TREND MICRO™

7.5 InterScan™ Messaging Security Suite

Administrator's Guide

Comprehensive threat protection at the Internet messaging gateway

for Windows™

Messaging Security

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

http://docs.trendmicro.com/en-us/enterprise/interscan-messaging-security.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.

© 2014 Trend Micro Incorporated. All Rights Reserved.

Document Part No. MSEM76206_131030

Release Date: February 2014

Document Version No.: 1.0

Product Name and Version No.: InterScan™ Messaging Security Suite 7.5

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

The user documentation for Trend Micro InterScan Messaging Security Suite 7.5 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

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

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

Table of Contents

About this Manual

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

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 1-12
About Trend Micro Smart Protection 1-15
About Command & Control (C&C) Contact Alert Services 1-17

Chapter 2: Getting Started

Opening the IMSS Management Console 2-2
Viewing the Management Console Using Secure Socket Layer 2-3
Creating an SSL Certificate 2-4
Changing the Management Console Password 2-5
Configuring Proxy Settings 2-6
IMSS Services 2-6

Opening the End-User Quarantine Console 2-7
Selecting a Scan Method 2-9

Chapter 3: Using the Configuration Wizard

Accessing the Configuration Wizard 3-2
Configuring SMTP Routing 3-2
Configuring Notification Settings 3-3
Configuring the Update Source 3-5
Configuring LDAP Settings 3-7
Configuring Internal Addresses 3-9
Configuring Control Manager Server Settings 3-10
Configuring Product Settings 3-12
Verifying Settings Summary 3-13

Chapter 4: Updating Components

Updating Engine and Pattern Files 4-2
Specifying an Update Source 4-3
Performing a Manual Update 4-5
Rolling Back a Component Update 4-6
Scheduled Component Updates 4-7

Chapter 5: Advanced Threat Scan Engine and Deep Discovery Advisor

Scan Technology 5-2
About Advanced Threat Scan Engine 5-2
About Deep Discovery Advisor 5-4

Part II: Configuring IMSS

Chapter 6: Configuring IP Filtering Settings

IP Filtering Service 6-2
Using Email Reputation 6-2
Configuring IP Filtering 6-8
Displaying Suspicious IP Addresses and Domains 6-20

Chapter 7: Scanning SMTP Messages

Message Transfer Agents 7-2
Configuring SMTP Routing 7-2
About Message Delivery 7-10

Chapter 8: Configuring Transport Layer Security Settings

About Transport Layer Security 8-2
IMSS Support of Transport Layer Security 8-3
Configuring Transport Layer Security Settings 8-4
TLS Settings for Messages Entering IMSS 8-5
TLS Settings for Messages Exiting IMSS 8-8

Chapter 9: Configuring POP3 Settings

Scanning POP3 Messages 9-2
Enabling POP3 Scanning 9-3
Configuring POP3 Settings 9-3

Part III: IMSS Policies

Chapter 10: Managing Policies

About Policies 10-2
How the Policy Manager Works 10-2

Chapter 11: Common Policy Objects

Policy Object Descriptions 11-2
Understanding Address Groups 11-2
Using BATV Keys 11-13
Using the Keyword & Expression List 11-17
Using the Notifications List 11-23
Using Stamps 11-28
Using the DKIM Approved List 11-32
Using the Web Reputation Approved List 11-33

Chapter 12: Internal Addresses

Configuring Internal Addresses 12-2
Searching for Users or Groups 12-5
Searching for an LDAP User or Group 12-6

Chapter 13: Configuring Policies

Adding Policies 13-2
Specifying a Route 13-2
Specifying Scanning Conditions 13-10
Specifying Actions 13-30
Finalizing a Policy 13-37

Chapter 14: Existing Policies

Modifying Existing Policies 14-2
Using the Domain and Email Exclusion List for the Global BATV Rule 14-3
Using the Domain List for the Global DKIM Enforcement Rule 14-5
Policy Example 1 14-6

Policy Example 2 14-10
Using the Asterisk Wildcard 14-16

Chapter 15: Scanning Exceptions

Setting Scan Exceptions 15-2
Configuring Exceptions for Security Settings Violations 15-3
Setting Scan Actions for Security Setting Violations 15-4
Setting Scan Actions for Malformed Messages 15-5

Part IV: Monitoring the Network

Chapter 16: Monitoring the Network

Monitoring Your Network 16-2
Viewing System Status 16-2
Statistics Summary 16-3

Chapter 17: Reports

Generating Reports 17-2
Managing One-time Reports 17-4
Scheduled Reports 17-7

Chapter 18: Logs

About Logs 18-2
Configuring Log Settings 18-2
Querying Logs 18-4

Chapter 19: Mail Areas and Queues

About Mail Areas and Queues 19-2
Configuring Quarantine and Archive Settings 19-2

Managing Quarantine Areas 19-4
Managing Archive Areas 19-7
Querying Messages 19-10
Viewing Quarantined Messages 19-15
Viewing Archived Messages 19-16
Viewing Deferred Messages 19-17
Configuring User Quarantine Access 19-18
Adding/Removing an EUQ Database 19-21
Removing an EUQ Database 19-22
Command-line Options for euqtrans Tool 19-23

Chapter 20: Notifications

Event Notifications 20-2
Configuring Delivery Settings 20-3
Configuring Event Criteria and Notification Message 20-5
EUQ Digest 20-7
Editing Notifications 20-8

Part V: Administering IMSS

Chapter 21: Backing Up, Restoring, and Replicating Settings

Importing and Exporting Settings 21-2
Backing Up IMSS 21-3
Restoring Settings with the Backup Database 21-6
Replicating Settings 21-10

Chapter 22: Using End-User Quarantine

About EUQ 22-2

EUQ Authentication 22-2
Configuring End-User Quarantine (EUQ) 22-2
Disabling EUQ 22-8

Chapter 23: Performing Administrative Tasks

Managing Administrator Accounts 23-2
Configuring Connection Settings 23-6
Managing Product Licenses 23-15

Chapter 24: Troubleshooting, FAQ, and Support Information

Troubleshooting 24-2
Frequently Asked Questions 24-12
Support Information 24-35

Appendix A: Default Directory Locations

Default Mail Queues A-2
eManager, Virus, and Program Logs A-3
Temporary Folder A-3
Notification Pickup Folder A-4
Configuring the SMTP Notification Server A-4

Index

Index IN-1

Preface

About this Manual

Topics include:

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

What's New

The following tables provides an overview of new features available in IMSS 7.5.

TABLE 1. IMSS 7.5 New Features

NEW FEATURE	DESCRIPTION
Command & Control (C&C) Contact Alert Services	Command & Control (C&C) Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.
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.
Web Reputation enhancement	The Web Reputation filter has been enhanced to enable detection of URLs that have not been rated by Trend Micro. This functionality helps improve protection against advanced threats that leverage short-lived websites.
Advanced threat management	IMSS integrates with the Advanced Threat Scan Engine (ATSE) to detect probable advanced threats in message attachments. IMSS can send a copy of a message to Deep Discovery Advisor for further analysis after the message is handled.

TABLE 2. IMSS 7.1 New Features

NEW FEATURE	DESCRIPTION
Policy Objects	Several information objects that can be used by policies have been removed from policy creation and given their own areas for configuration: • Address Groups • BATV Keys • 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.
Web Reputation	Protect your clients from malicious URLs embedded in email messages with Web reputation.
BATV Support	Bounce Address Tag Validation (BATV) protects your clients from bounced email message attacks.
NRS Terminology Change	Network Reputation Service (NRS) has been changed to Email reputation.
Detection Capability Enhancement	Use Domain Keys 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	IMSS now supports scanning Microsoft® Office 2007 and Adobe® Acrobat® 8 documents.
Expanded File Scanning Support	IMSS now supports scanning Microsoft® Office 2007 and Adobe® Acrobat® 8 documents.

New Feature	Description
New Migration Tools	New tools have been provided to help customers migrating from previous product versions.

Table 3. 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	IMSS provides 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	Three layers of spam protection: • Email reputation 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.
Delegated Administration	LDAP-integrated account management allows users to assign administrative rights for different configuration tasks.

New Feature	Description
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	IMSS provides detailed logging for all messages to track and identify message flow related issues.
Integration with Trend Micro Control ManagerTM	Perform log queries on Email reputation detections from Control Manager, in addition to other supported features.
Supports 8 bit to 7 bit-MIME transformation	IMSS 7.0 Service Pack 1 supports the transformation of 8 bit to 7 bit-MIME according to the standard defined in RFC 1652 SMTP Service Extension for 8bit-MIME transport. In the event that the next hop of the SMTP server does not support 8 bit MIME, IMSS will convert the message from 8 bit MIME to 7 bit MIME.

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 4. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
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 1-12*
- *About Trend Micro Smart Protection on page 1-15*
- *About Command & Control (C&C) Contact Alert Services on page 1-17*

About InterScan Messaging Security Suite

InterScan Messaging Security Suite (IMSS) 7.5 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
Advanced anti-malware protection	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks.	ATSE identifies both known and unknown advanced threats, protecting your system from new threats that have yet to be added to patterns.
Command & Control (C&C) Contact Alert Services	C&C Contact Alert Services allows IMSS to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects.	C&C Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.
Smart Scan	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.	Smart Scan leverages the Smart Protection Network to: • 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

Feature	Descriptions	Benefits
IntelliTrap	Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files. 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. 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.	IntelliTrap helps reduce the risk that a virus compressed using different file compression schemes will enter your network through email.
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.

Feature	Descriptions	Benefits
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.
Legal liability and business integrity	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.	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.

FEATURE	DESCRIPTIONS	BENEFITS
Mass mailing virus containment	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. When IMSS detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses. 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.	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. The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs℠ 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.
Protection from spyware and other types of grayware		
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		

FEATURE	DESCRIPTIONS	BENEFITS
Spam Prevention Solution (SPS)	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. SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license.	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	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. **Note** Activate SPS before you configure IP Profiler and Email reputation.	With the integration of IP Filtering, which includes IP Profiler and Email reputation, IMSS can block spammers at the IP level.
Administration and integration		
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.

Feature	Descriptions	Benefits
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.
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.

FEATURE	DESCRIPTIONS	BENEFITS
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.
Integration with Trend Micro Control Manager™	Trend Micro Control Manager™ (TMCM) 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
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.
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.

