file for instructions on how to update the product components.
Configuration by user interface redirect	Configure IMSS through the IMSS management console accessible from Control Manager.	Yes
Renew product registration	Renew IMSS product license from Control Manager.	Yes
Customized reporting from Control Manager	Control Manager provides customized reporting and log queries for email-related data.	Yes

FEATURE	DESCRIPTION	SUPPORTED?
Control Manager agent installation/uninstallation	Install or uninstall IMSS Control Manager agent from Control Manager.	No. IMSS Control Manager agent is automatically installed when you install IMSS. To enable/disable the agent, do the following from the IMSS management console: 1. Go to Administration > Connections . 2. Click the TCCM Server tab. 3. To enable/disable the agent, select/clear the check box next to Enable MCP Agent .
Event notification	Send IMSS event notification from Control Manager.	Yes
Command tracking for all commands	Track the status of commands that Control Manager issues to IMSS.	Yes

About Trend Micro Smart Protection

Trend Micro provides next-generation content security through smart protection services. By processing threat information in the cloud, Trend Micro smart protection reduces demand on system resources and eliminates time-consuming signature downloads.

Smart protection services include:

File Reputation Services

File reputation decouples the pattern file from the local scan engine and conducts pattern file lookups to the Trend Micro Smart Protection Network.

High performance content delivery networks ensure minimum latency during the checking process and enable more immediate protection.

Trend Micro continually enhances file reputation to improve malware detection. Smart Feedback allows Trend Micro to use community feedback of files from millions of users to identify pertinent information that helps determine the likelihood that a file is malicious.

Web Reputation Services

With one of the largest reputation databases in the world, Trend Micro web reputation tracks the credibility of domains based on factors such as age, historical location changes, and suspicious activity indicators discovered through malware behavior analysis. Trend Micro assigns reputation scores to specific pages instead of classifying entire sites to increase accuracy and reduce false positives.

Web reputation technology prevents users from:

- Accessing compromised or infected sites
- Communicating with Command & Control (C&C) servers used in cybercrime

The Need for a New Solution

The conventional threat handling approach uses malware patterns or definitions that are delivered to a client on a scheduled basis and stored locally. To ensure continued protection, new updates need to be received and reloaded into the malware prevention software regularly.

While this method works, the continued increase in threat volume can impact server and workstation performance, network bandwidth usage, and the overall time it takes to delivery quality protection. To address the exponential growth rate of threats, Trend Micro pioneered a smart approach that off-loads the storage of malware signatures to the cloud. The technology and architecture used in this effort allows Trend Micro to provide better protection to customers against the volume of emerging malware threats.

Trend Micro™ Smart Protection Network™

Trend Micro delivers File Reputation Services and Web Reputation Services to IMSS through the Trend Micro™ Smart Protection Network™.

The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. The Smart Protection Network uses lighter-weight clients to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

The Smart Protection Network provides File Reputation Services by hosting the majority of the malware pattern definitions. A client sends scan queries to the Smart Protection Network if its own pattern definitions cannot determine the risk of a file.

The Smart Protection Network provides Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. A client sends web reputation queries to the Smart Protection Network to check the reputation of websites that a user is attempting to access. The client correlates a website's reputation with the specific web reputation policy enforced on the computer to determine whether access to the site is allowed or blocked.

For more information on the Smart Protection Network, visit:

www.smartprotectionnetwork.com

About Marketing Email Message Scanning

Marketing email messages contain commercial or fund-raising content that the user may have requested. These email messages often do not include a functional opt-out facility. Managing marketing email messages separately from spam allows approved marketing messages to reach the end user. IMSS identifies marketing email messages in two ways:

- Email Reputation Services scoring the source IP address
- Trend Micro Anti-Spam Engine identifying message content

Administrators identify the email message source and define the rule criteria to take an action on those email messages. Every marketing email message rule has an exception list containing address objects that bypass message filtering. An address object is an email address, a single IP address or address range (IPv4 or IPv6), or the Classless Inter-Domain Routing (CIDR) block. The action attached to each rule appears as an option on the spam rule and can be any action applicable to spam rules.

Administrators have several options to understand marketing email message traffic in the network. Reports illustrate the highest senders and recipients of marketing email messages from external or internal sources. Administrators can also query detailed log information or view the email quarantine and release messages identified as permitted marketing email messages when necessary.

The marketing email message exception list can be exported and imported.

Chapter 2

Getting Started

This chapter explains how to log on to the management console and provides instructions on what to do immediately after installation to get the product up and running.

Topics include:

- *Opening the IMSS Management Console on page 2-2*
- *Viewing the Management Console Using Secure Socket Layer on page 2-3*
- *Changing the Management Console Password on page 2-4*
- *Configuring Proxy Settings on page 2-5*
- *IMSS Services on page 2-6*
- *Opening the End-User Quarantine Console on page 2-7*
- *Selecting a Scan Method on page 2-8*

Opening the IMSS Management Console

You can view the IMSS management console using a web browser from the server where you installed the program, or remotely across the network.

Procedure

1. Type the following URL:

```
https://<target server IP address>:8445
```



Tip

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

2. Type the logon credentials to open the management console.

The default logon credentials are as follows:

- Administrator user name: **admin**
- Password: **imss7.1**

3. Click **Log On**.
-



Note

If you are using Internet Explorer to access the management console, Internet Explorer will block the access and display a popup dialog box indicating that the certificate was issued from a different web address. Add the management console IP address to your Trusted sites list (**Internet Options > Security** in Internet Explorer) or ignore the message and click **Continue** to this website to proceed.

What to do next

Trend Micro recommends changing the password regularly, to prevent unauthorized access to the management console.

Using the Online Help

The IMSS management console comes with an Online Help that provides a description of each field on the user interface.

To access page-specific Online Help from the IMSS management console, click the Help (??) icon located at the top right corner of the page.

To access the table of contents for the Online Help, click the Help (??) icon next to the **Log Off** hyperlink on the right of the page header.



FIGURE 2-1. Table of Contents Access for Online Help

Viewing the Management Console Using Secure Socket Layer

The IMSS management console supports encrypted communication, using SSL. After installing IMSS, SSL communication should work because the installation contains a default certificate. Trend Micro suggests creating your own certificate to increase security.

If you want to use your own certificate, replace the following:

```
$IMSS_HOME/UI/tomcat/sslkey/.keystore
```

Creating an SSL Certificate

Procedure

1. Create the Tomcat SSL certificate for the IMSS management console, as follows:

```
%IMSS_HOME%\UI\javaJRE\bin\keytool -genkey -alias tomcat -  
keyalg RSA -sigalg SHA1withRSA -keystore %IMSS_HOME%\UI  
\tomcat\sslkey\.keystore -validity 3652
```

with a password value of `changeit` for both the certificate and the keystore itself

For more details on SSL configuration in Tomcat, visit:

<http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>

2. Create the Apache SSL certificate for the EUQ management console, as follows:

- a. Generate a Private Key and Certificate Signing Request (CSR):

```
openssl req -new > new.cert.csr
```

- b. Remove pass-phrase from the key:

```
openssl rsa -in privkey.pem -out new.cert.key
```

- c. Generate a Self-Signed Certificate:

```
openssl x509 -in new.cert.csr -out new.cert.cert -req -  
signkey new.cert.key -days 3652 -sha1
```

- d. Copy the certificate and key to the Apache path:

```
cp new.cert.cert $IMSS_HOME/UI/apache/conf/ssl.crt/  
server.crt
```

```
cp new.cert.key $IMSS_HOME/UI/apache/conf/ssl.key/  
server.key
```

Changing the Management Console Password

Trend Micro recommends periodically changing the password you use to access the management console.

**WARNING!**

If you are still using the default password, Trend Micro strongly recommends that you change the password immediately.

Procedure

1. Go to **Administration > Password**.
2. Specify the current password, the new password, and the new password confirmation.

**Note**

A valid password can contain letters, numbers and the following characters: `~!@#%&*()[]{}+~|:'<>?/.,= _.

The password must be between 4 and 32 alphanumeric characters.

3. Click **Save**.
-

Configuring Proxy Settings

If your network uses a proxy server, configure IMSS proxy settings. Proxy settings affect the following:

- Component updates (pattern files and scan engines)
- Product license registration
- Web Reputation queries

Procedure

1. Go to **Administration > Updates > Source**.
2. Under **Proxy Settings**, select **Use a proxy server for updates to patterns, engines, licenses, Web Reputation queries**

3. Specify the proxy protocol: **HTTP**, **SOCKS4**, or **SOCKS5**.
 4. Specify the host name or IP address of the proxy server.
 5. Specify the port the proxy server uses to connect to the Internet.
 6. Specify the user name you need for administrative access to the proxy server.
 7. Specify the corresponding password.
 8. Click **Save**.
-

IMSS Services

The scanner and policy services must be started to start protecting your network using IMSS. You can, however, choose whether to install or start the EUQ service.

- **Scanner Service:** Performs scanning of SMTP/POP3 traffic.
- **Policy Service:** Acts as a remote store of rules for the scanner service to enhance rule lookups.
- **EUQ Service:** Hosts a web-based management console to enable end users to view, delete and release spam messages addressed to them.

For more information on these services, refer to the *Installation Guide*.

Starting or Stopping Services

After you have successfully installed IMSS and configured the various settings, start the services to begin scanning for malware and other threats. You may need to stop IMSS services prior to performing an upgrade or backup function.

Procedure

1. Go to **Summary**.

The **System** tab appears.

2. Under **Managed Server Settings**, click the **Start** or **Stop** button for the service(s) to start or stop.
-

Opening the End-User Quarantine Console

Before you can access the End-User Quarantine (EUQ) web console, ensure that you have done the following:

1. Configured the LDAP settings. See [Configuring LDAP Settings on page 3-6](#).
2. Enabled User Quarantine Access. See [Enabling End-User Access on page 20-7](#).

You can view the EUQ web console from the computer where the program was installed or remotely across the network.

To view the console from another computer on the network, type the following URLs in an Internet browser:

- Primary EUQ service:

```
https://<target server IP address>:8447
```

- Secondary EUQ service:

```
https://<target server IP address>:8446
```



WARNING!

To successfully access all Web management consoles on secondary EUQ services, synchronize the system time of all EUQ services on your network.

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

Logon Name Format

The format of the logon name used when accessing the EUQ management console depends on the selected authentication type.

TABLE 2-1. EUQ Logon Name Formats

AUTHENTICATION TYPE	LOGON NAME FORMAT
LDAP	<p>The format of the logon name depends on the type of LDAP server you selected when configuring LDAP settings. The following are examples of valid logon name formats.</p> <ul style="list-style-type: none"> • Domino: user1/domain • Microsoft Active Directory <ul style="list-style-type: none"> • Without Kerberos: user1@domain.com (UPN) or domain\user1 • With Kerberos: user1@domain.com • Sun iPlanet Directory: uid=user1, ou=people, dc=domain, dc=com
SMTP	<p>Use any valid email address for the logon name.</p> <hr/> <p> Note IMSS supports <code>auth login</code>, <code>auth plain</code> and <code>starttls</code>.</p> <hr/>

Selecting a Scan Method

IMSS provides two scanning methods for detection of malware and other security threats.

Procedure

1. Navigate to **Policy > Scan Method**.

The **Scan Method** screen displays.

Scan Method

Scan Method

Smart Scan (Smart Protection Network) ⓘ
 Conventional Scan ⓘ

Smart Scan Proxy Settings

Use a proxy server to connect to the Smart Protection Network.

Proxy type: HTTP

Proxy server:

Proxy server port:

User name:

Password:

Save Cancel

2. Select one of the following malware scanning methods.

- **Smart Scan:** Smart Scan leverages threat signatures that are stored in the cloud.

When in Smart Scan mode, IMSS uses the Smart Scan Agent Pattern to check for security risks. The Smart Scan Agent Pattern is updated daily by Trend Micro and delivers the same protection provided by conventional anti-malware and antispyware patterns. If the Smart Scan Agent Pattern cannot determine the reputation of a file, IMSS queries the Smart Protection Network to provide up-to-date protection.

- **Conventional Scan:** Conventional scan leverages anti-malware and antispyware components stored locally.

The Virus Pattern contains information that helps IMSS identify the latest virus/malware and mixed threat attacks. Trend Micro creates and releases new versions of the Virus Pattern several times a week, and any time after the discovery of a particularly damaging virus/malware.



Conventional Scan is the default scan method.

3. Optional: Use an HTTP proxy server to connect to the Smart Protection Network. Specify the following:
 - Proxy server address
 - Proxy server port
 - User name
 - Password
4. Click **Save**.



IMSS automatically restarts the IMSS Scan Service whenever you change your scan method settings.

If Smart Scan is selected:

- IMSS attempts to connect to the Smart Protection Network immediately after you click **Save**. If a connection is not established, IMSS does not save your settings. Reselect a scan method and save your settings again.
- If there are ten (10) connection timeouts to the Smart Protection Network in three (3) minutes, IMSS reverts to Conventional Scan. To use Smart Scan again, go to the **Scan Method** screen and reselect Smart Scan.



When IMSS reverts to Conventional Scan, you can query system event logs for each scanner's connection timeouts. If any scanner has frequent connection timeouts, check the network configuration of that scanner. For details on querying system event logs, see [Querying System Event Logs on page 16-7](#).

- You can configure IMSS to send notifications for unsuccessful attempts to connect to the Smart Protection Network. For details on configuring notifications, see [*Notifications on page 18-1*](#).

Chapter 3

Using the Configuration Wizard

This chapter explains how to get IMSS up and running using the configuration wizard.

Topics include:

- *Accessing the Configuration Wizard on page 3-2*
- *Configuring Notification Settings on page 3-2*
- *Configuring the Update Source on page 3-4*
- *Configuring LDAP Settings on page 3-6*
- *Configuring Internal Addresses on page 3-8*
- *Configuring Control Manager Server Settings on page 3-10*
- *Configuring Product Settings on page 3-11*
- *Verifying Settings Summary on page 3-12*

Accessing the Configuration Wizard

Access the wizard using one of the following methods:

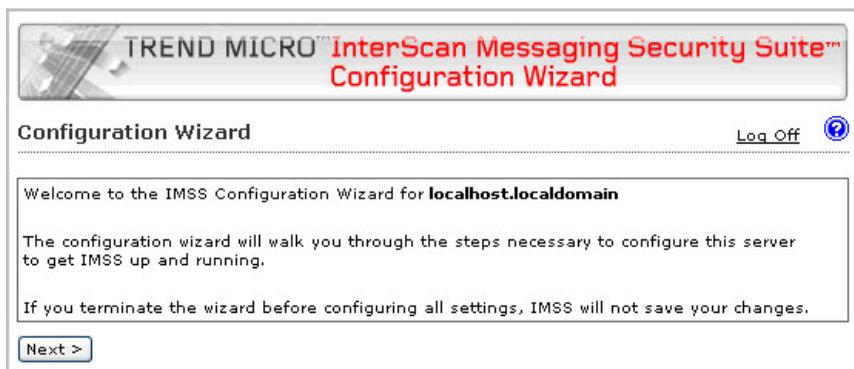
Procedure

- Log on to the web management console and make sure the **Open Configuration Wizard** is selected on the logon screen, and then log on.

The wizard opens.

- If you are already logged on to the web management console, go to **Administration > IMSS Configuration > Configuration Wizard**.

The wizard opens in a new window.



Configuring Notification Settings

Procedure

1. Click **Next**.

The **Notification Settings** screen appears.

Central Controller
Step 2 of 8

Notification Settings ⓘ

Configure email and SNMP trap notifications for **system and policy event notifications**

Email Settings

To address(es):* eddy_trend_rcv@test.com
Use a semicolon ";" to separate multiple addresses

Sender's email address:* eddy_trend_send@test.com

SMTP server address:* 10.64.48.11

SMTP server port:* 25

Preferred charset:* UTF-8 (utf-8) ▼

Message header:

Message footer:

SNMP Trap

Server name (IP or FQDN):

Community: public

< Back Skip Next >

Step

1. SMTP Routing
- 2. Notification Settings**
3. Update Source
4. LDAP Settings
5. Internal Addresses
6. TCM Settings
7. Product Settings
8. Settings Summary

2. Under **Email Settings**, configure the following:
 - **Recipient:** Specify the recipient email addresses.
 - **Sender's email address:** Specify the email address to appear as the sender.
 - **SMTP server address:** Specify the Fully Qualified Domain Name (FQDN) or the IP address (IPv4 or IPv6) of the SMTP server that delivers email on the network.
 - **SMTP server port:** Specify the port number that IMSS uses to connect to the SMTP server.
 - **Preferred charset:** IMSS will use this setting to encode the notification messages.
 - **Message header:** Specify the text to appear at the top of the notification.
 - **Message footer:** Specify the text to appear at the bottom of the notification.
3. Under **SNMP Trap**, configure the following:



Note

SNMP Trap is the notification message sent to the Simple Network Management Protocol (SNMP) server when events that require administrative attention occur.

- **Server name:** Specify the FQDN or IP address of the SNMP server.
 - **Community:** Specify the SNMP server community name.
-



Note

Community is the group that computers and management stations running SNMP belong to. To send the alert message to all SNMP management stations, specify “public” as the community name. For more information, refer to the SNMP documentation.

Configuring the Update Source

Procedure

1. Click **Next**.

The **Update Source** screen appears.

Central Controller
Step 2 of 7

Update Source ⓘ

Select an update source and configure proxy settings to enable IMSS to **update components** and **activate product licenses**.

Source

Trend Micro's ActiveUpdate server

Other Internet source

http://

Proxy Settings

Use a proxy server for updates to patterns, engines, licenses, and for Web Reputation queries.

Proxy type:* SOCKS4

Proxy server:* 2001:ODB:

Port:* 25

User name:

Password: *****

< Back Skip Next >

Step

1. Notification Settings
2. **Update Source**
3. LDAP Settings
4. Internal Addresses
5. TCMC Settings
6. Product Settings
7. Settings Summary

2. Configure the following update settings, which will determine from where IMSS will receive its component updates and through which proxy (if any) IMSS needs to connect to access the Internet:

OPTION	DESCRIPTION
Source	Click Trend Micro ActiveUpdate server to receive updates directly from Trend Micro. Alternatively, click Other Internet source and specify the URL of the update source that will check the Trend Micro ActiveUpdate server for updates. You can specify an update source of your choice or type the URL of your Control Manager server <code>http://<CM server address>/ControlManager/download/activeupdate/</code> , if applicable.
Proxy Settings	Select the Use a proxy server for updates to patterns, engines, licenses, Web Reputation queries check box and configure the proxy type, server name, port, user name, and passwords.

Configuring LDAP Settings



Note

Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or End-User Quarantine authentication.

Procedure

1. Click **Next**.

The **LDAP Settings** screen appears.

The screenshot shows the 'Central Controller' interface at 'Step 3 of 7'. The main heading is 'LDAP Settings'. Below the heading, there is a note: 'Enter LDAP settings **only** if you will use LDAP for user-group definition, administrator privileges, or web quarantine authentication. You must enable LDAP to use the web quarantine tool.' To the right of the main content is a 'Step' navigation pane with a list of steps: 1. Notification Settings, 2. Update Source, 3. LDAP Settings (highlighted), 4. Internal Addresses, 5. TCM Settings, 6. Product Settings, and 7. Settings Summary.

The 'LDAP Settings' section contains the following fields:

- LDAP server type:** A dropdown menu set to 'Microsoft Active Directory'.
- Enable LDAP1:** An unchecked checkbox.
- LDAP server:** A text input field containing '10.64.72.239'. Below it is the example text: 'Example: example.com or 123.123.123.123'.
- Listening port number:** A text input field containing '3268'.
- Enable LDAP2:** An unchecked checkbox.
- LDAP server:** A text input field (empty). Below it is the example text: 'Example: example.com or 123.123.123.123'.
- Listening port number:** A text input field containing '389'.

Below the LDAP settings is a section titled 'LDAP cache expiration for policy services and EUQ services' with a single field: 'Time to Live in minutes:' with a text input field containing '1440'.

LDAP admin

LDAP admin account:*

Password:*

Base distinguished name:*
 Example: DC=foo, DC=foonet, DC=org

Authentication method:* Simple  Advanced: using Kerberos authentication for Active Directory

Kerberos authentication default realm:

Default domain:

KDC and admin server:

KDC port number:

< Back Skip Next >

2. Complete the following to enable LDAP settings:
 - a. For **LDAP server type**, select one of the following:
 - **Domino**
 - **Microsoft Active Directory**
 - **Sun iPlanet Directory**
 - b. To enable one or both LDAP servers, select the check boxes next to **Enable LDAP 1** or **Enable LDAP 2**.
 - c. Specify the names of the LDAP servers and the port numbers they listen on.
 - d. Under **LDAP cache expiration for policy services and EUQ services**, specify a number that represents the time to live next to the **Time to Live in minutes** field.
 - e. Under **LDAP admin**, specify the administrator account, its corresponding password, and the base-distinguished name. See the following table for a guide on what to specify for the LDAP admin settings.

TABLE 3-1. LDAP Server Types

LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory™	Without Kerberos: user1@domain.com (UPN) or domain\user1 With Kerberos: user1@domain.com	dc=domain, dc=com	Simple Advanced (with Kerberos)
Lotus Domino™	user1/domain	Not applicable	Simple
Sun™ iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	Simple

- f. For **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos authentication default realm, Default domain, KDC and admin server, and KDC port number.

Configuring Internal Addresses

IMSS uses the internal addresses to determine whether a policy or an event is inbound or outbound.

- If you are configuring a rule for outgoing messages, the internal address list applies to the senders.
- If you are configuring a rule for incoming messages, the internal address list applies to the recipients.

Procedure

1. Click **Next**.

The **Internal Addresses** screen appears.

The screenshot shows the 'Central Controller' interface at 'Step 4 of 7'. The main heading is 'Internal Addresses' with a help icon. Below it is a descriptive text: 'Define your internal domains (known users or domains). IMSS uses these to determine which policies and events are "Incoming" and "Outgoing" for reporting and rule creation.' The main area is titled 'Internal domains and usergroups' and contains a form with a 'Enter domain' dropdown menu, a text input field, an '>>' button, and an 'Import from File' button. To the right is a 'Selected' list box with several empty rows. At the bottom are '< Back' and 'Next >' buttons. On the far right, a 'Step' list shows: 1. Notification Settings, 2. Update Source, 3. LDAP Settings, 4. Internal Addresses (highlighted), 5. TCM Settings, 6. Product Settings, 7. Settings Summary.

2. To define internal domains and user groups, do one of the following:
 - Select **Enter domain** from the drop-down list, specify the domain in the text box, and then click **>>**.
 - Select **Search for LDAP groups** from the drop-down list. A screen for selecting the LDAP groups appears. Specify an LDAP group name to search in the text box and click **Search**. The search result appears in the list box. To add it to the **Selected** list, click **>>**.
-

Configuring Control Manager Server Settings

Procedure

1. Click **Next**.

The **TMCM Server Settings** screen appears.

Central Controller
Step 5 of 7

TMCM Server Settings

To manage IMSS with Control Manager, enable the Control Manager MCP agent and configure all Control Manager server settings.

Enable MCP Agent

Server: *

Communication protocol: *

HTTP port: 80

HTTPS port: 443

Web server authentication:

User name: *

Password: *

Proxy Settings

Enable proxy

Proxy type: *

Proxy server: *

Port: *

User name:

Password: *

< Back Skip Next >

Step

1. Notification Settings
2. Update Source
3. LDAP Settings
4. Internal Addresses
5. **TMCM Settings**
6. Product Settings
7. Settings Summary

2. If you will use Control Manager to manage IMSS, do the following:
 - a. Enable the agent (installed with IMSS by default).
 - b. Next to **Server**, specify the Control Manager IP address (IPv4 or IPv6) or FQDN.
 - c. Next to **Communication protocol**, select **HTTP** or **HTTPS** and specify the corresponding port number.

The default port number for HTTP access is 80, and the default port number for HTTPS is 443.

- d. Under **Web server authentication**, specify the user name and password for the web server if it requires authentication.
- e. If a proxy server is between IMSS and Control Manager, select **Enable proxy**.
- f. Specify the proxy server port number, user name, and password.

Configuring Product Settings

Procedure

1. Click **Next**.

The **Product Settings** screen appears.

Central Controller
Step 6 of 7

Product Settings ? **Step**

You must **activate the IMSS Antivirus and Content Filter** to enable scanning and to update components. For added spam protection, activate Spam Prevention Solution and the IP Filter.

To obtain an Activation Code, register the product online using your Registration Key.

[Register Online](#)

Activate

Trend Micro Antivirus and Content Filter:

Spam Prevention Solution:

[< Back](#) [Next >](#)

Step

1. Notification Settings
2. Update Source
3. LDAP Settings
4. Internal Addresses
5. TMCM Settings
- 6. Product Settings**
7. Settings Summary

2. To obtain an Activation Code, click **Register Online** and follow the directions at the **Trend Micro Registration** website.
3. After obtaining the applicable Activation Codes, specify the Activation Code for each product or service to activate.

Verifying Settings Summary

Procedure

1. Click **Next**.

A **Settings Summary** screen appears.



2. If the settings are correct, click **Finish**.

To modify any specified setting, click **Back** and make changes.

Chapter 4

Updating Components

This chapter explains how to update IMSS components.

Topics include:

- *Updating Engine and Pattern Files on page 4-2*
- *Specifying an Update Source on page 4-3*
- *Performing a Manual Update on page 4-4*
- *Rolling Back a Component Update on page 4-6*
- *Scheduled Component Updates on page 4-6*

Updating Engine and Pattern Files

To ensure that your network is constantly protected against the latest malware, update IMSS components on a regular basis. You can choose to perform manual or scheduled updates.

The following table provides a list of all IMSS components.

TABLE 4-1. IMSS Components

COMPONENT	DESCRIPTION
Virus Scan Engine	The Virus Scan Engine detects Internet worms, mass-mailers, Trojans, phishing sites, spyware, network exploits and viruses in messages and attachments.
Virus Pattern	The Virus Pattern contains information that helps IMSS identify the latest viruses/malware and mixed attacks.
Spyware Pattern	The Spyware Pattern identifies spyware/grayware in messages and attachments.
IntelliTrap Pattern	The IntelliTrap Pattern detects real-time compression files packed as executable files.
IntelliTrap Exception Pattern	The IntelliTrap Exceptions Pattern contains a list of "approved" compression files.
Antispam Engine	The Antispam Engine detects spam in messages and attachments.
Antispam Pattern	The Antispam Pattern helps IMSS identify the latest spam in messages and attachments.
URL Filtering Engine	The URL Filtering Engine facilitates communication between IMSS and the Trend Micro URL Filtering Service. The URL Filtering Service is a system that rates URLs and provides rating information to IMSS.
Smart Scan Agent Pattern	The Smart Scan Agent Pattern contains pattern definitions used by IMSS when in Smart Scan mode. IMSS downloads this pattern from the update source using the same methods for downloading other components.

Specifying an Update Source

Before you can update the IMSS scan engine and pattern files, specify the update source. By default, IMSS downloads components from the Trend Micro ActiveUpdate server, which is the source for up-to-date components. However, if you are using Trend Micro Control Manager to manage IMSS, you can update the components from the Control Manager server.

If you did not specify the update source when configuring IMSS using the Configuration Wizard, provide the update source and/or any proxy settings.

Procedure

1. Go to **Administration > Updates**.

The **Updates** screen appears.

2. Click the **Source** tab.

Screenshot of the **Source** tab in the IMSS Configuration Wizard. The **Source** section has two radio buttons: **Trend Micro's ActiveUpdate server** (selected) and **Other Internet source**. Below the second radio button is a text box containing `http://`. The **Proxy Settings** section has a checkbox **Use a proxy server for updates to patterns, engines, licenses, and for Web Reputation queries.** which is unchecked. Below it are fields for **Proxy type:** `SOCKS4`, **Proxy server:** `2001:0DB::`, **Port:** `25`, **User name:** (empty), and **Password:** (masked with dots). **Save** and **Cancel** buttons are at the bottom.

3. Under **Source**, select one of the following:

- **Trend Micro ActiveUpdate server:** The default source for up-to-date components.
 - **Other Internet source:** Specify the URL or IP address of the Control Manager server or other update source.
4. If the connection to ActiveUpdate, Product Registration Server, and Web reputation servers must pass through a proxy server, select **Use a proxy server for updates to patterns, engines, licenses, and for Web Reputation queries**, and then configure the following:

OPTION	DESCRIPTION
Proxy type	Select HTTP, SOCKS4, or SOCKS5.
Proxy server	Specify the host name or IP address (IPv4 or IPv6) of the proxy server.
Port	Specify the port the proxy server uses to connect to the Internet.
Password	Specify the corresponding password.

5. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

Performing a Manual Update

Perform a manual update of IMSS components under the following circumstances:

- If you have just installed, deployed, or upgraded IMSS.
- If you suspect that your network's security is compromised by new malware and would like to update the components immediately.

Procedure

1. Go to the **Summary** screen.

Summary ?

System | **Statistics**

Enable Connections

Accept SMTP connections
 Enable IP Filtering ⓘ
 Accept POP3 connections
 ... ERS IP Profiler

Components Last refresh: Jul 13, 2013 7:36:04 PM

<input type="checkbox"/>	Name	Current Version	Availability	Update Schedule
<input type="checkbox"/>	Virus Scan Engine	9.700.1001	9.700.1001	15 minutes
<input type="checkbox"/>	Virus Pattern	10.151.00	10.151.00	15 minutes
<input type="checkbox"/>	Spyware Pattern	1.417.00	1.417.00	15 minutes
<input type="checkbox"/>	IntelliTrap Pattern	0.171.00	0.171.00	15 minutes
<input type="checkbox"/>	IntelliTrap Exception Pattern	0.889.00	0.889.00	15 minutes
<input type="checkbox"/>	Antispam Engine	7.000.1014	0.0	15 minutes
<input type="checkbox"/>	Antispam Pattern	20012.005	20012.005	15 minutes
<input type="checkbox"/>	URL Filtering Engine	3.000.1029	3.000.1029	15 minutes
<input type="checkbox"/>	Smart Scan Agent Pattern	9.735.00	0	15 minutes
	IMSS	Version: 9.735.00 Build: 2013071000	N/A	N/A

Managed Server Settings

Hostname	Connection	Scanner Service	Policy Service	Web Quarantine
imss752.thomas.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="button" value="Stop"/>	<input checked="" type="checkbox"/> <input type="button" value="Stop"/>	<input checked="" type="checkbox"/> <input type="button" value="Stop"/>

2. Under **Components**, verify the version numbers of the antivirus, antispyware, and antispam components that IMSS uses to protect your network.
3. To update all components, select the first check box on the column header next to the **Name** field. To update specific component(s), select the check box next to the desired component.
4. Click **Update**.

Rolling Back a Component Update

If you encounter any system issues after updating IMSS components, you can roll back to the previous version.

Procedure

1. Go to the **Summary** screen.
The **System** tab loads by default.
 2. To roll back all components to the previous versions, select the first check box on the column header next to the **Name** field. To roll back specific component(s), select the check box next to the desired component.
 3. Click the **Rollback** button.
-

Scheduled Component Updates

Updating components is a two-step process:

1. At the scheduled time, the IMSS admin database will first check the update source for new engine or pattern files.
2. IMSS scanners will then check the admin database at regular intervals for updated components. The default interval is three minutes.

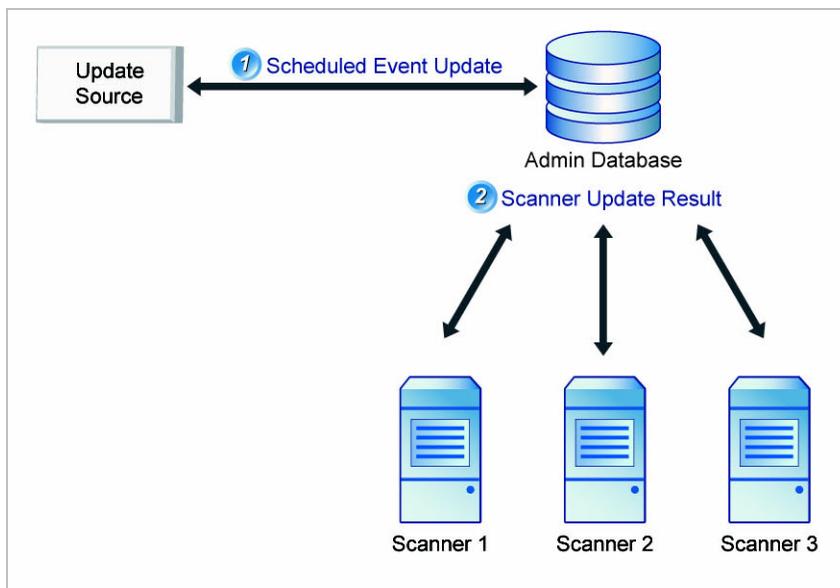


FIGURE 4-1. Scan engine and pattern file updates

Configuring Scheduled Updates

If you are unable to regularly download antivirus and antispam components, your network will be at risk from Internet threats. To automate the update process, configure an update schedule. If your network has limited Internet bandwidth, schedule updates during off-peak hours.

Procedure

1. Go to **Administration > Updates**.

The **Updates** screen appears with the **Schedule** tab selected by default.

The screenshot shows the 'Component Updates' window with the 'Schedule' tab selected. The window is titled 'Component Updates' and has a help icon in the top right corner. Below the title bar are two tabs: 'Schedule' (selected) and 'Source'. The main content area is divided into three sections:

- Enable scheduled update:** A checked checkbox.
- Update Component:** A list of components, each with a checked checkbox:
 - Virus Scan Engine
 - Advanced Threat Scan Engine
 - Virus Pattern
 - Spyware Pattern
 - IntelliTrap Pattern
 - IntelliTrap Exception Pattern
 - Antispam Engine
 - Antispam Pattern
 - URL Filtering Engine
 - Smart Scan Agent Pattern
- Update Schedule:** A section for configuring the update frequency. It includes:
 - Minutes intervals:** Selected with a radio button, set to 15 minutes.
 - hourly:** Unselected with a radio button, set to 00 minutes.
 - daily:** Unselected with a radio button, set to 0 hours and 00 minutes.
 - weekly:** Unselected with a radio button, set to Sunday, 0 days, and 00 minutes.

At the bottom of the window are 'Save' and 'Cancel' buttons.

2. Select the **Enable scheduled update** check box.
3. Under **Update Component**, select the components to update. Trend Micro recommends updating all components.
4. Under **Update Schedule**, select the update frequency:
 - **Minute intervals:** Updates every { } minutes per hour. Select the minute interval.

For example, if you select 15, the update is triggered four times an hour: at 00, 15, 30, 45 minutes. If you select 30, the update will be triggered twice an hour: at 00 and 30 minutes.

- **Hourly:** Updates every hour at { } minutes. Select the number of minutes after the hour.

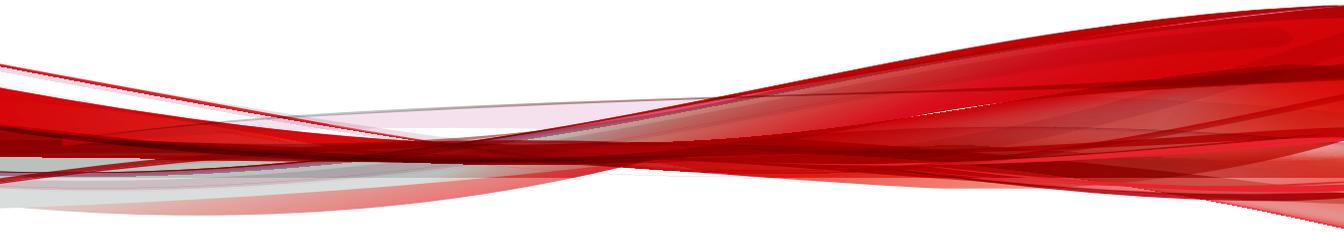
For example, if you select 15, the update is triggered at 15 minutes after the hour, every hour.

- **Daily:** Updates every day at the time you choose. Select the time of day.
- **Weekly:** Updates once a week at the specified day and time. Select a day of the week and the time of day.

5. Click **Save**.

Part II

Configuring IMSS



Chapter 5

Configuring IP Filtering Settings

This chapter provides general descriptions about the various configuration tasks to get IMSS up and running.

Topics include:

- *IP Filtering Service on page 5-2*
- *Using Email Reputation on page 5-2*
- *Configuring IP Filtering on page 5-8*
- *Displaying Suspicious IP Addresses and Domains on page 5-21*

IP Filtering Service

The IP Filtering service has two individual components: Email Reputation and IP Profiler.

- Email reputation filters connections from spam senders when establishing SMTP sessions.
- IP Profiler helps protect the mail server from attacks with smart profiles from the Intrusion Detection Service (IDS).



Tip

Trend Micro recommends deploying IP Filtering as the first line of defense in your messaging infrastructure.

Although most email systems have a multi-layer structure that often includes some pre-existing IP blocking, spam filtering, and virus filtering, Trend Micro recommends completely removing other IP blocking techniques from the messaging environment. IP Filtering should act as the precursor to any application filtering you might use.



Note

IP Filtering is only available from IPv4 networks. Incoming email messages from IPv6 networks are not blocked by Email Reputation or IP Profiler.

Using Email Reputation

Trend Micro maintains a list of IP addresses belonging to known spam senders in a central database. Email reputation filters spam by blocking the IP addresses stored in this database.

Using the SPS Activation Code

IP Filtering Service, which includes Email reputation and IP Profiler, uses the same license as Spam Prevention Solution (SPS). If you purchase the full SPS service package, you will receive a Registration Key that will allow you to create a customer account with

Trend Micro. Upon completion of the registration process, you will receive your Activation Code.

The Activation Code enables you to access the level of services according to your registration. When you activate SPS, the licensing information for IP Filtering will then appear.

For details on configuring Email Reputation, see *Configuring IP Filtering on page 5-8.*

Preparing Your Message Transfer Agent for Use With Email Reputation Services

Configure your MTA to perform the appropriate DNS queries for the type of Email Reputation to which you subscribed.

- **Standard:** Blocks connections with a 550 level error code (“connection refused”). The MTA returns this error code to the server initiating the connection because the IP address is in the Standard Reputation database as a known spammer.
- **Advanced:** Configure the MTA to make two DNS queries. If the MTA does not receive a response from the first query to the standard reputation database, it makes a second query to the dynamic reputation database. The MTA should return a temporarily deny connection 450 level error code (“server temporarily unavailable, please retry”) when a response is received from this database.

Legitimate email servers with compromised hosts temporarily sending spam may be listed in the dynamic reputation database. If the connection request is from a legitimate email server, it will re-queue and try sending the message later. This process will cause a short delay in mail delivery until the listing expires but will not permanently block the email.

Some servers may have additional options for handling questionable IP connections. These options include throttling or routing messages for more detailed scanning.

You can find instructions for configuring the MTA or firewall on the Trend Micro website:

<https://tmspn.securecloud.com/>

These instructions have been provided by the vendor or manufacturer of the product (MTA or firewall). Refer to your product manuals and/or technical support organization for detailed configuration and setup options.



Note

Insert your Activation Code to replace the instructional text example; do not include any dashes.