FEATURE	DESCRIPTION	SUPPORTED?
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
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

FEATURE	DESCRIPTION	SUPPORTED?
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
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 **TMCM 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

FEATURE	DESCRIPTION	SUPPORTED?
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 Command & Control (C&C) Contact Alert Services

Trend Micro Command & Control (C&C) Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. It leverages the Global Intelligence list compiled, tested, and rated by the Trend Micro Smart Protection Network to detect callback addresses.

With C&C Contact Alert Services, IMSS has the ability to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects. Administrators can configure IMSS to quarantine such messages and send a notification when a message is flagged. IMSS logs all detected email with C&C objects and the action taken on these messages. IMSS sends these logs to Control Manager for query purposes.

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 IMSS 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 2-5*
- *Configuring Proxy Settings on page 2-6*
- *IMSS Services on page 2-6*
- *Opening the End-User Quarantine Console on page 2-7*
- *Selecting a Scan Method on page 2-9*

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: **imss7.5**

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
```

Tools for Creating the SSL Certificate

On the Windows platform, some command line tools such as openssl are not installed by default. You may need to download and install these tools.

The 'keytool' command utility is shipped with Java Runtime, which is available at:

```
%IMSS_HOME%\ui\JavaJRE\bin
```

The 'openssl' command utility can be found at http://www.openssl.org.

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

   Note

   The IMSS management console listens on port 8444. The EUQ management console listens on port 8446.

   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
      ```

Note

The IMSS management console listens on port 8445. The EUQ management console listens on port 8447.

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

```
copy new.cert.cert %IMSS_HOME%\UI\apache\conf\ssl.crt
\server.crt

copy 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 3-7*.
2. Enabled User Quarantine Access. See *Enabling End-User Access on page 22-6*.

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 user logon name for accessing the EUQ Web management console depends on the LDAP server type you have selected when configuring LDAP settings. The following are examples of the logon name format for the three (3) types of supported LDAP servers:

Microsoft Active Directory

- Without Kerberos: `user1@imsstest.com (UPN)` or `imsstest \user1`
- With Kerberos: `user1@imsstest.com`

Lotus Domino

`user1/imsstest`

Sun iPlanet Directory

`uid=user1, ou=people, dc=imsstest, dc=com`

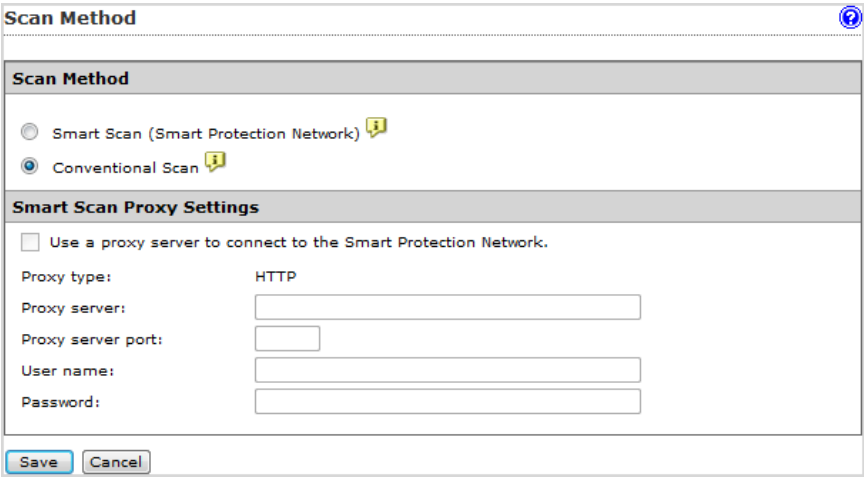
Selecting a Scan Method

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.



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.

Note

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**.

Note

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.

Note

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 18-6*.

- 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 20-1*.

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 SMTP Routing on page 3-2*
- *Configuring Notification Settings on page 3-3*
- *Configuring the Update Source on page 3-5*
- *Configuring LDAP Settings on page 3-7*
- *Configuring Internal Addresses on page 3-9*
- *Configuring Control Manager Server Settings on page 3-10*
- *Configuring Product Settings on page 3-12*
- *Verifying Settings Summary on page 3-13*

Accessing the Configuration Wizard

Access the wizard using one of the following methods:

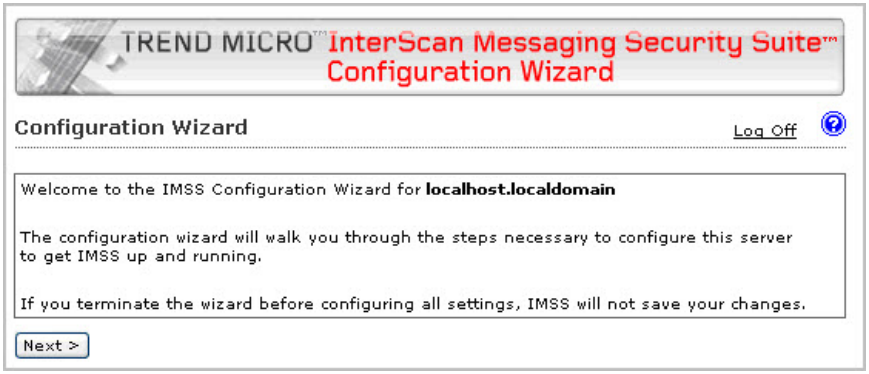
Procedure

- 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.

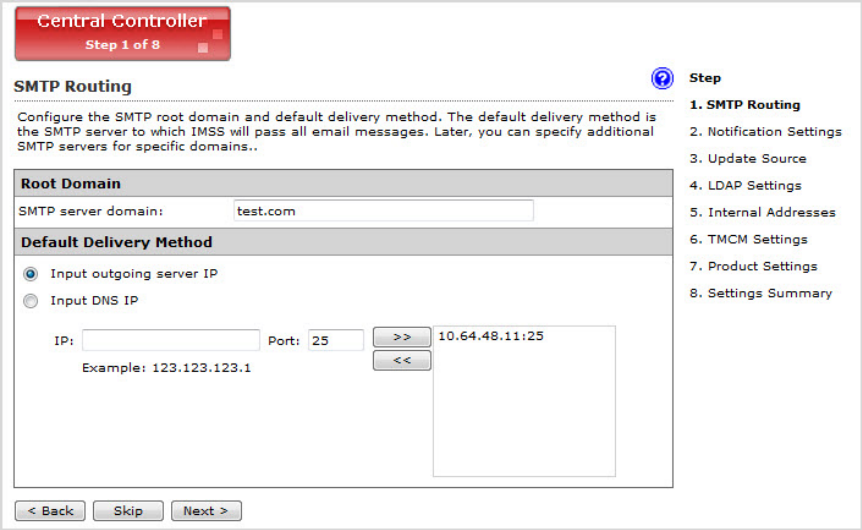


Configuring SMTP Routing

Procedure

1. Click **Next**.

The **SMTP Routing** screen appears.



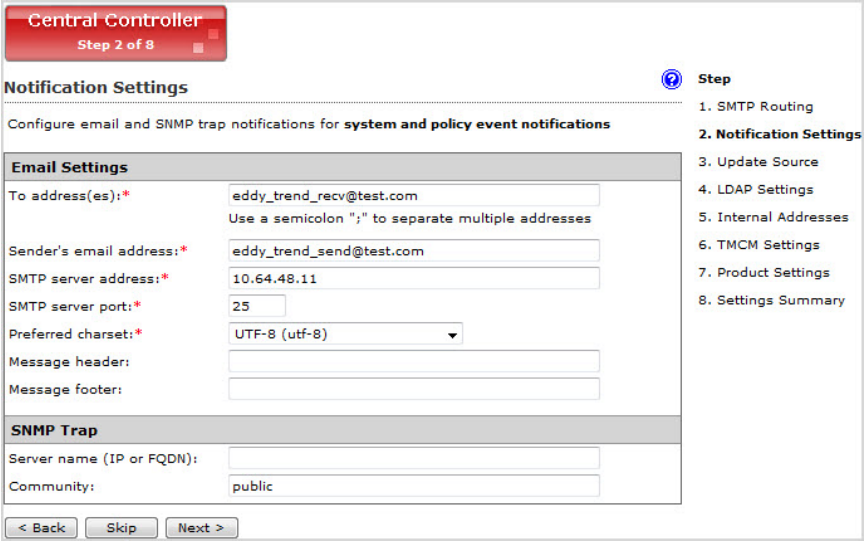
2. Specify the SMTP root domain and default delivery method.

Configuring Notification Settings

Procedure

1. Click **Next**.

The **Notification Settings** screen appears.



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) 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

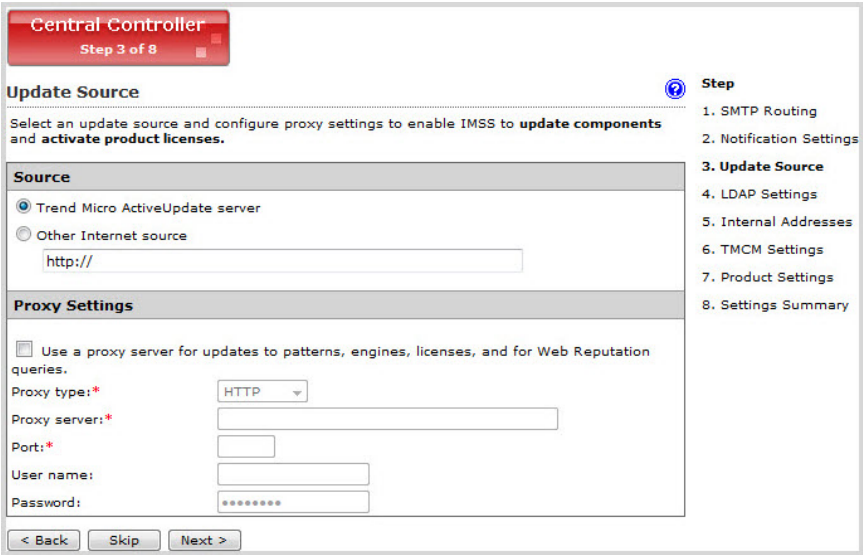
Community is the group that computers and management stations running SNMP belong to. To send the alert message to all SNMP management stations, specify "public" as the community name. For more information, refer to the SNMP documentation.

Configuring the Update Source

Procedure

1. Click **Next**.

   The **Update Source** screen appears.