Using the Email Reputation Management Console

Log on to the Email reputation management console to access global spam information, view reports, create or manage Email reputation settings, and perform administrative tasks.

This section includes basic instructions for using the Email reputation management console. For detailed instructions on configuring the settings for each screen, see the Email reputation management console Online Help. Click the help icon in the upper right corner of any help screen to access the Online Help.

Procedure

1. Open a web browser and type the following address:

<https://ers.trendmicro.com/>

2. Log on using your Email reputation user name and password.

The **Smart Protection Network** portal opens with the **Email** tab selected and the **General** screen displaying.

3. Select **Global Spam Statistics** from the menu.

The **Global Spam Statistics** screen appears.

The **Global Spam Statistics** screen ranks ISPs based on the amount of spam they send. The ISP Spam list displays the total spam volume from the top 100 ISPs for a specific week. The networks that are producing the most spam are ranked at the top. The ranking of the ISPs changes on a daily basis. The ISP Spam list displays the following:

TABLE 5-1. ISP Spam List

COLUMN	DESCRIPTION
Rank This Week	Displays the global rank for this week in terms of total spam volume.
Rank Last Week	Displays the global rank for the previous week in terms of total spam volume.
ASN	The Autonomous System Number (ASN) is a globally unique identifier for a group of IP networks having a single, clearly defined routing policy that is run by one or more network operators.
ISP Name	The registered name for a particular ASN. Some ISPs may have multiple ASNs and therefore appear more than once in the table.
Spam Volume (24 hours)	The estimated total spam that has been sent during the previous 24 hours. This total is updated every hour.
Botnet Activity	An indication of how active botnets are for your email servers. Botnets are groups of infected computers that are controlled by a spammer from a central location and are the largest source of spam on the Internet today. This number indicates the percentage change in the number of bots from the previous hour. To see botnet activity, you must add your email servers to the Valid Mail Servers list.

4. Click **News**.

The **News** screen appears displaying breaking news about new spam and new features available for Email reputation. Click the following tabs for information:

- **Spam News:** Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new

tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.

- **Release News:** Provides a brief overview of new features available in Email reputation.
5. To view reports that summarize the activity between the MTA and the Email reputation database servers, do the following:
 - a. Select **Report** from the menu.
A sub-menu appears.
 - b. Click one of the following:

TABLE 5-2. Report Types

REPORT	DESCRIPTION
Percentage Queries	The report shows the percentage of queries that returned an IP address match, which indicates that a sender trying to establish a connection with your email server is a known spammer. The reports are based on connections, not individual spam messages.
Queries per Hour	The report shows how many times your email server queried the reputation database.
Queries per Day	The report shows how many times per day your email server queried the reputation database.
Botnet Report	The report provides a quick summary of the last seven days of spam activity originating from the servers that you listed as valid mail servers. If there was any spam activity in the last seven days for any of the IP addresses that you specified, a red robot icon appears.

6. To manage protection provided by Email reputation settings:
 - a. Select **Policy** from the menu.
A sub-menu appears.
 - b. Click one of the following:

TABLE 5-3. Policy Settings

POLICY	DESCRIPTION
Settings	<p>Configure the Approved and Blocked senders lists.</p> <p>You can define your lists by individual IP address and Classless Inter-Domain Routing (CIDR) by Country, or by ISP.</p> <ul style="list-style-type: none"> • Approved Sender: Allows messages from the approved senders to bypass IP-level filtering. The Approved Sender lists are not applied to your MTA, but you can set up additional approved or blocked senders lists or do additional filtering at your MTA. • Blocked Sender: Instructs Email reputation to always block email messages from certain countries, ISPs, and IP addresses.
New ISP Request	<p>Trend Micro welcomes suggestions from customers regarding other Internet Service Providers (ISPs) to be added to the service.</p> <p>Provide as much information about an ISP as you can. This helps Trend Micro add the ISP to the service.</p>

POLICY	DESCRIPTION
Reputation Settings	<p>Configure Email reputation Standard and Advanced settings.</p> <p>Standard customers will see only the Enable Standard Settings section.</p> <p>Advanced customers will see both the Dynamic Settings and the Enable Standard Settings sections.</p>

7. To change your password, Activation Code, or to add your mail servers to Email reputation, click **Administration** from the menu.

Configuring IP Filtering

To configure IP Filtering, perform the following steps:

1. [Enabling Email Reputation and IP Profiler on page 5-8](#)
2. [Adding Hosts to the Approved List on page 5-10](#)
3. [Adding Hosts to the Blocked List on page 5-10](#)
4. [Enabling IP Profiler Rules on page 5-11](#)
5. [Configuring ERS on page 5-18](#)

Enabling Email Reputation and IP Profiler

Enable Email reputation and IP Profiler to begin IP Filtering protection. You can enable both or one type of protection.

Procedure

1. Go to **IP Filtering > Overview**.

The **IP Filtering Overview** screen appears.

IP Filtering Overview 

Enable IP Filtering

ERS IP Profiler

Blocked Domains IP Addresses  Refresh Last 1 day (Last 24 hours) ▾

DHA Attack 

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Bounced Mail

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Virus

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Spam

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Manual

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

2. Select the **Enable IP Filtering** check box. This will select both the Email reputation and IP Profiler check boxes.
3. Clear the **Email reputation** or **IP Profiler** check box if you do not require them.
4. Click **Save**.



Note

If you decide to disable IP filtering subsequently, uninstall ERS and IP Profiler manually. Disabling IP filtering from the management console only unregisters IP Profiler from IMSS but does not stop ERS and IP Profiler from running. For more information on uninstalling ERS and IP Profiler, see the Uninstalling Email Reputation Services and IP Profiler section of the IMSS Installation Guide.

Adding Hosts to the Approved List

IMSS does not filter hosts that appear in the Approved List.

Procedure

1. Go to **IP Filtering > Approved List**.

The **Approved List** screen appears.

2. Click **Add**.

The **Add IP/Domain/Subnet Address and Mask to Approved List** screen appears.

3. Select the **Enable** check box.

4. Specify the domain, IP address, or subnet address and mask for the host that you would like to add to the Approved List.

5. Click **Save**.

The host appears in the **Approved List**.

Adding Hosts to the Blocked List

IMSS blocks hosts that appear in the Blocked List.

Procedure

1. Go to **IP Filtering > Blocked List**.

The **Blocked List** screen appears.

2. Click **Add**.

The **Add IP/Domain/Subnet Address and Mask to Blocked List** screen appears.

3. Select the **Enable** check box.
4. Specify the domain, IP address, or subnet address and mask for the host that you would like to add to the Blocked List.
5. Select **Block temporarily** or **Block permanently**.
6. Click **Save**.

The host appears in the **Blocked List**.

Enabling IP Profiler Rules

Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting. Rules can be set for the following:

- Spam
- Viruses
- DHA attacks
- Bounced mail



WARNING!

Before enabling IP Profiler Rules, add all of your email server IP addresses (that send outgoing messages to IMSS) to the IP Filtering Approved List. To configure the IP Filtering Approved List, see [Adding Hosts to the Approved List on page 5-10](#).

Specifying IP Filtering Spam Settings

Procedure

1. Go to **IP Filtering > Rules**.

The **Rules** screen appears with 4 tabs, one for each type of threat.

Rules: IP Profiling Settings (IP Behavior Monitor)

Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting.

Spam | Virus | DHA Attack | Bounced Mail

Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

2. Click the **Spam** tab.

The **Spam** screen appears.

3. Select the **Enable** check box to enable blocking of spam.

4. Specify a value for the following:

- **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of spam messages exceeds the threshold you set.
- **Rate (%):** Specify the maximum number of allowable messages with spam threats.
- **Total mails:** Specify the total number of spam messages out of which the threshold percentage is calculated.

Consider the following example:

Duration to monitor: 1 hour at a rate of 20 out of 100.

During each one-hour period that spam blocking is active, IMSS starts blocking IP addresses when more than 20% of the messages it receives contain spam and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
 - **Block temporarily:** Block messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

Specifying IP Filtering Virus Settings

Procedure

1. Go to **IP Filtering > Rules**.

The **Rules** screen appears with 4 tabs, one for each type of threat.

The screenshot shows a configuration window for IP Filtering Virus Settings. It has four tabs: Spam, Virus (selected), DHA Attack, and Bounced Mail. The Virus tab contains the following settings:

- Enable
- Duration to monitor: 20 hour(s)
- Rate (%): 80 %
- Total mails: 1000
- Triggering action: Block temporarily (dropdown menu)

At the bottom of the window are three buttons: Save, Cancel, and Restore Defaults.

2. Click the **Virus** tab.
- The **Virus** screen appears.
3. Select the **Enable** check box to enable blocking of viruses.
 4. Configure the following:

- **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of messages with viruses exceeds the threshold you set.
- **Rate (%):** Type the maximum number of allowable messages with viruses (the numerator).
- **Total mails:** Type the total number of infected messages out of which the threshold percentage is calculated (the denominator).

Consider the following example.

Duration to monitor: 1 hour at a rate of 20 out of 100

During each one-hour period that virus blocking is active, IMSS starts blocking IP addresses when more than 20% of the messages it receives contain viruses and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
 - **Block temporarily:** Block messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

Specifying IP Filtering Directory Harvest Attack (DHA) Settings

Procedure

1. Go to **IP Filtering > Rules**.

The **Rules** screen appears with 4 tabs, one for each type of threat.

2. Click the **DHA Attack** tab.

The **DHA Attack** screen appears.

3. Select the **Enable** check box to enable blocking of directory harvest attacks.
4. Configure the following:
 - **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of messages signaling a DHA attack exceeds the threshold you set.
 - **Rate (%):** Type the maximum number of allowable messages with DHA threats (the numerator).
 - **Total mails:** Type the total number of DHA messages out of which the threshold percentage is calculated (the denominator).
 - **Sent to more than:** Type the maximum number of recipients allowed for the threshold value.
 - **Non-existing recipients exceeds:** Type the maximum number of non-existent recipients allowed for the threshold value. DHA attacks often include randomly generated email addresses in the receiver list.



Note

The LDAP service must be running to determine non-existing recipients.

Consider the following example.

Duration to monitor: 1 hour at a rate of 20 out of 100 sent to more than 10 recipients when the number of non-existing recipients exceeds 5.

During each one-hour period that DHA blocking is active, IMSS starts blocking IP addresses when it receives more than 20% of the messages that were sent to more than 10 recipients (with more than five of the recipients not in your organization) and the total number of messages exceeds 100.



Tip

Technically, the LDAP server is not a must-have. The DHA rule of IMSS can also obtain the DHA results returned from Postfix, which in turn passes these results to FoxProxy through the LDAP server or other means. FoxProxy then analyzes the results to determine if they are DHA attacks.

LDAP server is only one of the means by which Postfix checks if a user's mailbox exists.

5. Next to **Triggering action**, select one of the following
 - **Block temporarily:** Block messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.
 6. Click **Save**.
-

Specifying IP Filtering Bounced Mail Settings

Procedure

1. Go to **IP Filtering > Rules**.

The **Rules** screen appears with 4 tabs, one for each type of threat.

2. Click the **Bounced Mail** tab.

The **Bounced Mail** screen appears.

The screenshot shows the 'Bounced Mail' configuration window. It features a tabbed interface with 'Spam', 'Virus', 'DHA Attack', and 'Bounced Mail' tabs. The 'Bounced Mail' tab is selected. Inside the window, there is an 'Enable' checkbox which is currently unchecked. Below it are four configuration fields: 'Duration to monitor' (20 hour(s)), 'Rate (%)' (80 %), 'Total mails' (1000), and 'Triggering action' (Block temporarily). At the bottom of the window are three buttons: 'Save', 'Cancel', and 'Restore Defaults'.

3. Select the **Enable** check box to enable blocking of bounced mail.
4. Configure the following:
 - **Duration to monitor:** The number of hours that IMSS monitors email traffic to see if the percentage of messages signaling bounced mail exceeds the threshold you set.
 - **Rate (%):** Specify the maximum number of allowable messages signaling bounced mail (the numerator).
 - **Total mails:** Specify the total number of bounced messages out of which the threshold percentage is calculated (the denominator).

Consider the following example:

Duration to monitor: 1 hour at a rate of 20 out of 100

During each one-hour period that blocking for bounced mail is active, IMSS starts blocking IP addresses when more than 20% of the messages it receives are bounced messages and the total number of messages exceeds 100.



Note

The LDAP service must be running to check bounced mail.

5. Next to **Triggering action**, select one of the following:
 - **Block temporarily:** Block messages from the IP address and allow the upstream MTA to try again.

- **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.

6. Click **Save**.

Configuring ERS

Email reputation verifies IP addresses of incoming messages using the Trend Micro Email Reputation database.

Procedure

1. Go to **IP Filtering > ERS**.

The **ERS** screen appears.

Email Reputation ?

Email Reputation Services verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation database along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets as they first emerge.

Email Reputation Settings

Enable Email Reputation

View global spam information, reports, create or manage Approved and Blocked Sender IP address lists, perform administrative tasks, and configure the service.

[Email Reputation Portal](#)

Set Service Level

Standard: Uses the Standard Reputation database to block messages from known spam sources. [Click for more information.](#)

- Default intelligent action
- Connection closed with no returning code
- Connection rejected with:
 - SMTP error code:
 - SMTP error string : (alphanumeric letters)
 -
- Delay connection by: seconds
- Pass and log only

Advanced: Uses both Standard and Dynamic Reputation databases to block messages from known and suspected spam sources. [Click for more information.](#)

- Default intelligent action
- Connection closed with no returning code
- Connection rejected with:
 - SMTP error code:
 - SMTP error string : (alphanumeric letters)
 -
- Delay connection by: seconds
- Pass and log only

2. Select the **Enable ERS** check box.
3. Click a radio button next to one of the following, depending on your level of service, and configure the settings:

Standard:

- **Default intelligent action:** ERS permanently denies connection (550) for RBL + matches.
- **Take customized action for all matches:**
 - **SMTP error code:** Blocks any connections that have a certain SMTP code. Specify an SMTP code.
 - **SMTP error string:** Specify the message associated with the SMTP error code.

Advanced:

- **Default intelligent action:** ERS permanently denies connection (550) for RBL + matches and temporarily denies connection (450) for Zombie matches.
- **Take customized action for all matches:**
 - **SMTP error code:** Blocks any connections that have a certain SMTP code. Specify an SMTP code.
 - **SMTP error string:** Specify the message associated with the SMTP error code.

**Note**

The above SMTP error code and error string will be sent to the upstream MTA that will then take the necessary pre-configured actions, such as recording the error code and error string in a log file.

4. Click **Save**.
-

Displaying Suspicious IP Addresses and Domains

IMSS creates log entries of the IP addresses or domains that have sent messages violating scanning conditions, but are still not blocked because the total number of messages did not exceed the threshold you set for the given time period.

Procedure

1. Go to **IP Filtering > Suspicious IP**.
2. Configure any of the following:
 - Next to **Type**, select the check boxes next to the type of threat that the IP filter detected.
 - Next to **Dates**, select the date-time range within which IMSS blocked the sender.
 - If you know a specific IP address to query, specify it next to **IP**.
 - To display the corresponding domain names of the IP addresses, select the **Show Domain names** check box.
 - Next to **Logs per page**, select the number of log entries to display on the screen at a time.
3. Click **Display Log**.
4. Perform any of the additional actions:
 - To block an IP address temporarily, select the corresponding check box in the list, then click **Block Temporarily**.
 - To block an IP address permanently, select the corresponding check box in the list, then click **Block Permanently**.
 - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.

- To sort the table, click the column title.
-

Chapter 6

Scanning SMTP Messages

This chapter provides general descriptions on the various configuration tasks that you need to perform to get IMSS up and running. For further details, refer to the Online Help accessible from the management console.

Topics include:

- *Message Transfer Agents on page 6-2*
- *Enabling SMTP Connections on page 6-2*
- *Configuring SMTP Routing on page 6-2*
- *About Message Delivery on page 6-11*

Message Transfer Agents

IMSS supports three types of Message Transfer Agents (MTA). They are Postfix, Sendmail, and Qmail.

If you are using Postfix with IMSS and have deployed multiple scanner services, you can manage the SMTP routing settings for the scanner services centrally. From the IMSS management console, configure the SMTP settings and apply the same settings to all scanners.

If you are using Sendmail or Qmail, you will need to manually configure the SMTP settings in the respective MTA configuration files. For details, see *Preparing Message Transfer Agents* section of the *IMSS Installation Guide*.

Enabling SMTP Connections

Before IMSS can start scanning incoming and outgoing traffic on your network, enable SMTP connections.

Procedure

1. Go to **Summary** from the menu.
The **System** tab appears by default.
 2. Select the **Accept SMTP connections** check box.
 3. Click **Save**.
-

Configuring SMTP Routing

The following procedure explains the tasks required to configuring SMTP routing.

**Note**

IMSS 7.1 SP2 can communicate to upstream or downstream components in IPv6 networks.

1. *Configuring SMTP Settings on page 6-3*
2. *Configuring Connection Settings on page 6-4*
3. *Configuring Message Rule Settings on page 6-8*
4. *Configuring Message Delivery Settings on page 6-11*

Configuring SMTP Settings

Use the SMTP screen to configure SMTP settings for the MTA, such as the SMTP greeting message and the location of the mail processing queue, where IMSS saves messages before it scans and delivers them.

Procedure

1. Go to **Administration > IMSS Configuration > SMTP Routing**.

The **SMTP Routing** screen appears.

SMTP Routing

Apply settings to all scanners

SMTP | Connections | Message Rule | Message Delivery

Greeting Message

SMTP server greeting message:

ESMTP Postfix

Mail Processing Queue

The Mail Processing Queue is used to save messages prior to scanning or delivery.

Path: /var/spool/postfix

Example: /var/spool/postfix

Save Cancel

2. Select the **Apply** settings to all scanner check box.

This option applies all the settings configured in each tab to all scanners connected to the same IMSS administration database.

3. Specify SMTP server **Greeting Message** (displays when a session is created).
4. Specify the **Mail Processing Queue Path**.
5. Click **Save**.

Configuring Connection Settings

Configure SMTP connection settings for the MTA from the Connection settings screen.

Procedure

1. Go to **Administration > IMSS Configuration > SMTP Routing**.
2. Click the **Connections** tab.

The **Connections** screen appears.

The screenshot shows the 'Connections' configuration window. At the top, there are four tabs: 'SMTP', 'Connections' (which is active), 'Message Rule', and 'Message Delivery'. Below the tabs is the 'SMTP Interface' section, which contains the following settings:

- IP address:** A dropdown menu set to 'All interfaces'.
- Port:** A text input field containing '25'.
- Disconnect after:** A text input field containing '5' followed by the text 'minutes of inactivity'.
- Simultaneous connections:** Two radio buttons. The first is 'No limit'. The second is 'Allow up to' followed by a text input field containing '100' and the text 'connections'.

Below this is the 'Connection Control' section, which starts with the text 'You can either permit or deny computers to connect with the server.' It has two main radio button options:

- Accept all, except the following list:** This is selected. It has a sub-option 'Single computer' which is also selected. Below it is an empty text input field. Further down are examples: 'Examples: 123.123.123.123 or 2001:db8:10ff:iae:44f2'. There is also a sub-option 'Group of computers' which is not selected. Below it are fields for 'IP version' (set to 'IPv4'), 'Subnet address:' (with an empty input field), 'Example: 10.123.123.123', and 'Subnet mask:' (with an empty input field and 'Example: 255.255.255.0'). There are '>>' and '<<' buttons between the IP version and Subnet address fields. At the bottom of this section are 'Import from File' and 'Export' buttons.
- Deny all, except the following list:** This option is not selected.

At the bottom of the window is the 'Transport Layer Security Setting' section, which has a checkbox 'Enable Transport Layer Security' that is not checked. Below it is a sub-option 'Only accept SMTP connection by TLS' which is checked. There are three rows of settings, each with a 'Choose File' button, a status indicator, and an 'Upload' button:

- CA certificate:** Choose File button, 'No file chosen', Upload button.
- Private key:** Choose File button, 'No file chosen', Upload button.
- SMTP server certification:** Choose File button, 'No file chosen', Upload button.

At the very bottom of the window are 'Save' and 'Cancel' buttons.

3. Specify the **SMTP Interface** settings.

- **IP address:** Select the interface that will connect with your SMTP server.

Loopback address

The SMTP server will only listen to the IP address on the local computer.

All interfaces

If there are multiple IP addresses on the computer, the SMTP server will listen to any of the IP addresses available.

- **Port:** Specify the listening port of the SMTP server.
- **Disconnect after { } minutes of inactivity:** Specify a time-out value.
- **Simultaneous connections:** Click **No limit** or **Allow up to { } connections** and specify the maximum number of connections.

4. Specify the **Connection Control** settings.

- a. Select **Accept all, except the following list** to configure the "deny list" or **Deny all, except the following list** to configure the "permit list".
- b. Configure the list using any of the following options.
 - **Single computer:** Specify an IP address, and then click >> to add it to the list.
 - **Group of computers:**
 - i. Select the IP version. IMSS supports IPv4 and IPv6 addresses.
 - For IPv4 addresses, specify a subnet address and mask.
 - For IPv6 addresses, specify a subnet address.
 - ii. Click >> to add the group to the list.
 - **Import from file:** Click to import an IP list from a file. The following shows sample content of an IP list text file:

192.168.1.1

192.168.2.0:255.255.255.0

192.168.3.1:255.255.255.128

192.168.4.100

192.168.5.32:255.255.255.192

2001:db8:10ff::ae:44f2

2001:db8::/32

5. Specify the **Transport Layer Security** settings:

- a. Select **Enable Incoming Transport Layer Security**.

This option allows the IMSS SMTP Server to provide Transport Layer Security (TLS) support to SMTP clients, but does not require that clients use TLS encryption to establish the connection.

- b. Select **Only accept SMTP connection by TLS** for IMSS to only accept secure incoming connections.

This option enables the IMSS SMTP Server to accept messages only through a TLS connection.

- c. Click a **Browse** button next to one of the following:

- **CA certificate:** A CA certificate is usually used for verifying SMTP clients. However, IMSS does not verify the client and only uses the CA certificate for enabling the TLS connection.

Only upload this file if it is provided to you together with the public key. Otherwise, this file is not mandatory for enabling a TLS connection.

- **Private key:** The SMTP client encrypts a random number using IMSS SMTP server's public key and an encryption key to generate the session keys.

IMSS SMTP server then uses the private key to decrypt the random number in order to establish the secure connection. This key must be uploaded to enable a TLS connection.

- **SMTP server certification:** The IMSS SMTP server's public key made available to the SMTP clients for generating the session keys.

This key must be uploaded to enable a TLS connection.

d. Click **Upload** to save the file on the IMSS server.

6. Click **Save**.

Configuring Message Rule Settings

To set limits on the messages that IMSS can handle and to control email relay, configure all settings on the **Messages Rules** screen.

Email Relay

To prevent spammers from using the IMSS MTA as a relay for spam, configure relay control by adding the mail domains on your network to the **Incoming Message Settings** list. When IMSS receives a message, it looks at the final destination of the message and compares it to this list. IMSS discards the message under the following circumstances:

- The destination domain is not in this list
- The parent domain of the destination domain is not in this list
- The host is not on the **Permitted Senders of Relayed Mail** list

Incoming message settings are different from message delivery domain settings. For more information see [About Message Delivery on page 6-11](#).

Specifying Message Rules

Procedure

1. Go to **Administration > IMSS Configuration > SMTP Routing**.
2. Click the **Message Rule** tab.

The **Message Rule** screen appears.

SMTP | Connections | **Message Rule** | Message Delivery

Message Limits

Type 0 to remove any limitations.

Maximum message size (1 to unlimited): MB

Maximum number of recipients (1 to 99999):

Incoming Message Settings

Note: To ensure that IMSS receives incoming messages, Trend Micro recommends adding all internal domains in your network.

Add Domain

Example: example.com

Permitted Senders of Relayed Mail

The following hosts can relay mail to all domains and are excluded from the above relay restriction.

Host only

Same subnet as the host

Same IP class as the host

Specified IP addresses:

Single computer

Examples: 123.123.123.123 or 2001:db8:10ff::ae:44f2

Group of computers

IP version:

Subnet address:

Example: 10.123.123.123

Subnet mask:

Example: 255.255.255.0

3. Specify the **Message Limits** settings:
 - **Maximum message size:** Specify the number of megabytes.
 - **Maximum number of recipients:** Specify the number of recipients from 0 to 99999.
4. Specify the **Incoming Message Settings**.

IMSS relays the messages to the added domains.



Tip

When importing, import both the exact domain and all sub-domains for best results.

The following shows sample content of a domain list text file:

- domain.com: Imports the exact domain
 - *.domain.com: Imports all sub-domains
 - domain.org: Imports the exact domain
5. Specify the **Permitted Senders of Relayed Mail**.
 - Host only
 - Same subnet as the host
 - Same IP class as the host
 - Specified IP addresses
 6. Click **Save**.



Tip

For security reasons, Trend Micro recommends that you avoid open relay when configuring the message rule settings. For more information on how to avoid open relay, refer to the Online Help and the FAQ section in this manual.

About Message Delivery

IMSS maintains a routing table based on the domain names of recipient email addresses. IMSS then uses this routing table to route email messages (with matching recipient email addresses) to specified SMTP servers using domain-based delivery. Email messages destined to all other domains are routed based on the records in the Domain Name Server (DNS).

Incoming Message and Message Delivery Domains

The domains you configure for incoming message settings are different from the domains you configure for message delivery settings.

Incoming message domains

IMSS relays messages that are sent only to the incoming message domains. For example, if the incoming message domain list includes only one domain, "domain.com", IMSS will relay only messages that are sent to "domain.com".

Message delivery domains

IMSS delivers messages based on message delivery domains. For example, if the delivery domain includes "domain.com" and the associated SMTP server 10.10.10.10 on port 25, all email messages sent to "domain.com" will be delivered to the SMTP server 10.10.10.10 using port 25.

Configuring Message Delivery Settings

Specify settings for the next stage of delivery. IMSS checks the recipient mail domain and sends the message to the next SMTP host for the matched domain.

When importing a **Message Delivery** list, the list must be in a valid XML file. Each entry consists of the following:

```
[domain name],[server name or IP address]:[port number]
```

For example, all of the following are valid entries:

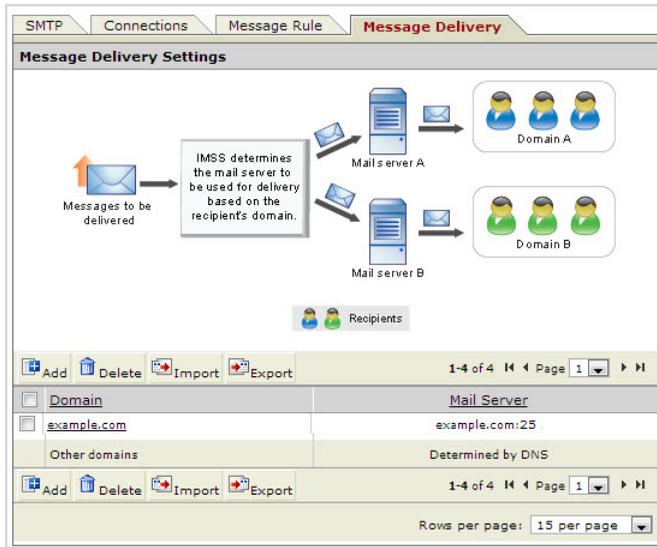
- domain1.com,192.168.1.1:2000
- domain2.net,192.168.2.2:1029

- domain3.com,smtp.domain3.com:25
- domain4.com,mail.domain4.com:2000
- domain5.com,[2001:db8:10ff::ae:44f2]:25

Procedure

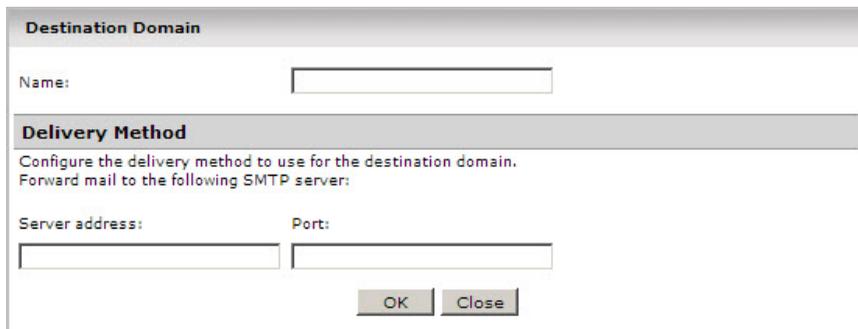
1. Go to **Administration > IMSS Configuration > SMTP Routing**.
2. Click the **Message Delivery** tab.

The **Message Delivery Settings** screen appears.



3. In the **Message Delivery Settings** section, click **Add**.

The **Destination Domain** screen appears.



The screenshot shows a dialog box titled "Destination Domain". It has a "Name:" label followed by an empty text input field. Below this is a section titled "Delivery Method" with the instruction "Configure the delivery method to use for the destination domain. Forward mail to the following SMTP server:". Underneath, there are two labels: "Server address:" and "Port:", each followed by an empty text input field. At the bottom right of the dialog box are two buttons: "OK" and "Close".

4. Specify the **Destination Domain** and **Delivery Method**.
5. Click **OK**.

The domain is added to the **Message Delivery Settings** table.

6. Click **Save**.

Chapter 7

Configuring POP3 Settings

This chapter provides instructions for configuring POP3 settings.

- *Scanning POP3 Messages on page 7-2*
- *Enabling POP3 Scanning on page 7-3*
- *Configuring POP3 Settings on page 7-4*

Scanning POP3 Messages

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as clients in your network retrieve them. Even if your company does not use POP3 messages, your employees might access their personal POP3 email accounts using email clients on their computers. Gmail® or Yahoo!® accounts are some examples of POP3 email accounts. This can create points of vulnerability on your network if the messages from those accounts are not scanned.

Understanding POP3 Scanning

The IMSS POP3 scanner acts as a proxy server (positioned between mail clients and POP3 servers) to scan messages as the clients retrieve them.

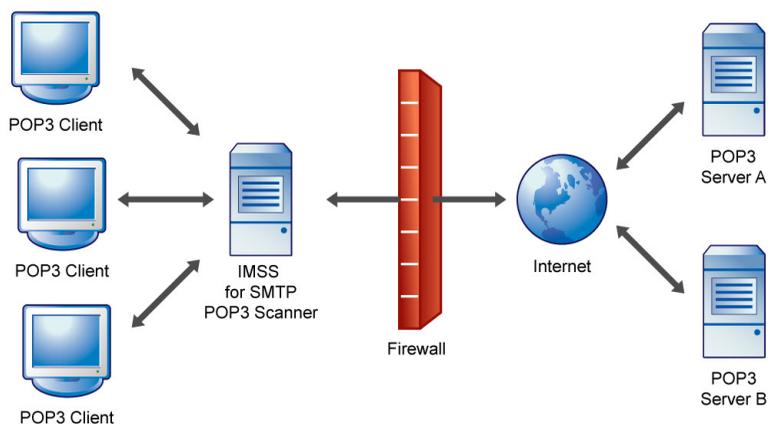


FIGURE 7-1. Scanning POP3 messages

To scan POP3 traffic, configure your email clients to connect to the IMSS server POP3 proxy, which connects to POP3 servers to retrieve and scan messages.

You can set up the following connection types:

- **Generic:** Allows you to access different POP3 servers using the same port, typically 110, the default port for POP3 traffic.
- **Dedicated:** Accesses the POP3 server using a specified port. Use these connections when the POP3 server requires authentication using a secure logon, such as APOP or NTLM.

**Note**

IMSS supports connections to IPv6 POP3 servers.

POP3 Requirements

For IMSS to scan POP3 traffic, a firewall must be installed on the network and configured to block POP3 requests from all the computers on the network, except the IMSS server. This configuration ensures that all POP3 traffic passes to IMSS through the firewall and that IMSS scans the POP3 data flow.

Enabling POP3 Scanning

Before IMSS can begin scanning POP3 traffic, enable POP3 scanning and configure POP3 settings.

Procedure

1. Go to **Summary**.
The **System** tab appears by default.
 2. Under **Enable Connections**, select the **Accept POP3 connections** check box.
 3. Click **Save**.
-

Configuring POP3 Settings

You can specify the IMSS server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection (through the APOP command or using NTLM), you may also set up a dedicated connection and assign a custom port.

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.

The **Components** tab appears by default.

2. Click the **POP3** tab.

The screenshot shows the 'Connections' configuration window with the 'POP3' tab selected. The window has a title bar 'Connections' and a help icon. Below the title bar are tabs for 'Components', 'LDAP', 'POP3', 'Database', and 'TMC Server'. The 'POP3' tab is active and contains the following sections:

- Generic POP3 Connection**: A section with the text 'Any POP3 server requested by user' and a text input field for 'Incoming IMSS port:' containing the value '110'.
- Dedicated POP3 Connections**: A section with 'Add' and 'Delete' buttons and a table with columns 'Incoming POP3 Port', 'POP3 Server', and 'POP3 Server Port'.
- Message Text**: A section with a text area for entering a message. The text above the area reads: 'The following text will be sent to users if messages they are trying to receive trigger a filter. The notification will be sent using the character set you choose on the Notifications Delivery Settings screen.'

At the bottom of the window are 'Save' and 'Cancel' buttons.

3. Do one of the following:

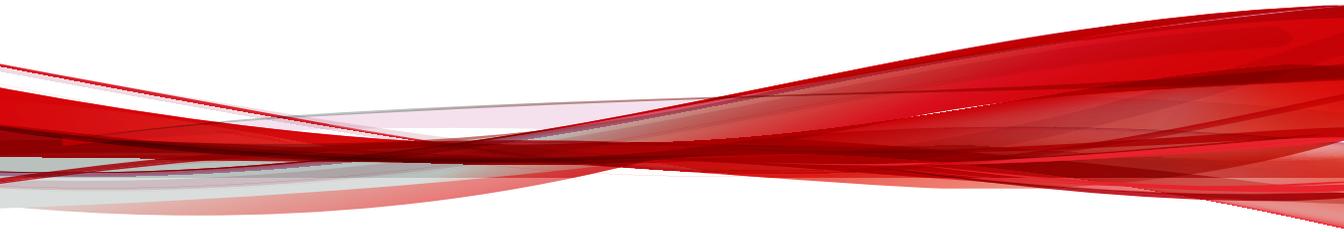
- To accept any POP3 server requested by a user, specify the incoming IMSS port number, if it is different from the default port 110.

- To access the POP3 server using a specific port for authentication purposes, click **Add** to create a new dedicated POP3 connection. Provide the required information and click **OK**.

4. Click **Save**.

Part III

IMSS Policies



Chapter 8

Managing Policies

This chapter provides instructions for creating, modifying, and managing IMSS policies.

Topics include:

- *How the Policy Manager Works on page 8-2*
- *Filter Policies that Display in the Policy List on page 8-3*

About Policies

IMSS policies are rules that are applied to SMTP and POP3 messages. Create rules to enforce your organization's antivirus and other security goals. By default, IMSS includes a Global Antivirus rule to help protect your network from viruses and related Internet threats. Because an antivirus rule addresses the most critical and potentially damaging types of messages, you should always keep it in the first position on the rule list so IMSS can analyze traffic for virus content first.

The antivirus rule does not protect against spam. For the best protection against spam, configure a custom rule that includes spam in the scanning conditions, and activate the IP Filtering product.



Note

Before creating a new policy, ensure that you have defined the internal addresses. See [Configuring Internal Addresses on page 10-2](#) for more information.

How the Policy Manager Works

You can create multiple rules for the following types of policies. Use policies to reduce security and productivity threats to your messaging system:

- **Antivirus:** Scans messages for viruses and other malware such as spyware and worms.
- **Others:** Scans spam or phishing messages, message content, and other attachment criteria.

An IMSS policy has the following components:

- **Route:** A set of sender and recipient email addresses or groups, or an LDAP user or group to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.
- **Filter:** A rule or set of rules that apply to a specific route, also known as scanning conditions. IMSS contains predefined filters that you can use to combat common

virus and other threats. You can modify these predefined filters or define your own filters.

- **Action:** The action that IMSS performs if the filter conditions are met. Depending on the filter result, a filter action is performed that determines how the message is finally processed.

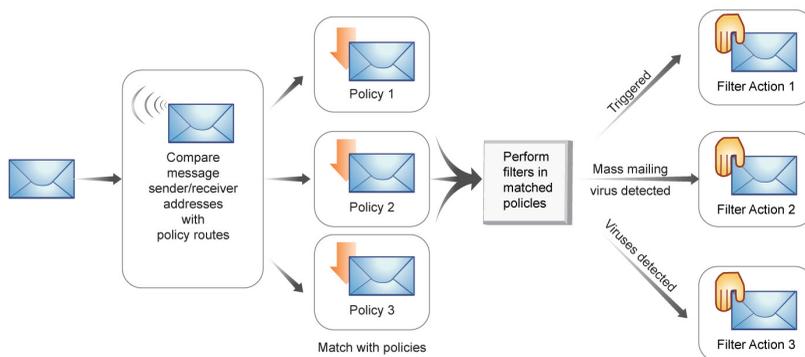


FIGURE 8-1. Simplified policy manager process flow



Note

For more information on how to create a policy, see [Adding Policies on page 11-2](#).

Filter Policies that Display in the Policy List

Procedure

1. Go to **Policy > Policy List**.

The **Policy** screen appears.

2. Configure the Filter by options:
 - a. Specify a route:
 - All routes: Displays all policies
 - Incoming: Displays policies that only monitor incoming messages
 - Outgoing: Displays policies that only monitor outgoing messages
 - Both directions: Displays policies that monitor "incoming", "outgoing", and "incoming and outgoing" messages
 - POP3: Displays policies that only monitor POP3 messages
 - b. Specify the type of protection the policy provides:
 - All types
 - Viruses and malware
 - Spam and phishing email
 - Marketing message
 - Web Reputation
 - Attachments
 - Content
 - Size
 - Other
 - c. Specify the users the policy protects:
 - All Groups
 - [Find user or group]
-

Chapter 9

Common Policy Objects

This chapter provides instructions for creating, modifying, and managing IMSS policies.

Topics include:

- *Policy Object Descriptions on page 9-2*
- *Understanding Address Groups on page 9-2*
- *Using the Keyword & Expression List on page 9-13*
- *Using the Notifications List on page 9-27*
- *Using Stamps on page 9-31*
- *Using the DKIM Approved List on page 9-35*
- *Using the Web Reputation Approved List on page 9-36*

Policy Object Descriptions

Common policy objects are items that can be shared across all policies, making policy creation easier for administrators.

TABLE 9-1. Policy Objects

POLICY OBJECTS	DESCRIPTION
Address Groups	Organize multiple email addresses into a single group.
Keywords & Expressions	Create keywords or expressions to prevent information leaks, block spam, or block derogatory messages from entering or moving in your network.
Notifications	Create messages to notify a recipient or email administrator that IMSS took action on a message's attachment or that the message violated IMSS rule scanning conditions.
Stamps	Create stamps to notify a recipient that IMSS took action on a message's attachment or that the message violated scanning conditions for rules.
DKIM Approved List	Messages from domains with matched DKIM signatures will not be scanned or marked as spam.
Web Reputation Approved List	Domains appearing in the Web Reputation Approved List will not be scanned or blocked by web reputation filters. However, other filters could block messages on the Web Reputation Approved List.

Understanding Address Groups

An address group is a list of email addresses to which your policy applies. Address groups allow you to organize multiple email addresses into a single group and apply the same policy to every address in the group.

For example, you have identified three types of content that you do not want transmitted through your company's email system and have defined three filters (in parentheses) to detect these types of content:

- Sensitive company financial data (FINANCIAL)
- Job search messages (JOBSEARCH)
- VBS script viruses (VBSCRIPT)

Consider the following address groups within your company:

- All Executives
- All HR Department
- All IT Development Staff

The filters that you use in the policies will be applied to these groups as follows:

ADDRESS GROUPS	FINANCIAL	JOBSEARCH	VBSCRIPT
All Executives	Not applied	Applied	Applied
All HR Department	Applied	Not applied	Applied
All IT Development Staff	Applied	Applied	Not applied

Executives, HR staff, and IT developers have legitimate business reasons to send financial information, job search-related correspondence and VBS files, respectively, so you would not apply some filters to those groups.

In IMSS, email addresses identify the different members of your organization and determine the policies that are applied to them. Defining accurate and complete address groups ensures that the appropriate policies are applied to the individuals in those groups.

Creating Address Groups

An address group is a collection of user email addresses in your organization. If you create an address group, you can apply rules to several email addresses at the same time, rather than applying rules to each address individually.

You can create address groups before creating any policies or when specifying the route during policy creation. You can also add an address group when modifying an existing

policy. Create address groups manually or import them from a text file that contains one email address per line.

**Tip**

While address groups can be created during policy creation, Trend Micro recommends creating address groups before you begin creating policies.

Procedure

1. Go to **Policy > Address Group**.

The **Address Groups** screen appears.

2. Click **Add**.

The **Add Address Group** screen appears.

Add Address Group

Address group > Add Address Group

Address groups can contain email addresses or wildcarded domains (examples: *@example.com, *@*.example.com....)

Save Cancel

Address group name:

Addresses:

Add

Import

Delete

Export

Save Cancel

3. Specify a group name, then do any of the following:

- **Add an individual address:**
 - Specify an email address and click **Add**. You can also use wildcard characters to specify the email address. For example, *@hr.com.
- **Import an address list:**
 - a. Click **Import**.
The **Import Address Group** screen appears.
 - b. Specify the file path and file name to import or click **Browse** and locate the file.
 - c. Select one of the following:
 - Merge with current list
 - Overwrite current list
 - d. Click **Import**.

**Note**

IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

4. Click **Save**.

The **Address Groups** screen appears with the new address group appearing in the Address Groups table.

Adding an Address Group During Policy Creation

You can create an address group when specifying the route during policy creation. This can be done by adding email addresses individually or importing them from a text file.

**Note**

IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

Procedure

1. Go to **Policy > Policy List**.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats.

The **Step 1: Select Recipients and Senders** screen appears.

4. Click the **Recipients** or **Senders** link.

The **Select addresses** screen appears.

Incoming Message To

Add Rule > Incoming Message To

Select addresses

Anyone

Any of the selected addresses

Enter email address

- Enter email address
- Search for LDAP users or groups
- Select address groups

Selected	

5. Select **Select Address Groups** from the drop-down list.

Incoming Message To ?

Add Rule > Incoming Message To

Save Cancel

Select addresses

Anyone

Any of the selected addresses

Select address groups

test

Add >

Selected	

Add Edit Delete

Save Cancel

6. Click **Add**.

The **Add Address Group** screen appears.

7. Specify a group name, then do one of the following:
 - Add an individual address:
 - Specify an email address and click **Add** to add email addresses individually. You can also use wildcard characters to specify the email address. For example, `*@hr.com`.
 - Import an **address** list:
 - a. Click **Import**.

The **Import Address Group** screen appears.

- b. Specify the file path and file name to import or click **Browse** and locate the file.
- c. Select one of the following:
 - **Merge with current list**
 - **Overwrite current list**
- d. Click **Import**.

**Note**

IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

8. Click **Save**.
-

Editing or Deleting an Address Group

You can edit or delete an address group from the **Address Groups** screen or by editing an existing policy.

Procedure

1. Go to **Policy > Address Groups**.

The **Address Groups** screen appears.

2. To edit an address group:
 - a. Click an existing address group from the Address Group table.

The **Address Group** screen appears.
 - b. Edit the address group as required.
 - c. Click **Save**.

The **Address Groups** screen appears.

3. To delete an address group:
 - a. Select the check box next to an address group.
 - b. Click **Delete**.
-

Editing or Deleting an Address Group from an Existing Policy

Procedure

1. Go to **Policy > Policy List**.
2. Click the link for an existing policy.
3. Click the **If recipients and senders are** link.
4. Click the **Recipients or Senders** link.

The **Select addresses** screen appears.

Incoming Message To

Default spam rule > Incoming Message To

Save Cancel

Select addresses

Anyone

Any of the selected addresses

Enter email address [v]

Add >

Selected

@	[trash]
test@imssrd.com	[trash]

Save Cancel

5. Select **Select address groups** from the drop-down list.

6. Select the desired address group and click the **Edit** or **Delete** button accordingly.

Exporting an Address Group

Export address groups to import to other IMSS servers. Export from existing policies or from the Address Group list.

Procedure

1. Go to **Policy > Address Groups**.
The **Address Groups** screen appears.
2. Click the address group to export.

The Address Group screen appears.

3. Click **Export**.

The **File Download** screen appears.

4. Click **Save**.

The **Save As dialog** box appears.

5. Specify the name and location to export the address group.
 6. Click **Save**.
-

Exporting an Address Group from an Existing Policy

Procedure

1. Go to **Policy > Policy List**.
2. Click the link for an existing policy.
3. Click the If recipients and senders are link.
4. Click the **Recipients** or **Senders** link.

The **Select addresses** screen appears.

5. Select **Select address groups** from the drop-down list.
6. Click **Edit**.

The **Address Group** screen appears.

7. Click **Export**.

The **File Download** screen appears.

8. Click **Save**.

The **Save As dialog** box appears.

9. Specify the name and location to export the address group.

10. Click **Save**.
-

Using the Keyword & Expression List

Keywords are special words or phrases. 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. To prevent the transmission of medical certificate files, configure IMSS to block files containing these keywords.

Expressions are data that have 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.

IMSS can take action on a message based on the content of its subject, body, or header. To filter messages by content, combine keywords or regular expressions in keyword expression lists.

Selecting Scanning Conditions for Content

Procedure

1. Create or modify an "Other" (not an Antivirus) policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
2. Under **Content**, on the **Scanning Conditions** screen, select the check boxes next to the parts of a message to which you want the content conditions to apply.
3. Click the link that specifies the part of the message to which you want to configure content conditions.

The **Keyword Expressions** screen appears with two columns:

- Available: Expressions available for use, but not currently in use.

- Selected: Expressions currently in use.
4. If you are configuring expressions for the header, select the check boxes next to the header items where the expression will apply.

5. Click **Add**.

The screen for managing keyword expressions appears.

6. Configure the expressions.
7. In the **Available** list, click the expression list you want to enable.
8. Click **>>**.

The expressions appear in the **Selected** list.

To keep an expression list available but temporarily prevent IMSS from using it, click the expression in the selected list, and then click **<<**.

9. Click **Save** to continue to the scanning conditions selection screen.
-

Configuring an Expression

Configure keyword and regular expressions to enable IMSS to scan message content. You can create keywords or expressions from the **Keywords & Expressions** screen or during rule creation.



Tip

While keywords or expressions can be created during policy creation, Trend Micro recommends creating keywords or expressions before you begin creating policies.

Keywords & Expressions

Create keywords or expressions on the **Keywords & Expressions** screen or during policy creation. Trend Micro recommends creating keywords or expressions before creating policies.

Each keyword list has built-in conditions that determine if the content triggers a detection. A keyword list must satisfy your chosen criteria before IMSS subjects it to a policy.

Expressions are a powerful string-matching tool. Ensure that you are comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance. When creating expressions:

- Note that IMSS follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit <http://www.pcre.org/>.
- Refer to the predefined expressions for guidance on how to define valid expressions.
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.
- There are several criteria that you can choose from when creating expressions. An expression must satisfy your chosen criteria before IMSS subjects it to a policy.

Creating Keywords or Expressions

Procedure

1. Go to **Policy > Keywords & Expressions**.

The **Keywords & Expressions** screen appears.

Keywords & Expressions ?			
<input type="button" value="Add"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>			
<input type="checkbox"/>	Keyword & Expression Name	Condition	Used in Policy
<input type="checkbox"/>	Profanity	Any specified	0
<input type="checkbox"/>	HOAXES	Any specified	0
<input type="checkbox"/>	Chainmail	Any specified	0
<input type="checkbox"/>	Sexual Discrimination	Any specified	0
<input type="checkbox"/>	Racial Discrimination	Any specified	0
<input type="checkbox"/>	HTML and script messages	Exceeds threshold	0
<input type="checkbox"/>	Credit Card Number	Any specified	0
<input type="checkbox"/>	Social Security Number	Any specified	0
<input type="checkbox"/>	Bounce Mail	Any specified	0

- Click **Add**.

The **Add Keyword Expression** screen appears.

Keywords & Expressions ?		
Keywords & Expressions > Add Rule		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		
List name:	<input type="text"/>	
Match:	Any specified <input type="button" value="v"/>	
<input type="button" value="Add"/> <input type="button" value="Delete"/>		
<input type="checkbox"/>	Keywords/Regular Expressions	Case Sensitive
		Description
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

- Next to **List name**, specify a descriptive name.
- Next to **Match**, select one of the following that specifies when IMSS takes action:
 - Any specified:** Message content matches any of the keywords or expressions in the list.

- **All specified:** Message content matches all keywords or expressions in the list.
- **Not the specified:** Message content does not match any of the keywords or expressions in the list.
- **Only when combined score exceeds threshold:** Message content contains one or more keywords or expressions in the list. If only one keyword or expression was detected, its score must be higher than the threshold. If several keywords or expressions are detected, their combined score must be higher than the threshold.

Next to **Total message score to trigger action**, specify a number that represents the maximum score for allowed keyword expressions. When you add an expression, you can set a value for the Score.

5. To create a new keyword expression, do the following:
 - a. Click **Add**.

The **Add Keyword Expression** list appears.

- b. Define the following parameters:

Keyword

Specify the keywords. For a partial match, specify the keyword. To specify an exact match, use **\b** before and after the keyword.

For example:

- keyword matches "keywords", "keyword"
- \bkeyword\b matches "keyword" only

Case sensitive

Make the keyword expression case sensitive.

Description

Specify a description for the added keyword expression to make it easier to understand.

- c. Click **Save**.
6. If you selected **Only when combined score exceeds threshold**:
 - a. Specify a threshold in the **Total message score to trigger action** field.
 - b. Select a value from the **Score** drop-down box.
7. Click **Save**.

The **Keywords & Expressions** screen appears with the new keyword or expression appearing in the table.

Adding/Editing a Keyword or Expression during Policy Creation/Modification

Procedure

1. Create or modify an "Other" (not an Antivirus) policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
2. Under **Content** on the **Scanning Conditions** screen, click the link that specifies the part of the message to which you want to configure content conditions.

The **Keyword Expressions** screen appears with two columns.
3. Click **Add** or **Edit** from the **Keyword Expressions** screen.

The configuration screen for keyword expression lists appears.
4. Next to **List name**, specify a descriptive name.
5. Next to **Match**, select one of the following that specifies when IMSS takes action:
 - **Any specified**: Message content can match any of the expressions in the list.
 - **All specified**: Message content must match all the expressions in the list.

- **Not the specified:** Message content must not match any of the expressions in the list.
 - **Only when combined score exceeds threshold:** Next to Total message score to trigger action, specify a number that represents the maximum score for allowed keyword expressions. When you add an expression, you can set a value for the Score.
6. To create an expression, click **Add**.
The **Add Keyword Expression** list appears.
 7. Specify the keywords. For a partial match, just specify the keyword. To specify an exact match, use **\b** before and after the keyword.
For example:
 - keyword matches "keywords", "keyword"
 - \bkeyword\b matches "keyword" only
 8. If you selected **Only when combined score exceeds threshold:**
 - a. Specify a threshold in the **Total message score to trigger action field**.
 - b. Select a value from the **Score** drop-down box.
 9. Click **Save**.
 10. To instruct IMSS to consider the capitalization of message content when it uses the filter, select the check box under **Case sensitive**.
 11. Click **Save** to continue modifying or creating the policy.
-

About Regular Expressions

IMSS treats all keyword expressions as regular expressions. IMSS supports the following regular expressions.

**Tip**

While keywords or expressions can be created during policy creation, Trend Micro recommends creating keywords or expressions before you begin creating policies.

Characters

REGULAR EXPRESSION	DESCRIPTION
.	Any character (byte) except newline
x	The character 'x'
\\	The character '\'
\a	The alert (bell) character (ASCII 0x07)
\b	<ol style="list-style-type: none"> If this meta-symbol is within square brackets [] or by itself, it will be treated as the backspace character (ASCII 0x08). For example, [b] or b If this meta-symbol is at the beginning (or end) of a regular expression, it means any matched string of the regular expression must check whether the left (or right) side of the matched string is a boundary. For example: <ul style="list-style-type: none"> \bluck > left side must be the boundary luck\b > right side must be the boundary \bluck\b > both sides must be the boundary If this meta-symbol appears in the middle of a regular expression, it will cause a syntax error.
\f	The form-feed character (ASCII 0x0C)
\n	The newline (line feed) character (ASCII 0x0A)
\r	The carriage-return character (ASCII 0x0D)
\t	The normal (horizontal) tab character (ASCII 0x09)
\v	The vertical tab character (ASCII 0x0B)

REGULAR EXPRESSION	DESCRIPTION
<code>\n</code>	The character with octal value 0n (0 <= n <= 7)
<code>\nn</code>	The character with octal value 0nn (0 <= n <= 7)
<code>\mnn</code>	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
<code>\xhh</code>	The character with a hexadecimal value 0xhh, for example, <code>\x20</code> means the space character

Bracket Expression and Character Classes

Bracket expressions are a list of characters and/or character classes enclosed in brackets `[]`. Use bracket expressions to match single characters in a list, or a range of characters in a list. If the first character of the list is the caret `^` then it matches characters that are not in the list.

For example:

EXPRESSION	MATCHES
<code>[abc]</code>	a, b, or c
<code>[a-z]</code>	a through z
<code>[^abc]</code>	Any character except a, b, or c
<code>[[alpha:]]</code>	Any alphabetic character (see below)

Each character class designates a set of characters equivalent to the corresponding standard C isXXX function. For example, `[alpha:]` designates those characters for which `isalpha()` returns true (example: any alphabetic character). Character classes must be within bracket expression.

CHARACTER CLASS	DESCRIPTION
<code>[alpha:]</code>	Alphabetic characters
<code>[digit:]</code>	Digits

CHARACTER CLASS	DESCRIPTION
[alnum:]	Alphabetic characters and numeric characters
[cntrl:]	Control character
[blank:]	Space and tab
[space:]	All white space characters
[graph:]	Non-blank (not spaces, control characters, or the like)
[print:]	Like [graph:], but includes the space character
[punct:]	Punctuation characters
[lower:]	Lowercase alphabetic
[upper:]	Uppercase alphabetic
[xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)

For a case-insensitive expression, [lower:] and [upper:] are equivalent to [alpha:].

Boundary Matches

EXPRESSION	DESCRIPTION
^	Beginning of line
\$	End of line

Greedy Quantifiers

EXPRESSION	DESCRIPTION
R?	Matches R, once or not at all

EXPRESSION	DESCRIPTION
R*	Matches R, zero or more times
R+	Matches R, one or more times
R{n}	Matches R, exactly n times
R{n,}	Matches R, at least n times
R{n,m}	Matches R, at least n but no more than m times

R is a regular expression.

Trend Micro does not recommend using "." in a regular expression. "." matches any length of letters and the large number of matches may increase memory usage and affect performance.

For example:

If the content is 123456abc, the regular expression ".*abc" match results are:

- 12345abc
- 23455abc
- 3456abc
- 456abc
- 56abc
- 6abc
- abc

In this example, replace ".*abc" with "abc" to prevent excessive use of resources.

Logical Operators

EXPRESSION	DESCRIPTION
RS	R followed by S (concatenation)
R S	Either R or S
R/S	An R but only if it is followed by S
(R)	Grouping R

R and S are regular expressions

Shorthand and meta-symbol

eManager provides the following shorthand for writing complicated regular expressions. eManager will pre-process expressions and translate the shorthand into regular expressions.

For example, {D}+ would be translated to [0-9]+. If a shorthand expression is enclosed in brackets (example: {}) or double-quotes, then IMSS will not translate that shorthand expression to a regular expression.

SHORTHAND	DESCRIPTION
{D}	[0-9]
{L}	[A-Za-z]
{SP}	[(),;:\.\<>@\[\]:]
{NUMBER}	[0-9]+
{WORD}	[A-Za-z]+
{CR}	\r
{LF}	\n
{LWSP}	[\t]

SHORTHAND	DESCRIPTION
{CRLF}	(\r\n)
{WSP}	[\t\f]+
{ALLC}	.

eManager also provides the following meta-symbols. The difference between shorthand and meta-symbols is that meta-symbols can be within a bracket expression.

META-SYMBOL	DESCRIPTION
\s	[[:space:]]
\S	[^[:space:]]
\d	[[:digit:]]
\D	[^[:digit:]]
\w	[[:alnum:]]
\W	[^[:alnum:]]

Literal string and escape character of regular expressions

To match a character that has a special meaning in regular expressions (example: +), you need to use the backslash \ escape character. For example, to match string C/C++, use the expression C\C\+\+.

Sometimes, you have to add many escape characters to your expression (example: C\C\+\+). In this situation, enclose the string C/C++ in double-quotes (example: .REG "C/C++") then the new expression is equivalent to the old one. Characters (except \ which is an escape character) within double-quotes are literal. The following are some examples:

EXPRESSION	DESCRIPTION
"C/C++"	Match string C/C++ (does not include double-quotes)

EXPRESSION	DESCRIPTION
"Regular\x20Expression"	Match string Regular Expression (does not include double-quotes), where \x20 means the space character.
"[xyz]\\"foo"	Match the literal string: [xyz]"foo

Change the adjacent <space> to "\x20" for the following in a regular expression:

- .AND.
- .OR.
- .NOT.
- .WILD.

Using the Notifications List

To notify a recipient or an email administrator that IMSS performed action on a message's attachment or that the message violated IMSS rule scanning conditions, send a notification.

Although you can create notifications during policy creation, Trend Micro recommends creating notifications before you begin creating policies.

For details about adding to the policy notifications list, see [Adding or Modifying Policy Notifications on page 9-28](#).

Sending Policy Notifications

Procedure

1. Create or modify a policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).

- Under **Monitor**, on the **Select Actions** screen during policy modification or creation, click **Send policy notifications**.

The **Notifications** screen appears with two columns:

- Available:** Notification messages available for use, but not currently in use.
- Selected:** Notification messages currently in use.

- Add or modify a notification.
- In the **Available** list, click the notifications you want to enable.
- Click >>.

The notifications appear in the **Selected** list.

To keep a notification available but temporarily prevent IMSS from using it, click the notification in the selected list, and then click <<.

- Click **Save** to continue creating or modifying the policy.

Adding or Modifying Policy Notifications

Create policy notifications from the **Policy Notifications** screen or during policy creation or modification.

Procedure

- Go to **Policy > Policy Notifications**.

The **Policy Notifications** screen appears.



<input type="checkbox"/> Notification Name	Used in Policy
<input type="checkbox"/> Notification of security settings violation	1
<input type="checkbox"/> Scanning exception	1
<input type="checkbox"/> Notification of encrypted message	1

2. Click **Add**.

The **Add/Edit Policy Notification** screen appears.

The screenshot shows the 'Policy Notifications' configuration interface. At the top, it says 'Policy Notifications > Add Policy Notification'. Below this is a section titled 'Notification Settings' with the following fields:

- Notification Name:** A text input field.
- From:** A text input field.
- To:** A text input field.
- Original mail sender
- Original mail recipient
- Email:**
 - Subject:** A text input field.
 - Message:** A checkbox labeled 'Attach the message' followed by a link 'Variables list'. Below this is a large text area for the message content.
- SNMP Trap:** A radio button selected for 'Disable', a dropdown menu set to '0, Default', and another radio button.
- Message:** A second large text area for the message content.

At the bottom of the form are 'Save' and 'Cancel' buttons.

3. Configure the following:

- **Name:** Specify a descriptive name for the notification.
- **From:** Specify a sender email address.
- **To:** Specify the receiver email addresses and select the check boxes next to Original Mail Sender and/or Original Mail Recipient. Separate each address with a semicolon (;).

- **Subject:** Specify the subject line of the notification.
 - **Message:** Specify the notification message.
4. To send the original message as an attachment of the notification message, select the check box next to **Attach the message**.
 5. To see the types of variables you can include in the message, click **Variables list**.
 6. To send an SNMP trap, configure the following:
 - a. Click one of the following:
 - **Disable (first radio button):** Avoid sending any trap IDs.
 - **Second radio button:** Select one of the default SNMP traps.
 - **Third radio button:** Specify a custom trap ID.
 - b. **Message:** Specify the notification message.
 7. Click **Save**.
-

Adding or Modifying a Policy Notification During Policy Creation or Modification

Procedure

1. Create or modify a policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
2. Under **Monitor** on the **Select Actions** screen, click **Send policy notifications**.

The **Notifications** screen appears with two columns:

- **Available:** Notification messages available for use, but not currently in use.
- **Selected:** Notification messages currently in use.

3. Click **Add** or **Edit**.

The configuration screen for the notification appears.

4. To send an email notification, configure the following:

- **Name:** Specify a descriptive name for the notification.
- **From:** Specify a sender email address.
- **To:** Specify the receiver email addresses and select the check boxes next to Original Mail Sender and/or Original Mail Recipient. Separate each address with a semicolon (;).
- **Subject:** Specify the subject line of the notification.
- **Message:** Specify the notification message.

5. To send the original message as an attachment of the notification message, select the check box next to **Attach the message**.

6. To see the types of variables you can include in the message, click **Variables list**.

7. To send an SNMP trap, configure the following:

- a. Click one of the following:
 - **Disable (first radio button):** Avoid sending any trap IDs.
 - **Second radio button:** Select one of the default SNMP traps.
 - **Third radio button:** Specify a custom trap ID.
- b. **Message:** Specify the notification message.

8. Click **Save**.

Using Stamps

To notify a recipient that IMSS took action on a message's attachment or that the message violated scanning conditions for rules, add a stamp to the beginning or end of the message body.

**Tip**

Add stamps only for messages that the intended recipients will eventually receive. If you are configuring a rule to delete messages that violate your scanning conditions, adding a stamp is not necessary.

Using Stamps in a Policy

Procedure

1. Create or modify a policy.
 - For information on creating a new rule, see *Adding Policies on page 11-2*.
 - For information on modifying an existing rule, see *Modifying Existing Policies on page 13-2*.
 2. While creating or modifying a policy on the **Select Actions** screen, select the check box next to **Insert stamp in body** or **Insert stamp in clean email messages** under **Modify**.
-

Creating Stamps

Create stamps from the Stamps screen or during policy creation or modification.

**Note**

While stamps can be created during policy creation, Trend Micro recommends creating stamps before you begin creating policies.

Procedure

1. Go to **Policy > Stamps**.
The **Stamps** screen appears.

Stamps Name	Used in Policy
Unscanned_attachment	1

- Click **Add** or select a stamp to edit from the **Stamp** list.

The **Add/Edit Stamp** screen appears.

- Next to **Name**, specify the name of the stamp
- Next to **Insert at**, click **End of message body** or **Beginning of message body**.
- Under **Text**, specify the message. To see the types of variables you can include in the message, click **Variables list**.
- To prevent possible damage to Transport Neutral Encapsulation Format (TNEF)-encoded messages or digitally signed messages, select **Do not stamp TNEF-encoded messages or digitally signed messages**.

7. Click **Save** to return to the Stamps screen.
-

Creating a Stamp During Policy Creation or Modification

Procedure

1. Create or modify a policy.
 - For information on creating a new rule, see *Adding Policies on page 11-2*.
 - For information on modifying an existing rule, see *Modifying Existing Policies on page 13-2*.
2. Under **Modify** on the **Select Actions** screen, click **Edit** next to **Insert stamp in body** or **Insert stamp in clean email messages**.

The **Stamps** screen appears showing the available stamps.

3. To add a new stamp, click **Add**. To modify an existing stamp, click it in the list box and then click **Edit**.

An edit screen appears.

4. Next to **Name**, specify the name of the stamp.
 5. Next to **Insert at**, click **End of message body** or **Beginning of message body**.
 6. Under **Text**, specify the message. To see the types of variables you can include in the message, click **Variables list**.
 7. To prevent possible damage to TNEF-encoded messages or digitally signed messages, select **Do not stamp TNEF-encoded messages or digitally signed messages**.
 8. Click **Save** to return to the **Stamps** screen.
 9. Click **Done**.
-

Using the DKIM Approved List

DomainKeys Identified Mail (DKIM) is a signature/cryptography-based email authentication that provides a method for validating a message during its transfer over the Internet. By validating that the message comes from the source it is claiming, IMSS provides spam and phishing protection for your network. Validated messages are not marked as spam and are not scanned for spam. This means false positives are reduced as is the need for scanning messages from a source that is known to be safe.

Enabling the DKIM Approved List

Procedure

1. Go to **Policy > DKIM Approved List**.

The **DKIM Approved List** screen appears.

DKIM (DomainKeys Identified Mail) Approved List

Email messages from domains appearing in the Approved Domains list, with matched DKIM signatures, will not be scanned or marked as spam.

DKIM Approved List

Enable the DKIM Approved List for use in policies.

Domain name:

Add >>

Example: *.domain.com or domain.com

Delete **Import** **Export**

Save **Cancel**

2. Select the **Enable the DKIM Approved List for use in policies** check box.
3. Populate the list with known safe domains.

Manually:

- a. Specify a domain name.
- b. Click **Add**.

Import a list:



Note

When importing a text file for the DKIM Approved List, only one domain should be on each line.

- a. Click **Import**.
The **Import DKIM Approved List** appears.
 - b. Specify the file path and file name or click **Browse** and locate the file.
 - c. Select one of the following:
 - Merge with current list
 - Overwrite current list
 - d. Click **Import**.
4. Click **Save**.
-

Using the Web Reputation Approved List

Web reputation protects users on your network from malicious URLs in messages. Web reputation does this by scanning URLs in messages and then comparing the URL with known malicious URLs in the Trend Micro Web reputation database. The Web Reputation Approved List provides administrators with a way to bypass scanning and blocking of URLs which the administrator knows to be safe.

Enabling the Web Reputation Approved List

Procedure

1. Create or modify an "Other" (not an Antivirus) policy.
 - For information on creating a new rule, see *Adding Policies on page 11-2*.
 - For information on modifying an existing rule, see *Modifying Existing Policies on page 13-2*.
 2. Under **Web Reputation** on the Scanning Conditions screen, click **Web Reputation settings**.

The **Web Reputation Settings** screen appears.
 3. Select the **Enable the use of the Web Reputation Approved List** check box.
 4. Click **Save**.

The **Step 2: Select Scanning Conditions** screen appears.
 5. Continue configuring the policy.
-

Adding to the Web Reputation Approved List

Domains added to the Web Reputation Approved List will not be scanned by IMSS. Only add domains that you know are safe.

Procedure

1. Go to **Policy > Web Reputation Approved List**.

The **Web Reputation Approved List** screen appears.

Web Reputation Approved List 

URLs appearing in the Web Reputation Approved List will not be scanned or blocked.

Web Reputation Approved List

Domain name: **Add >>**

Delete **Import** **Export**

Save **Cancel**

2. Populate the Web Reputation Approved List in one of the following ways:

Manually:

- a. Specify a domain. For example: *.trendmicro.com.
- b. Click **Add>>**.

Import a list:



Note

When importing a text file for the Web Reputation Approved List, only one domain should be on each line.

- a. Click **Import**.
The **Import Web Reputation Approved List** appears.
- b. Specify the file path and file name or click **Browse** and locate the file.
- c. Select one of the following:
 - Merge with current list
 - Overwrite current list
- d. Click **Import**.

3. Click **Save**.

Chapter 10

Internal Addresses

This chapter provides instructions for creating, modifying, and managing IMSS policies.

Topics include:

- *Configuring Internal Addresses on page 10-2*
- *Searching for Users or Groups on page 10-5*
- *Searching for an LDAP User or Group on page 10-6*

Configuring Internal Addresses

For reporting and rule creation, IMSS uses internal addresses to determine which policies and events are Inbound and Outbound:

- For incoming messages, specify the recipient's address, which is in range of the internal addresses. For example: internal address is `imsstest.com`, valid recipients include `jim@imsstest.com`, `bob@imsstest.com`.
- For outgoing messages, specify the sender's address, which is in range of the internal addresses. For example: internal address is `imsstest.com`, valid senders include `jim@imsstest.com`, `bob@imsstest.com`.
- For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

Setting Internal Addresses

Procedure

1. Go to **Policy > Internal Addresses**.

The **Internal Addresses** screen appears.

Internal Addresses

Note: Please specify a "known" set of users or domains. These shall encompass Incoming and Outgoing addresses for reporting and rule-creation purposes.

Internal domains and usergroups

Enter domain >>

Import from File

Export

Selected

test.com	

Save Cancel

2. Under **Internal Domains and User Groups**, select one of the following from the drop-down box:
 - **Enter domain:** Specify a domain and click >>. Do not type the "@" or user name parts of an email address. For example, domainname or domainname1.domainname2 are valid; user@domainname is invalid.

Note

You can use wildcards for domain names. For example, use *.domain.com to include all sub-domains for "domain.com". However, you cannot use two asterisks in the user name or domain name portion of the address, or use the "@" symbol. *.*@domain.com and user@*.* are both invalid.

- **Search for LDAP group:** A screen for searching the LDAP groups appears. Specify an LDAP group name (not an individual LDAP user) that you want to search in the text box and click **Search**. The search result appears in the list box. To add it to the Selected list, click the LDAP group and then click >>.

For more information, see [Searching for an LDAP User or Group on page 10-6](#)

**Note**

When searching an LDAP group for the internal addresses, you can use wildcards at the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, `A*`, `*A`, and `*A*` are all allowed. If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, `*A` and `*A*` are not allowed.

3. To import domains from a file, click **Import from File** and select the file.

**Tip**

Import both the exact domain and all sub-domains for best results.

The following shows sample content of a domain list text file:

- `domain.com`: Imports the exact domain
- `*.domain.com`: Imports all sub-domains
- `domain.org`: Imports the exact domain

**Note**

The import file must be a text file containing one domain per line. You can use wildcards when specifying the domain.

4. Click **Save**.
-

Exporting Internal Addresses

Procedure

1. Go to **Policy > Internal Addresses**.

The **Internal Addresses** screen appears.

2. Click **Export**.

A **File Download** dialog box appears.

3. Click **Save**.

A **Save As** dialog box appears.

4. Specify the location and file name.

5. Click **Save**.
-

Searching for Users or Groups

When you filter the list of rules by user or group, you can select from the following items:

- Email address
- LDAP group
- Address group

Procedure

1. Go to **Policy > Policy List**.
2. Next to Filter by, select **[find user or group]** from the last drop-down list.

The **Find Policy or User Group** screen appears.

3. Select one or both check boxes next to **Senders** or **Recipients**.
4. From the drop-down box, select one of the following:
 - **Email address**
 - **LDAP user or group**
 - **Address group**

5. In the text box, specify the key words for which to search.
 6. Click **Select**.
-

Searching for an LDAP User or Group

When specifying the route for a policy, instead of entering an individual email address or address group, you can also perform a search for a Lightweight Directory Access Protocol (LDAP) user or group.

Review the system requirement for the types of LDAP servers that IMSS supports.

- IBM™ Lotus Domino 6.0
- Microsoft™ Active Directory 2000, 2003, 2008 R2
- Sun iPlanet Directory 5.2
- OpenLDAP 2.4

The following steps provide instructions on adding an LDAP user or group when creating a new policy.

Procedure

1. Go to **Policy > Policy List**.
2. Click **Add**.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats, respectively.
4. Click the **Recipients** or **Senders** link.

The **Select Addresses** screen appears.

Incoming Message To ?

Add Rule > Incoming Message To

Save Cancel

Select addresses

Anyone

Any of the selected addresses

Enter email address v

Enter email address

Search for LDAP users or groups

Select address groups

Add >

Selected

Save Cancel

5. Select **Search for LDAP users or groups** from the drop-down list.

6. Specify the LDAP user or group that you want to search.

 **Note**

- a. You can use the asterisk wildcard when performing a search. See [Using the Asterisk Wildcard on page 13-14.](#)
 - b. You can also search for LDAP groups when adding internal addresses. See [Configuring Internal Addresses on page 10-2.](#)
-

7. Click **Search**.
 8. IMSS displays the LDAP user or group if a matching record exists on the LDAP server.
 9. Select the user or group and then click **Add** to add it to the recipient or sender list.
-

Chapter 11

Configuring Policies

This chapter provides instructions for creating, modifying, and managing IMSS policies.

Topics include:

- *Adding Policies on page 11-2*
- *Specifying a Route on page 11-2*
- *Specifying Scanning Conditions on page 11-10*
- *Specifying Actions on page 11-30*
- *Finalizing a Policy on page 11-37*

Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For information, see [Configuring Internal Addresses on page 3-8](#).

Creating a policy involves the following steps:

- Step 1: [Specifying a Route on page 11-2](#)
- Step 2: [Specifying Scanning Conditions on page 11-10](#)
- Step 3: [Specifying Actions on page 11-30](#)
- Step 4: [Finalizing a Policy on page 11-37](#)



Tip

To prevent a virus leak and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to all messages. Select all messages from the drop-down list when specifying the route for an antivirus rule.

Specifying a Route

The first step in adding a rule is configuring the following:

Route

A specific "To" and "From" combination that includes a recipient's and sender's email addresses, LDAP users or groups, or address groups. You can also configure exceptions to a route.

Route type

The direction of SMTP traffic, POP3 traffic, or all traffic.

Adding a Route

Procedure

1. Go to **Policy > Policy List**.

The **Policy List** screen appears.

2. Click **Add** and select one of the following:

- Antivirus
- Other

OPTION	DESCRIPTION
Antivirus	The Antivirus rule scans messages for viruses and other malware such as spyware and worms.
Other	The Other rule scans for spam or phishing messages, marketing messages, message content, encrypted messages, regulatory compliance, and other attachment criteria.

The **Add Rule** screen appears.

Add Rule

Policy List > New Rule

> **Step 1: Select Recipients and Senders** >>> Step 2 >>> Step 3 >>> Step 4

This rule will apply to **outgoing messages**

< Previous **Next >** Cancel

To: **Recipients**

From: **Senders**

Exceptions

If recipients and senders are **incoming** to AND from **Anyone**

Outgoing Message From

Add Rule > Outgoing Message From

Save Cancel

Select addresses

Anyone

Any of the selected addresses

Enter email address: Add >

Selected

< Previous **Next >** Save Cancel

3. Select the policy route type from the drop-down list next to **This rule will apply to**.
 - **incoming messages**
 - **outgoing messages**
 - **both incoming and outgoing messages**
 - **POP3**
 - **all messages**
4. Select the recipients and senders:

- For incoming messages, specify the recipient's address, which is in range of the internal addresses.

For example: internal address is `imsstest.com`, valid recipients include `jim@imsstest.com`, `bob@imsstest.com`.

- For outgoing messages, specify the sender's address, which is in range of the internal addresses.

For example: internal address is `imsstest.com`, valid senders include `jim@imsstest.com`, `bob@imsstest.com`.

- For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

**Note**

- a. You can use the asterisk wildcard when specifying an email address. For more information, see [Using the Asterisk Wildcard on page 13-14](#).
- b. 2. If you selected POP3, you cannot configure the route. The rule applies to all POP3 routes.
- c. If you selected "all messages" for a rule, the rule also applies to messages from any sender to any recipient.

-
5. Click **Next**.

The **Step 2: Select Scanning Conditions** screen appears.

Editing a Route

Procedure

1. Go to **Policy > Policy List**.

The **Policy List** screen appears.

2. Click the name of the policy to edit.

The **Summary** screen for the policy appears.

3. Click **Edit** for **If recipients and senders are**.

The **Recipients and Senders** screen for the policy appears.

4. Select the policy route type from the drop-down list next to **This rule will apply to**.
 - **incoming messages**
 - **outgoing messages**
 - **both incoming and outgoing messages**
 - **POP3**
 - **all messages**



Note

The **This rule will apply to** option cannot be modified in the Global DKIM Enforcement rule.

5. Select the recipients and senders:
 - For incoming messages, specify the recipient's address, which is in range of the internal addresses.

For example: internal address is `imsstest.com`, valid recipients include `jim@imsstest.com`, `bob@imsstest.com`.
 - For outgoing messages, specify the sender's address, which is in range of the internal addresses.

For example: internal address is `imsstest.com`, valid senders include `jim@imsstest.com`, `bob@imsstest.com`.
 - For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

**Note**

- a. You can use the asterisk wildcard when specifying an email address. For more information, see [Using the Asterisk Wildcard on page 13-14](#).
 - b. If you selected POP3, you cannot configure the route. The rule applies to all POP3 routes.
 - c. If you selected "all messages" for a rule, the rule also applies to messages from any sender to any recipient.
-

6. Click **Save**.
-

Route Configuration

A route is a specific "To" and "From" combination that includes a recipients' and sender's email addresses, LDAP users or groups, or address groups. You can also configure exceptions to a route.

Senders and recipients must be on the Internal Addresses list if you select incoming messages or outgoing messages when adding a new rule or modifying an existing rule:

- If you are configuring an outgoing message, the Internal Address list applies to the senders.
- If you are configuring an incoming message, the Internal Address list applies to the recipients.

Use the asterisk wildcard to include a range of email addresses. For example:

- `user@company.com`: Adds only the specific address.
- `*@company.com`: Adds any user at the domain `company.com`.
- `*@*.company.com`: Adds any user at any subdomain of `company.com`.

For example, `user1@accounting.company.com` would be included.

- `*@*`: Adds all addresses.

Configuring the Route

Procedure

1. Click one of the following on the **Select Recipients and Senders** screen:
 - **Recipients or Senders:** Appears if you selected incoming messages or outgoing messages.
 - **Users:** Appears if you selected both incoming and outgoing messages.
2. Under **Select addresses**, select one of the following:
 - **Anyone:** Select this option to remove any restriction on the recipients or senders.
 - **Enter address:** Specify the email address to add.
 - **Search for LDAP users or groups:** Specify the LDAP user or group name and click **Search**. The results display in the list box.
 - **Select address groups:** All existing address groups appear in the list. If there are a large number of email addresses that you will reuse for routes in several rules, click **Add** to create an address group.
3. If you are adding an email address or email address group, click **Add>**. If you are adding an LDAP or address group, click it in the list box, and then click **Add>**.
4. To remove any email address or email address group from the **Selected** list, click the trash can icon.
5. Click **Save**.