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 `http://<CM server address>/ControlManager/download/activeupdate/`, 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

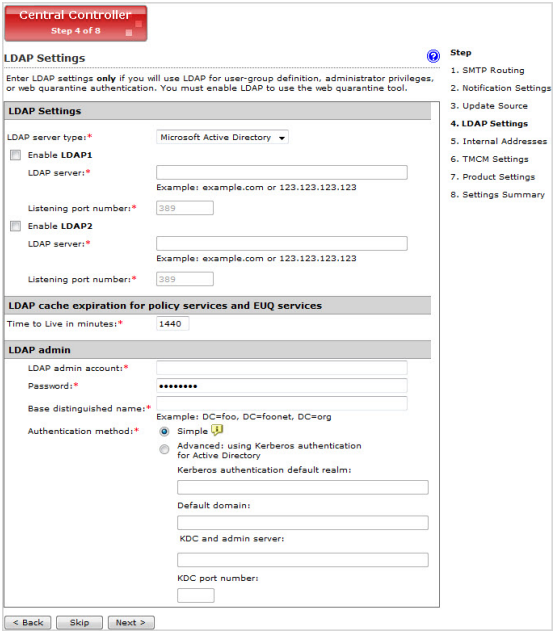
Note

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.



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

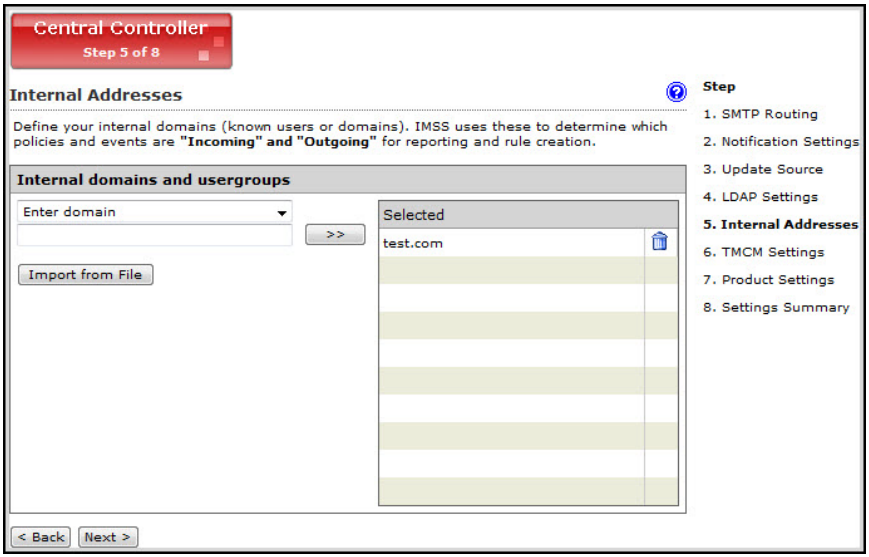
IMSS uses the internal addresses to determine whether a policy or an event is inbound or outbound.

- 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.



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 **>>**.

Note

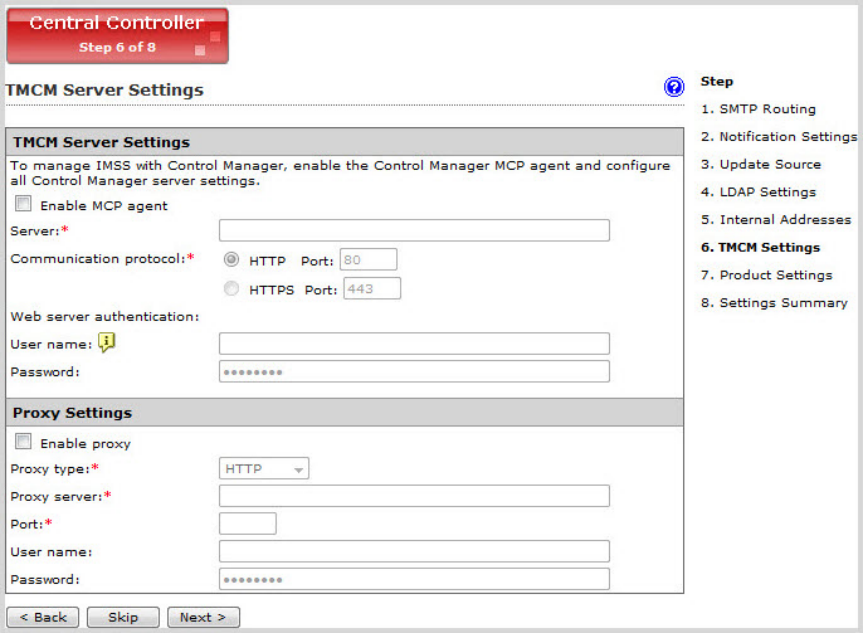
IMSS can only import a domain list from a text file (`.txt`). Ensure that the text file contains only one domain per line. You can also use wildcard characters to specify the domain. For example, `*.com` or `*.example.com`.

Configuring Control Manager Server Settings

Procedure

1. Click **Next**.

The **TMCM Server Settings** screen appears.



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 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**.

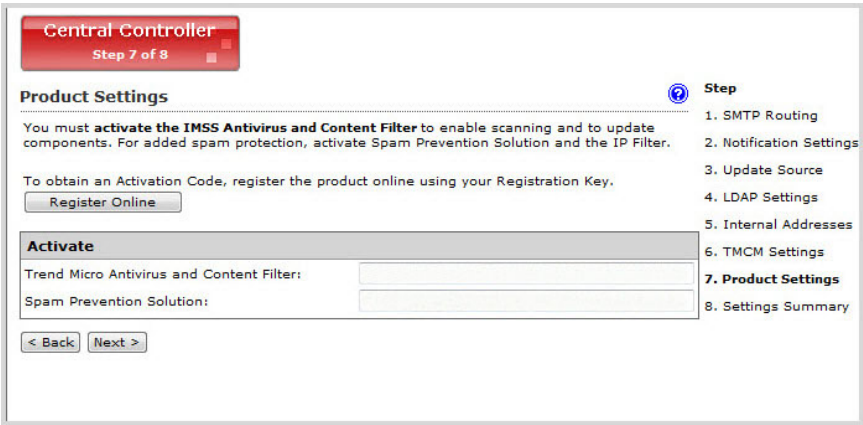
f. Specify the proxy server port number, user name, and password.

Configuring Product Settings

Procedure

1. Click **Next**.

   The **Product Settings** screen appears.



2. To obtain an Activation Code, click **Register Online** and follow the directions at the **Trend Micro Registration** website.

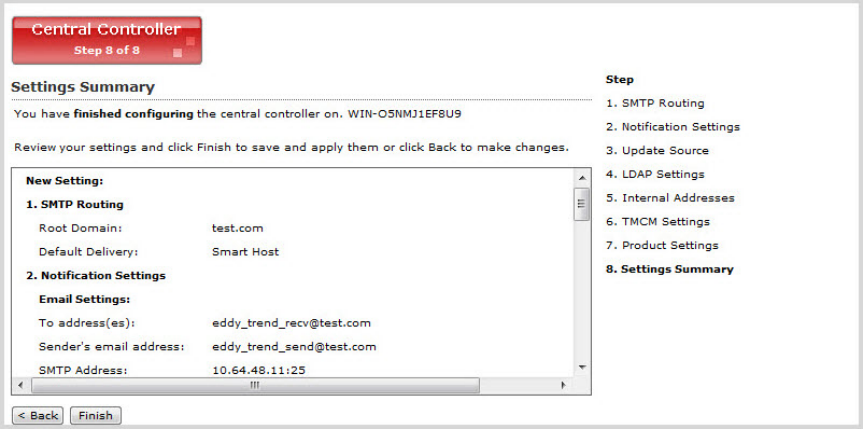
3. After obtaining the applicable Activation Codes, specify the Activation Code for each product or service to activate.

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 4-5*
- *Rolling Back a Component Update on page 4-6*
- *Scheduled Component Updates on page 4-7*

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.
Advanced Threat Scan Engine	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.
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.

COMPONENT	DESCRIPTION
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.

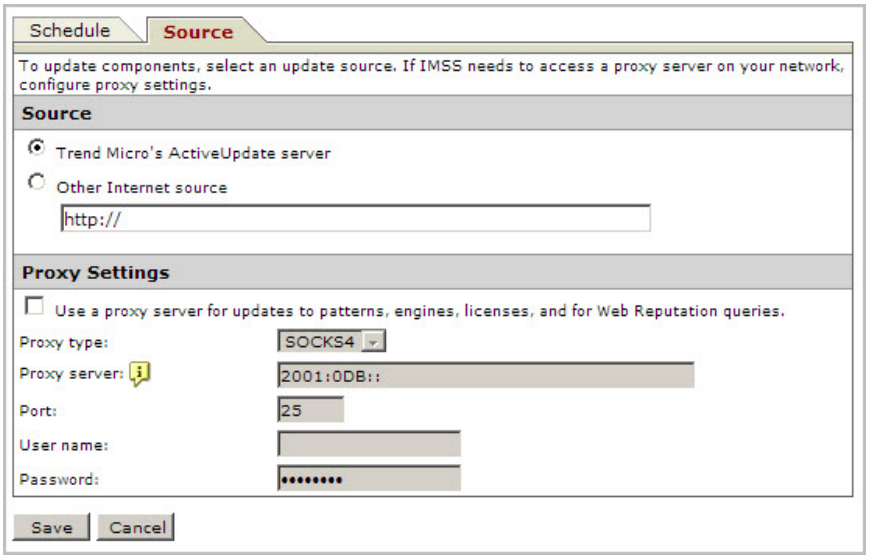
If you did not specify the update source when configuring IMSS using the Configuration Wizard, provide the update source and/or any proxy settings.

Procedure

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

   The **Updates screen** appears.

2. Click the **Source** tab.



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) 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**.

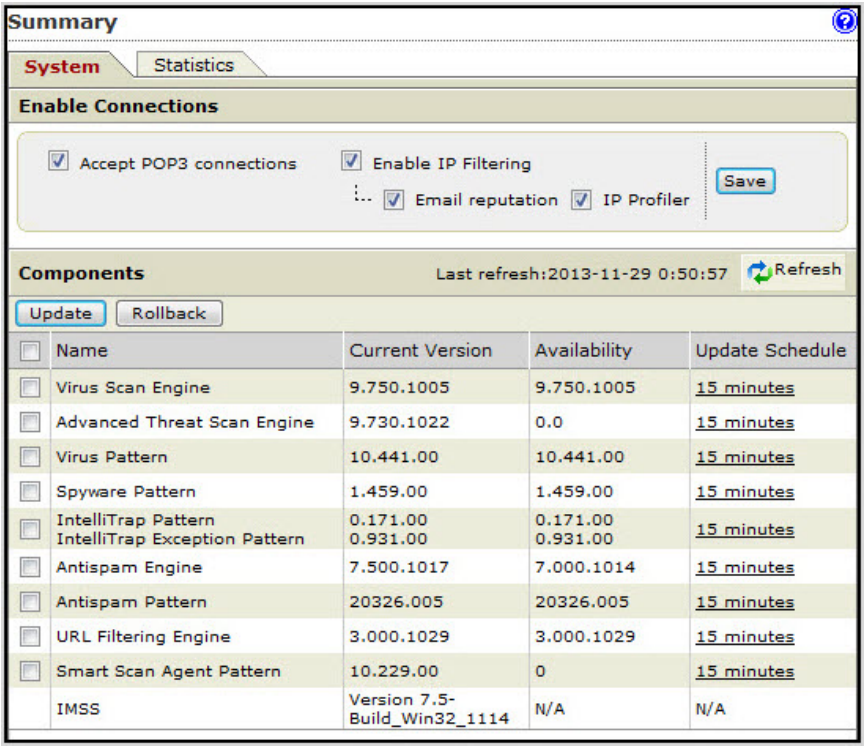
Performing a Manual Update

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.



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.

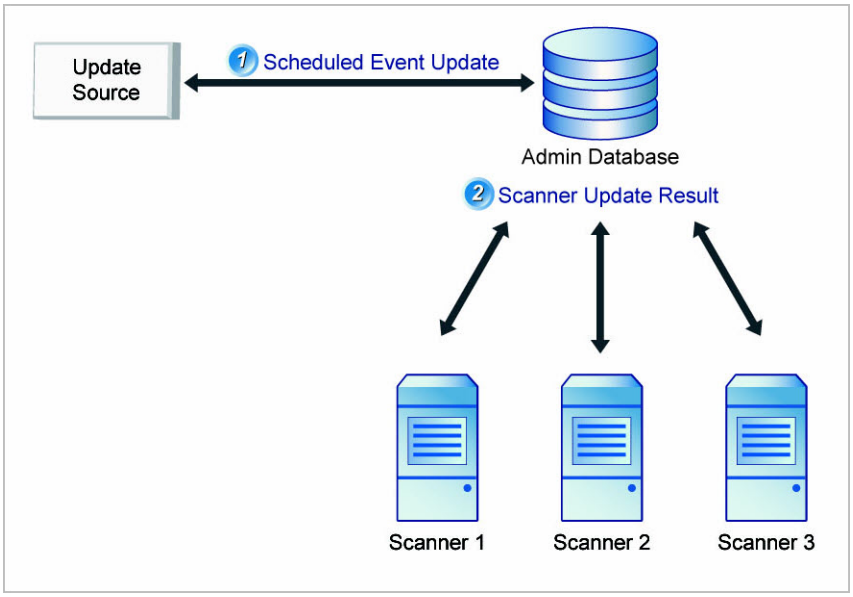


FIGURE 4-1. Scan engine and pattern file updates

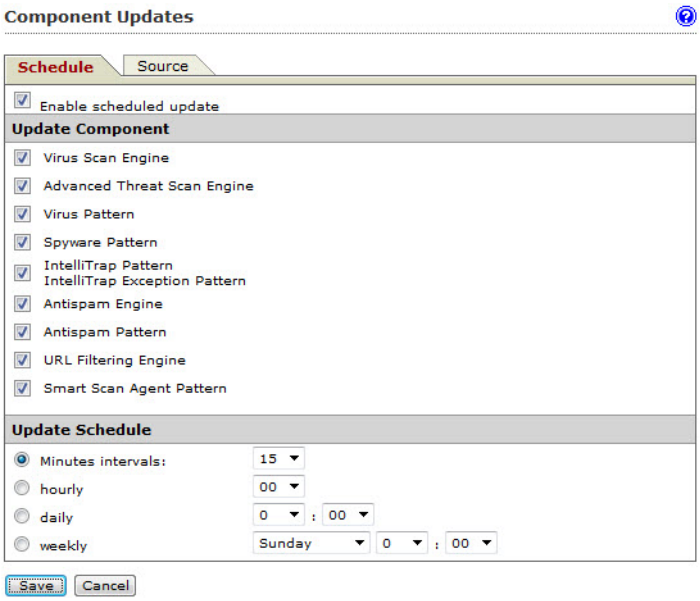
Configuring Scheduled Updates

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.



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**.

Chapter 5

Advanced Threat Scan Engine and Deep Discovery Advisor

This chapter explains how to enable Advanced Threat Scan Engine and configure Deep Discovery Advisor.

Topics include:

- *Scan Technology on page 5-2*
- *About Advanced Threat Scan Engine on page 5-2*
- *About Deep Discovery Advisor on page 5-4*

Scan Technology

IMSS allows you to select the level of malware detection appropriate for your company's security policy by configuring the scan engine.

The following table outlines the scanning technology available in IMSS.

TABLE 5-1. Scan Technology

SCAN TECHNOLOGY	DESCRIPTION
Virus Scan Engine	The Virus Scan Engine employs basic pattern matching and heuristic scanning technology to identify threats.
Advanced Threat Scan Engine (ATSE)	ATSE performs aggressive scanning to check for less conventional threats such as document exploits. By enhancing the features of the Virus Scan Engine, ATSE detects possible advanced threats that can be sent to Deep Discovery Advisor for further analysis. **Note** Deep Discovery Advisor is a separately licensed product. IMSS integrates with the Virtual Analyzer in Deep Discovery Advisor.

About Advanced Threat Scan Engine

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.

Major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities
- Enhanced parsers for handling file deformities

Important

Because ATSE identifies both known and unknown advanced threats, enabling ATSE may increase the possibility of legitimate files being flagged as malicious. Trend Micro recommends sending detected files to a controlled virtual environment for further observation and analysis.

Understanding Advanced Threats

Advanced threats use less conventional means to attack or infect a system. Heuristic scanning can detect advanced threats to mitigate damage to company systems. Enabling ATSE adds another layer of protection to systems against threats that are typically used in targeted attacks.

Some types of advanced threats that ATSE detects include:

- **Exploits**: Exploits are pieces of code purposely created by attackers to take advantage of software vulnerabilities. Such code is typically incorporated into malware.
- **Targeted attacks**: Targeted attacks refer to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. These attacks seek to maintain a persistent presence within the target's network so that the attackers can move laterally and extract sensitive information.
- **Zero-day threats**: Zero-day threats exploit previously unknown vulnerabilities in software.

Tip

Trend Micro recommends enabling ATSE.

Enabling Advanced Threat Scan Engine

Procedure

1. Navigate to **Policy** > **Scan Engine**.
2. Select **Enable Advanced Threat Scan Engine**.

3. Click **Save**.

The IMSS daemon is automatically restarted when ATSE is enabled.

About Deep Discovery Advisor

Trend Micro™ Deep Discovery Advisor is a separately licensed product that provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines.

Deep Discovery Advisor is designed to:

- Collect, aggregate, manage, and analyze logs into a centralized storage space
- Provide advanced visualization and investigation tools that monitor, explore, and diagnose security events within the corporate network

IMSS integrates with the Virtual Analyzer in Deep Discovery Advisor. IMSS sends suspicious messages, including attachments, to Virtual Analyzer for further analysis. Virtual Analyzer performs content simulation and analysis in an isolated virtual environment to identify characteristics commonly associated with many types of malware.

In particular, Virtual Analyzer checks if files attached to messages contain exploit code. Although many files include non-executable data, attackers find ways to cause such files to exploit vulnerabilities in programs and operating systems that run them. Because of this, sending malicious files to target users has become an effective way for attackers to compromise systems.

For more information, see the *Deep Discovery Advisor Administrator's Guide*.

ATSE Detections and Deep Discovery Advisor

IMSS leverages ATSE to determine which messages are sent to Deep Discovery Advisor. When enabled, ATSE provides an additional layer of protection against advanced threats, such as document exploits and other threats used in targeted attacks.

ATSE detections are identifiable through the prefixes **HEUR** and **EXPL**. If the detection name contains one of these prefixes, IMSS:

- Sends the entire message (including attachments) to Deep Discovery Advisor for further analysis.
- Logs the detection as a **Probable advanced threat**.

Deep Discovery Advisor assigns a risk level to each analyzed message. IMSS queries this risk level approximately 15 minutes after sending the message to Deep Discovery Advisor. After receiving the risk level, IMSS logs the detection as a **Probable advanced threat** or an **Analyzed advanced threat** based on the risk level and the security level that you select on the IMSS management console.

Note

If IMSS does not receive a risk level, or if the risk level returned is invalid, IMSS logs the detection as a **Probable advanced threat**.

Deep Discovery Advisor Risk Levels and IMSS Security Level Settings

IMSS takes action on ATSE-detected messages based on the risk level returned by Deep Discovery Advisor and the security level that you select on the IMSS management console.

Note

IMSS does not delete suspicious attachments from messages detected by ATSE.

The following table contains the security levels and the corresponding Deep Discovery Advisor risk levels that trigger an action from IMSS.

Tip

Trend Micro recommends setting the security level to **Low**.