**Tip**

When selecting an LDAP group as the recipients or senders, you can use wildcards at the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server.

To prevent virus leaks and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to all messages at all times.

Configuring Exceptions for Routes

Click the link next to **Exceptions**, on the **Add Rule** screen. The **Exceptions** screen appears for the traffic direction (incoming, outgoing, both incoming and outgoing messages, or all messages).

Procedure

1. Click the link next to **Exceptions**, on the **Add Rule** screen.

The **Exceptions** screen appears for the traffic direction (incoming, outgoing, both incoming and outgoing messages, or all messages).

2. Under **Select addresses**, select one of the following for both the "From" and "To" addresses:
 - **Enter email address:** Type the email address to add.
 - **Search for LDAP users or groups:** Type the LDAP user or group name and click Search. The results display in the list box.
 - **Select address groups:** All existing address groups appear in the list. If there are a large number of email addresses that you will reuse for routes in a rule, click Add to create an address group.
3. If you are adding an email address, click **Add>**. If you are adding an LDAP or address group, click it in the list box, and then click **Add>**.
4. To remove a sender-recipient pair from the list, click the trash can icon.

5. Click **Save**.
-

Specifying Scanning Conditions

After selecting the senders and recipients for a new rule or modifying the senders and recipients for an existing rule, configure the rules to filter message traffic based on several conditions.

The scanning conditions vary depending on whether **Antivirus** rules or **Other** rules are being created.

Procedure

1. Select the check boxes as desired, from the **Step 2: Select Scanning Conditions** screen. The categories of scanning conditions for the **Antivirus** and the **Other** rule types vary as follows:
 - Antivirus rule
 - a. **Files to Scan:** Set the default method for scanning messages and specific file types containing viruses and other malware.

TABLE 11-1. Files to Scan

SETTING	DESCRIPTION
All scannable files	Attempt to scan all files.
IntelliScan: uses "true file type" identification	Use IntelliScan to identify malicious code that can be disguised by a harmless extension name.

SETTING	DESCRIPTION
Specific file types	<p>Select the check box next to one of the following types of file extensions to scan:</p> <ul style="list-style-type: none"> • Application and executables: Click the link and select the sub-types to scan. • Documents: Click the link and select the sub-types to scan. • Compressed files: Click the link and select the sub-types to scan. • Specified file extensions: Specify the extension in the text box. You do not need to type the period (.) before the extension. You can also use an asterisk wildcard for the extension.

- b. **IntelliTrap Settings:** Scan compressed files for viruses/malware and send samples to TrendLabs for investigation.
 - **IntelliTrap:** Scan message attachments that contain real-time compressed executable files.
 - **Send the IntelliTrap samples to TrendLabs:** IMSS can automatically send messages with attachments that IntelliTrap catches to TrendLabs.
 - c. **Spyware/Grayware Scan:** Scan for other types of threats such as spyware and adware.
- Other rule
 - a. Select one of the following next to **Take rule action when**, which specifies when IMSS can take action on a message:
 - **all conditions matched (AND):** When a message matches all of the conditions.
 - **any conditions matched (OR):** When a message matches any of the conditions.

- b. **Spam/Phishing Email:** Scans messages identified as spam and phishing messages. Spam messages are generally unsolicited messages containing mainly advertising content. Phishing messages, on the other hand, originate from senders masquerading as trustworthy entities.
 - **Spam detection settings:** Click the link to select a level of spam protection and configure lists for approved and blocked senders and text exemptions.
 - **Phishing email**
- c. **Web Reputation:** Scans URLs in messages to protect against phishing and other malicious websites.
- d. **Marketing Messages :** Scans messages against the ERS score to approve certain marketing messages.
- e. **Attachment:** Scans messages for file attachments that match the selected criteria, such as attachments with specific extensions or belonging to a certain true file type.
 - **Name or extension:** Click the link to configure filter settings for specific file names or extension names.
 - **MIME content type:** Click the link to configure filter settings for MIME content types.
 - **True file type:** Click the link to configure filter settings for common executable, document, image, media, and compressed files.
 - **Size is {>, <, =} {size} {MB, KB, B}:** Select to filter attachments of a size that is more than, less than, or equal to a certain number of bytes, kilobytes, or megabytes. Specify a number that represents the file size.
 - **Number is {>, <, =} {number}:** Select to filter the number of attachments that is more than, less than, or equal to a certain number. Specify a number that represents the total number of attachments for each message.
 - **Password protected zip files (unscannable files):** Select to filter password protected zip files that cannot be scanned by IMSS.

-
- f. **Size:** Scans messages that match the specified message size.
- **Message size is {>, <, =} {size} {MB, KB}:** Select to filter messages of a size that is more than, less than, or equal to a certain number of kilobytes, or megabytes. Specify a number that represents the message size.
- g. **Content:** Scans messages containing the keyword expressions that match those expressions specified in the subject, body, header, or attachment keyword expressions links.
- **Subject keyword expressions:** Click the link to manage your expression lists.
 - **Subject is blank:** Select to filter messages without a subject. Sometimes spam messages do not contain subject lines.
 - **Body keyword expressions:** Click the link to manage your expression lists.
 - **Header keyword expressions:** Click the link to manage your expression lists. Headers include Subject, To, From, CC, and other headers that you can specify.
 - **Attachment keyword expressions:** Click the link to manage your expression lists. Attachments include attachment names and attachment content.
- h. **Others:** Scans messages in which the number of recipients match the specified number. Also scans messages that are received within the specified time range.
- **Number of recipients is {>, <, =} {number}:** Select to filter the number of recipients. Specify a number that represents the total number of recipients for each message.
 - **Received time range:** Click the link to select a day and time within which a message was received.
 - **Encrypted messages:** Select to filter encrypted messages that cannot be decrypted by IMSS.
-

Selecting Scanning Conditions for Spam

Spam criteria includes a spam catch rate/detection threshold setting and configurable lists for approved and blocked senders and for text exemption rules.

Procedure

1. Under **Spam/Phishing Email** on the scanning conditions selection screen for the Other rule type, select the check box next to **Spam detection settings**.

2. Click **Spam detection settings**.

The **Spam Detection Settings** screen appears.

3. To enable spam scanning, select the check box next to **Select a spam catch rate** or specify a detection threshold.

If you do not select this check box, IMSS will not label any messages that violate this rule as spam. You can, however, still take actions on any senders in the Blocked Senders list below.

4. Select one of the following spam catch rates or specify a detection threshold.
 - **High:** Catches more spam. Select a high catch rate if too much spam is getting through to your clients.
 - **Medium:** Catches an average amount of spam (the default selection).
 - **Low:** Catches less spam. Select a low catch rate if IMSS is tagging too many legitimate messages as spam.
 - **Specify a detection threshold:** Specify a threshold value (between 3.0 and 10.0) that represents how critically IMSS analyzes messages to determine if they are spam.

**Note**

A higher threshold value means that a message must be very "spam-like" for IMSS to consider it spam. This decreases the spam catch rate, but it also results in a lower number of false positives. If IMSS is tagging too many legitimate messages as spam (too many false positives), specify a higher threshold value.

A lower threshold value means that a message only needs to be slightly "spam-like" for IMSS to consider it spam. This increases the spam catch rate, but it also results in a higher number of false positives. If IMSS is letting too much spam through to your clients as legitimate messages, specify a lower threshold value.

5. Click **DKIM approved list** to enable or disable use of the DKIM Approved List. IMSS does not scan or mark messages as spam, if the messages come from domains appearing in the DKIM approved list.
 6. Select the check boxes next to any of the following lists to enable them:
 - **Approved sender list:** Prevents IMSS from identifying messages from senders in this list as spam.
 - **Blocked sender list:** Forces IMSS to identify messages from senders in this list as spam.
 - **Text exemption list:** Prevents IMSS from identifying messages that contains any of the text in this list as spam.
-

**Note**

For instructions on configuring the lists, see [Configuring Approved and Blocked Sender Lists on page 11-15](#).

7. Click **Save** to continue selecting scanning conditions.
-

Configuring Approved and Blocked Sender Lists

To provide added flexibility to spam filtering scanning conditions, IMSS provides the following lists:

Approved sender list

Prevents IMSS from identifying messages from senders in this list as spam.

Blocked sender list

Forces IMSS to identify messages from senders in this list as spam.

Configure the lists when you select spam scanning conditions.

Procedure

1. Select the check box next to **Approved sender list** or **Blocked sender list**.
2. To add addresses manually, do the following:
 - a. Next to **Email address**, specify the address. To add multiple addresses, use the asterisk (*) wildcard.
 - b. Click **Add**.The address appears in the list.
3. To import an address group from a file on a local host to the IMSS server, do the following:
 - a. Click **Import**.
 - b. Click **Browse** and locate the file. A dialog box appears.
 - c. Click **Open**.
 - d. If addresses are already in the list, choose whether to merge them or overwrite them with the imported list.
 - e. Click **Import**.
4. To export an address group as a file on the IMSS server, do the following:
 - a. Click **Export**. A Save dialog box appears.
 - b. Click **Save**.
 - c. Specify a name for the file and a location to save the file.
 - d. Click **Save**. The file saves to the location and a dialog appears.
 - e. Click **Close**.

5. Click **Save**.
-

Configuring Spam Text Exemption Rules

IMSS does not identify any of the text in the text exemption list as spam. Configure rules for this list if you want users to always receive messages that contain specific keywords.

Use regular expressions to define the conditions. Type a backslash character before any of the following characters:

\ | () { } [] ^ \$ * + . ?

Procedure

1. When configuring the spam scanning conditions, select the **Exclude messages matching text exemption rules** check box under **Text Exemption Rules**.
2. To add a new text exemption rule, click **Add**. To configure an existing rule, click it in the list box, and then click **Edit**.

The **Text Exemption Rules** screen appears.

3. Next to **Name**, specify a descriptive name for the text exemption rule.
4. Next to **Scan area**, select a portion of the message.

**Note**

If you select **Subject**, **From**, **To**, or **Reply-to** as the scan area and use **Line beginning** to match the header, provide only the header content for **Line beginning**.

Example:

- a. Select **From** as the scan area.
- b. Under **Strings to match**, provide a message string for **Line beginning**. For example, `test@trendmicro.com`.

If you select **All Headers** as the scan area and use **Line beginning** to match the header, provide the header name as well.

Example:

- a. Select **All Headers** as the scan area.
 - b. Under **Strings to match**, provide both the header name and a message string for **Line beginning**. For example, `From: test@trendmicro.com`.
-

5. Next to **Items are case sensitive**, select the check box to consider the text case as well as the content.
 6. Under **Strings to match**, specify the text strings in the text boxes. Line beginning means matching regular expressions at the beginning of a line. Line end means matching regular expressions at the end of a line.
 7. Click **Save**.
-

Configuring Web Reputation Settings

Enable and configure Web Reputation settings to protect your clients from malicious URLs in messages.

Enabling Web Reputation Settings

Procedure

1. Create or modify an “Other” (not an Antivirus) policy.

- For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
2. Under Web Reputation on the **Scanning Conditions** screen, select the **Web Reputation settings** check box.
 3. Click **Next** to continue configuring the policy.
-

Configuring Web Reputation Settings

Procedure

1. Create or modify an “Other” (not an Antivirus) policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
2. Under Web Reputation on the **Scanning Conditions** screen, select **Web Reputation settings**.
3. Click **Web Reputation Settings**.

The **Web Reputation Settings** screen appears.
4. Select one of the following security levels.
 - **High**: Blocks more websites embedded in messages but also increases the risk of false positives. Select **High** if your users are visiting too many malicious websites.
 - **Medium**: Blocks an average number of malicious websites. **Medium** is the default setting because it blocks most web threats while keeping the false positive count low.
 - **Low**: Blocks fewer websites embedded in messages and reduces the risk of false positives. Select **Low** if IMSS is blocking too many legitimate websites.

5. Select **Enable the use of the Web Reputation Approved List** to prevent IMSS from scanning and blocking domains included in the Web Reputation Approved List.
 6. Click **Save**.
-

Configuring Marketing Message Exceptions

The exception list is a white list of email and IP addresses to ignore when filtering content. Add up to 5000 addresses by either adding individual addresses or by importing multiple addresses from a text file. The policy takes effect on addresses in their order in the list.

Procedure

1. Create or modify an "Other" (not an Antivirus) policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
2. Under **Marketing Messages**, click **Marketing message settings**.

The **Marketing Message Settings** screen appears.

Marketing Message Settings

Messages from email and IP addresses in the exception list are not scanned or blocked.

Marketing Message Exception List

Enable Exception List

Email or IP address:

Define each exception list entry by:

- Email address:
user@company.com,
@.company.com
- IPv4 address or address range:
10.64.12.1, 10.64.12.1-10
- IPv4 address / subnet mask:
10.64.12.0/24
- IPv6 address or address range:
2001::10, 2001::10-64
- IPv6 address / subnet mask:
2001::10/64

3. Select **Enable Exception List**.
4. Add email or IP addresses using the following methods:
 - a. Specify an email or IP address and then click **Add>>**.
The address appears in the list.
 - b. Import email addresses from a text file on a local host to the IMSS server.
For details, see [Importing Marketing Email Exceptions on page 11-22](#).
5. Optional: Export the address list as a text file.
6. Click **Save**.

Importing Marketing Email Exceptions

Before you begin

Complete *Configuring Marketing Message Exceptions* on page 11-20



Note

- Each line in the file should contain only one email address or IP address that follows any of the valid formats. IMSS does not import incorrectly formatted addresses.
- If the list already contains an email address or IP address that is in the file, the address is ignored.
- If the file contains greater than 5000 address, only the first 5000 are imported.

Procedure

1. In the right pane of the **Marketing Message Settings** rule screen, click **Import**.

The **Import Marketing Message Exception List** screen appears.

Import Marketing Message Exception List

File: No file chosen

Note: Specify only one email or IP address per line

Merge option: Merge with current list
 Overwrite current list

2. Click **Choose File** and then select the import file.

Examples of valid input:

Email addresses

```
user@company.com  
*@*.company.com
```

IPv4 addresses

```
123.123.123.123  
62.36.52.1-255  
62.36.52.0/24
```

IPv6 addresses

```
1050:0:0:0:5:600:300c:326b  
ff06::c3
```

3. Select one of the following merge options:
 - Select **Merge with current list** to append the addresses in the file to the existing exceptions list.
 - Select **Overwrite current list** to replace the existing list with the addresses in the file.
 4. Click **Import**.
-

Selecting Scanning Conditions for Attachments

IMSS can filter email traffic based on the files attached to messages.

Specifying Scanning Conditions for Attachment Names or Extensions

Procedure

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **Name or extension**.
2. Click **Name or extension**.
The **Attachment Name or Extension** screen appears.
3. Next to **Select**, select one of the following:

- **Selected attachment names:** IMSS takes action on messages with attachments of the selected names.
 - **Not the selected attachment names:** IMSS takes action on messages with attachments that are not of the selected names.
4. Select the check boxes next to the attachments to scan or not scan.
 5. To add your own attachment name, do the following:
 - a. Select the check box next to **Attachments named**.
 - b. Click **Import** to import from an existing text file. Another window appears.

Alternatively, specify the names in the text box. Use a semicolon (;) to separate values. You can also use an asterisk wildcard for the extension.
 - c. Click **Save**.
 6. Click **Save** to continue selecting scanning conditions.
-

Specifying MIME Content Type Scanning Conditions

Procedure

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **MIME content type**.
2. Click **MIME content type**.

The **Attachment MIME Type** screen appears.
3. Next to **Select**, select one of the following:
 - **Selected attachment types:** IMSS takes action on messages with attachments of the selected types.
 - **Not the selected attachment types:** IMSS takes action on messages with attachments that are not of the selected types.
4. Select the check boxes next to the MIME content types to filter.

5. To add your own MIME types, type them in the text box.

Use a semicolon (;) to separate values. You can also use an asterisk wildcard for the MIME type.

6. Click **Save** to continue selecting scanning conditions.
-

Specifying True File Type Scanning Conditions

Procedure

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **True file type**.
 2. Click **True file type**.
The **Attachment True File Type** screen appears.
 3. Next to **Select**, select one of the following:
 - **Selected attachment types:** IMSS takes action on messages with attachments of the selected types.
 - **Not the selected attachment types:** IMSS takes action on messages with attachments that are not of the selected types.
 4. Select the check boxes next to the true file types to filter.
 5. Click **Save** to continue selecting scanning conditions.
-

Specifying Attachment Size Scanning Conditions

Procedure

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Size is {>, <, =} {size} {MB, KB, B}**.
2. Select the comparison symbol (>, <, =).

3. Specify a number to represent the size.
 4. Select Megabytes, Kilobytes, or Bytes (**MB, KB, B**).
 5. Continue selecting scanning conditions.
-

Specifying Attachment Number Scanning Conditions

Procedure

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Number of attachments** {>, <, =} {number}.
 2. Choose the comparison symbol (>, <, =).
 3. Specify a number to represent the number of attachments.
 4. Continue selecting scanning conditions.
-

Blocking Password Protected Zip Files

Procedure

- Under **Attachment** on the scanning conditions screen, select the check box next to **password protected zip files (unscanned files)**.
-

Selecting Scanning Conditions for Message Size

IMSS can take action on a message based on its total size, including all attachments.

Procedure

1. Under **Size** on the scanning conditions selection screen, select the check box next to **Message size is** {>, <, =} {size} {MB or KB}.
2. Select the comparison symbol (>, <, =).

3. Specify a number to represent the size of the message.
 4. Select **Megabytes** or **Kilobytes (MB or KB)**.
 5. Continue selecting scanning conditions.
-

Selecting Scanning Conditions for Message Content

IMSS can take action on a message based on its content and where the content appears. See [Configuring an Expression on page 9-14](#) for more information on how to specify the content to filter.

Procedure

1. Go to **Policy > Policy List**.
The **Policy** screen appears.
2. Create or modify an "Other" (not an Antivirus) policy.
3. Under **Content**, on the **Step 2: Select Scanning Conditions** screen, select the check boxes next to the parts of a message to which you want the content conditions to apply.
4. Click the link that specifies the part of the message to which you want to configure content conditions. The **Keyword Expressions** screen appears with two columns:
 - **Available:** Expressions available for use, but not currently in use.
 - **Selected:** Expressions currently in use.
5. If you are configuring expressions for the header, select the check boxes next to the header items where the expression will apply.
6. Click **Add**.
The screen for managing keyword expressions appears.
7. Configure the expressions.
8. In the **Available** list, click the expression list you want to enable.

9. Click >>.

The expressions appear in the **Selected** list.

To keep an expression list available but temporarily prevent IMSS from using it, click the expression in the selected list, and then click <<.

10. Click **Save** to continue to the scanning conditions selection screen.
-

Specifying "Other" Scanning Conditions

IMSS can filter email traffic based on the following:

- Number of recipients
 - Message arrival time
 - Message content is encrypted
-

Procedure

1. Go to **Policy > Policy List**.

The **Policy** screen appears.

2. Create or modify an "Other" (not an Antivirus) policy.
 - For information on creating a new rule, see [Adding Policies on page 11-2](#).
 - For information on modifying an existing rule, see [Modifying Existing Policies on page 13-2](#).
3. Under **Other**, on the Scanning Conditions screen, select the check boxes next to the following:
 - **Number of recipients is {>, <, =} {number}**: Blocks messages if the number of recipients is less than, exceeds, or is equal to the specified limit.
 - **Received time range**: Blocks messages if they enter your network within the specified time range.

- **Password protected zip files(uns scanned files):** Blocks encrypted messages that cannot be decrypted by IMSS.
-

Selecting Scanning Conditions for Number of Recipients

IMSS can take action on a message based on the number of recipients to which the message is addressed.

Procedure

1. Under **Others** on the scanning conditions selection screen, select the check box next to **Number of recipients is {>, <, =} {number}**.
 2. Select the comparison symbol (>, <, =).
 3. Specify a number to represent the number of recipients.
 4. Continue selecting scanning conditions.
-

Setting Scanning Conditions for Message Arrival Time

IMSS can take action on a message based on the time it arrived.

Procedure

1. Under **Others** on the scanning conditions selection screen, select the check box next to **Received time range**.
2. Click **Received time range**.
The **Time Range** screen appears.
3. Next to **Select**, select one of the following:
 - **Anytime within selected ranges**
 - **Anytime except selected ranges**
4. From the time drop-down boxes, select the day, start time, and end time.

5. Click **Add**.
 6. Click **Save** to continue selecting scanning conditions.
-

Specifying Actions

The main actions for both the Antivirus and Other rules are similar, although there are minor differences in the options listed. Select the desired action(s) from the following categories:

Intercept

Allows you to choose whether you would like IMSS to intercept the messages and prevent them from reaching the recipients. Choosing the intercept option allows you to specify an action for IMSS to take on intercepted messages.

Modify

Instructs IMSS to make some alterations to the messages or the attachments, such as inserting a stamp or tagging the subject.

Monitor

Instructs IMSS to send a notification, archive or blind copy the messages if you would like to further analyze them.

Procedure

1. Click **Next** from the **Step 2: Select Scanning Conditions** screen.

The **Step 3: Select Actions screen** appears.



The screen that appears in this step depends on the type of rule that you are creating. The antivirus rule contains two tabs that allow you to configure the main actions and the actions for special viruses.

Specifying Actions for "Other" Rules

Procedure

1. Configure **Intercept** settings.

OPTION	DESCRIPTION
Do not intercept messages	This specific rule does not intercept messages. If there are other rules, IMSS will process the message. If there are no rules, IMSS passes the message to your network.
Delete entire message	Deletes the message and all attachments.
Quarantine	IMSS puts the message and its attachments into the quarantine area that you select from the drop-down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 17-2 .
Change recipient	IMSS sends the message to another recipient. Specify the recipient email address and separate multiple recipients with a semicolon (;).
Handoff	<p>IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:</p> <ul style="list-style-type: none"> • Next to Host, Specify the FQDN or IP address of the mail server. • Next to Port, specify the port number through which the mail server receives email traffic. <hr/> <p> Note IMSS can only track a message before it is handed off. After the handoff, the message is no longer traceable as it is not in the control of IMSS.</p> <p>IMSS does not support IPv6 handoff server addresses.</p>

2. Configure **Modify** settings.

OPTION	DESCRIPTION
Insert X-header	Inserts a user-specified message to the header of messages.
Delete attachments	Select an action for IMSS to take: <ul style="list-style-type: none"> • Delete matching attachment: Remove only the attachment that matches the attachment scan condition. • Delete all attachments: Remove all attachments.
Insert stamp in body	Insert text at the beginning or end of the message. From the drop-down box, select the name of the stamp to insert or click Edit to go to the Stamps screen and manage your stamps.
Tag subject	Add text to the subject line of the message. Click Tag subject to edit the tag.
Postpone delivery to	Delay delivery until a specified hour of the day. Select the hour of the day and minutes from the drop-down boxes.

3. Configure **Monitor** settings.

OPTION	DESCRIPTION
Send policy notifications	Send a message to one or more recipients. To select a type of notification, click Send policy notifications. For instructions on creating notifications, see Using the Notifications List on page 9-27 .
Archive modified to	Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 17-2 .
BCC	Blind carbon copy the message to another recipient. Specify the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

Specifying Actions for "Virus" Rules Main Actions

Main Actions allow you to specify the default actions that IMSS takes when messages match the scanning conditions specified in Step 2: Scanning Conditions.

Procedure

1. Configure **Intercept** settings.

OPTION	DESCRIPTION
Do not intercept messages	This specific rule does not intercept messages. If there are other rules, IMSS will process the message. If there are no rules, IMSS passes the message to your network.
Delete entire message	Deletes the message and all attachments.
Quarantine	IMSS puts the message and its attachments into the quarantine area that you select from the drop-down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 17-2 .
Change recipient	IMSS sends the message to another recipient. Specify the recipient email address and separate multiple recipients with a semicolon (;).
Handoff	<p>IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:</p> <ul style="list-style-type: none"> • Next to Host, specify the FQDN or IP address of the mail server. • Next to Port, specify the port number through which the mail server receives email traffic. <hr/> <p> Note IMSS can only track a message before it is handed off. After the handoff, the message is not traceable anymore as it is no longer within the control of IMSS.</p>

2. Configure **Modify** settings.



Note

Options under **If IMSS finds a virus** are only available for Antivirus rules.

OPTION	DESCRIPTION
If IMSS finds a virus	<p>Select the check box to enable actions if IMSS finds a virus or other malware, and then click one of the following:</p> <ul style="list-style-type: none"> • Use ActiveAction: Enable IMSS to automatically use pre-configured scan actions for specific types of viruses/malware. • Attempt to clean attachments. If unable to clean: Select an action for IMSS to take if it cannot clean the attachment: <ul style="list-style-type: none"> • Delete matching attachment: Remove only the attachments with viruses/malware. • Delete all attachments: Remove all attachments. • Delete attachments: Select an action for IMSS to take. <ul style="list-style-type: none"> • Delete matching attachment: Remove only the attachment with viruses/malware. • Delete all attachments: Remove all attachments.
Insert X-header	<p>Inserts a user-specified message to the header of messages.</p> <hr/> <p> Note If you configure multiple rules to add an x-header, the X-header appears only once in the message. The X-header appears as configured in the last rule.</p> <hr/>
Insert stamp in body	<p>Insert text at the beginning or end of the message. From the drop-down box, select the name of the stamp to insert or click Edit to go to the Stamps screen and manage your stamps.</p>
Insert safe stamp for clean mails	<p>Insert text into clean messages signifying that the message is safe. From the drop-down box, select the name of the stamp to insert or click Edit to go to the Stamps screen and manage your stamps.</p> <hr/> <p> Note The Insert safe stamp for clean mails option is not available on the Special Viruses tab.</p> <hr/>
Tag subject	<p>Add text to the subject line of the message. Click Tag subject to edit the tag.</p>

OPTION	DESCRIPTION
Postpone delivery time	Delay delivery until a specified hour of the day. Select the hour of the day and minutes from the drop-down boxes.

3. Configure **Monitor** settings.

OPTION	DESCRIPTION
Send policy notifications	Send an message to one or more recipients. To select a type of notification, click Send policy notifications. For instructions on creating notifications, see Using the Notifications List on page 9-27 .
Archive modified to	Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 17-2 .
BCC	Blind carbon copy the message to another recipient. Specify the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

Specifying Actions for "Virus" Rules Special Viruses

Special Virus settings allow you to specify the actions that IMSS takes if the messages match any of the following criteria. The actions specified on this screen will override the default actions specified on the **Main Actions** tab.

Add Rule ?

[Policy List](#) > New Rule

Step 1 >>> Step 2 >>> **Step 3: Select Actions** >>> Step 4

Enable mass-mailing behavior: this will overwrite all other actions ▼

Enable spyware/grayware: this will overwrite all other actions ▼

Enable IntelliTrap behavior: this will overwrite all other actions ▼

- **Mass mailing:** IMSS takes the actions specified in this section if it detects mass mailing messages.
- **Spyware/grayware:** Allows you to specify the corresponding actions if you have selected any of the Spyware/Grayware Scanning options on the Scanning Conditions screen in step 2. For more information, see [Specifying Scanning Conditions on page 11-10](#). If IMSS detects spyware/grayware in a message, it takes the actions that are specified here.



IMSS takes the default action for messages matching the Spyware/Grayware Scanning conditions if you do not select alternative actions.

- **IntelliTrap:** Allows you to specify the corresponding actions if you have selected the IntelliTrap Setting options on the Scanning Conditions screen in step 2. See [Specifying Scanning Conditions on page 11-10](#).



IMSS takes the default action for messages matching the IntelliTrap conditions if you do not select alternative actions.

Creating a Tag Subject

To notify a recipient that IMSS took action on a message's attachment or that the message violated scanning conditions for a rule, add a brief message to the beginning of the subject line. Add a tag only for messages that the intended recipients will eventually receive. If you are configuring a rule to delete messages that violate your scanning conditions, adding a tag is not necessary.

Procedure

1. When you select actions, click **Tag subject** under Modify actions.
An edit screen appears.
2. Specify the text to insert in the subject line next to **Tag**.

3. To prevent possible damage to digitally signed messages, select **Do not tag digitally signed messages**.
 4. Click **Save** to continue selecting actions.
 5. To use a tag, select the check box next to **Tag subject** under **Modify**.
-

Finalizing a Policy

After you select actions for a rule, name and enable the rule. Also, assign an order number that represents its position within the hierarchy of rules. IMSS allows you to add any notes to the rule that you think are necessary for future reference. You can also modify this information for an existing rule.

When viewing rules, note the following:

-  The green check mark button indicates that the rule is active.
-  The red cross mark button indicates that the rule is saved but inactive.
-  The gray cross mark button indicates that the rule and the Activation Code for the product are both inactive.



Note

You can enable and disable rules by clicking the buttons.

Finalizing a Rule

Procedure

1. Use one of the following methods to open the screen:
 - When creating a new policy, click **Next** on the **Step 3: Select Actions** screen. The Step 4: Name and Order screen appears.

- When finalizing an existing policy, click the name of the policy in the policy list on the **Policy > Policy List** screen.

Add Rule ?

Policy List > New Rule

Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Name and Order**

Rule Notes

Enable

Rule Name:

Order Number:

Order	Existing Rules	Action	Modified	Status
1	Global antivirus rule	Active action	December 25, 2006	✔
2	Default spam rule	Quarantine	December 25, 2006	✔

If recipients and senders are
outgoing
to Anyone
AND
from *@test.com

And scanning conditions match
Subject is blank

Then action is
Quarantine message

- Select the **Enable** check box to activate the rule.
- Specify a name for the rule in the **Rule Name** field.
- In the **Order Number** field, specify the priority in which IMSS will perform the scan. IMSS applies the rule to messages according to the order you specify.
- Click the **Notes** tab.

The **Notes** screen appears.



Add Rule

[Policy List](#) > New Rule

Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Name and Order**

< Previous Finish Cancel

Rule **Notes**

Created:

Last modified:

Notes:

< Previous Finish Cancel

6. Specify a note to distinguish the new rule from other rules.
7. If you are creating a new policy, verify that the information on the screen is correct. If any information about the rule is incorrect, click **< Previous** and make your changes.
8. Click **Finish** to complete a new rule or **Save** to modify an existing rule.

Chapter 12

Scanning Exceptions

This chapter provides instructions for managing IMSS scanning exceptions.

Topics include:

- *Setting Scan Exceptions on page 12-2*
- *Configuring Exceptions for Security Settings Violations on page 12-3*
- *Setting Scan Actions for Security Setting Violations on page 12-4*
- *Setting Scan Actions for Malformed Messages on page 12-5*

Setting Scan Exceptions

Under certain circumstances, you may want to prevent IMSS from scanning certain types of messages that could be part of a DoS attack. For example, messages with extremely large attachments require significant IMSS server resources to scan fully. Additionally, messages addressed to hundreds of recipients are most likely spam or some type of attack.

Rather than consuming IMSS resources to scan these types of messages, set scan exceptions to bypass scanning and instruct IMSS to take action on the messages immediately.



WARNING!

1. For the actions specified in Scan Exceptions to take effect, verify that the Global antivirus rule is enabled.
2. For malformed messages, when a message triggers the scan exception, IMSS stops scanning and takes the corresponding actions. That means IMSS will not trigger any policy rules when a scan exception occurs.

For security setting violations and encryption exceptions, IMSS will not stop scanning after the action of the scan exception executes. IMSS continues checking other policy rules. IMSS will stop scanning if it encounters a terminal scan action.

Configuring Scan Exceptions

Procedure

1. Go to **Policy > Scanning Exceptions**.
 2. To set scan exception conditions for messages based on several conditions, click the **Security settings violations** link under Exception.

The **Security Settings Violations** screen appears.
 3. To set an action for an exception type, click the corresponding link under **Action**.
-

Configuring Exceptions for Security Settings Violations

The scan exceptions for the security settings violations on this screen apply to all senders and receivers.

Procedure

1. On the **Scanning Exceptions** screen, click **Security settings violations** under **Exception**.
The **Security Settings Violations** screen appears.
 2. To set limits on the types of messages IMSS can scan, configure the following:
 - **Total message size exceeds { } MB**: Specify the maximum number of megabytes.
 - **Total # recipients exceeds { } recipients**: Specify the maximum number of recipients.
 - **Total # embedded layers in compressed file exceeds { } layers**: Select the maximum number of layers.
 - **Total decompressed size of any single file exceeds { } MB**: Specify the maximum number of megabytes.
 - **Total # files in compressed file exceeds { } files**: Specify the maximum number of files.
 3. Click **Save**.
The **Scanning Exceptions** screen reappears.
-

Setting Scan Actions for Security Setting Violations

The scan actions for the security settings violations on this screen apply to all senders and receivers.

Procedure

1. On the **Scanning Exceptions** screen, click the action name link under **Actions** for **Security settings violations**.

The screen for configuring actions appears.

2. Configure **Intercept** settings.

OPTION	DESCRIPTION
Do not intercept messages	IMSS does not take action on the message. IMSS processes the message using other rules if other rules exist.
Delete entire message	Deletes the message and all attachments.
Quarantine to	IMSS moves the message and its attachments into the quarantine area that you select from the drop-down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 17-2 .
Handoff	<p>IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:</p> <ul style="list-style-type: none"> • Next to Host, specify the FQDN or IP address of the mail server. • Next to Port, specify the port number through which the mail server receives email traffic.

OPTION	DESCRIPTION
	 Note IMSS can only track a message before it is handed off. After the handoff, the message is not traceable anymore as it is no longer within the control of IMSS. IMSS does not support IPv6 handoff server addresses.

3. Configure **Monitor** settings.

OPTION	DESCRIPTION
Send policy notifications	Send a notification message to one or more recipients. To select a type of notification, click Send policy notifications. For instructions on creating notifications, see Using the Notifications List on page 9-27 .
Archive	Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 17-2 .
BCC	Blind carbon copy the message to another recipient. Specify the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

4. Click **Save**.

Setting Scan Actions for Malformed Messages

The scan actions for malformed messages security settings violations on this screen apply to all senders and receivers.

Procedure

1. On the **Scanning Exceptions** screen, click the action name link under **Actions** for **Malformed messages**.

The screen for configuring actions appears.

2. Configure **Intercept** settings.

OPTION	DESCRIPTION
Do not intercept messages	IMSS does not take action on the message. IMSS processes the message using other rules if other rules exist.
Delete entire message	Deletes the message and all attachments.
Quarantine to	IMSS moves the message and its attachments into the quarantine area that you select from the drop-down box. For instructions on creating a new quarantine area, see Configuring Quarantine and Archive Settings on page 17-2 .
Handoff	<p>IMSS hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:</p> <ul style="list-style-type: none"> • Next to Host, specify the FQDN or IP address of the mail server. • Next to Port, specify the port number through which the mail server receives email traffic. <hr/> <p> Note IMSS can only track a message before it is handed off. After the handoff, the message is not traceable anymore as it is no longer within the control of IMSS.</p> <p>IMSS does not support IPv6 handoff server addresses.</p>

3. Configure **Monitor** settings.

OPTION	DESCRIPTION
Send policy notifications	Send a notification message to one or more recipients. To select a type of notification, click Send policy notifications. For instructions on creating notifications, see Using the Notifications List on page 9-27 .

OPTION	DESCRIPTION
Archive	Archive the message to an archive area. For instructions on creating a new archive area, see Configuring Quarantine and Archive Settings on page 17-2 .
BCC	Blind carbon copy the message to another recipient. Specify the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

4. Click **Save**.
-

Chapter 13

Existing Policies

This chapter provides instructions for creating, modifying, and managing InterScan Messaging Security Suite policies.

Topics include:

- *Modifying Existing Policies on page 13-2*
- *Policy Example 1 on page 13-5*
- *Policy Example 2 on page 13-9*
- *Using the Asterisk Wildcard on page 13-14*

Modifying Existing Policies

Modification of rules follows a different process from rule creation.

Procedure

1. Go to **Policy > Policy List**.

2. Click the name of the rule to edit.

The **Summary** screen for the rule appears.

3. Click **Edit** for **If recipients and senders are** .

4. Configure the route settings.

For more information, see [Specifying a Route on page 11-2](#).

5. Click **Edit** for one of the following:

- **And scanning conditions match** (Antivirus and Other rules)
- **And domains listed here do not pass DKIM verification.** (Global DKIM rule)

6. Configure the scan settings. For more information, see the following:

- For Antivirus and Other rules: [Specifying Scanning Conditions on page 11-10](#)
- For the Global DKIM Enforcement rule: [Using the Domain List for the Global DKIM Enforcement Rule on page 13-3](#)
- [Using the Domain List for the Global DKIM Enforcement Rule on page 13-3](#)

7. Click **Edit** for **Then action is**.

8. Configure the action settings.

For more information, see [Specifying Actions on page 11-30](#).

9. Click **Save**.

Using the Domain List for the Global DKIM Enforcement Rule

IMSS marks incoming messages as spam from domains appearing in the Domain List that:

- Do not pass DKIM validation
- Do not have a DKIM-Signature

Adding Domains to the Domain List in the Global DKIM Enforcement Rule

Procedure

1. Click **Policy > Policy List**.

The **Policy** screen appears.

2. Click the **Global DKIM Enforcement rule** link.

The **Policy Summary** screen appears.

3. Click **Edit** in the **And domains listed here do not pass DKIM verification** row.

The **Scanning Conditions** screen appears.

4. Populate the Domain List in one of the following ways:

- Manually:
 - a. Specify a domain name.
 - b. Click **Add**.
- Import a list:



Note

When importing a text file for the Domain List, only one domain should be on each line.

- a. Click **Import**. The Import DKIM Enforcement List appears.
 - b. Specify the file path and file name or click **Browse** and locate the file.
 - c. Select one of the following:
 - **Merge with current list**
 - **Overwrite current list**
 - d. Click **Import**.
5. Click **Save**.
-

Modifying Recipients and Senders for Existing Rules

Procedure

1. Go to **Policy > Policy List**.
2. Click the name of the rule to edit.

The **Summary [policy name]** screen for the rule appears.
3. Click **Edit** for **If recipients and senders** are.
4. Select the policy route type from the drop-down list next to **This rule will apply to**.
 - **incoming messages**
 - **outgoing messages**
 - **both incoming and outgoing messages**
 - **POP3**
 - **all messages**
5. Select the recipients and senders:
 - For incoming messages, specify the recipient email address, which is in range of the internal addresses. (Example: internal address is `imsstest.com`, valid recipients include `jim@imsstest.com`, `bob@imsstest.com`).

- For outgoing messages, specify the sender's address, which is in range of the internal addresses. (Example: internal address is `imsstest.com`, valid senders include `jim@imsstest.com`, `bob@imsstest.com`).
- For both incoming and outgoing messages, the rule applies to senders or recipients that match the email address.
- • You can use the asterisk wildcard when specifying an email address.
- If you selected POP3, you cannot configure the route. The rule applies to all POP3 routes.
- If you selected "all messages" for a rule, the rule also applies to messages from any sender to any recipient.