Security Level	Description	Risk Level
High	Apply action on all messages exhibiting any suspicious behavior	• High risk • Medium risk • Low risk
Medium	Apply action on messages with a moderate to high probability if being malicious	• High risk • Medium risk
Low	Apply action only on messages with a high probability of being malicious	• High risk

Note

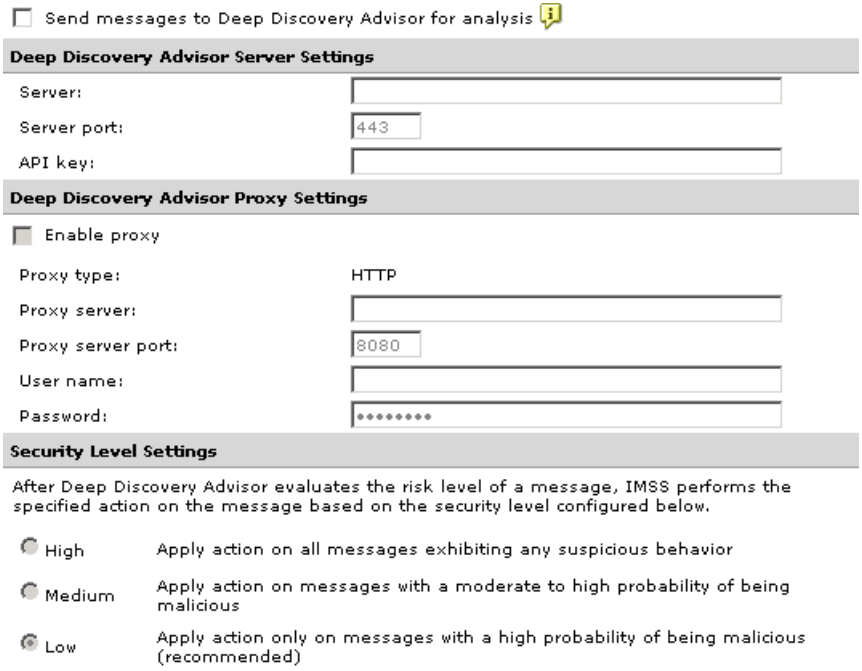
If you select the **Quarantine** action in a virus rule and IMSS receives a valid risk level from Deep Discovery Advisor, the risk level and security level determine if IMSS intercepts and reprocesses the message. If you select any other action, IMSS processes the message according to the rule configuration and logs the Deep Discovery Advisor risk level.

Configuring Deep Discovery Advisor Settings

Procedure

1. Navigate to **Administration** > **IMSS Configuration** > **Deep Discovery Advisor Configuration**.

The **Deep Discovery Advisor Configuration** screen appears.



2. Select **Send messages to Deep Discovery Advisor for analysis**.
3. Configure the Deep Discovery Advisor server settings.
   - Server
   - Server port
   - API key
4. Configure the Deep Discovery Advisor proxy server settings.
   - Proxy server
   - Proxy server port
   - User name

- Password

Note

IMSS supports only HTTP proxies.

5. Configure the **Security Level** settings for the messages that Deep Discovery Advisor analyzes.

Note

The security level determines the Deep Discovery Advisor risk level that triggers an action from IMSS. For more information, see *Deep Discovery Advisor Risk Levels and IMSS Security Level Settings on page 5-5*.

The available security level settings are: **High**, **Medium**, and **Low**. Trend Micro recommends setting the security level to **Low**.

6. Click **Save**.

Note

IMSS can notify you if Deep Discovery Advisor is unable to return a valid or complete analysis result. For more information, see *Configuring Event Criteria and Notification Message on page 20-5*.

Part II

Configuring IMSS

Chapter 6

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 6-2*
- *Using Email Reputation on page 6-2*
- *Configuring IP Filtering on page 6-8*
- *Displaying Suspicious IP Addresses and Domains on page 6-20*

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 6-8.*.

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 6-1. 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 6-2. 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.

REPORT	DESCRIPTION
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 6-3. Policy Settings

POLICY	DESCRIPTION
Settings	Configure the Approved and Blocked senders lists. You can define your lists by individual IP address and Classless Inter-Domain Routing (CIDR) by Country, or by ISP. • **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	Trend Micro welcomes suggestions from customers regarding other Internet Service Providers (ISPs) to be added to the service. Provide as much information about an ISP as you can. This helps Trend Micro add the ISP to the service.

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

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 6-8*
2. *Adding Hosts to the Approved List on page 6-10*
3. *Adding Hosts to the Blocked List on page 6-10*
4. *Enabling IP Profiler Rules on page 6-11*
5. *Configuring Email Reputation on page 6-17*

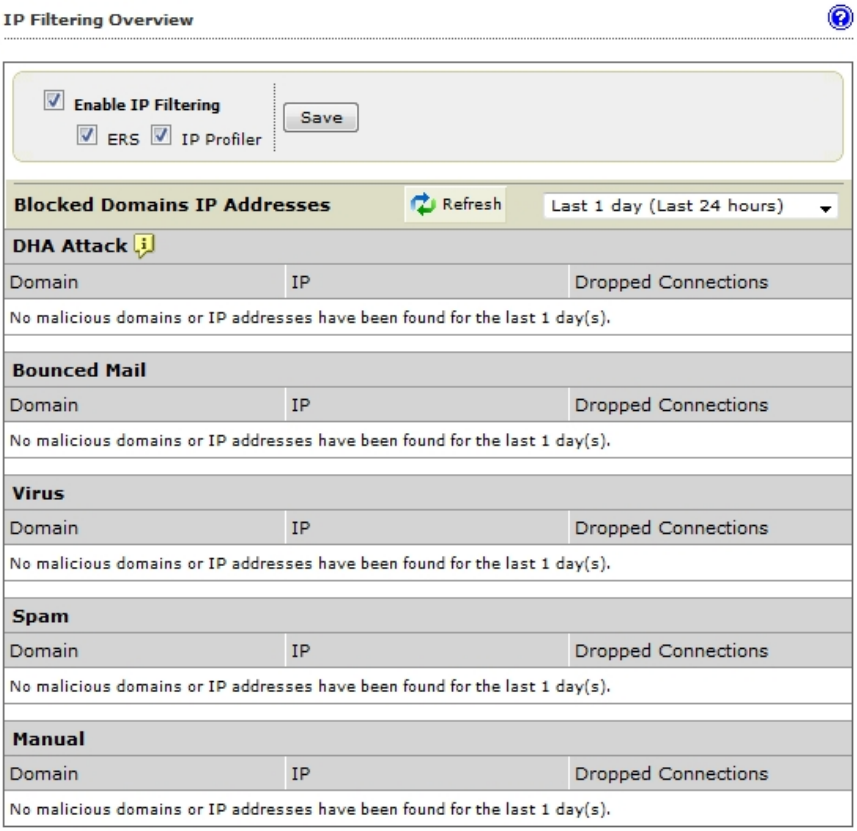
Enabling Email Reputation and IP Profiler

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.



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 Email Reputation and IP Profiler manually. Disabling IP filtering from the management console only unregisters IP Profiler from IMSS but does not stop Email Reputation and IP Profiler from running.

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!

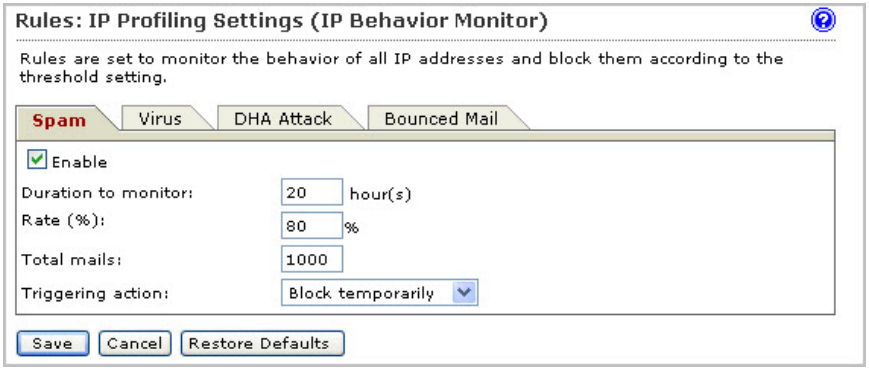
Before enabling IP Profiler Rules, add all of your email server IP addresses (that send outgoing messages to IMSS) to the IP Filtering Approved List. To configure the IP Filtering Approved List, see *Adding Hosts to the Approved List on page 6-10*.

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.



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.

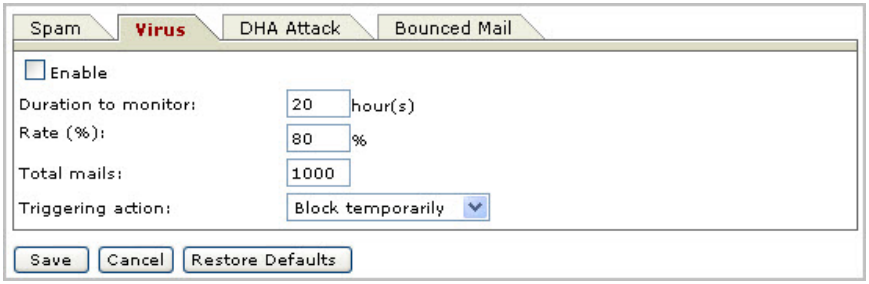
6. Click **Save**.

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.



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**.

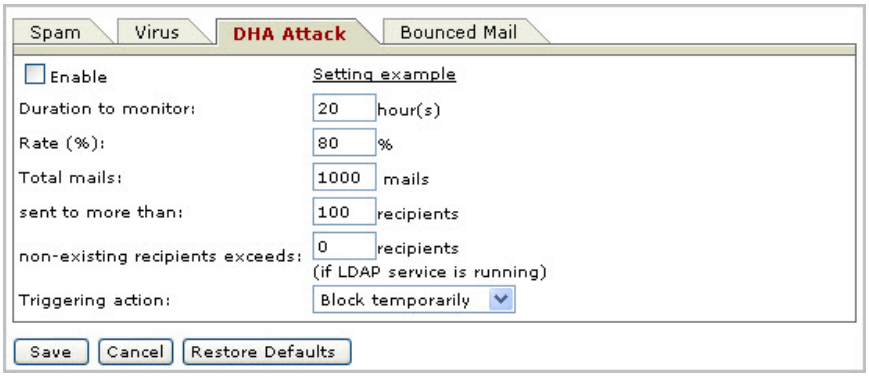
Specifying IP Filtering Directory Harvest Attack (DHA) Settings

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.

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**.

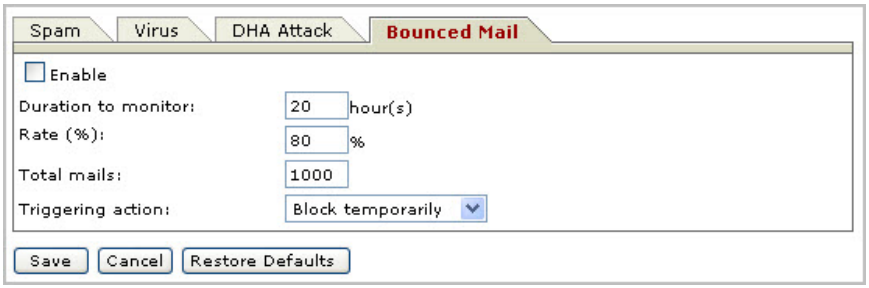
Specifying IP Filtering Bounced Mail Settings

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.



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**.

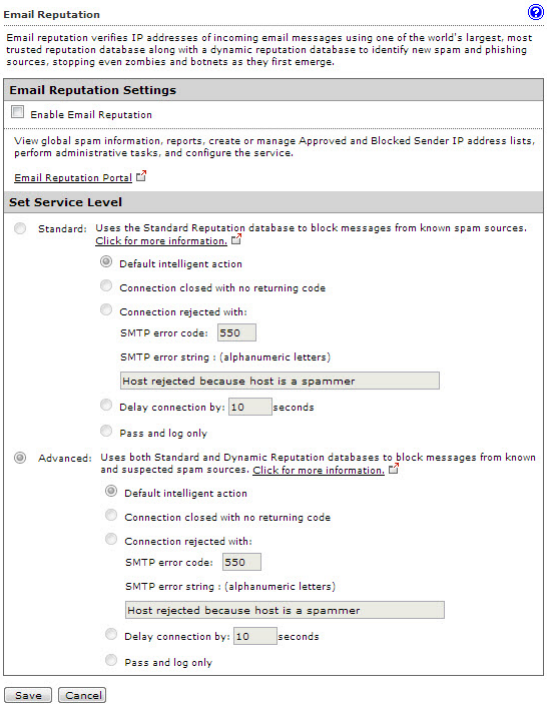
Configuring Email Reputation

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

Procedure

1. Go to **IP Filtering** > **Email Reputation**.

   The **Email Reputation** screen appears.



2. Select the **Enable Email reputation** 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:** Email reputation permanently denies connection (550) for RBL+ matches.

- **Connection closed with no returning code:** Blocks all connections without providing an associated error code.
- **Connection rejected with:**
  - **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.
- **Delay connection by**: Delays all connections by the specified time in seconds.
- **Pass and log only**: Allows and records all connections.

Advanced:

- **Default intelligent action:** Email reputation permanently denies connection (550) for RBL+ matches and temporarily denies connection (450) for Zombie matches.
- **Connection rejected with:**
  - **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.

- **Delay connection by**: Delays all connections by the specified time in seconds.
- **Pass and log only**: Allows and records all connections.

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 7

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 7-2*
- *Configuring SMTP Routing on page 7-2*
- *About Message Delivery on page 7-10*

Message Transfer Agents

IMSS comes bundled with its own Message Transfer Agent (MTA). If you 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.

Configuring SMTP Routing

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

1. *Configuring SMTP Settings on page 7-2*
2. *Configuring Connection Settings on page 7-3*
3. *Configuring Message Rule Settings on page 7-6*
4. *Configuring Message Delivery Settings on page 7-10*

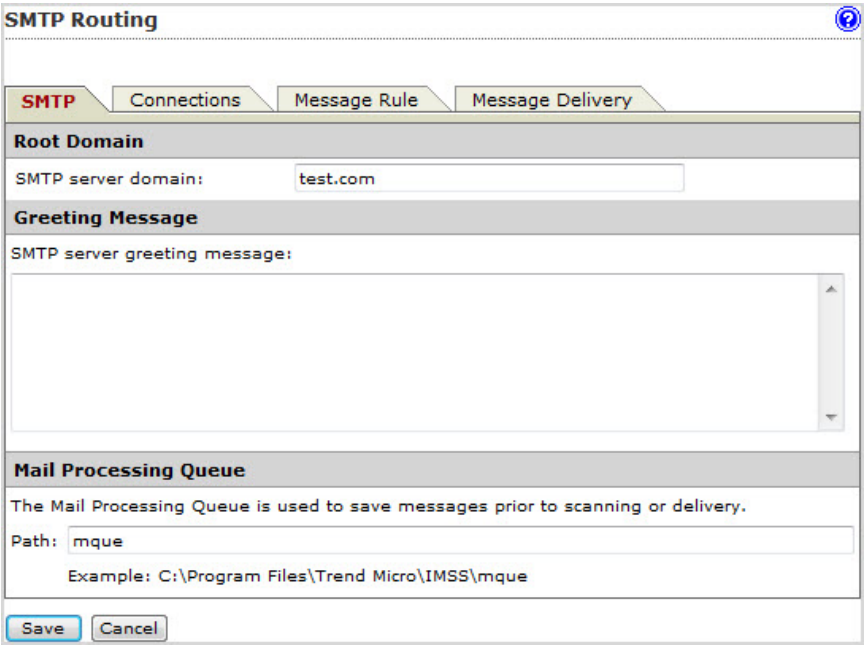
Configuring SMTP Settings

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.



2. Specify the domain name for the SMTP server in the **SMTP server domain** field.
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

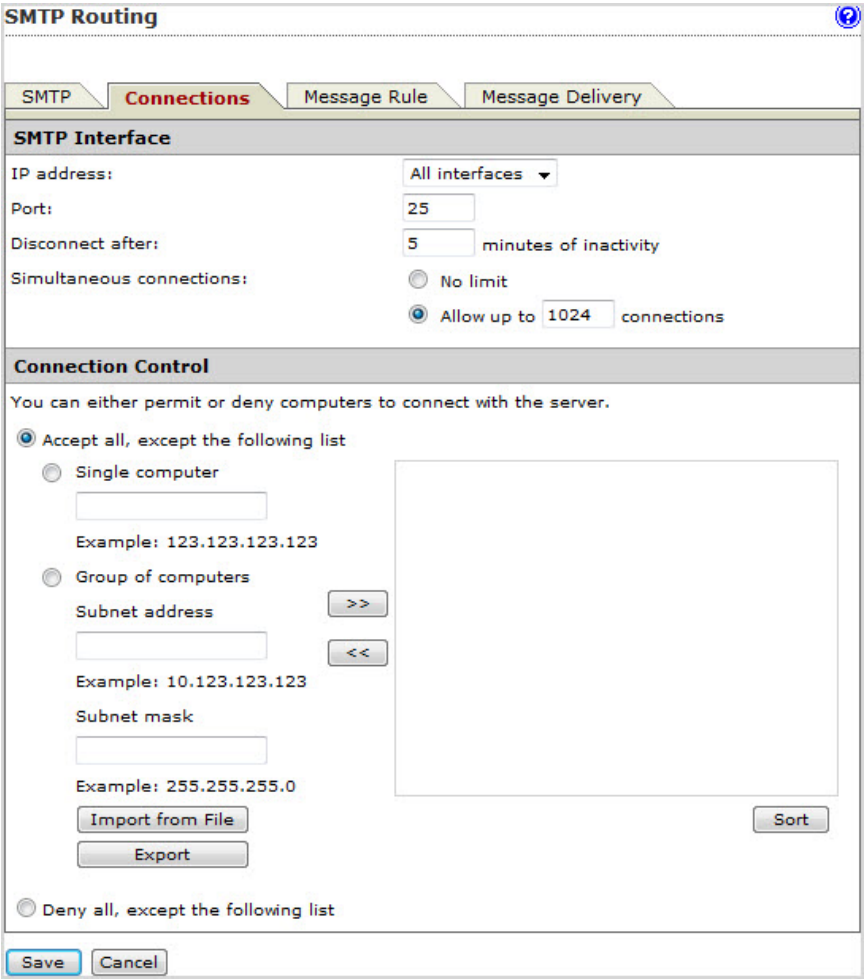
Configure SMTP connection settings for the MTA from the Connection settings screen.

Procedure

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

2. Click the **Connections** tab.

   The **Connections** screen appears.



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. Specify a subnet address and mask for an IP address group.

        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

5. 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

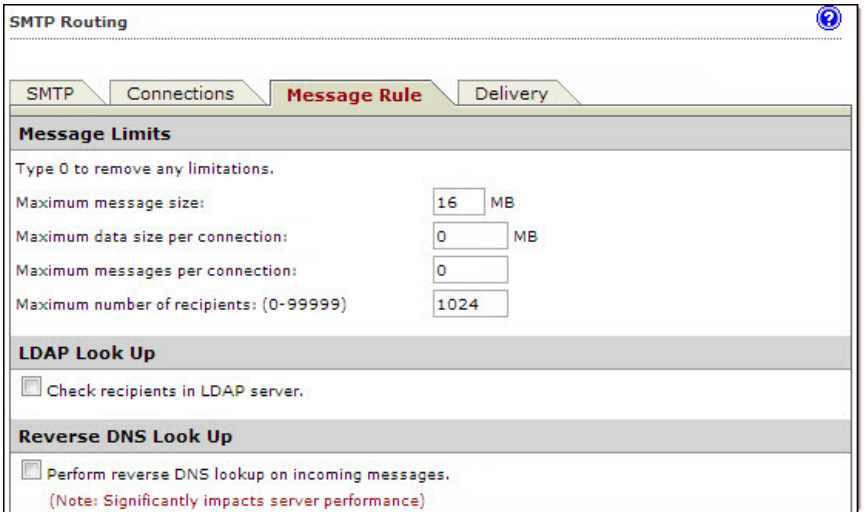
Incoming message settings are different from message delivery domain settings. For more information see *About Message Delivery on page 7-10*.