6. Click **Save**.

Policy Example 1

Create a rule to delete attachments with specific file names or extensions and then stamp the affected incoming message with an explanation to the recipients.

- *Step 1: Specify the Route on page 13-5*
- *Step 2: Specify the Scanning Conditions on page 13-6*
- *Step 3: Specify the Actions on page 13-7*
- *Step 4: Specify the Priority on page 13-9*

Step 1: Specify the Route

Procedure

1. Go to **Policy > Policy List**.
2. Click **Add**.
3. Select **Other** from the drop-down list.

The **Step 1: Select Recipients and Senders** screen appears.

4. Next to **This rule will apply to**, select incoming messages from the drop-down list.
5. Click the **Recipients** link.

The **Select addresses** screen appears.

- To apply this rule to any recipients, select **Anyone**.
- To apply this rule to specific recipients, select **Any of the selected addresses**, and then specify the target email address or group.

6. Click **Save**.

The **Step 1: Select Recipients and Senders** screen re-appears.

Step 2: Specify the Scanning Conditions

Procedure

1. Click **Next**.

The **Step 2: Select Scanning Conditions** screen appears.

2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Name or extension** condition, select the check box next to it.

- Click **Name or extension**.

The **Attachment Name or Extension** screen appears.

- Select the file extensions to block or consider blocking.
- Click **Save**.

The **Step 2: Select Scanning Conditions** screen re-appears.

Step 3: Specify the Actions

Procedure

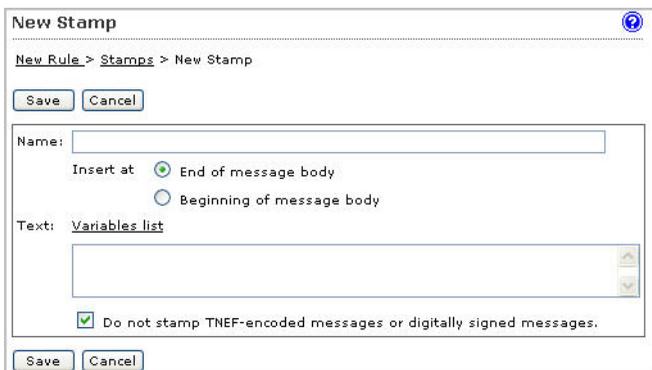
- Click **Next**.
The **Step 3: Select Actions** screen appears.
- Under **Modify**, to enable the **Delete attachment** action, select the check box next to it.
- Select **Matching attachment** from the drop-down list if it is not already selected.
- Select the check box next to **Insert stamp in body**.
- If there is no suitable stamp available from the drop-down list, click **Edit**.

The **Stamps** screen appears.



6. Click **Add** to create a new stamp.

The **New Stamp** screen appears.



7. Specify the required information.

8. Click **Save**.

The **Stamps** screen re-appears.

9. Click **Done**.

The **Select Actions** screen re-appears.

10. Select the newly created stamp from the drop-down list.

Step 4: Specify the Priority

Procedure

1. Click **Next**.

The **Step 4: Name and Order** screen appears.

2. Specify the rule name and order number.
3. Click **Finish**.

The newly created rule will appear highlighted in the **Policy List** screen.

Policy Example 2

Create a rule that quarantines messages containing specific keywords in the subject or body and then apply this rule to all recipients except administrators.

- *Step 1: Specify the Route on page 13-9*
- *Step 2: Specify the Scanning Conditions on page 13-11*
- *Step 3: Specify the Actions on page 13-13*
- *Step 4: Specify the Priority on page 13-14*

Step 1: Specify the Route

Procedure

1. Go to **Policy > Policy List**.

The **Policy List** screen appears.

2. Click **Add**.
3. Select **Other** from the drop-down list.

The **Step 1: Select Recipients and Senders** screen appears.

4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.
5. Click the **Recipients** link.

The **Select addresses** screen appears.

6. Select **Anyone**.
7. Click **Save**.

The **Step 1: Select Recipients and Senders** screen re-appears.

8. Click the **Sender to Recipient** link next to **Exceptions**.

The **Exceptions** screen appears.

9. Under **From (sender)**, type ***@*** to specify any sender.
10. Under **To (recipient)**, specify the administrator's email address.
11. Click **Add**.

The sender-recipient pair appears in the list.

12. To add other administrators or recipients, repeat steps 9 to 11.
13. Click **Save** after you finish adding all the desired recipients.

The **Step 1: Select Recipients and Senders** screen re-appears.

Step 2: Specify the Scanning Conditions

Procedure

1. Click **Next**.

The **Step 2: Select Scanning Conditions** screen appears.

2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**.

The **Keyword Expressions** screen appears.



<input type="checkbox"/>	Keyword & Expression Name	Condition	Used in Policy
<input type="checkbox"/>	Profanity	Any specified	0
<input type="checkbox"/>	HOAXES	Any specified	0
<input type="checkbox"/>	Chainmail	Any specified	0
<input type="checkbox"/>	Sexual Discrimination	Any specified	0
<input type="checkbox"/>	Racial Discrimination	Any specified	0
<input type="checkbox"/>	HTML and script messages	Exceeds threshold	0
<input type="checkbox"/>	Credit Card Number	Any specified	0
<input type="checkbox"/>	Social Security Number	Any specified	0
<input type="checkbox"/>	Bounce Mail	Any specified	0
<input type="checkbox"/>	test	Any specified	0

5. If the desired keywords are not available from the existing list, click **Add** to create a new keyword list.

The **New Keyword Expression** screen appears.

Keyword Expressions

New Rule > Keyword Expressions > New Keyword Expression

Save Cancel

List name:

Match: Any specified

Keywords/Regular Expressions	Case Sensitive	Description
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/>	

Save Cancel

6. Specify the required information.
7. To add an individual keyword expression, click **Add**.

The **Add Keyword Expressions** screen appears.

Add Keyword Expression

New Rule > Keyword Expressions > Add Keyword Expression

Save Cancel

You may use any combination of keywords and regular expressions to define a keyword expression.

Keyword:

Type a backslash \ immediately before the following characters: . \ | () { } [] ^ \$ * + or ?

Case sensitive

Description:

Save Cancel

8. Specify the desired keyword expression and click **Save**.
- The **New Keyword Expression** screen re-appears.
9. Repeat steps 7 and 8 for additional keyword expressions.

- After you have added all the required keyword expressions, specify the List name for the new keyword list and click **Save**.

The **New Keyword Expression** screen re-appears.

- Select the new list and click >> to insert the list into the Selected box.
- Click **Save**.

The **Step 2: Select Scanning Conditions** screen re-appears.

- To enable the **Body Keyword Expression** condition, select the check box next to it.
- Click **Body Keyword Expression**.

The **Keyword Expressions** screen appears.

- Select the new keyword list and click >> to insert the list into the Selected box.
- Click **Save**.

The **Step 2: Select Scanning Conditions** screen re-appears.

Ensure that both the Subject keyword and Body keyword expressions are selected.

Content	
<input checked="" type="checkbox"/>	Subject keyword expressions
<input type="checkbox"/>	Subject is blank
<input checked="" type="checkbox"/>	Body keyword expressions
<input type="checkbox"/>	Header keyword expressions
<input type="checkbox"/>	Attachment keyword expressions

Step 3: Specify the Actions

Procedure

- Click **Next**.

The **Step 3: Select Actions** screen appears.

- Under **Intercept**, select **Quarantine to**.

3. Accept the **Default Quarantine** area or click the drop-down list to select the desired quarantine area.
-

Step 4: Specify the Priority

Procedure

1. Click **Next**.

The **Step 4: Name and Order** screen appears.

2. Specify the rule name and order number.

3. Click **Finish**.

The newly created rule will appear highlighted in the **Policy list** screen.

Using the Asterisk Wildcard

You can use the asterisk (*) as a wildcard in email addresses when defining routes and in file names.

Wildcards in Email Addresses

Wildcards can appear in the name or domain sections of an email address. The following are valid examples:

- **name@***: Valid representation of the whole name.
- ***@domain.tld, name@*.tld**: Valid representation of the whole name or the domain (not the top level domain (TLD)).
- ***@*.tld**: Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a subdomain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:

- **name@domain.*.tld**: Invalid representation of a subdomain.
- **name@domain.***: Invalid representation of a TLD.
- ***name@domain.tld**: Invalid use in conjunction with a name.

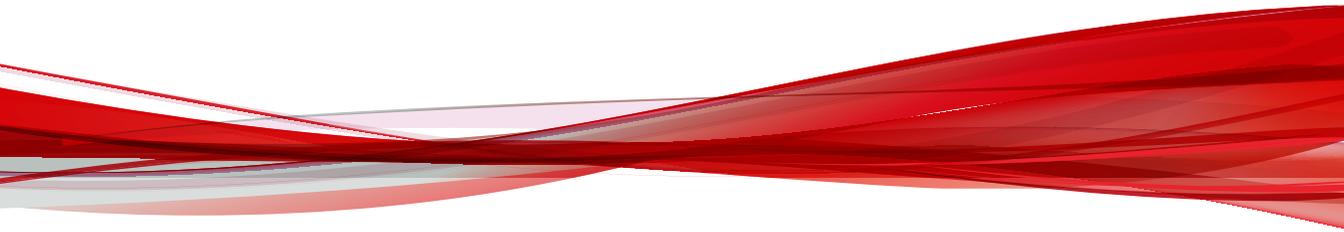
Wildcards in File Names

You can use wildcard characters in file names the same way you can use them in email addresses. Use an asterisk in the name or the extension sections of a file name, but not in conjunction with a partial name or extension. The following are valid examples:

- ***.***: Valid representation of all files.
- ***.extension**: Valid representation of all files of a certain extension.
- **name.***: Valid representation of files with a specific name but with any extension.
- ***name.***: Valid representation of a name.
- **name.*extension**: Valid representation of an extension.

Part IV

Monitoring the Network



Chapter 14

Monitoring the Network

This section provides you with general instructions on the tasks that you need to perform for day-to-day maintenance. For more information on each field on the management console, refer to the Online Help.

Topics include:

- *Monitoring Your Network on page 14-2*
- *Viewing System Status on page 14-2*
- *Interpreting the Statistics on page 14-4*

Monitoring Your Network

IMSS provides a set of tools that enable you to monitor network traffic. You can obtain useful information such as the statistics on the performance of IMSS components, or generate reports that display a breakdown of messages matching various scanning conditions.

Viewing System Status

The **System Status** screen provides at-a-glance information about the status of IMSS components and services.

Procedure

1. Go to **Summary**.
2. Manage settings.

OPTION	DESCRIPTION
Enable Connections	View the connections currently enabled (POP3, Email reputation, and IP Profiler). To enable or disable connections: <ol style="list-style-type: none">a. Select or clear the check box next to a connection item.b. Click Save.
Components	View the version numbers of the antivirus, antispyware, and antispam components that IMSS uses to protect your network. To manually update components: <ol style="list-style-type: none">a. Select the check box next to the component to update.b. Click Update. To roll back to the previous version of the components: <ol style="list-style-type: none">a. Select the check box next to the component to roll back.

OPTION	DESCRIPTION
	<p>b. Click Rollback.</p> <p>To refresh the page:</p> <ul style="list-style-type: none"> Click Refresh to connect to the update source and display the latest component versions in the Availability column.
Managed Server Settings	<p>View other IMSS services registered to this IMSS admin database.</p> <p>To start or stop managed server services:</p> <ul style="list-style-type: none"> Click Start or Stop under the service to change. <p>To unregister managed server services:</p> <ul style="list-style-type: none"> When a managed service is inactive (it is disconnected from the IMSS server), the Unregister button appears in the Connection column next to the specific service. To remove the managed service from this IMSS server, click Unregister. <hr/> <p> Note</p> <p>A managed service could become disconnected for any of the following reasons:</p> <ul style="list-style-type: none"> You removed the scanner. The IMSS manager service stopped. The scanner server is shut down.

Statistics Summary

The **Statistics** screen shows the following information:

Performance Overview

The incoming, outgoing, and total number of messages that IMSS processed. The processing speed is also displayed in messages per minute.

Scan Performance

The scanning conditions that were violated. Message counts will overlap. The percentage in column refers to the total number of messages.

IP Filtering Performance

The type of threat IMSS blocked using the IP filtering product.

Viewing Statistics

Procedure

1. Go to **Summary** from the menu.

2. Click the **Statistics** tab.

The **Statistics** screen appears.

3. Select the desired last number days/hours from the **Show** drop-down list.



Note

IMSS automatically updates these statistics in its database every hour at 20 minutes past the hour.

Interpreting the Statistics

IMSS presents performance statistics in both graphical and table formats. This section explains how the values are derived and helps you to understand the information by breaking down the Statistics tab into the three main sections, which are Performance Overview, Scan Performance, and IP Filtering Performance.

**Note**

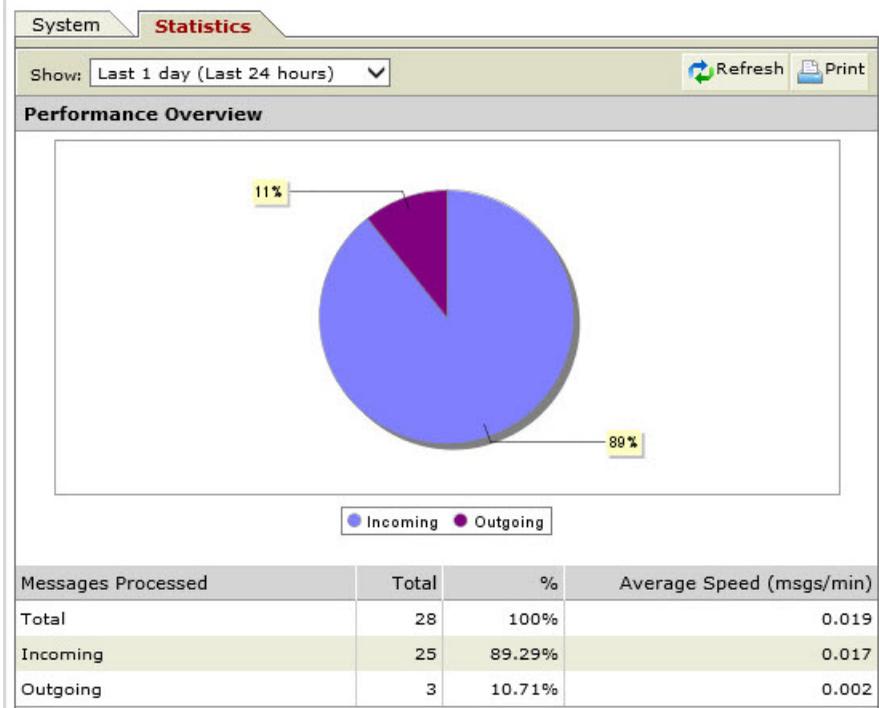
- The values (in percentages) for the same type of threat shown in the chart and table are computed differently.
 - In the table, the total number of messages matching each scanning condition or IP filtering type consists of overlaps. For example, if a message matches more than one scanning condition, such as spam and attachment, this message will be counted twice, once in the total number for spam and a second time in the total number for attachment. Values in the chart, however, do not include such overlaps.
-

Performance Overview

This section shows the total number of incoming and outgoing messages in your network and their corresponding values measured as percentages of the total. The total number includes messages blocked by the following components in ascending order:

- IP Profiler
- ERS
- Scan Engine

IMSS automatically updates these statistics in its database every hour. You can click Refresh to update the screen, but any newly updated statistics in the database will not display on the screen until IMSS has completed the next hourly database update.



Scan Performance

This section shows a breakdown of the number of messages matching various types of scanning conditions specified in the policy rules, and their corresponding values in percentages.

- Chart

Value = Number of messages matching the specific scanning condition divided by the number of messages matching all scanning conditions.

Example:

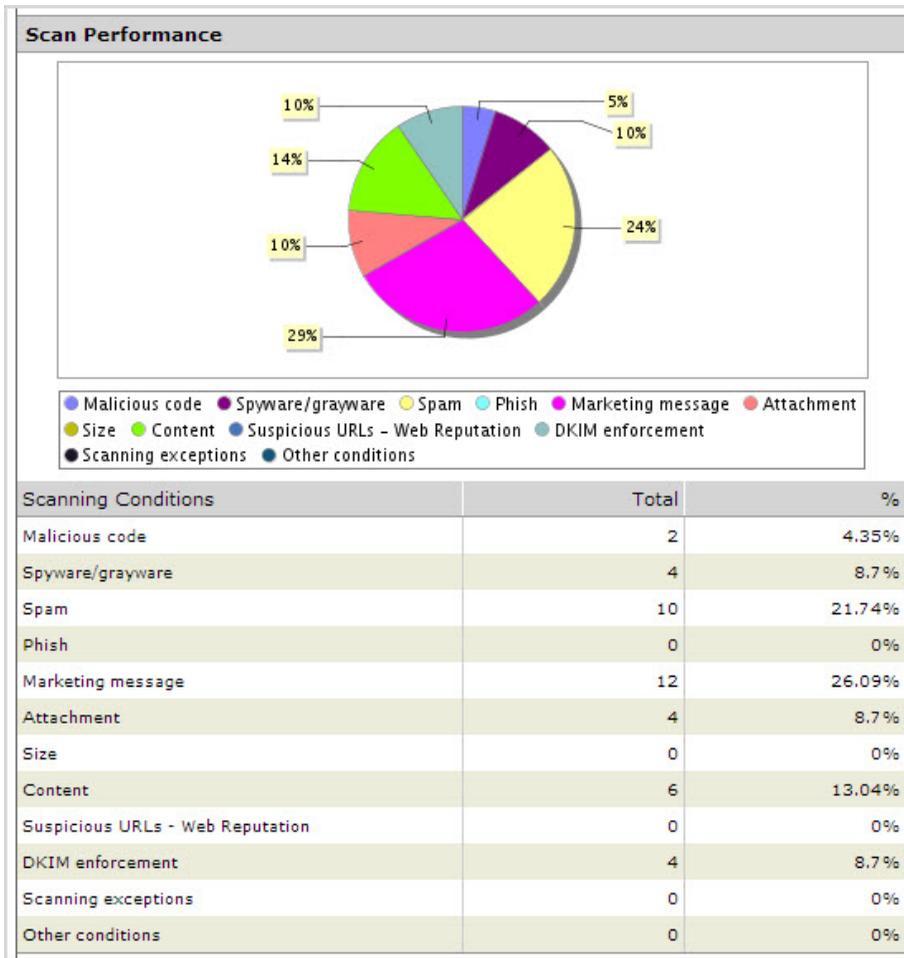
Percentage of spam messages: $71\% = 66 / 93$

- Table

Value = Number of messages matching the specific scanning condition divided by the total number of messages processed.

Example:

Percentage of spam messages: $22\% = 66 / 300$



IP Filtering Performance

This section shows the number of connections blocked by the following:

- The four types of IP Filtering rules, namely, spam, virus, DHA attack, and bounced mail

- IP addresses that you have manually entered
- ERS

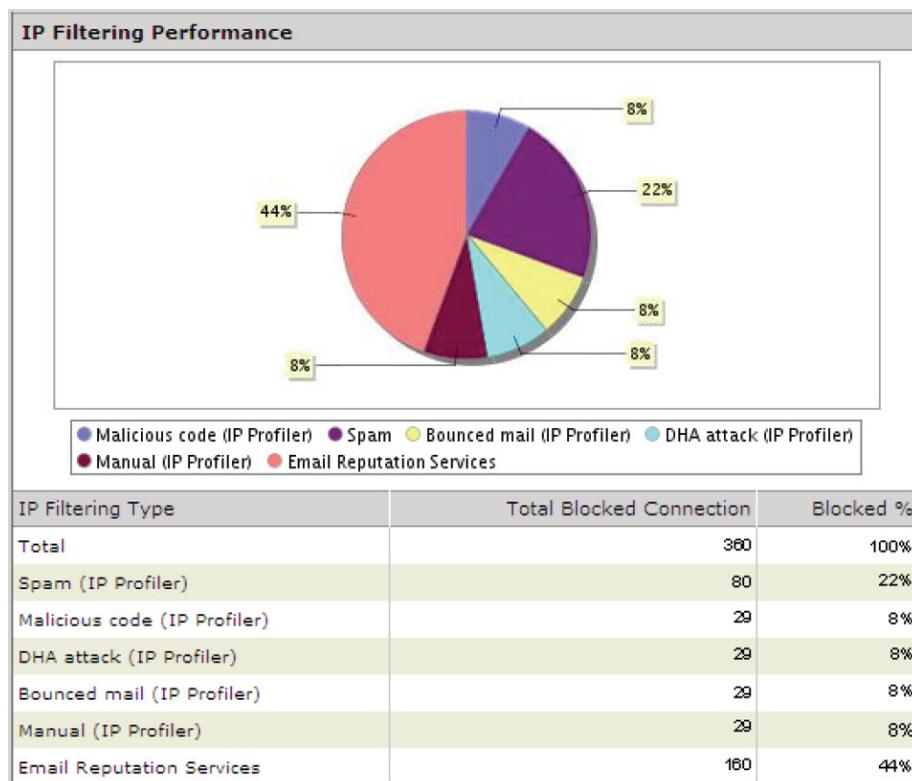
Values in the chart and table are computed as follows:

Value = Number of messages matching the specific IP filtering rule divided by the total number of messages blocked by IP Profiler and ERS.

Example:

Total number of messages blocked by IP Profiler and ERS = 360

Percentage of spam messages: $22\% = 80 / 360$



Chapter 15

Reports

This section provides information on generating one time and scheduled reports.

Topics include:

- *Generating Reports on page 15-2*
- *Managing One-time Reports on page 15-4*
- *Accessing Scheduled Reports on page 15-9*

Generating Reports

Depending on your needs, you can choose to generate a one-time report on demand or schedule a report to be run at specific intervals. IMSS offers you the flexibility of specifying the content for each report and the option of viewing or saving the result in HTML or CSV format.

Types of Report Content

You can select from the following types of content to be included in the report:

TABLE 15-1. Summary Reports

REPORT CONTENT	DESCRIPTIONS
Policy and traffic summary	Shows the total number and size of incoming and outgoing messages, the number of messages matching specific scanning conditions, and a summary of quarantine events.
Virus and malicious code summary	Shows a summary of the virus message count by actions.
Spam summary	Shows a summary of the total spam message count by antispam engine, Email reputation, IP Profiler, and actions.
Sender IP address blocking summary	Includes "IP Profiler Summary" and "Email Reputation IP Blocking Summary". The former shows a summary of the total number of sender connections that reached IP Profiler and are blocked by the different IP Filtering rules. The latter shows the total sender connections that reached Email reputation and are blocked by Email reputation.

TABLE 15-2. Top 10 Reports

REPORT CONTENT	DESCRIPTIONS
Top 10 traffic email addresses	Top 10 email addresses ranked by the total sent and received message count.
Top 10 virus names	Top 10 virus names ranked by their detection count.
Top 10 blocked IP addresses for Directory Harvest Attack (DHA)	Top 10 IP addresses ranked by the blocked count for DHA attack.
Top 10 blocked IP addresses for bounced mail attack	Top 10 IP addresses ranked by the blocked count for bounced mail attack.
Top 10 virus recipients and senders	Top 10 virus recipients and senders ranked by their total received and sent virus message counts.
Top 10 most frequently triggered rules	Top 10 rule names ranked by the number of messages that triggered each rule.
Top 10 spam recipients	Top 10 spam recipient addresses ranked by their total received spam message count.
Top 10 blocked IP addresses by Email reputation	Top 10 blocked IP addresses ranked by the number of connections dropped by Email reputation.
Top 10 blocked IP addresses for spam	Top 10 IP addresses ranked by the blocked count for spam.
Top 10 blocked IP addresses for viruses or malicious code	Top 10 IP addresses ranked by the blocked count for viruses.
Top 10 senders of messages with suspicious URLs	Top 10 sender addresses ranked by their total received messages that contained suspicious URLs.
Top 10 marketing message recipients and senders	Top 10 email addresses ranked by their total received and sent marketing message counts.

Managing One-time Reports

Generate a one-time report for an at-a-glance summary of IMSS protection. For future reference, IMSS retains all one-time reports on this screen.

You can also enable IMSS to automatically generate daily, weekly, or monthly reports.

To view the list of one-time reports that were previously generated, go to **Reports > One-time Reports**.

Procedure

- To change the display, do any of the following:
 - To sort the table, click any of the column headings that are underlined.
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select a number from the drop-down box that represents which page to view.
 - To change the number of items that appear in the list at a time, select a new display value from the drop-down box at the bottom of the table.

- To generate a report, click **Add**, then specify the report details.

The **Output** column shows “In progress” while the report generates.

- To view the report, click one of the following formats under Output:
 - **HTML**: Opens the report in another browser window.
 - **CSV**: Saves the report to a comma-separated value file that you can open with a spreadsheet application.
- To delete a report, select the check box next to it and click **Delete**.

**Note**

ERS and IP Profiler report content is not available unless you activate those products. For more information on activating ERS and IP Profiler, see [Managing Product Licenses on page 21-15](#).

Adding One-time Reports

You can generate one-time reports on demand to help monitor the traffic on your network.

Procedure

1. Go to **Reports > One-time Report**.

2. Click **Add**.

The **Add One-time Report** screen appears. For a list of available reports, see [Types of Report Content on page 15-2](#).

3. Configure the report settings and then click **Save**.

OPTION	DESCRIPTION
Name	Specify a descriptive name.
Dates	Select the time span that the report will cover.
Report Content	Select the content to include in the report.

The report takes several minutes to generate. The message **In progress** appears in the report table.

One-time Reports		
<input type="checkbox"/> Report Name	Date ▾	Output
<input type="checkbox"/> Traffic and policy summary	May 30, 2010 4:35:52 AM	In progress

1-1 of 1 Page 1 10 per page

After the report generates, the hyperlinks **HTML** and **CSV** display in the report table.

One-time Reports		
<input type="checkbox"/> Report Name	Date ▾	Output
<input type="checkbox"/> Virus and malicious code summary	May 30, 2010 4:38:47 AM	HTML CSV
<input type="checkbox"/> Traffic and threat summary	May 30, 2010 4:38:15 AM	HTML CSV
<input type="checkbox"/> Traffic and policy summary	May 30, 2010 4:35:52 AM	HTML CSV

1-3 of 3 Page 1 10 per page

- Under **Output**, select the output format to export the report data.

Report generation occurs once every five minutes. Report generation could require as much as five minutes in addition to the time required to aggregate reporting data and make the necessary calculations.

Scheduled Reports

Use scheduled reports to automate report generation. IMSS provides daily, weekly, and monthly reports.

Configuring Scheduled Reports

Scheduled reports generate automatically according to the schedules you configure.

Procedure

1. Go to **Reports > Settings**.

The **Scheduled Report Settings** screen appears.

Report Type	Status	Schedule	Configure	# to Save
Daily reports	X	2:00	Settings	60
Weekly reports	X	Sunday at 2:00	Settings	20
Monthly reports	X	Day 1 at 2:00	Settings	5

2. Click the **Settings** link for one of the following report types:

- Daily reports
- Weekly reports
- Monthly reports

The report settings screen appears (example: **Daily Report Settings**).

Daily Report Settings 

[Scheduled Report Settings](#) > Daily Report Settings

Generate daily reports

Start time: 2 
hh

Report Content

- Policy and traffic summary
- Virus and malicious code summary
- Spam summary
- Sender IP address blocking summary
- Deep Discovery Advisor analysis summary
- Top 10 traffic email addresses
- Top 10 virus names
- Top 10 IP addresses for DHA attack addresses
- Top 10 IP addresses for bounced mail attack addresses
- Top 10 virus recipients and senders
- Top 10 most frequently triggered rule names
- Top 10 spam recipients
- Top 10 IP addresses blocked by Email reputation
- Top 10 IP addresses blocked for spam
- Top 10 IP addresses blocked for viruses or malicious code
- Top 10 senders of messages that contained suspicious URLs
- Top 10 C&C email recipients and senders

3. Configure the report settings.

For report options, see [Types of Report Content on page 15-2](#).

**Note**

When configuring monthly report settings, if you choose to generate the report on the 29th, 30th, or 31st day, IMSS will generate the report on the last day of the month for months with fewer days. For example, if you select 31, IMSS will generate the report on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Click **Save**.

The report status changes.

5. Specify the number for each type of report that you would like to retain.

6. Click **Save**.

7. Go to **Reports > Scheduled Reports**.

The **Archived Scheduled Reports** screen appears.

**Note**

The report has not generated yet.

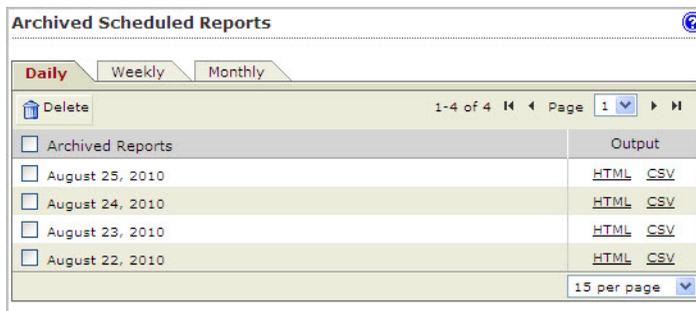
8. After the report generates, see [Accessing Scheduled Reports on page 15-9](#) for available report options.

Accessing Scheduled Reports

Procedure

1. Go to **Reports > Scheduled Reports** from the menu.

The **Schedule Reports** screen appears.



2. Select a tab that corresponds to the generation frequency.
 - **Daily**
 - **Weekly**
 - **Monthly**
3. For available report options, see [Using Scheduled Reports on page 15-10](#).

Using Scheduled Reports

Go to **Reports > Scheduled Reports** and then open either the **Daily**, **Weekly**, or **Monthly** tab.

Procedure

- To view the report, click one of the following formats under **Output**:
 - **HTML**: Opens the report in another browser window.
 - **CSV**: Saves the report to a comma-separated value file that you can open with a spreadsheet application.
- To change the display, do one of the following:
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page.

- To change the number of items that appears in the list at a time, select a new display value from the drop-down box at the bottom of the table.
 - To delete a report, select the check box next to it and click **Delete**.
-

Chapter 16

Logs

This chapter provides you with general instructions on the tasks that you need to perform for the day-to-day maintenance of IMSS. For more information on each field on the management console, refer to the Online Help.

Topics include:

- *[About Logs on page 16-2](#)*
- *[Configuring Log Settings on page 16-2](#)*
- *[Querying Logs on page 16-4](#)*

About Logs

Logs enable you to monitor various types of events and information flow within IMSS. They also serve as an important resource for troubleshooting.

To enable logs and benefit from the information, do the following:

- **Step 1:** *Configuring Log Settings on page 16-2*
- **Step 2:** *Querying Logs on page 16-4*

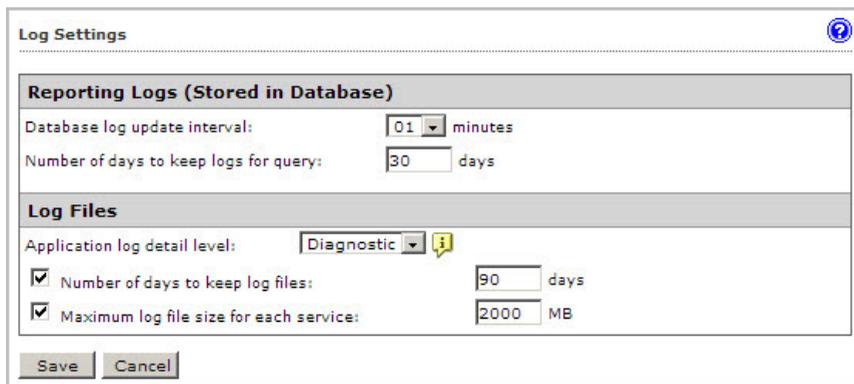
Configuring Log Settings

You can configure the level of detail that IMSS writes to the logs and the length of time it stores them. In addition, you can set the update period that controls how frequently the scanner services write their local logs to the IMSS admin database.

Procedure

1. Go to **Logs > Settings**.

The **Log Settings** screen appears.



The screenshot shows the 'Log Settings' window with the following configuration:

Reporting Logs (Stored in Database)	
Database log update interval:	01 minutes
Number of days to keep logs for query:	30 days

Log Files	
Application log detail level:	Diagnostic ⓘ
<input checked="" type="checkbox"/> Number of days to keep log files:	90 days
<input checked="" type="checkbox"/> Maximum log file size for each service:	2000 MB

Buttons: Save, Cancel

2. Configure **Reporting Logs**.

- **Database log update interval:** IMSS updates the logs regularly at every interval. Select a number between 1 and 60 for the interval. Selecting 60 means that IMSS updates the logs once every hour.
 - **Number of days to keep logs for query:** Specify a value between 1 and 60 that represents the number of days IMSS preserves the report logs in the IMSS admin database.
3. Under **Log Files**, configure the following:
- **Application log detail level:** The level of log detail. Select one of the following:
 - **Normal:** The standard level of detail. This level provides the basic information needed by an administrator for daily monitoring and maintenance.
 - **Detailed:** A high level of detail. All IMSS processes write detailed information to the logs, including: POP3 session information, the policy matched, the filter executed, and the action taken.
 - **Diagnostic:** Comprehensive information on each event or action. Diagnostic level logs include all information from the detailed level, plus SMTP routing information, and the route match information that determined which policy was applied.
 - **Debug:** The most complete and verbose level of detail. Debug logs are only recommended when troubleshooting.

**Note**

Diagnostic or debug logs might consume excessive IMSS resources and could reduce system performance.

- **Number of days to keep log files:** Select the check box and specify a number between 1 and 150 that represents the number of days IMSS keeps the local log files. To prevent IMSS from deleting the log files, clear the check box.
- **Maximum log file size for each service:** Select the check box and specify a number between 100 and 99999 that represents the size in MB for local log files for each type of process or service. To remove any size restriction, clear the check box.

**Note**

IMSS log files are stored in the folder `/opt/trend/imss/log`.

IP Profiler log files are stored in the folder `/opt/trend/ipprofiler/logs`.

Daily log files for each event type are created at midnight and have the suffix "`<Date>.<Count>`". The `<Count>` suffix is incremented if there is more than one (1) log file per day.

If the log file size exceeds the maximum log file size for each service, IMSS will delete the oldest file.

4. Click **Save**.
-

Querying Logs

You can perform queries on the following types of events or information:

Message tracking

Records message details such as the sender, recipient(s), message size, attachment(s), and the final action that IMSS has taken. The query result also indicates the name and type of the policy rule that was triggered.

System events

Provides details on system events such as scan engine and pattern file updates, scanner service status changes, administrator operations, and errors that IMSS encountered.

Policy events

Provides details on the policy rules that were triggered, the actions taken, and the message details.

Quarantine events

Provides details on quarantine events, for example, the percentage of release events in all the quarantine events.

MTA events

Provides connection details of Postfix on the local computer where the central controller is installed.

IP filtering

Provides the time when IMSS started and stopped blocking messages from the queried IP address.

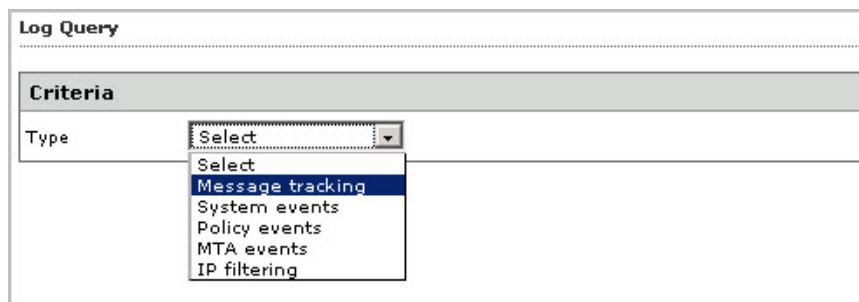
For most log queries, IMSS supports wildcards (*) and exact matches (for example, to view mail recipients whose name includes A or B, set the recipient(s) to “*A*; *B*”). IMSS uses exact matching by default. Leaving the search condition blank displays all logs. For multiple-condition items, use semicolons (;) to separate the entries for recipient(s) and attachment(s).

Querying Message Tracking Logs

Procedure

1. Go to **Logs > Query**.

The **Log Query** screen appears.



The screenshot shows the 'Log Query' interface. Under the 'Criteria' section, there is a 'Type' field with a dropdown menu. The dropdown menu is open, showing the following options: 'Select', 'Message tracking', 'System events', 'Policy events', 'MTA events', and 'IP filtering'. 'Message tracking' is currently selected and highlighted in blue.

2. Next to **Type**, select **Message tracking**.

The query screen for message event logs appears.

3. Next to **Dates**, select a date and time range.
4. Specify any of the following additional information:
 - **Subject**

- **Message ID**
- **Sender**
- **Recipient(s)**
- **Attachment(s)**



Note

- a. Use the asterisk wildcard for partial searches on any field.
-

5. Click **Display Log**.

A timestamp, sender, recipient, subject, and last known action appear for each event.

6. Click the timestamp link to see the following information:

- **Timestamp**
- **Sender**
- **Recipient**
- **Subject**
- **Original size**
- **Attachments**
- **Message ID**
- **Internal ID**
- **Scanner**
- **Final action**
- **Action details**

7. Perform any of the additional actions:

- To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.

- To print the query results, click **Print current page**.
 - To save the query result to a comma-separated value file, click **Export to CSV**.
-

Querying System Event Logs

Procedure

1. Go to **Logs > Query**.

2. Next to **Type**, select **System events**.

The query screen for system event logs appears.

3. In the second drop-down box next to **Type**, select one of the following:

- **All events**: Displays the timestamp and descriptions for all system events.
- **Updates**: Displays the timestamp of all scan engines and pattern file updates from the ActiveUpdate server to the IMSS admin database.
- **Service status**: Displays the timestamp and descriptions when the scanner service is started or stopped.
- **Audit log**: Displays the timestamp and descriptions for operations performed by specified administrator accounts.



Note

As an enhanced log category of system events, **Audit log** replaces **Admin activity** on the IMSS management console. Audit logs record various administrator operations and provide a way to query activities of specified administrator accounts.

- **Errors**: Displays the timestamp and descriptions for all errors that IMSS encountered.

4. In the third drop-down box next to **Type**, select the server to view.

5. Next to **Dates**, select a date and time range.

6. If you select **Audit log**, specify any administrator account whose configuration changes you want to search for next to **Admin accounts**.



Use semicolons to separate multiple administrator accounts.

7. Next to **Description keywords**, specify any keywords to search for.
8. Click **Display Log**.

A timestamp, host name, and description appear for each event. If you select **Audit log**, administrator information also appears for each event.

9. Perform any of the additional actions:
 - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
 - To sort the table, click the column title.
 - To print the query results, click **Print current page**.
 - To save the query result to a comma-separated value file, click **Export to CSV**.
-

Querying Policy Event Logs

Procedure

1. Go to **Logs > Query**.
2. Next to **Type**, select **Policy events**.

The query screen for policy event logs appears.

3. In the second drop-down box next to **Type**, select one of the following items related to the policy and the rules you configured for the policy:
 - **All**
 - **Virus or malicious code**

- Spam/phish
- Web Reputation

**Note**

If you select **Web Reputation**, IMSS displays two additional drop-down lists that contain website content categories. Select any category name to narrow down your log query.