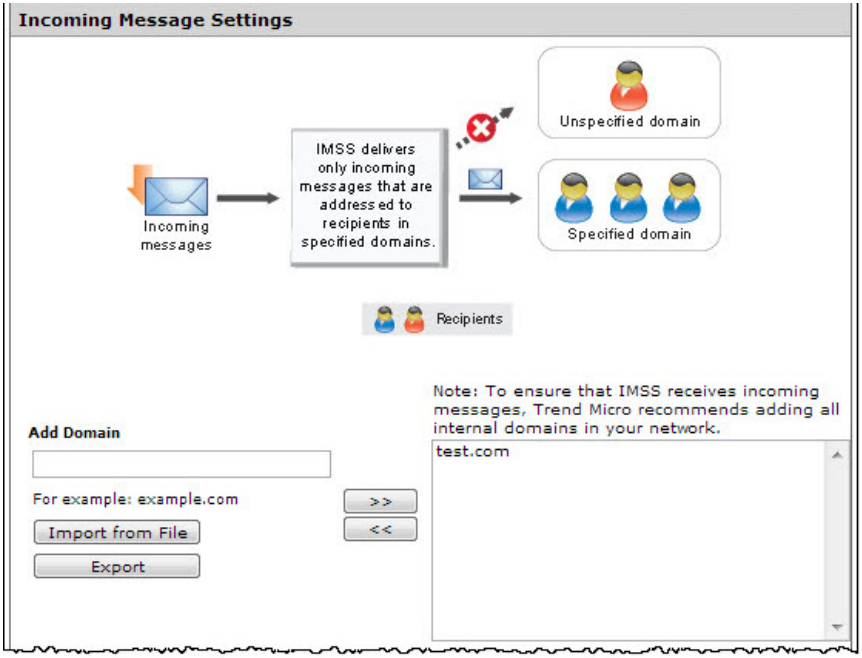
Specifying Message Rules

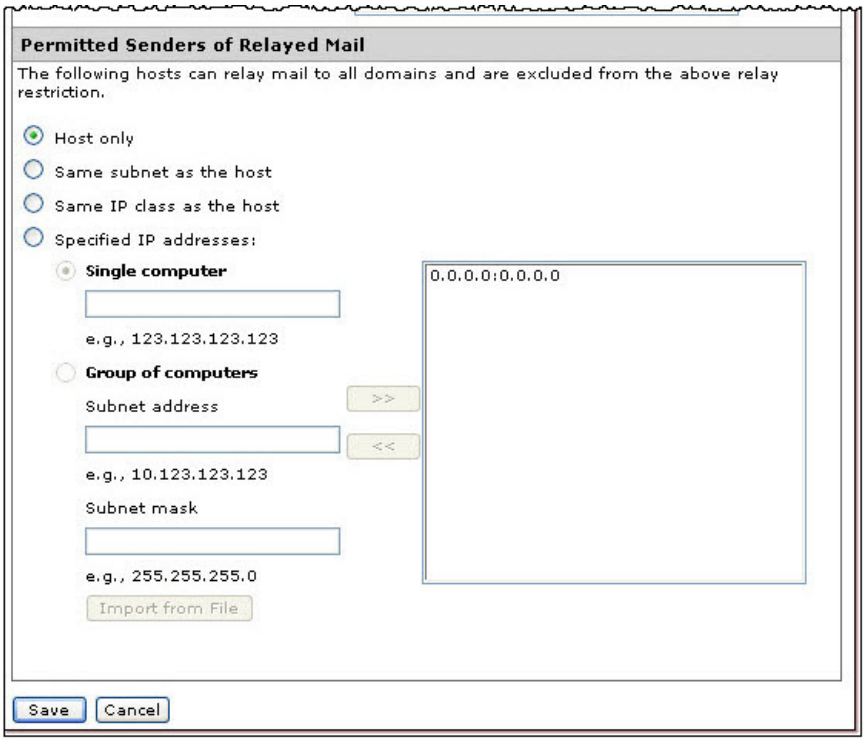
Procedure

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

   The **Message Rule** screen appears.


SMTP Routing
SMTP
Connections
Message Rule
Delivery
Message Limits
Type 0 to remove any limitations.
Maximum message size:
16
MB
Maximum data size per connection:
0
MB
Maximum messages per connection:
0
Maximum number of recipients: (0-99999)
1024
LDAP Look Up
Check recipients in LDAP server.
Reverse DNS Look Up
Perform reverse DNS lookup on incoming messages.
(Note: Significantly impacts server performance)


Incoming Message Settings
Incoming messages
IMSS delivers only incoming messages that are addressed to recipients in specified domains.
Unspecified domain
Specified domain
Recipients
Note: To ensure that IMSS receives incoming messages, Trend Micro recommends adding all internal domains in your network.
Add Domain
For example: example.com
Import from File
Export
>>
<<
test.com



3. Specify the **Message Limits** settings:

   - **Maximum message size:** Specify the number of megabytes.
   - **Maximum data size per connection:** Specify the maximum data for each connection.
   - **Maximum messages per connection:** Specify the maximum number of messages for each connection.
   - **Maximum number of recipients:** Specify the number of recipients from 0 to 99999.

4. Select the check box under **LDAP Look Up** to check recipients on the LDAP server, if desired.

5. Select the check box under **Reverse DNS Look Up** to perform a check on the domain name associated with an incoming IP address, if desired.

6. 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

   Note

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

7. Specify the **Permitted Senders of Relayed Mail**.

   - Host only
   - Same subnet as the host
   - Same IP class as the host
   - Specified IP addresses

8. 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.

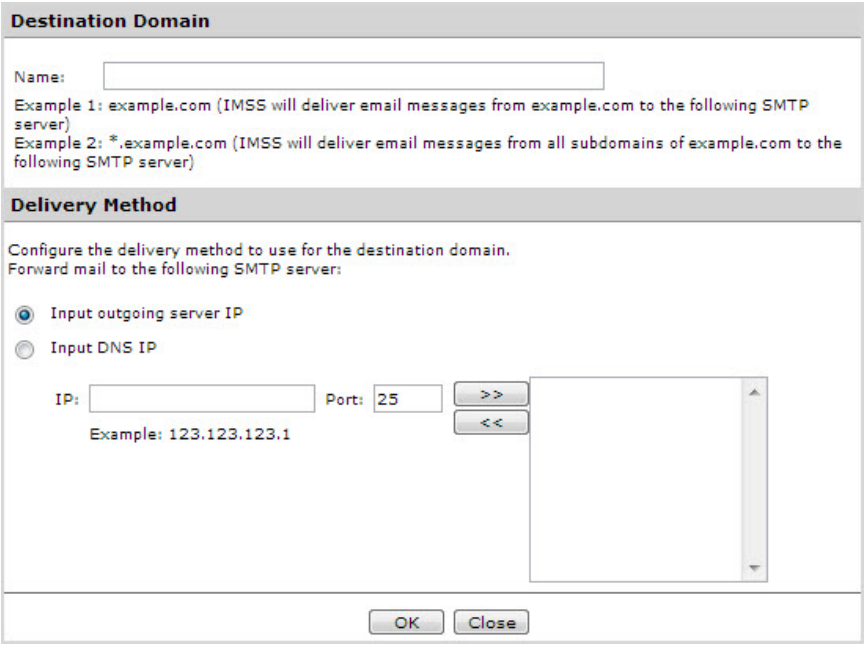
Procedure

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 **Adding Domain** screen appears.



4. Specify the **Destination Domain** and **Delivery Method**.

5. Select one of the following:

   - **Input outgoing server IP**: Provide an IP address and port number for the outgoing message server and click **>>**.
   - **Input DNS IP**: Provide an IP address for the DNS server and click **>>**. If the field is left blank, the system default DNS server is used.

6. Click **OK**.

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

7. Specify the settings for **Delivery Retry Attempts** to define the number of times and the interval at which IMSS will retry the delivery.

8. Specify the **Hop Limit** to determine the maximum number of times IMSS will pass undeliverable messages around the servers before aborting delivery.
9. Specify the **Masquerade Domain** that will overwrite the senders' real domain names for outgoing messages.
10. Select the check box under **Disable "Received" header** if you do not want IMSS to insert the "Received:" header when processing messages.
11. Click **Save**.

Valid XML file content with the required details for a domain:

When importing a Domain-based Delivery list, the list must be in a valid XML file.

```
<?xml version="1.0" encoding="UTF-8"?>

<IMSS_DBD>

<!--
```

This section defines version and platform information for IMSS from which this Domain-based Delivery file exported.

```
Do NOT edit this section. This section is used for version
checking during imports.

-->

<key section="MetaInfo">

<value name="version">7.1</value>

<value name="build">0000</value>

<value name="platform">Win32</value>

</key>

<!--

This section defines the relay methods if either of the
following conditions are satisfied:
```

```
1. Cannot find an exact match

2. The Domain-based relay methods list is empty.

The syntax is same as that used for domain-based relays.

-->

<key section="DefaultRelay">

<value name="UseMethod">1</value>

<value name="SmartHostCount">1</value>

<value

name="SmartHost0">user.client.domain.example.com:25</value>

</key>

<!--

This section defines domain-based relay settings for specific
domains.

Each key defines one domain relay with its name in the "domain"
property.

IMSS supports two relay methods: Smart host and DNS query:

1. UseMethod=0: DNS query method (default value)

2. UseMethod=1: Smart host method

IMSS supports multiple options for each kind of relay method,
for example:

UseMethod=1

SmartHostCount=2

SmartHost0=<ip_of_downstream_mta0>:25

SmartHost1=<ip_of_downstream_mta1>:25
```

```
or

UseMethod=0

DNSServerCount=2

DNSServer0=<ip_of_dns_server0>

DNSServer1=<ip_of_dns_server1>

(DNS query allows blank lists. If DNSServerCount=0, MTAs will
use the system default DNS server)


Syntax for SmartHost should use the following formats:

hostname_or_ip:port:auth:username:password

- hostname_or_ip : Host name or IP address (only IPv4 addresses
or names are supported).

- port : Host port. The default value is 25.

- auth : Authentication is required.

- 1: MTA will try authentication

A user name and password might be required.

The default value is 0.

- username : User name used for authentication. The default
value is a blank user name.

- password : Password used for authentication.

Use the IMSS 'password' utility to generate the password.


Syntax for DNS Servers should use the following format:

hostname_or_ip

hostname_or_ip : The IP address or host name of the DNS server
(only IPv4 addresses or names are supported).
```

```
-->
<key domain="example.com">
<value name="UseMethod">1</value>
<value name="SmartHostCount">1</value>
<value name="SmartHost0">user.client.domain.example.com:25</
value>
</key>
</IMSS_DBD>
```

Chapter 8

Configuring Transport Layer Security Settings

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.

- *About Transport Layer Security on page 8-2*
- *IMSS Support of Transport Layer Security on page 8-3*
- *TLS Settings for Messages Entering IMSS on page 8-5*
- *TLS Settings for Messages Exiting IMSS on page 8-8*

About Transport Layer Security

In IMSS, Transport Layer Security (TLS) provides a secure communication channel between servers over the Internet, ensuring the privacy and integrity of the data during transmission.