- Marketing message
 - DKIM enforcement
 - Attachment
 - Size
 - Content
 - Others
 - Scanning exceptions
4. Specify any of the following additional information:
- Sender
 - Recipient(s)
 - Rule
 - Subject
 - Attachment(s)
 - Message ID

If you leave any text box blank, all results for that item appear.

5. Click **Display Log**. A timestamp, action, rule, and message ID appear for each event.
6. Click the timestamp link to see the following information:

- **Timestamp**
- **Sender**
- **Recipient**
- **Subject**
- **Original size**
- **Violating attachments**
- **Rule type**
- **Rule(s)**
- **Action**
- **Message ID**
- **Internal ID**
- **Reason**
- **Scanner**

7. Perform any of the additional actions:

- To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
- To sort the table, click the column title.
- To print the query results, click **Print current page**.
- To save the query result to a comma-separated value file, click **Export to CSV**.



Note

- `"*A*;*B*"` means a string that has A or B.
 - `"A*;*B"` means a string that starts with A or ends with B.
 - `","` represents the OR operation.
-

Querying Quarantine Event Logs

Procedure

1. Go to **Logs > Query**.

2. Next to **Type**, select **Quarantine events**.

The query screen for quarantine event logs appears.

3. Next to **Dates**, select a date and time range.

4. Next to **Rule(s)**, specify any rule name keywords to search for.

5. Click **Display Log**.

A rule name, quarantine event count, release event count, and release percentage appear for each rule.

6. Perform any of the additional actions:

- To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
 - To sort the table, click the column title.
 - To print the query results, click **Print current page**.
 - To save the query result to a comma-separated value file, click **Export to CSV**.
-

Querying MTA Event Logs

Procedure

1. Go to **Logs > Query**.

2. Next to **Type**, select **MTA events**.

The query screen for MTA event logs appears.

3. Next to **Dates**, select a date and time range.

4. Click **Display Log**.

A timestamp, action, rule, and message ID appear for each event.

5. Perform any of the additional actions:

- To change the number of items that appears in the list at a time, select a new display value from the **Results per page** drop-down box on the top of the table.
 - To print the query results, click **Print current page**.
 - To save the query result to a comma-separated value file, click **Export to CSV**.
-

Querying IP Filtering Logs

Procedure

1. Go to **Logs > Query**.
2. Next to **Type**, select **IP filtering**.
3. In the second drop-down box next to **Type**, select one of the following items related to IP Filtering:
 - **All**
 - **ERS**
 - **DHA attack**
 - **Bounced mail**
 - **Virus**
 - **Spam**
 - **Manual**: Refers to the IP addresses that you have specified in the blocked list.
4. Next to **Dates**, select a date and time range.
5. Next to **IP**, provide any IP address to search.

6. Click **Display Log**. Information appears for the time that IMSS both started and stopped blocking each IP address or domain.
 7. Perform any of the additional actions:
 - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
 - To print the query results, click **Print current page**.
 - To save the query result to a comma-separated value file, click **Export to CSV**.
-

Chapter 17

Mail Areas and Queues

This chapter provides information about IMSS archive areas and mail queues.

Topics include:

- *Quarantine and Archive on page 17-2*
- *Configuring Quarantine and Archive Settings on page 17-2*
- *Managing Quarantine Areas on page 17-4*
- *Managing Archive Areas on page 17-6*
- *Querying Messages on page 17-9*
- *Viewing Quarantined Messages on page 17-13*
- *Viewing Archived Messages on page 17-14*
- *Configuring User Quarantine Access on page 17-15*
- *Adding an EUQ Database on page 17-17*
- *Command-line Options for euqtrans Tool on page 17-18*

Quarantine and Archive

Quarantine and archive are among some of the actions that you can configure IMSS to take when messages match certain rules. Generally, you configure IMSS to quarantine messages that you would like to analyze before deciding whether to delete or release to the intended recipient(s). Archive, on the other hand, allows you to store messages for future reference.



Note

IMSS 7.1 SP2 supports incoming message scanning from IPv6 networks.



Note

In order to use End-User Quarantine, first configure the LDAP settings. For more information, see [Configuring LDAP Settings on page 3-6](#).

Configuring Quarantine and Archive Settings

Quarantine and archive settings allow you to manage quarantine and archive areas and allocate the amount of disk space per scanner for storing quarantined or archived messages.

Procedure

1. Go to **Quarantine & Archive > Settings**.

The **Quarantine and Archive Settings** screen appears.

Area	Expiration	Size	Items	EUQ
<input type="checkbox"/> Default Quarantine	15 day(s)	0MB	0	

2. Click the **Quarantine** tab (default) or **Archive** tab, to configure a quarantine area or an archive area.

The list of areas appears in the table below.

3. To modify the total disk size allowed for all quarantine areas or archive areas for each scanner service, specify the size of the area next to **Disk quota (per scanner)**, and then select **MB** or **GB** from the drop-down box.
4. Click **Add**, to add a quarantine or archive area.
5. Next to **Name**, specify a descriptive name.
6. Next to **Delete messages older than**, specify the number of days after which IMSS deletes the quarantined or archived messages. The value is exclusive. For example, if you specify 15, IMSS deletes the quarantined messages on the 16th day.
7. Select **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)**, to automatically save messages to the EUQ database for a quarantine area.

**Note**

After selecting **Synchronize all spam and email messages, that do not violate virus, phishing or Web reputation rules, to the EUQ database (for this area only)**, a check mark appears under the EUQ column of the table on the **Quarantine and Archive Settings** screen.

8. Click **Save**.
- The **Quarantine and Archive Settings** screen reappears.
9. To view or modify a quarantine or archive area, click the name of the area and configure the settings above.
 10. To delete a quarantine or archive area, select the check box next to it and click **Delete**.
 11. After modifying any settings, click **Save**.
-

Managing Quarantine Areas

IMSS can quarantine messages on the server in the following directory:

```
$IMSS_HOME/queue/quarantine
```



Tip

Trend Micro recommends quarantining messages that you think you might want to analyze and possibly send to the intended recipient later. Create different types of quarantine areas for different types of messages, such as messages that violate spam scanning conditions or messages that violate message content conditions.

Related information

- [Managing the Quarantine from the Actions Screen of a Policy Rule](#)
- [Managing the Quarantine Settings](#)

Managing the Quarantine from the Actions Screen of a Policy Rule

If you are configuring the actions for a rule, do the following:

Procedure

1. Click **Edit** next to **Quarantine** to under **Intercept** actions.
The **Quarantines** screen appears showing the available quarantine areas.
2. Do one of the following:
 - To add a new quarantine area, click **Add**.
 - To modify an existing quarantine area, click the area name and then click **Edit**.
An edit screen appears.
3. Next to **Name**, specify the name of the quarantine area.

4. To automatically delete quarantined messages after a certain number of days, next to **Delete messages older than**, specify the number of days from 1 to 60.

This number represents the number of days after which IMSS deletes the quarantined messages. The value is exclusive. For example, if you specify 15, IMSS deletes the quarantined messages on the 16th day.

5. Select **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)** to automatically save messages to the EUQ database.

**Note**

After selecting **Synchronize all spam and email messages, that do not violate virus, phishing or Web reputation rules, to the EUQ database (for this area only)**, a check mark appears under the EUQ column of the table on the **Quarantine and Archive Settings** screen.

6. Click **Save** to return to the **Quarantines** screen.
 7. Click **Done** to continue selecting actions.
 8. To quarantine messages, select the radio button next to **Quarantine to** under **Intercept** and select the desired quarantine area from the drop-down box.
-

Managing the Quarantine Settings

Procedure

1. Go to **Quarantine & Archive > Settings**.

The **Quarantine and Archive Settings** screen appears with the **Quarantine** tab displayed by default.

2. Next to **Disk quota per scanner service**, do the following:
 - a. Specify the maximum size for the area.
 - b. Select **MB** or **GB**.



When the total disk size for all the quarantined messages exceeds the quota on a scanner, the oldest quarantined messages are deleted first to keep the size under the quota.

3. Do one of the following:
 - To add a new quarantine area, click **Add**.
 - To modify an existing quarantine area, click the area name.
4. Next to **Name**, specify the name of the quarantine area.
5. To automatically delete quarantined messages after a certain number of days, next to **Delete messages older than**, specify the number of days from 1 to 60.

This number represents the number of days after which IMSS deletes the quarantined messages. The value is exclusive. For example, if you specify 15, IMSS deletes the quarantined messages on the 16th day.

6. Select **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)** to automatically save messages to the EUQ database.



After selecting **Synchronize all spam and email messages, that do not violate virus, phishing or Web reputation rules, to the EUQ database (for this area only)**, a check mark appears under the EUQ column of the table on the **Quarantine and Archive Settings** screen.

7. Click **Save** to return to the **Quarantine and Archive Settings** screen.
 8. Click **Save**.
-

Managing Archive Areas

IMSS can archive messages on the server in the following directory:

`$IMSS_HOME/queue/archive`

Managing the Archive from the Actions Screen of a Policy Rule

If you are configuring the actions for a rule, do the following:

Procedure

1. Click **Edit** next to **Archive modified to** under **Monitor** actions.

The **Archives** screen appears showing the available quarantine areas.

2. Do one of the following:
 - To add a new archive area, click **Add**.
 - To modify an existing archive area, click the area name and then click **Edit**.

An edit screen appears.

3. Next to **Name**, specify the name of the archive area.
4. To automatically delete archived messages after a certain number of days, next to **Delete messages older than**, specify the number of days from 1 to 60.

This number represents the number of days after which IMSS deletes the archived messages. The value is exclusive. For example, if you specify 15, IMSS deletes the archived messages on the 16th day.

5. Click **Save** to return to the **Archives** screen.
 6. Click **Done** to continue selecting actions.
 7. To archive messages, select the radio button next to **Archive modified to** under **Monitor** and select the desired archive area from the drop-down box.
-

Managing the Archive Settings

Procedure

1. Go to **Quarantine & Archive > Settings**.

The **Quarantine and Archive Settings** screen appears with the **Quarantine** tab displayed by default.

2. Click the **Archive** tab.
3. Next to **Disk quota per scanner service**, do the following:
 - a. Specify the maximum size for the area.
 - b. Select **MB** or **GB**.



When the total disk size for all the archived messages exceeds the quota on a scanner, the oldest archived messages are deleted first to keep the size under the quota.

4. Do one of the following:
 - To add a new quarantine area, click **Add**.
 - To modify an existing quarantine area, click the area name and then click **Edit**.

An edit screen appears.

5. Next to **Name**, specify the name of the archive area.
6. To automatically delete archived messages after a certain number of days, next to **Delete messages older than**, specify the number of days from 1 to 60.

This number represents the number of days after which IMSS deletes the archived messages. The value is exclusive. For example, if you specify 15, IMSS deletes the archived messages on the 16th day.

7. Click **Save** to return to the **Quarantine and Archive Settings** screen.
 8. Click **Save**.
-

Querying Messages

You can perform a query on quarantined and archived messages before deciding which action to perform. After viewing the message details, you can choose to release or delete archived messages from IMSS.



Tip

Trend Micro recommends quarantining items that could pose a risk to your network, such as messages and attachments that violate antivirus rules. Before you resend any quarantined message, make sure that it does not pose a threat to your network.

Trend Micro recommends archiving only items that you want to reference later.

Querying the Quarantine Areas

Procedure

1. Go to **Quarantine & Archive > Query**.

The **Quarantine and Archive Query** screen appears. The **Quarantine** tab displays by default. If it does not display, click **Quarantine**.

Area	Expiration	Size	Items	EUQ
<input type="checkbox"/> <u>Default Quarantine</u>	15 day(s)	0MB	0	

2. Under **Criteria**, configure the following:
 - **Search:** Select the quarantine area, the reason the message was quarantined, and the scanner that scanned the message.

- **Dates:** Select a date and time range.
3. Specify values for the following:
 - **Sender**
 - **Subject**
 - **Recipient(s)**
 - **Attachment(s)**
 - **Rule**
 - **Message ID**

**Note**

When querying a message containing multiple recipients or attachments, type `*string*` (where string is the name of one of the recipients or attachments).

4. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject, and reason for quarantining the message.
5. To change the display, do any of the following:
 - To sort the table, click any of the column headings (except reason).
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select the desired page to view from the drop-down list.
 - To change the number of items that appears in the list at a time, select a new display value from the drop-down list at the bottom of the table.
6. To view details about any quarantined message, click the timestamp for the item. The **Quarantine Query** screen appears showing the message and all of its details.
7. To resend any message, click the check box next to it in the query result table, and then click one of the following options:
 - **Deliver:** The message is sent directly to the recipient, bypassing all rules except virus scan rules.

- **Reprocess:** The message only bypasses the current rule, and may be quarantined again by other filters.

**Tip**

Trend Micro does not recommend resending messages that violated antivirus filters. Doing so could put your network at risk.

-
8. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

**Note**

IMSS only records and shows the attachment names if you have specified **Attachment** as a scanning condition. However, if the number of attachments in the message exceeds the maximum number specified in condition, the attachment name will not be shown.

Querying the Archive Areas

Procedure

1. Go to **Quarantine & Archive > Query**.
The **Quarantine** tab displays by default.
2. Click the **Archive** tab.
3. Under **Criteria**, configure the following:
 - **Search:** Select the archive area, the reason the message was archived, and the scanner that scans the message.
 - **Dates:** Select a time range.
4. Specify values for the following:
 - **Sender**
 - **Subject**

- **Recipient(s)**
- **Attachment(s)**
- **Rule**
- **Message ID**

**Note**

When querying a message containing multiple recipients or attachments, type `*string*` (where string is the name of one of the recipients or attachments).

5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject, and reason for archiving the message.
6. To change the display, do any of the following:
 - To sort the table, click any of the column headings (except reason).
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select the desired page to view from the drop-down list.
 - To change the number of items that appears in the list at a time, select a new display value from the drop-down list at the bottom of the table.
7. To view details about any archived message, click the timestamp for the item.

The **Archive Query** screen appears showing the message and all of its details.

8. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

**Note**

IMSS only records and shows names of attachments if you have specified Attachment as a scanning condition. However, if the number of attachments in the message exceeds the maximum number specified in condition, the attachment name will not be shown.

Viewing Quarantined Messages

All messages that IMSS quarantines can be queried and viewed.

Procedure

1. After you perform a query for quarantined messages, click the timestamp for the quarantined item in the query result table. The **Quarantine Query** screen appears showing the following information:
 - **Timestamp**
 - **Sender**
 - **Reason**
 - **Recipient**
 - **Rules**
 - **Subject**
 - **Scanner**
 - **Original Size**
 - **Message ID**
 - **Internal ID**
 - **Attachments**
2. Next to **Message view**, click either **Header** or **Message**.
3. Click any of the following buttons:
 - **Back to List**: Return to the query screen.
 - **Deliver** : Resend the message to its original recipients.
 - **Reprocess**: IMSS scans the message again and acts accordingly.
 - **Delete**: Delete the message.

- **Download** : Save the message to your computer.



Tip

Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Viewing Archived Messages

All messages that IMSS archives can be queried and viewed.

Procedure

1. After you perform a query for archived messages, click the timestamp for the archived item in the query result table. The **Archive Query** screen appears showing the following information:
 - **Timestamp**
 - **Sender**
 - **Reason**
 - **Recipient**
 - **Rules**
 - **Subject**
 - **Scanner**
 - **Original Size**
 - **Message ID**
 - **Internal ID**
 - **Attachments**
2. Next to **Message view**, click either **Header** or **Message**.

3. Click any of the following buttons:
 - **Back to List:** Return to the query screen.
 - **Delete:** Delete the message.
 - **Download :** Save the message to your computer.

**Tip**

Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Configuring User Quarantine Access

You can grant all or selected end users access to the EUQ management console. This allows them to manage the spam messages addressed to them by visiting `https://<target server IP address or hostname>:8447`.

Procedure

1. Go to **Administration > End-User Quarantine > User Quarantine Access**.

The **User Quarantine Access** screen appears.

End-User Quarantine ?

These groups can access quarantined spam items and will use LDAP authentication with the designated IMSS server.

EUQ Authentication | **User Quarantine Access**

Enable access ?

Allow end user to deliver quarantined mail in EUQ directly ?

Allow end users to retrieve quarantined email messages with alias email addresses ?

Keep quarantined spam for:

Set maximum number of approved senders

Maximum approved senders per end-user:

Specify the logon notice

Specify the greeting displayed to users on the EUQ logon page. The maximum length is 2,000 characters. For better security, Trend Micro recommends not using HTML. To configure the administrator logon notice, refer to the [Logon Notice](#) page.

Select LDAP groups to enable access

Enable All

Select groups from LDAP Search below.

2. Select **Enable access**.
3. Select **Allow end user to deliver quarantined mail in EUQ directly** to allow end users to deliver quarantined messages directly to the recipient. The message bypasses all rules except virus scanning rules.
4. Select **Allow end users to retrieve quarantined email messages with alias email addresses** to allow end users to retrieve quarantined messages using alias email addresses configured in Microsoft Exchange.
5. Select the number of days to keep quarantined spam messages.

6. Select the maximum number of senders each end-user can approve when sifting through the quarantined messages.
 7. Specify a logon notice that appears on the user's browser when he/she starts to access the quarantined messages.
 8. Under **Select LDAP groups**, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.
 9. To add individual LDAP groups, clear the **Enable all** check box and do either of the following:
 - Search for groups:
 - a. From the drop-down list, select Search LDAP groups.
 - b. Specify the group name.
 - c. Click **Search**. The groups appear in the table below.
 - d. Click the LDAP groups to add.
 - e. Click **>>**. The groups appear in the **Selected Groups** table.
 - Browse existing groups:
 - a. From the drop-down list, select **Browse LDAP groups**. The groups appear in the table below.
 - b. Click the LDAP groups to add.
 - c. Click **>>**. The groups appear in the **Selected Groups** table.
 10. Click **Save**.
-

Adding an EUQ Database

If you have an existing EUQ database, you may add new EUQ databases if you want to do the following:

- Perform load balancing

- Allow more end users to access EUQ

Registering an EUQ Database

You may register an EUQ database from the web management console if the database was already installed but unregistered. Otherwise, run the IMSS installation program to add a new EUQ database to the system.

Procedure

1. Go to **Administration** > **IMSS Configuration** > **Connections** from the menu.

The **Components** tab appears by default.

2. Click the **Database** tab.
3. Click the **Register** button.

The **EUQ Database Settings** screen appears.

4. Specify the database settings.

- Server
- Database name
- User name
- Password

5. Click **OK**.
-

Command-line Options for euqtrans Tool

The following table explains the command-line options for the euqtrans script.

TABLE 17-1. Command-line Options for euqtrans Tool

OPTION	DESCRIPTION
all	Transfer the individual Approved Senders Lists and information about the quarantined mail messages from the database that was removed to the new location (database) based on the updated Table and Database mapping.
approvedsender	Transfer the individual Approved Senders Lists from the database that was removed to the new location (database) based on the new mapping.

Chapter 18

Notifications

This chapter provides you with general instructions on the tasks that you need to perform for the day-to-day maintenance of IMSS. For more information on each field on the management console, refer to the Online Help.

Topics include:

- *Event Notifications on page 18-2*
- *Configuring Delivery Settings on page 18-2*
- *Configuring Event Criteria and Notification Message on page 18-4*
- *EUQ Digest on page 18-6*
- *Configuring a Logon Notice on page 18-8*
- *Editing Notifications on page 18-9*

Event Notifications

You can configure IMSS to send an email or SNMP notification to you or specific users upon the occurrence of the following categories of events:

TABLE 18-1. Event notifications

EVENT	DESCRIPTION
System Status	Informs you when certain IMSS performances fall below the desired level. For example, when a scanner service stops working, or when the number of messages in the delivery queue exceeds the desired quantity.
Scheduled Update Event	Alerts you when IMSS is able or unable to perform a scheduled update of the scan engine or pattern files from the update source onto the admin database.  Note For more information, see Scheduled Component Updates on page 4-6 .
Scanner Update Result	Alerts you when IMSS is unable to update the engine or pattern files on any scanner.

Configuring Delivery Settings

The delivery settings allow you to specify email and SNMP trap settings to deliver system and policy event notification messages.



Note

IMSS 7.1 SP2 supports sending notifications to IPv6 servers.

Procedure

1. Go to **Administration > Notifications**.

The **Events** tab appears by default.

2. Click the **Delivery Settings** tab.

Notifications

Events	Delivery Settings	Web EUQ Digest	Logon Notice
Email Settings			
Recipient(s):	<input type="text" value="root@localhost"/>		
	Use a semicolon ";" to separate multiple addresses		
Sender's email address:	<input type="text" value="postmaster@localhost"/>		
SMTP server address: 	<input type="text" value="127.0.0.1"/>		
SMTP server port:	<input type="text" value="10026"/>		
Preferred charset:	<input type="text" value="English (us-ascii)"/> 		
Message header:	<input type="text"/>		
Message footer:	<input type="text"/>		
SNMP Trap			
Server name (IP or FQDN):	<input type="text"/>		
Community:	<input type="text" value="public"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			

3. Under **Email Settings**, configure the following:
 - **Recipient(s)**: Specify the recipient email addresses.
 - **Sender's email address**: Specify the email address to appear as the sender.
 - **SMTP server address**: Specify the Fully Qualified Domain Name (FQDN) or the IP address of the SMTP server that delivers email on the network.
 - **SMTP server port**: Specify the port number that IMSS uses to connect to the SMTP server.
 - **Preferred charset**: IMSS will use this setting to encode the notification messages.

- **Message header:** Specify the text to appear at the top of the notification.
 - **Message footer:** Specify the text to appear at the bottom of the notification.
4. Under **SNMP Trap**, configure the following:
- Server name
 - Community

OPTION	DESCRIPTION
Server name	<p>Specify the FQDN or IP address of the SNMP server. SNMP Trap is the notification message sent to the Simple Network Management Protocol (SNMP) server when events that require administrative attention occur.</p> <hr/> <p> Note SNMP servers do not support IPv6-formatted addresses.</p>
Community	<p>Specify the SNMP server community name. Community is the group that computers and management stations running SNMP belong to. To send the alert message to all SNMP management stations, specify 'public' as the community name. For more information, refer to the SNMP documentation.</p>

5. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

Configuring Event Criteria and Notification Message

You can set the criteria under which IMSS will trigger a notification message and also customize the message content for each event.

Procedure

1. Go to **Administration > Notifications**.

The **Events** tab appears by default.

Notifications 

Events | Delivery Settings | Web EUQ Digest | Logon Notice

System Events Notification		
System Status	Email	SNMP
Notify every <input type="text" value="10"/> minutes		
Service on any scanner stops for more than <input type="text" value="10"/> minutes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Free disk space on any scanner is less than <input type="text" value="10240"/> MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delivery queue contains more than <input type="text" value="10000"/> messages	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Retry queue contains more than <input type="text" value="10000"/> messages	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scheduled Update Event	Email	SNMP
Scheduled update of Virus Pattern, Spyware Pattern, IntelliTrap Pattern, and IntelliTrap Exception Pattern is:		
Unsuccessful	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Successful	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scheduled update of Virus Scan Engine or URL Filtering Engine is:		
Unsuccessful	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Successful	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scheduled update of Antispam Engine or Antispam Pattern is:		
Unsuccessful	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Successful	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Scanner Update Result	Email	SNMP
Applying engine or pattern update fails on any scanner	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Smart Scan Event	Email	SNMP
Unable to connect to the Smart Protection Network	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. Under **System Status**, configure the following:

- **Notify every { } minutes:** Specify the notification frequency for all performance notifications.

To edit each of the following notifications, click the link.

- **Service on any scanner stops for more than:** Specify the number of minutes.
- **Free disk space on any scanner is less than:** Specify the number of MB.
- **Delivery queue contains more than:** Specify the number of messages.
- **Retry queue folder contains more messages than:** Specify the number of messages.



Note

The notifications **Delivery queue contains more messages than** and **Retry queue folder contains more messages than** only function when IMSS runs with Postfix.

3. Under **Scheduled Update Event**, click the **Unsuccessful** and **Successful** links to edit notifications for component updates.

Scheduled Update Event is the event in which the latest engine and pattern files from the Update Source are updated onto the IMSS admin database.

4. Under **Scanner Update Results**, click the **Applying engine or pattern update fails on any scanner** link to edit the notification.

Scanner Update Results are the results of updating the latest engine and pattern files from the IMSS admin database onto the scanners.

5. Under **Smart Scan Event**, click **Unable to connect to the Smart Protection Network** to edit the notification.

This notification is sent when IMSS reverts to Conventional Scan after several unsuccessful attempts to connect to the Smart Protection Network.

6. Select the **Email** and/or **SNMP** check boxes according to how you would like to receive the notification.
 7. Click **Save**.
-

EUQ Digest

The EUQ digest is a notification that IMSS sends to inform users about messages that were processed as spam and temporarily stored in the EUQ.

**Note**

IMSS sends EUQ digests only if there are new quarantined messages since the last digest.

IMSS does not send EUQ digests for distribution list addresses. To manage the quarantined messages of distribution lists, users must log on to the EUQ management console.

The EUQ digest provides the following information:

- **Total spam mail count:** Number of new messages in EUQ since the last notification
- **Message list:** Summary of new messages processed as spam
 - **Sender:** Sender email address
 - **Subject:** Subject line
 - **Size:** Message size (including attachments)
 - **Received:** Date and time the message was received

Configuring EUQ Digest Settings

Procedure

1. Go to **Administration > Notifications**.
The **Events** tab displays by default.
2. Click **Web EUQ Digest**.
3. Select the check box next to **Enable EUQ Digest**.
4. Under **Digest Schedule**, click the radio button next to one of the following frequencies:
 - **Daily:** Select the time of day from the drop-down boxes.
 - **Weekly:** Select the day and time of day from the drop-down boxes.
5. Under **Digest Mail Template**, specify the subject and notification content.

To see a list of variables to include in the notification, click **Variables list**.

6. Click **Save**.

Configuring a Logon Notice

A logon notice is a customizable message displayed to administrators on the logon page.

Procedure

1. Go to **Administration > Notifications**.

The **Events** tab displays by default.

2. Click **Logon Notice**.

The screenshot shows the 'Notifications' configuration page with the 'Logon Notice' tab selected. The page title is 'Notifications' with a help icon. The tabs are 'Events', 'Delivery Settings', 'Web EUQ Digest', and 'Logon Notice'. The main content area contains the instruction: 'Specify the greeting displayed to administrators on the logon page. The maximum length is 2,000 characters. Only plain text is supported. To configure the EUQ logon notice, refer to the [User Quarantine Access page](#).' Below this is a text input field containing 'dsfs'. At the bottom are 'Save' and 'Cancel' buttons.

3. Specify a logon notice that will be displayed to administrators.

4. Click **Save**.
-

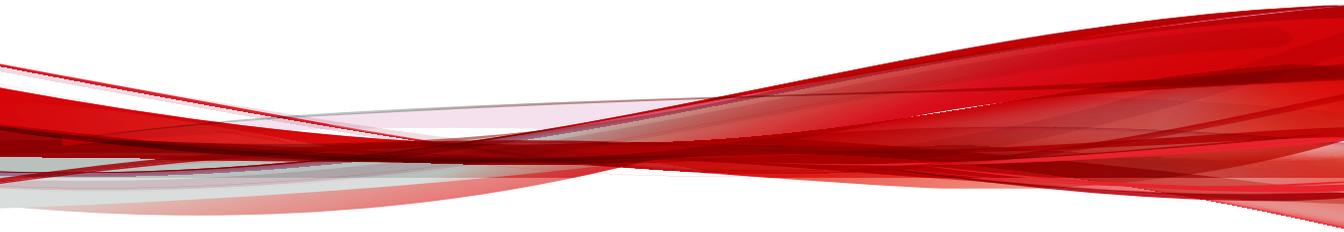
Editing Notifications

Procedure

1. Go to **Administration > Notifications**.
 2. Click the notification to edit.
The edit screen for that notification appears.
 3. Specify the subject and message, or SNMP message.
To see a list of variables to include in the notification, click **Variables list**.
 4. Click **Save**.
-

Part V

Administering IMSS



Chapter 19

Backing Up, Restoring, and Replicating Settings

This chapter provides instructions on how to back up and restore IMSS configuration settings. If you have deployed multiple IMSS scanners and are using Trend Micro Control Manager simultaneously, you can also replicate IMSS settings without having to reconfigure settings for each new scanner.

Topics include:

- *Importing and Exporting Settings on page 19-2*
- *Backing Up IMSS on page 19-4*
- *Restoring IMSS on page 19-6*
- *Replicating Settings on page 19-7*

Importing and Exporting Settings

Use the **Import/Export** screen to create a backup of IMSS settings. Keeping a backup allows you to easily re-apply your settings to an IMSS 7.1 SP2 server . You can also replicate a configuration across several IMSS 7.1 SP2 servers by importing the same configuration file into the desired servers.



Important

Only the following configurations are compatible with IMSS Linux 7.1 SP2. Other configurations are not supported.

- IMSS Linux 7.0 SP1
 - IMSS Linux 7.1 Patch 3
 - IMSS Linux 7.1 SP1
 - IMSS Linux 7.1 SP2
 - IMSS Solaris 7.0 SP1 Patch 4
-



Note

IMSS 7.1 SP2 recognizes addresses imported in IPv6 format, and can export addresses in IPv6 format. However, you must manually import or export `imss.ini` settings.

Exporting Configuration Files

During export, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any IMSS services .
- Register/unregister any EUQ database to/from IMSS.
- Start other export or import tasks.

Procedure

1. Go to **Administration > Import/Export**.
 2. Click **Export**.
 3. When the dialog box appears, click **Save** and save it to your computer.
 4. To return to the **Import/Export** screen, click **Return**.
-

Importing Configuration Files

During import, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any IMSS services .
- Register/unregister any EUQ database to/from IMSS.
- Start other export or import tasks.

Procedure

1. Log on to the IMSS management console.
2. Verify that no services are starting or stopping. If services are starting or stopping, wait until the operation has completed.
3. Go to **Administration > Import/Export**.
4. Under **Import Configuration Files**, click **Browse...** and locate the file.

**Note**

When importing IMSS Linux 7.1 SP2 configurations, the imported configuration file must be from an IMSS Linux 7.1 SP2 build number that is equal to or older than the current build number.

5. Click **Import**.

The original IMSS settings and rules, such as domain-based delivery settings, will be deleted and replaced by the imported settings and rules.

Backing Up IMSS

After you have installed IMSS and configured the required settings, it is always prudent to create backups of the settings so that you can restore IMSS quickly in the event of a system failure.

You can choose to perform a full or minimal backup of IMSS as follows:

- **Full:** Backs up all IMSS local configuration and binary files stored in `/opt/trend` and database-related files in `/var/imss`.
- **Minimal:** Backs up only IMSS configuration settings stored in `/opt/trend/imss/config`.



Note

1. The backup and restore instructions in this manual are targeted at the all-in-one deployment of IMSS. In the case of distributed deployment, you need to back up the following:
 - a. The database files or tables on the computer(s) where you installed the databases.
 - b. The local binary and configuration files on every computer where you installed IMSS components.
 2. If you perform a minimal backup, you may need to install previous hot fixes, patches, or service packs after restoring IMSS.
-

Performing a Full Backup

Procedure

1. Stop all IMSS-related processes:

```
/opt/trend/imss/script/imssstop.sh stop
```

2. Stop Postfix.
3. Back up the folder `/opt/trend/` and `/var/imss/`.
4. Back up all Postfix configuration files under `/etc/postfix`.

For example, `main.cf`, `master.cf`, `allowAccessList`, `denyAccessList`.

5. Start Postfix.
6. Start all IMSS-related processes:

```
/opt/trend/imss/script/imssstart.sh
```

Performing a Minimal Backup

Procedure

1. Stop all IMSS-related processes.
For details, see [Performing a Full Backup on page 19-4](#).
2. Stop Postfix.
3. Back up the `/opt/trend/imss/config` folder.
4. Back up the folder `/ect/postfix`.
5. Back up all database tables.
6. Start Postfix.
7. Start all IMSS-related processes.

For details, see [Performing a Full Backup on page 19-4](#).

Restoring IMSS

In the event of a system failure, you can restore IMSS depending on whether you have performed a full or minimal backup previously.

Performing a Full Restoration

Procedure

1. Install a new IMSS server on one computer, ensuring that the IP address, database user name, and password are the same as the original.
 2. Stop all IMSS-related processes. For details, see [Performing a Full Backup on page 19-4](#).
 3. Stop Postfix.
 4. Restore the folders `/var/imss/` and `/opt/trend/` using the previous backup.
 5. Restore Postfix configuration files.
 6. Start Postfix.
 7. Start all IMSS-related processes. For details, see [Performing a Full Backup on page 19-4](#).
-

Performing a Minimal Restoration

Procedure

1. Install a new IMSS server on one computer, ensuring that the IP address, database user name, and password are the same as the original.
2. Stop all IMSS-related processes. For details, see [Performing a Full Backup on page 19-4](#).
3. Stop Postfix.

4. Restore the `/opt/trend/imss/config/` folder using the previous backup.
 5. Restore Postfix configuration files.
 6. Import the previous database table backup into the new database.
 7. Start all IMSS-related processes. For details, see [Performing a Full Backup on page 19-4](#).
-

Replicating Settings

If you have installed multiple IMSS scanners that do not share the same admin database, you can use Trend Micro Control Manager to replicate settings across these scanners without having to configure each scanner separately. If the scanners share the same admin database, it is not necessary to replicate settings.

Do the following if you intend to replicate settings using Control Manager:

- **Step 1:** Back up IMSS settings.
For details, see [Backing Up IMSS on page 19-4](#).
- **Step 2:** Enable the MCP agent.
- **Step 3:** Replicate settings from the Control Manager management console.

Enabling Control Manager Agent

IMSS automatically installs the Trend Micro Management Communication Protocol agent during installation. To integrate with Control Manager, provide the Control Manager server details and enable the agent from the management console.

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.
The **Components** tab appears by default.
2. Click the **TMCM Server** tab.

The **TCCM Server Settings** screen appears.

The screenshot shows the 'Connections' window with the 'TCCM Server' tab selected. The window is titled 'TCCM Server Settings' and contains the following fields and controls:

- Un-register All Agents** button
- Enable MCP Agent**
- Server:** [Text input field]
- Communication protocol:**
 - HTTP port:** [80]
 - HTTPS port:** [443]
- Web server authentication:**
 - User name:** [Text input field]
 - Password:** [Password input field]
- Proxy Settings**
 - Enable proxy**
 - Proxy type:** [HTTP]
 - Proxy server:** [Text input field]
 - Port:** [Text input field]
 - User name:** [Text input field]
 - Password:** [Password input field]

At the bottom of the window are **Save** and **Cancel** buttons.

3. Provide the required information.
4. Select the check box next to **Enable MCP Agent**.
5. Click **Save**.

Replicating Settings from Control Manager

After enabling the Management Communication Protocol agent from the IMSS management console, you can start to replicate IMSS settings by logging on to the Control Manager management console.

Procedure

1. Go to **Products** from the Control Manager menu.

The **Product Directory** screen appears.

2. Locate the source IMSS scanner from the Product Directory tree.
 3. Mouseover **Configure**.
A drop-down list appears.
 4. Select **Configuration Replication** from the drop-down list.
 5. Select the check box next to the target server.
 6. Click the **Replication** button.
-

Chapter 20

Using End-User Quarantine

This chapter explains how to use End-User Quarantine (EUQ).

Topics include:

- *About EUQ on page 20-2*
- *EUQ Authentication on page 20-2*
- *Configuring End-User Quarantine (EUQ) on page 20-2*
- *Disabling EUQ on page 20-13*

About EUQ

IMSS provides web-based EUQ to improve spam management. The web-based EUQ service allows end users to manage the spam quarantine of their personal accounts. Messages that are determined to be spam are quarantined. These messages are indexed into a database by the EUQ agent and are then available for end users to review, delete, or approve for delivery.

You can specify the period to keep messages in the quarantine. IMSS automatically deletes messages that are not released from quarantine. Deleted messages cannot be recovered.

EUQ Authentication

Enabling EUQ requires one of the following authentication methods:

- **LDAP authentication:** Before enabling EUQ, configure LDAP settings using any of the following ways:
 - Go to **Administration > IMSS Configuration > Connections**, then click the **LDAP** tab.
 - Go to **Administration > IMSS Configuration > Configuration Wizard**. For details, see *Configuring LDAP Settings on page 3-6*.
- **SMTP authentication:** Specify recipient domains and server addresses on the **EUQ Authentication** screen during the enabling process.

Configuring End-User Quarantine (EUQ)

To allow end-users to access quarantined spam items that IMSS might have misidentified as spam, do the following:

1. *Enabling EUQ on page 20-3*
2. *Configuring SMTP Server Settings on page 20-5*

3. [Starting the EUQ Service on page 20-7](#)
4. [Enabling End-User Access on page 20-7](#)
5. [Opening the End-User Quarantine Management Console Remotely on page 20-11](#)

Enabling EUQ

Enabling EUQ requires one of the following authentication methods:

- LDAP
- SMTP

For details about EUQ authentication, see [EUQ Authentication on page 20-2](#).

Procedure

1. Go to **Administration > End-User Quarantine**.
The **EUQ Authentication** tab appears by default.
2. Click the **User Quarantine Access** tab.

End-User Quarantine

End users can manage quarantined messages through SMTP authentication.

EUQ Authentication

User Quarantine Access

Enable access 

Allow end user to deliver quarantined mail in EUQ directly 

Allow end users to retrieve quarantined email messages with alias email addresses 

Keep quarantined spam for: 

Set maximum number of approved senders

Maximum approved senders per end-user: 

Specify the logon notice

Specify the greeting displayed to users on the EUQ logon page. The maximum length is 2,000 characters. For better security, Trend Micro recommends not using HTML. To configure the administrator logon notice, refer to the [Logon Notice](#) page.

3. Select **Enable access**.



Note
After enabling EUQ, the EUQ service starts automatically. To manually start the service, see *Starting the EUQ Service on page 20-7*.

4. Click **Save**.



Note
Your settings will not be saved automatically. To avoid losing your information, do not navigate away from the page without clicking **Save**.

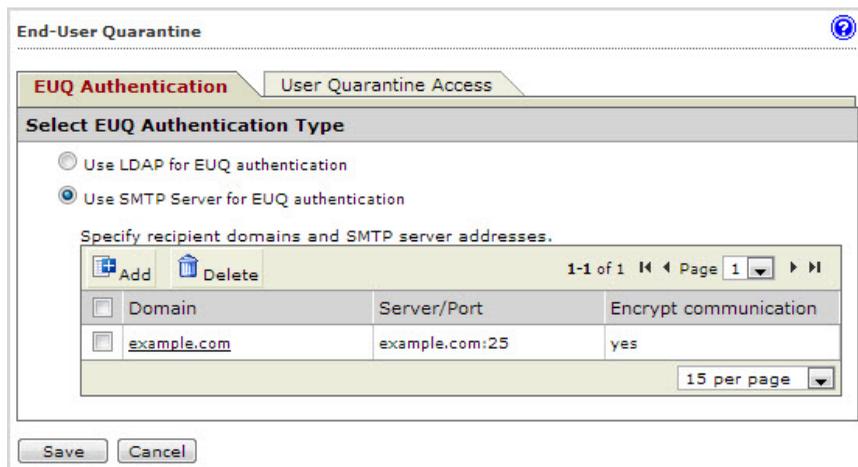
What to do next

- The EUQ service automatically starts. To manually start the service, see [Starting the EUQ Service on page 20-7](#).

Configuring SMTP Server Settings

Procedure

1. Go to **Administration > End-User Quarantine**.
The **EUQ Authentication** tab appears by default.
2. Select **Use SMTP Server for EUQ authentication**.
The SMTP settings section appears.



The screenshot shows the 'End-User Quarantine' configuration window. The 'EUQ Authentication' tab is active, and the 'Use SMTP Server for EUQ authentication' option is selected. Below this, there is a section titled 'Specify recipient domains and SMTP server addresses.' which contains a table with the following data:

Domain	Server/Port	Encrypt communication
<input type="checkbox"/> example.com	example.com:25	yes

At the bottom of the window, there are 'Save' and 'Cancel' buttons.

3. Click **Add**.

The **SMTP Server Configuration** screen appears.

Email Domain

Specify a domain to be used in quarantine management.

Domain: ⓘ

Server Address and Port

Specify the SMTP server address and port to be used in domain authentication.

Server address:

Port:

Encrypt communication: ⓘ

OK Close

4. Specify the following information:

- **Recipient domains to be used in managing quarantined messages:** Indicate domains that will be used to access the EUQ console. IMSS uses the recipient's domain to determine the SMTP server to be used for authentication.



Note

You can use the following formats to specify domains:

- company.com
- *.company.com: Any subdomain of company.com
- *: Any domain

A domain can only be listed once. Only unique domains will be added to the list.

- **SMTP server address and port to be used in authenticating the specified domain:** Indicate the server address and port that will be used to assign the server address for the destination domain.



Use the default port 25 or specify a different port.

Only one SMTP server can be assigned to a domain. However, more than one domain can be mapped to an SMTP server.

5. Click **OK**.

The information appears in the SMTP settings table.

Starting the EUQ Service

After configuring EUQ settings, start the EUQ service.

Procedure

1. Go to **Summary**.
The **Summary** screen appears.
2. In the **Managed Server Settings** section, click **Start** under **Web Quarantine**.
3. In the Managed Services table, click **Start** under EUQ Service.

After a moment, the EUQ service starts.

Enabling End-User Access

Enable end user access to allow the users to access quarantined spam items that IMSS might have misidentified as spam. The clients use LDAP or SMTP authentication to access the IMSS EUQ service.



Note

To allow users to manage messages on the EUQ management console, add their individual email addresses to the list of users on your LDAP server.

When using SMTP authentication, you do not need to configure LDAP settings.

Procedure

1. Go to **Administration > End-User Quarantine**.

The **EUQ Authentication** tab appears by default.

2. Click the **User Quarantine Access** tab.

The **User Quarantine Access** screen appears. The displayed screen depends on the authentication method you selected during the enabling process.

EUQ Authentication **User Quarantine Access**

Enable access ⓘ

Allow end user to deliver quarantined mail in EUQ directly ⓘ

Allow end users to retrieve quarantined email messages with alias email addresses ⓘ

Keep quarantined spam for: 7 days ▾

Set maximum number of approved senders

Maximum approved senders per end-user: 50 ▾

Specify the logon notice

Specify the greeting displayed to users on the EUQ logon page. The maximum length is 2,000 characters. For better security, Trend Micro recommends not using HTML. To configure the administrator logon notice, refer to the [Logon Notice](#) page.

Select LDAP groups to enable access

Enable All

Select groups from LDAP Search below.

Search LDAP groups ▾

Search

Selected Groups

>>
<<

Save Cancel

FIGURE 20-1. LDAP authentication

End-User Quarantine

End users can manage quarantined messages through SMTP authentication.

EUQ Authentication

User Quarantine Access

Enable access 

Allow end user to deliver quarantined mail in EUQ directly 

Allow end users to retrieve quarantined email messages with alias email addresses 

Keep quarantined spam for: days 

Set maximum number of approved senders

Maximum approved senders per end-user: 

Specify the logon notice

Specify the greeting displayed to users on the EUQ logon page. The maximum length is 2,000 characters. For better security, Trend Micro recommends not using HTML. To configure the administrator logon notice, refer to the [Logon Notice](#) page.

FIGURE 20-2. SMTP authentication

3. Select **Enable access**.
4. Select **Allow end user to deliver quarantined mail in EUQ directly** to allow end users to deliver quarantined messages directly to the recipient. The message bypasses all rules except virus scanning rules.
5. Select **Allow end users to retrieve quarantined email messages with alias email addresses** to allow end users to retrieve quarantined messages using alias email addresses configured in Microsoft Exchange.
6. Select the number of days to keep quarantined spam.
7. Select the maximum number of approved senders for each end-user.
8. Specify a logon notice that appears on the user's browser when he/she starts to access the quarantined messages.
9. Under Select LDAP groups, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.

10. To add individual LDAP groups, clear the **Enable all** check box and do either of the following:
 - **Search for groups:**
 - a. From the drop-down list, select **Search LDAP groups**.
 - b. Specify the group name.
 - c. Click **Search**. The groups appear in the table below.
 - d. Click the LDAP groups to add.
 - e. Click **>>**. The groups appear in the Selected Groups table.
 - **Browse existing groups:**
 - a. From the drop-down list, select **Browse LDAP groups**. The groups appear in the table below.
 - b. Click the LDAP groups to add.
 - c. Click **>>**. The groups appear in the Selected Groups table.
 11. Click **Save**.
-

Opening the End-User Quarantine Management Console Remotely

You can view the EUQ management console remotely across the network or from the computer where the program was deployed. Ensure that JavaScript is enabled on your browser.

Primary EUQ service

```
https://<target server IP address>:8447
```

Secondary EUQ service

```
https://<target server IP address>:8446
```

**WARNING!**

To successfully access all management consoles on secondary EUQ services, synchronize the system time of all EUQ services on your network.

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

Logon Name Format

The format of the logon name used when accessing the EUQ management console depends on the selected authentication type.

TABLE 20-1. EUQ Logon Name Formats

AUTHENTICATION TYPE	LOGON NAME FORMAT
LDAP	<p>The format of the logon name depends on the type of LDAP server you selected when configuring LDAP settings. The following are examples of valid logon name formats.</p> <ul style="list-style-type: none"> • Domino: user1/domain • Microsoft Active Directory <ul style="list-style-type: none"> • Without Kerberos: user1@domain.com (UPN) OR domain\user1 • With Kerberos: user1@domain.com • Sun iPlanet Directory: uid=user1, ou=people, dc=domain, dc=com
SMTP	<p>Use any valid email address for the logon name.</p> <hr/> <p> Note IMSS supports <code>auth login</code>, <code>auth plain</code> and <code>starttls</code>.</p> <hr/>

Disabling EUQ

Before disabling EUQ, inform your users that they should manage their quarantined spam.

Procedure

1. Go to **Administration > End-User Quarantine > User Quarantine Access**.
 2. Deselect the **Enable access** check box.
 3. Click **Save**.
-

Chapter 21

Performing Administrative Tasks

This chapter explains how to perform important administrative tasks, such as managing accounts, changing a device IP address, and using the backup data port.

Topics include:

- *Managing Administrator Accounts on page 21-2*
- *Configuring Connection Settings on page 21-6*

Managing Administrator Accounts

To reduce bottlenecks in administering IMSS, you can delegate administrative tasks to other staff by creating new administrator accounts. After creating the accounts, assign the desired permissions to the various areas of the management console. The default "admin" account has access to all IMSS features.

Adding Administrator Accounts

Created accounts have three permission settings for IMSS features:

- **Full:** Users have complete access to the features and settings contained in the menu item.
- **Read:** Users can view features and settings contained in the menu item, but cannot modify them.
- **None:** Users will not see the menu item, preventing them from viewing or configuring any of the settings in the menu item.

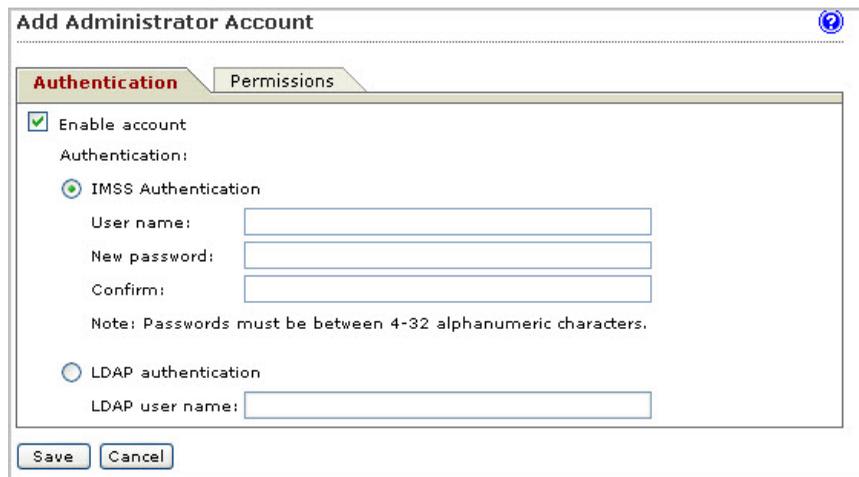
Procedure

1. Go to **Administration > Admin Accounts**.

The **Admin Accounts** screen appears.

2. Click **Add**.

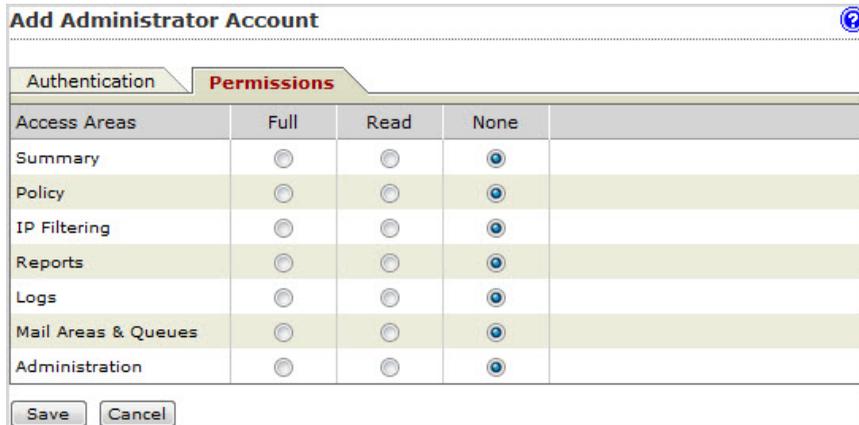
The **Add Administrator Account** screen appears with the **Authentication** tab displaying.



The screenshot shows a window titled "Add Administrator Account" with a help icon in the top right corner. Below the title bar are two tabs: "Authentication" (selected) and "Permissions". Under the "Authentication" tab, there is a checked checkbox for "Enable account". Below this, the "Authentication:" section contains two radio button options: "IMSS Authentication" (selected) and "LDAP authentication". The "IMSS Authentication" section includes three text input fields for "User name:", "New password:", and "Confirm:", followed by a note: "Note: Passwords must be between 4-32 alphanumeric characters." The "LDAP authentication" section includes a text input field for "LDAP user name:". At the bottom of the form are "Save" and "Cancel" buttons.

3. Specify authentication settings:
 - a. Select **Enable account**.
 - b. Select an authentication type:
 - **IMSS Authentication:** Specify the user name, new password, and the new password confirmation.
 - **LDAP authentication:** Specify the LDAP user name.
4. Click the **Permissions** tab.

The **Permissions** screen appears.



Access Areas	Full	Read	None
Summary	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
IP Filtering	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Reports	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Logs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Mail Areas & Queues	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Administration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Save Cancel

5. Specify Permissions settings:
 - a. Select **Full**, **Read**, or **None** for each of the following access areas that appear on the IMSS management console menu:
 - **Summary**
 - **Policy**
 - **IP Filtering**
 - **Reports**
 - **Logs**
 - **Mail Areas & Queues**
 - **Administration**
 - b. Click **Save**.

**Note**

Only the default IMSS administrator account can add new administrator accounts. Custom administrator accounts cannot do so even if you assign full permission to the **Administration** area.

Custom administrator accounts with full administration rights can only change their own IMSS passwords. If you forget the default administrator account password, contact Trend Micro technical support to reset the password.

Editing Administrator Accounts

You can change the permissions of a custom administrator account whenever there is a revision of roles or other organizational changes.

Procedure

1. Go to **Administration > Admin Accounts**.

The **Admin Accounts** screen appears.

2. Click the account name hyperlink.
 3. Make the required changes.
 4. Click **Save**.
-

Deleting Administrator Accounts

You can delete the permissions of a custom administrator account whenever there is a revision of roles or other organizational changes.

Procedure

1. Select the check box next to the account to be removed.
2. Click **Delete**.

3. At the confirmation message, click **OK**.

**Note**

You can only delete custom administrator accounts, not the default IMSS administrator account.

Configuring Connection Settings

To enable the scanner to receive messages and enhance the performance policy services when performing rule lookups, configure the connection settings.

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.

The **Components** tab appears by default.

The screenshot shows the 'Connections' configuration window with the following settings:

Section	Setting	Value
Settings for All Scanners	IMSS manager port:	15505
	Policy service port:	5060
Settings for All Policy Services	Protocol:	HTTP
	Keep-alive:	<input type="checkbox"/> Enable
	Maximum number of backlogged requests:	100
	Buttons	Save, Cancel

2. Under **Settings for All Scanners**, specify the port number that IMSS uses to communicate with scanners.

**Note**

If the user does not set the port number or the firewall could not open this port, the managed server appears as disconnected in the **Summary** page. Furthermore, any changes will not take effect on the managed service(s).

3. Under **Settings for All Policy Services**, configure the following:
 - **Policy service port:** Specify the port number that IMSS uses to communicate with policy services. The default port number that the policy service uses to communicate with IMSS is 5060.
 - **Protocol:** Select the type of protocol the scanner uses to communicate with the policy service (HTTP or HTTPS).
 - **Keep-alive:** Select the check box to enhance policy retrieval by maintaining a constantly active connection between the scanner and policy services.
 - **Maximum number of backlogged requests:** Specify a number that represents the maximum number of requests IMSS will preserve until it can process them later.
 4. Click **Save**.
-

About LDAP Settings

Configure LDAP settings for user-group definition, administrator privileges, or end-user quarantine authentication.

If the LDAP settings on the **Administration > Connections > LDAP** screen are not configured, the following LDAP related features will not work:

- **Policy > Internal Addresses > [Search for LDAP groups]**
- **Policy > [any rule] > [Sender to Recipient] > [Search for LDAP user and groups]**
- **Administration > End-User Quarantine > User Quarantine Access > [Select LDAP groups to enable access]**
- **Administration > Admin Accounts > Add > [LDAP authentication]**

Configuring LDAP Settings

Procedure

1. Go to **Administration > IMSS Configuration > Connections > LDAP** tab.
2. Next to **LDAP server type**, select the type of LDAP servers on your network:
 - **Domino**
 - **Microsoft Active Directory**
 - **Sun iPlanet Directory**
3. Next to **Enable LDAP 1**, select the check box.
4. Next to **LDAP server**, specify the server name or IP address.
5. Next to **Listening port number**, specify the port number that the LDAP server uses to listen to access requests.
6. Configure the settings under **LDAP 2** if necessary.
7. Under **LDAP cache expiration for policy services and EUQ services**, specify the **Time to live** in minutes.

Time To Live: Determines how long IMSS retains the LDAP query results in the cache. Specifying a longer duration enhances LDAP query during policy execution. However, the policy server will be less responsive to changes in the LDAP server. A shorter duration means that IMSS has to perform the LDAP query more often, thus reducing performance.

8. Under **LDAP admin**, specify the administrator account, the corresponding password and the base distinguished name. Refer to the table below for assistance on what to specify under this section according to the LDAP server type:

TABLE 21-1. LDAP Server Types

LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory	Without Kerberos: user1@domain.com (UPN) or domain\user1 With Kerberos: user1@domain.com	dc=domain, dc=com	Simple Advanced (with Kerberos)
IBM Domino	user1/domain	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	Simple

9. Select an authentication method:
 - **Simple**
 - **Advanced:** Uses Kerberos authentication for Active Directory. Configure the following:
 - **Kerberos authentication default realm:** Default Kerberos realm for the client. For Active Directory use, the Windows domain name must be upper case (Kerberos is case-sensitive).
 - **Default domain:** The Internet domain name equivalent to the realm.
 - **KDC and admin server:** Hostname or IP address of the Key Distribution Center for this realm. For Active Directory, it is usually the domain controller.
 - **KDC port number:** The associated port number.
10. Click **Save**.

If you are using the Configuration Wizard, click **Next**.



Note

IBM Domino and Sun iPlanet only support Simple Authentication method.

If the domain name in LDAP administrator account can be resolved by DNS, the Kerberos authentication will succeed no matter what value you type in the default realm.

If the domain name in LDAP administrator account cannot be resolved, Kerberos will use the default realm to check.

Enabling and Disabling LDAP Servers

LDAP servers can be enabled or disabled depending on the requirements for your network.

Procedure

1. Go to **Administration > IMSS Configuration > Connections > LDAP** to access the LDAP tab.
 2. Select or deselect one of the available LDAP servers.
 3. Click **Save**.
-

Configuring POP3 Settings

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as your clients retrieve them.



Tip

To use the POP3 message filter, enable **Accept POP3 connection** from **System Status** screen. This option is not selected by default.

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.

The **Components** tab displays by default.

2. Click the **POP3** tab.
3. To configure a connection from unknown POP3 servers on the Internet, specify the port number IMSS uses for incoming POP3 connections under **Generic POP3 Connection**.
4. To configure connections from specific POP3 servers, do the following:
 - a. Click **Add** under **Dedicated POP3 Connections**.
The **Dedicated POP3 Connection** window appears.
 - b. Specify the port IMSS uses for incoming POP3 connections, the POP3 server IP address, and the POP3 server port number.
 - c. Click **OK**.
 - d. To modify an existing connection, click the connection name.
5. Under **Message Text**, modify the message that IMSS sends to users if messages that they are trying to receive trigger a filter and are quarantined or deleted.
6. Click **Save**.

**Note**

The incoming port on your scanners must be idle or the IMSS daemon might not function properly.

Configuring POP3 Generic Services

For a generic POP3 service, the POP3 client logs on using the **USER** command and specifies the actual POP3 server and optional port number along with the user's name using the **UserServerSeparator** character to separate the values.

Example 1: To connect user "User1" to server "Server1", and the **UserServerSeparator** character is "#", the client issues the following **USER** command:

```
USER User1#Server1
```

Example 2: To connect to port 2000 on Server1, the following command is used:

```
USER User1#Server1#2000
```

**Note**

If you do not specify a port number, IMSS uses the default value of 110.

The following example shows how to configure generic POP3 settings for Outlook:

Procedure

1. Specify the POP3 server address with IMSS scanner IP 192.168.11.147.
 2. Specify user name `test123#192.168.11.252`.
 3. Set POP3 port to `110`.
-

Configuring POP3 Dedicated Services

For a POP3 dedicated service, the POP3 service always connects to a specific POP3 server. IMSS uses this service for a POP3 logon and for any type of logon using the AUTH command. For this service, a separate port on the proxy has to be set up for each specific POP3 server that any client might want to connect.

The following example shows how to configure dedicated POP3 settings in Microsoft Outlook:

Procedure

1. Specify the POP3 server address with IMSS scanner IP 192.168.11.147.
 2. Specify user name `test123`.
 3. Set the POP3 port to `1100`, which is the port that the IMSS dedicated POP3 service is listening on.
-

Configuring Database Settings

Configure the database connection settings so IMSS can save messages and data.

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.

The **Components** tab displays by default.

2. Click the **Database** tab.

The IMSS admin database type, database server name or IP address, and user name appear at the top of the table.

3. To register an EUQ database to IMSS, click **Register** under **EUQ Database**.



Note

You must use the installer to install the EUQ database, which then registers it to IMSS automatically.

4. Type the EUQ database server FQDN or IP address, port number, administrator user name and password.
5. Click **OK**.
6. To modify an existing database, click the database name.
7. To unregister an existing database from IMSS, select the check box next to a database, and then click **Unregister**.



Note

You can re-add the database at another time. Unregistering the database does not delete or otherwise affect the actual database server; IMSS just stops using the database.

Configuring TCM Settings

To use Trend Micro Control Manager (TCM) 5.5 or above to manage IMSS, enable the Control Manager/MCP agent on the IMSS server and configure Control Manager server settings. If a proxy server is between the Control Manager server and IMSS, configure proxy settings. If a firewall is between the Control Manager server and IMSS, configure port forwarding to work with the firewall's port-forwarding functionality.



Note

For additional information about Control Manager, see the Control Manager documentation.

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.

The **Components** tab displays by default.

2. Click the **TCM Server** tab.
3. Under **TCM Server Settings**, specify the following parameters:

OPTION	DESCRIPTION
Enable MCP Agent	Select the check box to enable the agent.
Server	Specify the Control Manager IP address or FQDN.
Communication protocol	Select HTTP or HTTPS and specify the corresponding port number. The default port number for HTTP access is 80, and the default port number for HTTPS is 443.
Web server authentication	Specify the credentials to access the Control Manager web server.

4. Under **Proxy Settings**, specify the following parameters:

OPTION	DESCRIPTION
Enable proxy	Select the check box to enable the proxy server.

OPTION	DESCRIPTION
Proxy type	Select the protocol that the proxy server uses: HTTP , SOCKS4 , or SOCKS5 .
Proxy server	Specify the proxy server FQDN or IP address, port number, and the user name and password.
Port	Specify the port for the proxy server.
User name	Specify the user name to access the proxy server.
Password	Specify the password for the user name.

5. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

If you enabled the agent, it will soon register to the Control Manager server. If you disabled the agent, IMSS will soon log off from the Control Manager server. Verify the change on the Control Manager management console.

Unregistering from Control Manager

Procedure

1. Go to **Administration > IMSS Configuration > Connections**.
The **Components** tab displays by default.
 2. Click the **TCCM Server** tab.
 3. Click the **Un-register All Agents** button.
-

Managing Product Licenses

You can activate IMSS products through the management console. If a product license expires, renew the license, obtain a new Activation Code, and specify the code through the management console. If the product remains inactive, its features are disabled.

For component descriptions, see [Component Descriptions on page 21-16](#).

Component Descriptions

IMSS can use the following components:

COMPONENT	DESCRIPTION
Cloud Pre-Filter	Provides message approved and blocked list filters and scanning for spam, viruses, and other threats before the messages reach your network.
Trend Micro Antivirus and Content Filter	Basic scanning and filtering functionality. You can think of this product as the IMSS program itself.
Spam Prevention Solution (SPS)	A built-in filter that helps IMSS identify content typically found in spam.

COMPONENT	DESCRIPTION
<p>IP Filtering Service</p>	<p>Automatically blocks known spam senders. IP Filtering includes the following:</p> <ul style="list-style-type: none"> • Email reputation Trend Micro Email reputation technology was designed to be used to identify and block spam before it enters a computer network by routing Internet Protocol (IP) addresses of incoming mail connections to Trend Micro Smart Protection Network server for verification against extensive reputation databases. • IP Profiler IP Profiler allows you to configure threshold settings and determine the action IMSS performs when it detects any of the four potential Internet threats: <ul style="list-style-type: none"> • Spam: Messages with unwanted advertising content. • Viruses: Various virus threats, including Trojan programs. • Directory Harvest Attack (DHA): A method spammers use to add your user's email addresses to spam databases. • Bounced Mail: Messages returned to the sender because the messages were sent with the sender's domain in the sender address.

Viewing Your Product Licenses

Monitor your product licenses from the **Product Licenses** screen.

Procedure

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

A brief summary of each license appears:

- **Product**
- **Version**
 - **Full:** Indicates that you have purchased the full licensed product.
 - **Evaluation:** Indicates that you are using an evaluation version of the product that expires after an elapsed time. The evaluation period varies according to the Activation Code you have obtained.

Fourteen (14) days before the expiration of the evaluation period, you will see a warning message on the management console.

To continue using IMSS after the evaluation period, purchase a licensed version of IMSS and specify the new Activation Code.

- **Activation Code:** A 31 alphanumeric character code in the format: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx.

Trend Micro will send you an Activation Code by email when you register a product online. You can then copy and paste this Activation Code on the **Product License** page.

- **Seats:** The number of endpoints/servers the license supports.
 - **Status:** Indicates whether the product has expired or has been activated.
 - **Maintenance expiration:** The date when you will no longer be able to download the latest scan engine and virus pattern files from the Trend Micro ActiveUpdate server. To ensure that your network is protected against the latest web threats, contact your sales representative to renew your license.
2. Click **View detailed license online** for the license you want to view.
3. Click **Check Status Online** to check the status of your license agreement on the Trend Micro website.
-

Renewing or Activating a License

There are two ways to renew a license:

Obtain a new Activation Code

Contact your sales representative to obtain a new Activation Code, and then specify the code on the **Product Licenses** screen.

Extend the life of an existing Activation Code

Contact your sales representative to extend the lifetime of your Activation Code, and then either manually update the license status or wait until IMSS automatically updates it.

Renewing a License Using a New Activation Code

Procedure

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

A brief summary of each license appears.

2. Click **Enter a new code** next to Activation Code.

The **Enter a New Code** screen appears.

3. Next to **New Activation Code**, specify the new code.

4. Click **Activate**.

The management console might access the Trend Micro website to activate the license.

If you are unable to reach the Trend Micro website, verify your network settings and try again.

Renewing a License Using an Existing Activation Code

Procedure

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

A brief summary of each license appears.

2. Click **View detailed license online** to view detailed information about the license.
3. Click **Check Status Online**. The management console accesses the Trend Micro web site to activate the license.

If you are unable to reach the Trend Micro website, verify your network settings and try again.

IMSS checks the status of your license 90, 60, 30, and 0 days before the expiration of the current license, and every day after the expiration of the current license. Once renewed, IMSS automatically updates the stored license information.



Tip

You can wait for IMSS to automatically update the license status. However, Trend Micro recommends that you manually update it as soon as you extend the lifetime of the Activation Code.

Activating Products

If you do not have an Activation Code, use the Registration Key that came with your product to register online.

Activate products from one of the following screens:

- Go to **Product Settings Product Activation** in the Configuration Wizard
- Go to **Administration > Product Licenses**

Activating from the Configuration Wizard

Procedure

1. If you do not have an Activation Code, click **Register Online**.

Upon successful registration, Trend Micro will send you the Activation Code in an email message.

2. Specify the Activation Code to activate any of the following:
 - Trend Micro Antivirus and Content Filter
 - Spam Prevention Solution
3. Click **Next**.



Note

The Activation Code comes in the format: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX.

Activating from the Product Licenses

Procedure

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

A brief summary of each license appears.

2. Click **Enter a new code** next to Activation Code.

The **Enter a New Code** screen appears.

3. Specify the new code next to New Activation Code.
4. Click **Activate**.

The management console may access the Trend Micro website to activate the license. If you are unable to reach the Trend Micro website, verify your network settings and try again.

Chapter 22

Troubleshooting, FAQ, and Support Information

This chapter explains how to troubleshoot common IMSS issues, search the Trend Micro Knowledge Base, and contact support.

Topics include:

- *Troubleshooting on page 22-2*
- *Frequently Asked Questions on page 22-12*
- *Support Information on page 22-33*

Troubleshooting

For common issues that you might encounter when configuring or administering IMSS, see [Troubleshooting Issues on page 22-2](#). If you have additional problems, check the Trend Micro Knowledge Base.

For troubleshooting and FAQ information pertaining to the deployment of IMSS, refer to the *IMSS Installation Guide*.

Troubleshooting Issues

ISSUE	DESCRIPTION AND RESOLUTION
General	
Unable to access the management console or other components.	<p>The target port is not in the firewall approved list. Open the ports as shown in IMSS Ports on page 22-11 in the firewall.</p> <p>If you are unable to access the management console, do the following:</p> <ol style="list-style-type: none"> 1. Start the database process, <code>dbctl.sh</code>, before starting the Central Controller process, <code>S99ADMINUI</code>. 2. If you are still unable to access the management console, restart the Central Controller process, <code>S99ADMINUI</code>. <p>For more details, refer to Using IMSS Scripts on page A-2.</p>
No access to the management console	The management console URL is not a trusted site in Internet Explorer. Add the URL to the trusted sites.
The <code>imssps</code> daemon is running but refusing connections.	If the <code>imssps</code> daemon is running, the policy service is working. Check the connection between the policy service and scanner service and verify your LDAP settings.

ISSUE	DESCRIPTION AND RESOLUTION
<p>Unable to activate products (Antivirus/eManager, SPS, Email Reputation, IP Filtering) or update components</p>	<p>To activate Email Reputation, IMSS needs to connect to Trend Micro. This process requires an HTTP query with a valid DNS setting. Therefore, if a DNS server is not available or has connection problems, activation cannot occur.</p> <p>To verify your DNS server settings:</p> <ul style="list-style-type: none"> Use the following command: <pre>nslookup licenseupdate.trendmicro.com</pre> <p>The command should return the IP address of your IMSS server.</p> <p>If a proxy server is required to connect to the Internet, verify your proxy settings to ensure the HTTP request reaches http://licenseupdate.trendmicro.com.</p> <p>To verify your proxy settings from the management console:</p> <ol style="list-style-type: none"> Go to Administration > Updates. The Schedule tab displays by default. Click the Source tab. Configure the proxy settings. Click Save.
<p>Email notifications do not properly display.</p>	<p>If your computer is running a non-English operating system and the notification message was not written in English, it may appear distorted. Modify the character set through the management console.</p> <p>To modify the character set:</p> <ol style="list-style-type: none"> Go to Administration > Notifications > Delivery Settings. Next to Preferred Charset, select the character set in which the messages will be encoded.

ISSUE	DESCRIPTION AND RESOLUTION
Cannot query message logs in IMSS.	IMSS scanner records the log with local time. To query message logs, synchronize the date/time on all computers with IMSS.
Server displays as disconnected in the System Status screen.	<p>A managed server could become disconnected for any of the following reasons:</p> <ul style="list-style-type: none"> • The scanner was removed from your network. • The IMSS manager service has stopped. • Network connection issue has occurred. <p>Check your firewall settings for the Manager Service listening port.</p>
When viewing detailed information for quarantined or archived messages, attachment information is sometimes not available.	<p>IMSS records attachment information only when the triggered rule is for an attachment.</p> <p>Check the reason why IMSS quarantined the message.</p>
IMSS does not receive email messages.	<ol style="list-style-type: none"> 1. Check if the IMSS scanner service and SMTP service are running. 2. Check if a different application is using the required port. Free up port 25.
Services are not running normally.	The database has not been started or the database was started after the IMSS services started. Restart all IMSS services.
After enabling Web Reputation, the scan time for messages increases significantly.	<p>Web Reputation needs to query the Trend Micro Web Reputation servers. Verify the HTTP connectivity from the IMSS scanner to the external network.</p> <p>For Web Reputation issues, check the <code>wrsagent.*</code> files under the <code>{Installation_Path}\imss\log</code> folder.</p>
End-User Quarantine Issues	

ISSUE	DESCRIPTION AND RESOLUTION
<p>Unable to access the EUQ management console</p>	<p>Do the following:</p> <ol style="list-style-type: none"> Verify that you are using the correct URL and port number. <p>To view the console from another computer on the network, type the following URLs:</p> <ul style="list-style-type: none"> Primary EUQ service: <code>https://<target server IP address>:8447</code> Secondary EUQ service: <code>https://<target server IP address>:8446</code> <ol style="list-style-type: none"> Verify that the system time of each EUQ service on your network is synchronized. <p>The first instance of the EUQ service, the primary EUQ service, runs Apache Web Server (httpd) while listening on port 8447 (HTTPS).</p> <p>This Web Server serves as a connection point for the EUQ clients and for load balancing for all EUQ services. If the Apache server is not up and running, users will not be able to access the EUQ management console from the normal IP address:</p> <p><code>https://{Primary EUQ Service IP address}:8447/</code></p>

ISSUE	DESCRIPTION AND RESOLUTION
<p>Users are unable to log on to EUQ management console</p>	<p>Do the following:</p> <ol style="list-style-type: none"> 1. On the LDAP server, verify that the user accounts are in the correct group. Only user accounts in the approved group can access EUQ. 2. Verify LDAP and User Quarantine Access settings through the IMSS management console: <ol style="list-style-type: none"> a. Go to Administration > IMSS Configuration > Connections > LDAP. b. Verify all settings, especially the LDAP type and server information. If you are using Kerberos authentication, ensure that the time for all IMSS computers and the LDAP server is synchronized. c. Go to Administration > End-User Quarantine. d. Select Enable User Quarantine Access. e. Verify that the correct LDAP groups appear under Selected Groups and that the user account belongs to the selected groups. 3. Verify that users are using the correct logon name and password. For more information, see Logon Name Format on page 2-7. 4. If the issue persists even after verifying the above settings, do the following: <ol style="list-style-type: none"> a. Go to Logs > Settings. b. Set the application log level to Debug. c. Select System Status, restart the Web EUQ service. d. Request the user to try logging on to the EUQ management console again. e. Send the log file <code>imssuieuq.yyyymmdd</code> located in <code>/opt/trend/imss/logs</code> to Trend Micro's technical support.

ISSUE	DESCRIPTION AND RESOLUTION
<p>The EUQ digest does not correctly display quarantined message information.</p>	<p>Verify that the correct character set is selected:</p> <ol style="list-style-type: none"> 1. Go to Administration > Notifications > Delivery Settings. 2. Next to Preferred charset, select the character set that will properly display the digest information.
<p>Some quarantined messages are not appearing on the EUQ management console</p>	<p>On the EUQ management console, users can only access the quarantined messages if the administrator configures EUQ to allow access.</p> <p>To make quarantine areas visible to end users:</p> <ol style="list-style-type: none"> 1. Go to Quarantine & Archive > Settings. 2. Click the link of the quarantine area that you want to synchronize to EUQ. 3. Select the check box next to Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only). This allows end users to view and manage the messages from the EUQ Web console. <p>After enabling this option, all non-malicious messages (messages that do not trigger antivirus rules, anti-phishing conditions, or Web Reputation) quarantined in this area synchronize with the EUQ database. This allows end users to view and manage the messages from the EUQ management console.</p> <p>End users cannot access malicious messages.</p>
<p>Cannot enable LDAP with Kerberos authentication.</p>	<p>Kerberos protocol requires time synchronization between the Kerberos server and IMSS.</p> <p>Synchronize the date/time for all computers with IMSS.</p> <p>Check whether the DNS server is configured correctly.</p>
<p>IP Filtering Issues</p>	

ISSUE	DESCRIPTION AND RESOLUTION
FoxProxy cannot start up	<p>There are several reasons why FoxProxy might not start. To find out the reason, view the IP Profiler logs. To view IP Profiler logs:</p> <ol style="list-style-type: none">1. Go to the directory where IP Profiler is installed (by default: <code>/opt/trend/ipprofiler/config</code>).2. Open <code>foxproxy.ini</code>.3. Change the value for <code>log_level</code> to 4.4. Restart FoxProxy by typing the following: <pre>/opt/trend/ipprofiler/script/foxproxyd restart</pre>5. Open the log file by typing the following: <code>/opt/trend/ipprofiler/logs/foxproxy-general.****</code>
Unable to connect to FoxProxy	Verify that FoxProxy is running and that it binds on port 25.
FoxProxy processes messages slowly	<p>When FoxProxy receives messages, it performs a DNS query on FoxDNS. If Bind is not running, FoxProxy continues to wait until the DNS query times out.</p> <p>Verify that the bind service is running on the computer where FoxDNS is installed:</p> <ol style="list-style-type: none">1. Type the following command: <pre>ps -ef grep named</pre>2. Start the service if it is not running.

ISSUE	DESCRIPTION AND RESOLUTION
<p>Unable to view connections that FoxProxy is blocking</p>	<p>Every five (5) minutes, FoxProxy sends information about blocked connections to the IMSS server.</p> <p>Wait for at least five minutes before viewing the connection information.</p> <p>To change this time value:</p> <ol style="list-style-type: none"> 1. Open <code>foxproxy.ini</code>. 2. Modify the value for <code>report_send_interval</code>. 3. Restart FoxProxy by typing the following: <pre style="margin-left: 20px;">/opt/trend/ipprofiler/script/foxproxyd restart</pre>
<p>FoxDNS is not functioning.</p>	<p>Verify that the BIND service is running:</p> <ol style="list-style-type: none"> 1. Specify the following command: <pre style="margin-left: 20px;">ps -ef grep named</pre> 2. Start the service if it is not running.

ISSUE	DESCRIPTION AND RESOLUTION
<p>No IP Profiler log information exists</p>	<p>The following IP Profiler-related log files are in the IMSS admin database:</p> <ul style="list-style-type: none"> • foxmsg.**** • foxnullmsg.**** • foxreport.**** <p>Verify that the log files exist:</p> <ol style="list-style-type: none"> 1. Go to the log directory where IMSS is installed (by default: /opt/trend/imss/log/). 2. If the files are not present, use the following command to check if imssmgr is running: <pre>ps -ef grep imssmgr</pre> 3. Check if FoxProxy is running: <pre>ps -ef grep foxproxy</pre> 4. Verify that IP Profiler is enabled. In the table <code>t_foxhuntersetting</code>, the following should exist: <pre>record: 'Type' = 1 and 'enable' = TRUE</pre>
<p>ERS does not work after being enabled from the management console.</p>	<p>ERS may not work due to the following reasons:</p> <ul style="list-style-type: none"> • IP Filtering Service was not activated. ERS shares the same Activation Code with IP Filtering Service. If IP Filtering Service was not activated, activate IP Filtering Service and then activate ERS. • The computer on which the scanning service is installed cannot access the Internet. MTA cannot get a response for the DNS query for Activation Code validation. Confirm that the computer where the scanner service is installed has access to the Internet. <p>Activate SPS and confirm that the computer with SPS installed can access the Internet.</p>

ISSUE	DESCRIPTION AND RESOLUTION
<p>The MTA settings on the SMTP Routing management console screen are not being written into the Postfix configuration files</p>	<p>By default, the settings on the SMTP routing screen will not be automatically applied to Postfix on each scanner.</p> <p>To apply the settings to all scanners:</p> <ol style="list-style-type: none"> 1. Go to Administration > IMSS Configuration > SMTP Routing. <p>The SMTP Routing screen appears.</p> <ol style="list-style-type: none"> 2. Select the Apply settings to all scanners check box. 3. Click Save. <p>After a few minutes, the IMSS manager process on each scanner synchronizes the settings to Postfix. To restart the IMSS manager immediately, use the command:</p> <pre>/opt/trend/imss/script/S99MANAGER restart</pre> <p>If the process above does not work, check the local configuration file <code>/opt/trend/imss/config/imss.ini</code> to verify the <code>enable_postset_thd</code> key is set to yes or is blank.</p>
<p>IP profiler does not block IP addresses in the Blocked List.</p>	<p>The changes require about one (1) minute to take effect.</p> <p>Wait one (1) minute before checking the list again.</p>
<p>Blocked IP address does not display in the Overview page</p>	<p>The Overview page displays the top 10 blocked IP addresses by type for the last 24 uninterrupted hours. For example, at 16:12 today the Overview page displays data from 16:00 yesterday to 16:00 today.</p> <p>View the Overview page after an hour.</p>

IMSS Ports

The following table outlines all ports used by IMSS in their default configuration.

TABLE 22-1. IMSS Ports

MODULE	PORT	DESCRIPTION
Admin UI	8445	Tomcat listening port (HTTPS)
Bind	53	Name-domain server
EUQ UI	8009	Tomcat AJP (load balance) port
EUQ UI	8446	Tomcat listening port
EUQ UI	8447	Load balancer
Manager	15505	SOAP server
Policy Server	5060	SOAP listening port
Scanner	110	POP3 listening port

Frequently Asked Questions

This section answers various Frequently Asked Questions.

Postfix MTA Settings

If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally?

To control all the Postfix computers from the web management console, enable the **Apply settings to all scanners** option. Choose **Administrator > SMTP Routing > SMTP** from the menu.

Can I make an exception on the settings for some Postfix instances separately?

To make an exception for some Postfix settings, search for the key "detach_key_postfix" in `imss.ini`, and add the keys that you do not want to apply from the web management console. For example:

```
detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory
```

The parameters above will not be overwritten by any settings that you configure through the web console. You can modify `main.cf` manually.



Note

"{Parameter1}:{Parameter2}:...:{Parameter n}" means you can use one or more parameters by separating them using colons.

You can find the parameter names in the table `tb_postfixconfig` from the database, under the column `fieldname`.



WARNING!

Use extreme caution when modifying the configuration file.

IMSS Components

Can I move the Central Controller from one computer to another?

Yes. First, run the IMSS installation script to uninstall the Central Controller from the computer. Next, run the IMSS installation script and install the Central Controller on the other computer.

How can I set up and maintain the database?

The following commands can help you maintain the database:

- `pg_dump -d imss -U sa > YYYYMMDD.HHMMSS.backup`: Back up the database.
- `psql -Usa -d imss < ./YYYYMMDD.HHMMSS.backup`: Retrieve the latest data if errors occur.
- `vacuum`: Clean up the database on tables that are frequently accessed or on tables that have large amounts of data. Use this command when email traffic is low or when the device is not connected to your network.
- `vacuumfull`: Clean up the entire database when the database is not being heavily utilized or when the device is not connected to your network.
- `redirect_stderr=` and `log_rotate_***=`: Turn on these options in `postgresql.conf` to redirect old database log entries to the system log, which is rotatable. You can name the log file to start with a dash “-”.

Is IMSS policy service able to work if LDAP is not up and running?

Yes, the policy service still works even if the LDAP server is not up and running.

For example:

- IMSS continues to work as usual.
 - If the LDAP server is active but the port of the LDAP server is inaccessible.
 - If the policy server has the non-expired cache of the LDAP user or group.
- IMSS spends about one minute to perform each rule query. The policy server will bypass the LDAP-related rules and continue to process other rules. This may slow down message scanning and result in long mail queues.
 - If the LDAP server is not running or the port of the LDAP server is inaccessible.

Email Reputation

How do I configure Email reputation to not block certain IP addresses or domains?

Add the IP addresses/domains to the Email reputation approved list by doing the following:



Note

If the domain cannot be resolved by the DNS service, the domain will not work in the approved list.

Procedure

1. Log on to the management console.
 2. Click **IP Filtering > Approved List**.
 3. Add the IP addresses or domains that you do not want blocked to the Approved List.
-

How do I specify the Activation Code for ERS?

You can provide the Activation Code during installation, or you can modify it after installation.

To modify the Activation Code, edit the Postfix configuration files located in the same computer as Email reputation. These files are `main.cf`, `imss_rbl_reply`, and `imss_rbl_reply.user`.

The `imss_rbl_reply.user` file may not exist. If it exists, modify it. Otherwise, you can omit it.

After installing Email reputation, you should see similar contents in the three configuration files as follows:

- **main.cf**

```
smtpd_client_restrictions = reject_rbl_client
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com,
reject_rbl_client
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com
```

- **imss_rbl_reply**

```
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450
Service temporarily unavailable; $rbl_class [$rbl_what]
blocked using Trend MicroEmail
Reputation Service. See
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=
$rbl_what${rbl_reason?; $rbl_reason}
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 550
Service unavailable; $rbl_class [$rbl_what] blocked
using Trend MicroRBL+. See
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=
$rbl_what${rbl_reason?; $rbl_reason}
```

- **imss_rbl_reply.user**

```
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.q.mail-abuse.com 450
error message; $rbl_class [$rbl_what] blocked using
Trend Micro Email Reputatio
Service. See
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=
$rbl_what${rbl_reason?; $rbl_reason}
"APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R.r.mail-abuse.com 450
error message; $rbl_class [$rbl_what] blocked using
Trend Micro RBL+. See
http://www.mail-abuse.com/cgi-bin/lookup?ip_address=
$rbl_what${rbl_reason?; $rbl_reason}
```

Replace the old Activation Code with your new Activation Code in these three files. The old Activation Code shown in the above examples is:

```
APRSJFK8BDTM2EEDBJY3LH5RJZ5CR9R
```

**Note**

You do not need to type the dash '-' for the Activation Code.

After editing the configuration files, restart Postfix using the commands:

```
# postfix stop  
  
# postfix start
```

IP Profiler

How can I purge the FoxProxy log?

A log purge program exists in the IP Profiler installation directory (by default: `/opt/trend/ipprofiler/bin/TmFoxPurgeLog`).

The settings about log purge function are in the configuration file `foxproxy.ini`. The keys are as follows:

- `log_purge`
- `log_purge_unit`
- `log_purge_num`

Which process monitors FoxProxy's status? Which process rescues it when it shuts down?

FoxProxy is a multiple-process program. The main process only monitors child processes. If child processes are stopped, the main process rescues them. But if the main process is stopped, the child processes cannot be rescued.

If you are experiencing any problems with FoxProxy, verify that the main process is running.

Which process/component performs DNS queries?

The DNS queries are performed directly by FoxProxy.

The installer gives users the option to install a DNS server on the Central Controller, if the installer does not detect any existing DNS server. When you install IP Profiler, the installer will prompt you for the IP address of the Central Controller.

Why is the domain name of an IP address that was added to the blocked/approved list always N/A?

IMSS does not determine the domain name of an IP address that was added to the blocked/approved list (IMSS does resolve the IP address of an added domain name).

Why does the IP Filtering Suspicious IP screen also display the connection information of blocked IP addresses?

The **IP Filtering > Suspicious IP** screen shows all information for successful connections. Therefore, although an IP address is now in the blocked list, the previous connections for this IP address, which have not been blocked, are shown.

How does IP Profiler process email?

The IP Filter decides if the source IP address is a safe IP address. IMSS scanner service queries matched policies from the IMSS policy service. The policies are applied to the email in the required order. If a policy specifies that an email should be quarantined, deleted or delivered, then the action is taken and the remaining policies are not applied.

Can the IP Profiler use an existing BIND server?

Yes. The IP profiler requires a BIND server. When a user installs IMSS and a BIND server is already present on the computer, IP profiler will use the BIND server. If a BIND server is not present, IMSS installs a new BIND server.

How can I configure BIND version 9.x to make sure IP Profiler works well?

If you did not install BIND version 9.x during installation or migration, but you want to use IP Profiler later, do the following:

Procedure

1. If an old BIND server exists, uninstall it on the target computer if the version is lower than 9.x.
2. Run the command `tar -xvf imss.tar` to get the `bind.tar` file.
3. Copy `bind.tar` to a specified folder.
4. Run the command `tar -xvf bind.tar` to extract the file.
5. Type the `cd` command to change to the `bind` folder. Outside the folder, you can view the following:

```
bash-2.03# pwd
/export/home/bob
bash-2.03# ls
bind bind.tar
```

6. Run the following commands:

```
chgrp -R imss bind
chown -R imss bind
chmod -R 555 bind
```

```
cp -f bind/named.conf /etc
```

```
cp -f bind/rndc.key /etc
```

```
mkdir -p /var/named
```

```
chmod 770 /var/named
```

7. If there is no named group or user, run the following command:

```
groupadd named
```

```
useradd -g named -s /bin/false -d /var/named named
```

8. Run the following commands to configure BIND server:

```
chown named:named /var/named
```

```
mkdir -p /var/run/named
```

```
chmod 770 /var/run/named
```

```
chown named:named /var/run/named
```

```
chown named:named /etc/named.conf
```

```
chown named:named /etc/rndc.key
```

```
chmod 555 /etc/named.conf
```

```
chmod 555 /etc/rndc.key
```

9. Modify foxdns.ini as follows:

```
vi $IMSS_HOME/config/foxdns.ini
```

```
#$IMSS_HOME is /opt/trend/imss/ by default.
```

```
#modify the following item:
```

```
# /export/home/bob/bind is the folder for bind
```

```
dig_path=/export/home/bob/bind/dig
rndc_path=/export/home/bob/bind/rndc
named_pid_path=/var/run/named/named.pid
named_db_path=/var/named/ipprofiler
```

10. Type `bash-2.03# /export/home/bob/bind/named` to run the BIND server.
 11. Restart S99FOXDNS at `$IMSS_HOME/imss/script`.
-

When does IMSS 7.1 SP2 send an email message to "Foxhunter_proxy@domain"?

IMSS sends an email message to "Foxhunter_proxy@domain" under the following three conditions:

- When FoxProxy receives an "Incomplete" message.
- When FoxProxy receives a "Null" message.
- When FoxProxy rejects a connection, it will send a statistics mail every 5 minutes. You can configure the time interval by modifying the `report_send_interval` (unit in seconds) setting in `foxproxy.ini`.

Is the LDAP service mandatory for analyzing whether an incoming traffic is a form of DHA attack?

Technically, LDAP service is not required. The DHA rule of IMSS 7.1 relies on the result returned from Postfix, which in turn passes the result to FoxProxy, a sub-module of IP Profiler, for analysis. The LDAP server is just one of the many means by which Postfix checks for the existence of a recipient's mailbox.

Mail Areas & Queues

Can I use special characters to perform queries?

Yes, you can use the following special characters to perform queries:

- **Asterisk (*):** Used as a wildcard character to search for characters. You can use the asterisk (*) to search for email addresses or file names.

To search for email addresses, refer to the following examples:

TABLE 22-2. Search for email addresses

EXAMPLE	DESCRIPTION
*	Valid representation of all email addresses.
@domain.tld, name@.tld	Valid representation of the whole name or the domain (not the top level domain (TLD)).
@.tld	Valid representation of both the name and the domain (not the TLD).

To search for file names, refer to the following examples:

TABLE 22-3. Search for file names

EXAMPLE	DESCRIPTION
.	Valid representation of all files.
*.extension	Valid representation of all files of a certain extension.
name.*	Valid representation of files with a specific name but of any extension.

- **Semicolon (;):** Used as a separator when searching for multiple recipients or attachments.

Why is there a quarantined message without a message ID when the user views message details?

IMSS reprocesses notification email messages for security reasons. Therefore, if a notification email message was quarantined due to a policy violation, the notification email message generated by IMSS would not have a message ID.

If you do not want IMSS to scan the notification email messages, you can disable notification email message scanning:

1. Modify the following setting in the [general-notification] section of the `imss.ini`:

```
NotificationSkipScan=1
```

2. Restart the IMSS daemon by typing the following commands:

```
net stop TmImssScan
```

```
net start TmImssScan
```

3. Restart the IMSS Scan Service as follows:

- Go to **Control Panel > Administrative Tools > Services**.
- Right click on **Trend Micro IMSS Scan Service** and choose **Restart**.



Note

Trend Micro recommends against disabling the scanning for notification email messages.

End-User Quarantine

If I am using Kerberos, why are users unable to log on to the EUQ console with a short name: “domain\user_name”?

Kerberos servers cannot accept user names in the format: `Domain\user_name`.
Kerberos requires the format:

user_name@domain.xxx

If I installed Microsoft Exchange Server and have set multiple mail addresses for each user, how do I enable EUQ to check multiple mail addresses for one user?

If you installed one Microsoft Exchange Server together with Active Directory, you can do the following:

Procedure

1. Open the table **tb_global_setting** in IMSS administrator database and replace the value of LDAP-->mail_attr from "mail" to "proxyAddresses".
 2. Restart all IMSS services.
-

How do I send a non-English EUQ digest?

Do the following:

Procedure

1. In the web management console, click **Administration > Notifications > Web EUQ Digest**.

The **Web EUQ Digest** screen appears.

2. Type the EUQ subject or content in the non-English language.
3. Click **Administration > Notifications > Delivery Settings**.

The **Delivery Settings** screen appears.

4. Select any non-English language as the Preferred character set.
-

How can I speed up LDAP access if the LDAP server is Active Directory?

There are two methods to speed up access. The method you use depends on the port number you can use: port 389 or port 3268.

Active Directory uses port 3268 for the Global Catalog. LDAP queries directed to the global catalog are faster because they do not involve referrals to different domain controllers.



Note

Trend Micro recommends using port 3268 for LDAP queries to Active Directory.

Active Directory uses port 389 for LDAP query. If one item cannot be queried in one domain controller, it uses the LDAP referral mechanism to query another domain controller. Use port 389 if your company has only one domain or if port 3268 is unavailable.

Using Port 3268 for LDAP Queries

Procedure

1. Click **Administration > IMSS Configuration > Connections**.
The **Connections** screen appears.
 2. Click the **LDAP** tab.
 3. Select the LDAP server to modify.
 4. Configure the LDAP listening port value: 3268.
-

Using Port 389 for LDAP Queries

Procedure

1. Click **Administration > IMSS Configuration > Connections**.

The **Connections** screen appears.

2. Click the **LDAP** tab.
3. Select the LDAP server to modify.
4. Configure the LDAP listening port value: 389.
5. Add the following key into the `imss.ini` file, which is at `$IMSS_HOME\config`.

```
[LDAP-Setting]
```

```
DisableAutoChaseReference=yes
```

6. Restart all IMSS services
-

What user logon name formats does IMSS support for Active Directory?

Active Directory supports the following logon name formats:

- Example 1: bob@imsstest.com



Note

The logon name is not an email address (though it appears as one).

- Example 2 (pre-Windows 2000): IMSSTEST\bob



Note

The pre-Windows 2000 format is not supported by Kerberos authentication.

Why are some users unable to use Kerberos SSO?

Users who are bound to SPN (Service Principal Name) cannot use Kerberos SSO.

Spam Protection Service

How is the spam catch rate determined?

Specify a threshold value between 3.0 and 10.0 for IMSS to classify a message as spam. A high threshold value means that a message must be very "spam-like" to be classified as spam (this decreases the spam catch rate but reduces the likelihood of false positives). A lower threshold value means that a message only needs to be slightly "spam-like" to be classified as spam (this increases the spam catch rate and may lead to more false positives).

ActiveUpdate

How do I roll back a pattern file?

Click the **Rollback** button on the **Summary** screen.

Other FAQs

Can the database server be referenced by hostname?

Yes. You can specify the hostname or IP address.

Can the IP address for IMSS or IMSS components be changed?

Yes.

Changing the IP Address for IMSS (Central Controller + Scanner)

Procedure

1. Stop all IMSS services by running the `$IMSS_Home/imss/script/imssstop.sh stop` command or stop the services individually.

For more information on IMSS scripts, see *IMSS Scripts on page A-1*.

2. Change the server IP address.
3. Start the database service if it is installed on this server. If IMSS installed the database use the following command:

```
$IMSS_Home/imss/script/dbctl.sh start
```

4. Change the IP address in the `odbc.ini` and `euqodbc.ini` files. The files are located in the IMSS configuration folder: `$IMSS_Home/imss/config/`.
5. Change the database URL and user name/password in `%IMSS_HOME%/UI/adminUI/ROOT/WEB-INF/struts-config-common.xml`
6. Change the following database data:

tb_component_list

Specify the computer name and all scanner IP addresses.

tb_euq_db_info

Specify the EUQ database computer settings.

tb_global_setting

In section [cmagent] name [ConfigUrl], change the web console URL.

7. Start all IMSS services with the following command:

```
$IMSS_Home/imss/script/imssstart.sh
```

How does IMSS process a partial message?

The key `BypassMessagePartial` in the IMSS configuration file `imss.ini` controls how IMSS processes partial messages.

IMSS rejects partial messages as a malformed message if `BypassMessagePartial=no` in the `imss.ini` file.

If the key is set to yes (default setting), IMSS will bypass partial messages.

What file format can IMSS import when configuring policy settings?

IMSS can only import .txt file containing only one item per line. Following are examples of how you can import a text file from the web management console:

Procedure

1. When specifying the attachment to be scanned:
 - a. Click **Policy > Policy List** from the menu.
 - b. Click the link of an existing rule to edit a rule.
 - c. Click the **And scanning conditions match** link.
 - d. Click the **Name or extension** link under the Attachment section.
 - e. Select the check box next to **Attachment named**.
 - f. Click **Import**. The imported file should be a text file containing one file name or extension per line.

 2. When configuring the spam detection settings:
 - a. Click **Policy > Policy List** from the menu.
 - b. Click the link of an existing rule to edit a rule.
 - c. Click the **And scanning conditions match** link.
 - d. Click the **Spam detection settings** link.
 - e. Select the check box next to **Approved sender list** or **Blocked sender list**.
 - f. Click **Import**. The imported file should be a text file containing one email address per line.
-

Why are newly created administrator accounts not able to access the User Quarantine Access, Admin Accounts, and Product License pages?

Only the default IMSS admin account has the permission to access the **User Quarantine Access**, **Admin Accounts**, and **Product License** pages. Custom admin accounts cannot access these pages.

Why are changes to the IMSS configuration settings not applied immediately?

There is a lapse between the time you modify the configuration settings from the management console and the time modifications are actually updated on the IMSS server.

Policy settings will be reloaded in no longer than three (3) minutes. If you want the settings to load faster, modify the

`policy_server=>dbChangePollIntervalInSecs` setting in the `tb_global_setting` table of the IMSS administrator database as desired.

For other general settings, `imssmgr` will take no longer than one (1) minute to reload the new settings modified from the management console.



Note

Trend Micro recommends that you do not send mail to IMSS immediately after modifying the configuration settings from the management console.

Are there limits on the following items?

- Senders and recipients for each rule
- Mail addresses in one address group
- Approved/Block Senders for SPS rule

The total size of each rule cannot exceed 640KB. The total size includes the rule route (senders/recipients), rule filter (scanning condition), and rule action. Assuming that each

email address/LDAP account consists of 20 characters, IMSS can support at least 10,000 senders/recipients for the rule route.

The maximum number of mail addresses for one address group is 10,000.

The maximum number of Approved/Block Senders for SPS rule is 5000.

How can I modify the log paths?

If you want to modify some log paths, locate the following keys in `imss.ini` and change the default settings as desired.

```
[general]
sys_log_path=/opt/trend/imss/log
event_log_path=/opt/trend/imss/log
policy_evt_log_path=/opt/trend/imss/log
```

Can IMSS 7.1 SP2 configure its own relay restrictions if a third-party upstream server is not installed?

No. IMSS 7.1 cannot configure its own relay restrictions as it does not have its own MTA on the Linux platform. You can only configure relay restrictions using a third-party MTA.

How can I modify the Access Control List (ACL) for the IMSS scanner?

You can modify the following settings in `imss.ini`.

- Add the target IP address to the parameter `smtp_allow_client_ip`.
- Alternatively, disable ACL check by setting `open_to_all_connections=yes`.
- To ensure that other computers are able to connect to the scanner, insert the target IP addresses in the parameter `proxy_smtp_server_ip`.

For more details, refer to the comments in `imss.ini`.

Why are messages from some senders always received as attachments? Why is the message body replaced by the disclaimer or stamp?

When the character set of the stamp is different from the character set of the message content, IMSS will encounter issues inserting the stamp into the message body after scanning the message. In this situation, IMSS will create a new message, insert the stamp into the message body, and attach the original message. The message content, however, will not be changed.

How can I specify a keyword expression to represent a blank header for matching fields such as "From", "To", or "Subject" when creating rules with the content filter?

If you are going to use a regular keyword expression to represent a blank header, Trend Micro recommends that you use `"^ (\s) *$"` (without the quotation marks). The expression `"^ (\s) *$"` (without the quotation marks) represents a blank header or whitespace characters.

For example, if you want to check if a message's **From** header is blank, edit a rule's scanning condition as follows:

Procedure

1. Go to **Policy > Policy List**.
 2. Click the link for an existing rule to edit the rule.
 3. Click **And scanning conditions match**.
 4. Click **Header keyword expressions** under the **Content** section.
 5. Click **Add** to create a new keyword expression.
 6. Add the content as `"^ (\s) *$"` (without the quotation marks).
-

Why does the message size scan condition not work for encrypted messages?

IMSS treats encrypted messages as a special type of message. Most scan conditions do not apply. IMSS requires the use of the encrypted message scan condition to scan or perform actions on encrypted messages.

Support Information

Troubleshooting Resources

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

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

<http://community.trendmicro.com/>

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 from the appropriate drop-down list and specify any other related information.

The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.

4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, 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 Intelligence Community

Trend Micro cyber security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to <http://www.trendmicro.com/us/security-intelligence/index.html> to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://www.trendmicro.com/vinfo> to learn more about:

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

- Weekly malware reports.

Contacting Trend Micro

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

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code

- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Email Reputation Services

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

<https://ers.trendmicro.com/>

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

<http://esupport.trendmicro.com/solution/en-us/1055473.aspx>

Web Reputation Services

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

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

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

Other Resources

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

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

<http://trendedge.trendmicro.com/>

Download Center

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

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

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

TrendLabs

TrendLabsSM is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of

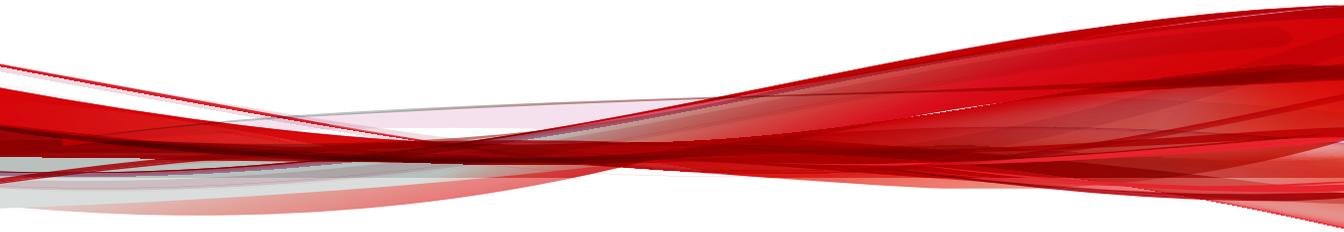
these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

Appendices

Appendices



Appendix A

IMSS Scripts

This appendix provides you with a list of IMSS scripts and their respective parameters that you can invoke from the command line.

Using IMSS Scripts

IMSS scripts provide a convenient and alternative means of performing administrative tasks from the command line.

The following table lists the IMSS scripts, the respective parameters and the functions that the scripts perform.



Note

All scripts listed in the table (except `foxproxyd`) are located in:

```
/$IMSS_Home/imss/script
```

`foxproxyd` is located in:

```
/$IMSS_Home/ipprofiler/script
```

TABLE A-1. IMSS Scripts

SCRIPT	PARAMETERS	DESCRIPTION
<code>dbctl.sh</code>	<code>start / stop / status / reload / restart</code>	Postgres database service
<code>db_maintain.sh</code>	<p>{<code>vacuum reindex analyze all</code>}</p> <p>[<code>vacuum</code>] - Vacuum admin db and all euq db.</p> <p>[<code>reindex</code>] - Reindex admin db and all euq db.</p> <p>[<code>analyze</code>] - Analyze admin db and all euq db.</p> <p>[<code>all</code>] - Vacuum && Reindex && Analyze.</p>	<p>Used by S99SCHEDULED for database maintenance.</p> <hr/> <p> Note Do not run this script on its own.</p> <hr/>
<code>euqtrans</code>	<code>all / approved sender</code>	Transfers EUQ database data or approved senders

SCRIPT	PARAMETERS	DESCRIPTION
forceUpdate.sh	DBDSN username password	Notifies the policy server to reload the policy settings
foxproxyd	start / stop / restart	IP Profiler service
imssstop.sh	stop	Forces all IMSS services to stop.
imssstart.sh		Start all IMSS services
postfixctl.sh	start / stop / reload / restart	Postfix daemon
regipro.sh	reg / unreg	Register or unregister IP Profiler to or from the admin database.
S99ADMINUI	start / stop / restart	Central Controller
S99CLEANEUQ		Removes expired quarantined data from the EUQ and admin databases as configured under the Administration > User Quarantine Access area of the management console.
S99CLEANEXPIRE		Removes expired quarantined and archived data from the EUQ and admin databases as configured under the Quarantine & Archive > Settings area of the management console.
S99CMAGENT	start / stop / restart / unregister / isregistered	CMAgent service
S99DIGEST		Sends the EUQ digest message
S99EUQ	start / stop / restart	EUQ service
S99FOXDNS	start / stop / restart	Foxdns service
S99IMSS	start / stop / restart	IMSS scanner service
S99MANAGER	start / stop / restart	Manager service
S99MONITOR	start / stop / restart	Manager monitor service

SCRIPT	PARAMETERS	DESCRIPTION
S99POLICY	start / stop / restart	Policy service
S99REPORT	<p>[option] start / stop / restart</p> <p>[option]:</p> <ul style="list-style-type: none"> • -s: generates centralized reports (covers all one-time and scheduled reports configured on the management console) • -h: generates hourly individual traffic data • -t: generates hourly traffic data • -d: performs database log maintenance 	<p>Used by S99SCHEDULED to generate related reports.</p> <hr/> <p> Note Do not run this script on its own.</p> <hr/>
S99SCHEDULED	start / stop	Starts the scheduled task.
S99UPDATE	start / stop / restart	<p>Used by S99SCHEDULED to run the scheduled update.</p> <hr/> <p> Note Do not run this script on its own.</p> <hr/>
S99WRSAGENT	start / stop / restart	WRS agent service

Appendix B

Default Directory Locations

This appendix provides information on the default directory locations that IMSS uses for mail processing.

Topics include:

- *Default Mail Queues on page B-2*
- *eManager, Virus, and Program Logs on page B-3*
- *Temporary Folder on page B-3*
- *Notification Pickup Folder on page B-4*

Default Mail Queues

The following table shows the various mail directories that store the mail messages managed by IMSS.

TABLE B-1. Default IMSS Mail Locations

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_malform= /opt/trend/imss/queue/ malform		Stores malformed messages.
queue_archive= /opt/trend/imss/queue/ archive		Stores archived messages.
queue_quarantine = /opt/trend/imss/queue/ quarantine		Stores quarantined messages.
queue_notify= /opt/trend/imss/queue/ notify	queue_notify_big= /opt/trend/imss/queue/ notifybig	Stores notification messages.
queue_postpone= /opt/trend/imss/queue/ postpone	queue_postpone_big= /opt/trend/imss/queue/ postponebig	Stores postponed messages.
queue_deliver= /opt/trend/imss/queue/ deliver	queue_deliver_big= /opt/trend/imss/queue/ deliverbig	Stores messages for final delivery.
queue_reprocess= /opt/trend/imss/queue/ reprocess	queue_reprocess_big= /opt/trend/imss/queue/ reprocessbig	Stores messages pending reprocessing.

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_handoff= /opt/trend/imss/queue/ handoff	queue_handoff_big= /opt/trend/imss/queue/ handoffbig	Stores messages pending handoff.
queue_undeliverable= /opt/trend/imss/queue/ undeliverable		Stores undeliverable messages.
queue_unnotify= /opt/trend/imss/queue/ unnotify		Stores undeliverable notification messages.

eManager, Virus, and Program Logs

Many modules in IMSS write log information for troubleshooting purposes to the following folder:

```
/opt/trend/imss/log
```

Temporary Folder

IMSS stores all application-generated temporary files in the temporary folder:

```
/opt/trend/imss/temp/
```



Note

This directory is not configurable.

Notification Pickup Folder

IMSS stores all notification messages, picks them up from the following folders, and then delivers them to a specified SMTP notification server:

```
/opt/trend/imss/queue/notify/
```

and

```
/opt/trend/imss/queue/notifybig
```

Configuring the SMTP Notification Server

For details, see [Configuring SMTP Routing on page 6-2](#).

Procedure

- Go to **Administration > Notifications > Delivery Settings**.



Note

The `queue_notify_big` queue is for large mail messages.

Index

A

- about IMSS, 1-2
- activate
 - license, 21-19
 - product, 21-20
- add
 - administrator accounts, 21-2
- address group
 - add, 9-5
 - delete, 9-8
 - edit, 9-8
- address groups
 - examples of, 9-2
 - understand, 9-2
- administrator accounts
 - add, 21-2
 - delete, 21-5
 - edit, 21-5
 - manage, 21-2
- adware, 1-9
- AJP, 22-12
- antivirus rule, 11-10
- APOP, 7-4
- approved list
 - add hosts, 5-10
- approved senders list
 - configure, 11-15
- archive
 - configure settings, 17-2
- archive areas
 - manage, 17-6
- archived messages
 - view, 17-14
- asterisk wildcard

- use, 13-14

- attachment size
 - scanning conditions, 11-25
- audience, xiv

B

- back up
 - IMSS, 19-4
- blocked list
 - add hosts, 5-10
- blocked senders list
 - configure, 11-15
- bounced mail settings
 - configure, 5-16

C

- change
 - web console password, 2-4
- commands, A-2
- community, 22-33
- component update, 4-6
- Configuration Wizard
 - accessing, 3-2
- configure
 - approved senders list, 11-15
 - archive settings, 17-2
 - blocked senders list, 11-15
 - connection settings, 6-4, 21-6
 - Control Manager server settings, 3-10
 - delivery settings, 18-2
 - Direct Harvest Attack (DHA) settings, 5-14
 - Email reputation, 5-18
 - expressions, 9-14
 - internal addresses, 3-8, 10-2

- IP Filtering, 5-8
- IP Filtering bounced mail settings, 5-16
- IP Filtering spam settings, 5-12
- IP Filtering virus settings, 5-13
- LDAP settings, 3-6, 21-7
- log settings, 16-2
- Messaged Delivery settings, 6-11
- Message Rule settings, 6-8
- notification messages, 18-4
- notification settings, 3-2
- other scanning exceptions scan actions, 12-5
- POP3 settings, 7-4, 21-10
- product settings, 3-11
- quarantine settings, 17-2
- route, 11-7
- scan exceptions, 12-2
- scheduled reports, 15-6
- security setting violation exceptions, 12-3
- security setting violation scan actions, 12-4
- SMTP routing, 6-2
- SMTP settings, 6-3
- spam text exemption rules, 11-17
- TMCM settings, 21-14
- update source, 3-4
- User Quarantine Access, 17-15
- Web EUQ Digest settings, 18-6
- configure event criteria, 18-4
- connection settings
 - configure, 6-4, 21-6
- Control Manager
 - enable agent, 19-7
 - replicate settings, 19-8
 - see Trend Micro Control Manager, 1-11

- Control Manager server settings
 - configure, 3-10
- Conventional scan, 2-9
- D**
- delete
 - address group, 9-8
 - administrator accounts, 21-5
- delivery settings
 - configure, 18-2
- dialers, 1-9
- Direct Harvest Attack (DHA) settings
 - configure, 5-14
- display
 - domains, 5-21
 - suspicious IP addresses, 5-21
- documentation, xv
- domains
 - display, 5-21
- E**
- edit
 - address group, 9-8
 - administrator accounts, 21-5
- email relay, 6-8
- Email reputation
 - Administration Console, 5-4
 - configure, 5-18
 - enable, 5-8
- email threats
 - spam, 1-4
 - unproductive messages, 1-4
- enable
 - Control Manager agent, 19-7
 - Email reputation, 5-8
 - End-User Access, 20-7
 - IP Profiler, 5-8

- IP Profiler rules, 5-11
- POP3 scanning, 7-3
- End-User Access
 - enable, 20-7
- ERS
 - MTA settings, 5-3
 - using, 5-2
- EUQ, 20-2
 - authentication, 20-2
 - disable, 20-13
 - open the console, 20-11
 - start, 20-7
 - web console, 20-11
 - Web console, 2-7
- event criteria
 - configure, 18-4
- event notifications, 18-2
- export notes, 19-2
- expression lists
 - manage, 9-13
- expressions
 - configure, 9-14
 - regular, 9-20
- F**
- FAQ
 - ERS, 22-15
 - EUQ, 22-23
 - IMSS components, 22-13
 - IP Profiler, 22-17
 - mail areas, 22-22
 - postfix, 22-12
 - queues, 22-22
- File Reputation Services, 1-14
- filtering, how it works, 1-6
- filters
 - examples of, 9-2
- G**
- generate
 - reports, 15-2
- H**
- hacking tools, 1-10
- I**
- import notes, 19-2
- IMSS
 - about, 1-2
 - backing up, 19-4
 - restore, 19-6
 - scripts, A-2
- internal addresses
 - configure, 3-8, 10-2
- IP Filtering
 - configure, 5-8
 - configure bounced mail settings, 5-16
 - configure Direct Harvest Attack (DHA) settings, 5-14
 - configure spam settings, 5-12
 - configure virus settings, 5-13
- IP Filtering Service
 - about, 5-2
- IP Profiler
 - enable, 5-8
 - enable rules, 5-11
- J**
- joke program, 1-9
- L**
- LDAP settings
 - configure, 3-6, 21-7
- LDAP User or Group
 - search for, 10-6
- license

- activate, 21-19
- renew, 21-19
- logs, 16-2
 - configure settings, 16-2
 - query, 16-4
 - query IP filtering, 16-12
 - query message tracking, 16-5
 - query MTA event, 16-11
 - query policy event, 16-8
 - query system event, 16-7

M

manage

- administrator accounts, 21-2
- expression lists, 9-13
- notifications list, 9-27
- one-time reports, 15-4
- policies, 8-1
- product licenses, 21-16

manual update, 4-4

mass mailing viruses

- pattern, 1-5

message delivery, 6-11

Message Delivery settings

- configure, 6-11

Message Rule settings

- configure, 6-8

message size

- scanning conditions, 11-26

MIME content type

- scanning conditions, 11-24

MTA

- with ERS, 5-3

N

new features, x

notes

- export, 19-2
- import, 19-2
- notification messages
 - configure, 18-4
- notifications
 - event, 18-2
- notification settings
 - configure, 3-2
- notifications list
 - manage, 9-27

O

one-time reports

- manage, 15-4

online

- community, 22-33

online help, xv

other rule, 11-11

P

password

- Web console, 2-4

password cracking applications, 1-10

pattern files

- update, 4-2

permitted senders, 6-10

policies

- add, 11-2

- example 1, 13-5

- finalize, 11-37

- manage, 8-1

policy notification

- add, 9-28

- edit, 9-28

POP3 messages

- scan, 7-2

POP3 scanning

- enable, 7-3
- POP3 settings
 - configure, 7-4, 21-10
- product licenses
 - manage, 21-16
 - view, 21-17
- product services, 2-6
- product settings
 - configure, 3-11

Q

- quarantine
 - configure settings, 17-2
- quarantine and archive, 17-2
- quarantine areas
 - manage, 17-4
- quarantined messages
 - view, 17-13
- query
 - archive areas, 17-11
 - IP filtering logs, 16-12
 - logs, 16-4
 - messages, 17-9
 - MTA event logs, 16-11
 - policy event logs, 16-8
 - quarantine areas, 17-9
 - system event logs, 16-7

R

- readme file, xv
- remote access tools, 1-10
- renew
 - license, 21-19
- replicating settings, 19-7
- reports
 - content, 15-2
 - generate, 15-2

- manage one-time, 15-4
- scheduled reports, 15-6, 15-10
- restore
 - IMSS, 19-6
- roll back
 - components, 4-6
- route
 - configure, 11-7
 - specify, 11-2

S

- scan
 - POP3 messages, 7-2
 - SMTP messages, 6-1, 6-2
- scan actions
 - configure other scanning exceptions settings, 12-5
- scan engine
 - update, 4-2
- scan exceptions
 - configure, 12-2
- Scan methods, 2-8
- scanning conditions, 11-25
 - attachment names, 11-23
 - attachment number, 11-26
 - attachments, 11-23
 - attachment size, 11-25
 - extensions, 11-23
 - message size, 11-26
 - MIME content type, 11-24
 - spam, 11-14
 - specify, 11-10
 - true file type, 11-25
- scheduled reports
 - access, 15-6
 - configure, 15-6
 - use, 15-10

- scheduled updates, 4-7
- security risks
 - spyware/grayware, 1-9
- security setting violations
 - configure exceptions, 12-3
 - configure scan actions, 12-4
- services, 2-6
 - IP Filtering Service, 5-2
- Smart Protection, 1-14
- Smart Protection Network, 1-16
- Smart Scan, 2-9
- SMTP
 - notification server, B-4
- SMTP messages
 - scan, 6-1, 6-2
- SMTP routing, 6-3
 - configure, 6-2
- SMTP settings
 - configure, 6-3
- spam settings
 - configure, 5-12
- spam text exemption rules
 - configure, 11-17
- specify
 - actions, 11-30
 - route, 11-2
 - scanning conditions, 11-10
 - update source, 4-3
- spyware/grayware, 1-9
 - adware, 1-9
 - dialers, 1-9
 - entering the network, 1-10
 - hacking tools, 1-10
 - joke program, 1-9
 - password cracking applications, 1-10
 - remote access tools, 1-10

- risks and threats, 1-10
- start
 - EUQ, 20-7
- support
 - knowledge base, 22-33
 - resolve issues faster, 22-35
 - TrendLabs, 22-37
- suspicious IP addresses
 - display, 5-21
- System Status screen, 14-2

T

- tag subject
 - add, 11-36
- TMCM settings
 - configure, 21-14
- transport layer, 6-7
- TrendLabs, 22-37
- Trend Micro Control Manager, 1-11
 - agent, 1-11
 - server, 1-11
- troubleshooting, 22-2
 - activating products, 22-3
 - email notifications, 22-3
 - EUQ quarantined messages, 22-7
 - EUQ web console access, 22-6
 - imssps daemon, 22-2
 - IP Filtering, 22-7
 - Web EUQ digest, 22-7
- true file type, 11-25

U

- update
 - automatically, 4-7
 - manually, 4-4
 - pattern files, 4-2
 - scan engine, 4-2

update source
 configure, 3-4
 specify, 4-3
User Quarantine Access
 configure, 17-15

V

view
 archived messages, 17-14
 product licenses, 21-17
 quarantined messages, 17-13
virus settings
 configure, 5-13

W

web console password
 change, 2-4
Web EUQ Digest
 configure settings, 18-6
Web Reputation Services, 1-15
what's new, x



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: MSEM76416/140429