Two servers (Server A and Server B) establish a TLS connection through a handshaking procedure as described below:

1. The handshake begins when Server B requests a secure connection with Server A by sending a list of ciphers.
2. Server A then selects one cipher presented by Server B and replies with its digital certificate that may have been signed by a Certificate Authority (CA).
3. Server B verifies Server A's identity with the trusted CA certificate. If the verification fails, Server B may choose to stop the TLS handshake.
4. Upon verifying Server A's identity, Server B proceeds to generate the session keys by encrypting a message using a public key.
5. This message can only be decrypted using the corresponding private key. Server B's identity is thus authenticated when Server A is able to decrypt the message successfully using the private key.
6. The handshake completes and the secure connection is established after the servers have created the material required for encryption and decryption.

IMSS applies TLS on traffic entering IMSS and traffic exiting IMSS, not on incoming or outgoing message traffic.

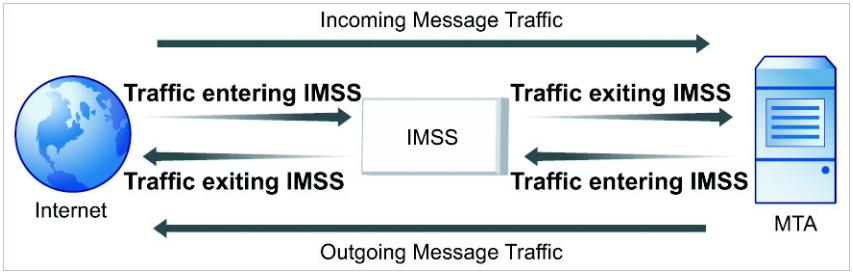


FIGURE 8-1. IMSS TLS Communication

IMSS Support of Transport Layer Security

IMSS supports the following for TLS communication

SUPPORTED OBJECT	FORMAT	
Trusted CA certificates	Distinguished Encoding Rules (DER)	.cer
	Privacy Enhanced Mail (PEM)	.crt
	Public Key Cryptography Standards (PKCS) #7	.p7b

Note

IMSS supports the Transport Layer Security protocols: TLS 1.0 and SSL 3.0.

Supported Object	Format	
Separate certificate and private key (Pvk)	Single certificate (DER, PEM)	• .cer • .crt • .pem
	Pvk file (PEM)	.pem
	Certificate chain (PEM)	.pem
Certificate and Pvk in same file	Single certificate and Pvk in PEM format	.pem
	Single certificate and Pvk in PKCS #12 format	• .pfx • .p12
	Certificate chain and Pvk in PEM format	.pem
	Certificate chain and Pvk in PKCS #12 format	• .pfx • .p12

Note

IMSS supports RSA and DSA private keys.

IMSS supports MD5 and SHA1 signature algorithms.

IMSS does not support SHA2 (including SHA256, SHA384, SHA512).

Configuring Transport Layer Security Settings

Check the following before you configure a TLS connection in IMSS:

Obtain a digital certificate:

You may obtain a digital certificate through one of the following methods:

- Generate the certificate and public/private key pairs using some certificate generator or key generator tools, then request a certificate authority to sign the certificate.

- Apply for the certificate and public/private key pairs from a certificate authority.

Ensure that the certificate format is valid:

Ensure that the signed certificate contains both the private key and certificate information.

TLS Settings for Messages Entering IMSS

IMSS applies TLS to messages that enter and exit the server where IMSS is installed. Message traffic can enter IMSS from two directions:

- Message traffic from the Internet that is to be delivered to your clients.
- Message traffic from your clients to the client's intended recipient

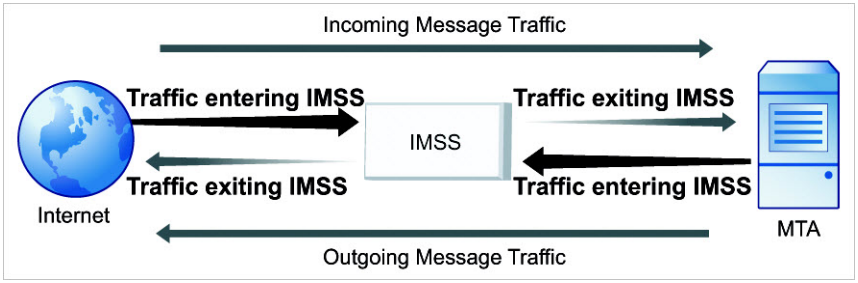


FIGURE 8-2. TLS: Traffic Entering IMSS

Configuring TLS Settings for Messages Entering IMSS

Procedure

1. Go to **Administration** > **IMSS Configuration** > **TLS Settings**.

   The **Transport Layer Security Settings** screen appears, displaying the **Messages Entering IMSS** tab.

2. Select **Enable TLS on messages entering IMSS** to enable TLS on traffic entering IMSS.
3. Specify Secure SMTP settings:
   a. Select **Enable Secure SMTP**.
   b. Specify a port number for Secure SMTP.
4. Configure IMSS server certificate settings for messages entering IMSS:
   a. Click **Edit Certificates** next to Server Certificate.

      The **Certificates** screen appears.
   b. Click **Update**.

      The **Importing Certificate and Private Key** dialog box appears.
   c. Import the certificate.
   d. Import the private key.
   e. Optionally specify the password for the key.
   f. Click **OK**.

      The **Certificates** screen displays updated information about the certificate and the public key.
   g. Click **Save**to return to the **Messages Entering IMSS** tab.
5. Configure trusted CA certificate settings:
   a. Click **Configure** next to Trusted CA Certificates.

      The **Trusted CA Store (Incoming)** screen appears.
   b. Click **Import**.

      The **Adding Certificate** dialog box appears.
   c. Import the certificate.
   d. Click **OK**.

The **Trusted CA Store (Incoming)** screen displays the CA added to the trusted CA list.

e. Click **Save** to return to the **Messages Entering IMSS** tab.

6. Add domains to the IP Address/Domain List:

a. Click **Add** under IP Address/Domain List. The **Add TLS IP or Domain** dialog appears.

b. Specify a domain, IP address, or IP address and subnet mask in the IP or domain field.

Tip

Trend Micro recommends adding IP addresses. Adding domains can impact performance because a query will have to be performed to resolve the domain.

---

c. Specify one of the following from the Security level drop-down list:

- **None (Disable):** IMSS does not use TLS for the specified IP address or domain.
- **May (optional TLS):** IMSS declares support for TLS for the specified IP address or domain. The client can choose whether to start a TLS connection.
- **Encrypt (TLS with encryption):** IMSS requires TLS for communication for the specified IP address or domain. Communication between IMSS and the client is encrypted.
- **Verify (TLS with client certificate verification):** For the IP address or Domain, IMSS not only requires clients to start TLS connections, IMSS also requires clients to send their certificates to IMSS so IMSS can verify the client's identity.

d. Specify one of the following from the **Cipher grade** drop-down list, if any option other than **None (Disable)** was selected from the **Security level** drop-down list:

- **Low:** Communication between IMSS and clients use up to 64-bit encryption.

- **Medium:** Communication between IMSS and clients use up to 128-bit encryption.
- **High:** Communication between IMSS and clients use 128-bit or greater encryption.

e. Click **OK**.

TLS Settings for Messages Exiting IMSS

IMSS applies TLS to messages that enter and exit the server where IMSS is installed. Message traffic can exit IMSS from two directions:

- Message traffic from the Internet that is to be delivered to your clients.
- Message traffic from your clients to the client's intended recipient

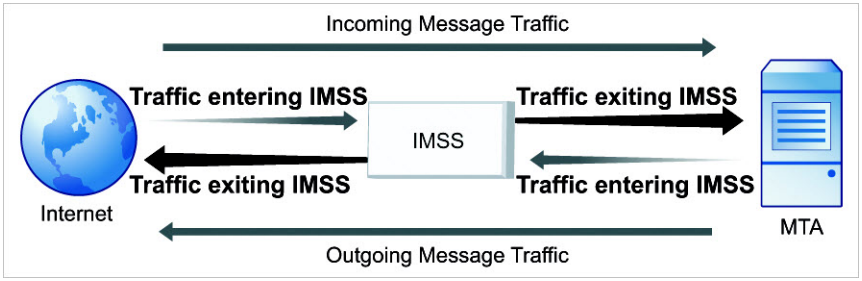


FIGURE 8-3. TLS: Traffic Exiting IMSS

Configuring TLS Settings for Messages Exiting IMSS

Procedure

1. Go to **Administration** > **IMSS Configuration** > **TLS Settings**.

   The **Transport Layer Security Settings** screen appears, displaying the **Messages Entering IMSS** tab.

2. Click **Messages Exiting IMSS**.

   The **Messages Exiting IMSS** screen appears.

3. Click **Enable TLS on messages exiting IMSS**, to enable TLS on traffic exiting IMSS.

4. Configure IMSS client certificate settings for messages exiting IMSS:

   a. Click **Edit Certificates** next to Client Certificate.

      The **Certificates** screen appears.

   b. Click **Import**.

      The **Importing Certificate and Private Key** dialog box appears.

   c. Import the certificate.

   d. Import the private key.

   e. Specify the password for the key.

   f. Click **OK**.

      The**Certificates** screen displays updated information about the certificate and the public key.

   g. Click **Save** to return to the **Messages Exiting IMSS** tab.

5. Configure trusted CA certificate settings:

   a. Click **Configure** next to Trusted CA Certificates.

      The**Trusted CA Store (Outgoing)** screen appears.

   b. Click **Import**.

      The **Adding Certificate** dialog box appears.

   c. Import the certificate.

   d. Click **OK**.

      The **Trusted CA Store (Outgoing)** screen displays the CA added to the Trusted CA list.

e. Click **Save** to return to the **Messages Exiting IMSS** tab.

6. Add domains to the Domain List:

   a. Click **Add** under Domain List.

      The **Add TLS Domain** dialog appears.

   b. Specify a domain in the **Domain** field.

   c. Specify one of the following from the **Security level** drop-down list:

      - **None (Disable):** IMSS does not use TLS for the specified domain.
      - **May (optional TLS):** IMSS declares support for TLS for the specified domain. The server can choose whether to start a TLS connection.
      - **Encrypt (TLS with encryption):** IMSS requires TLS for communication for the specified domain. Communication between IMSS and the server is encrypted.
      - **Verify (TLS with client certificate verification):** For the domain, IMSS not only starts a TLS connection to the server, but also requires the server to send its certificate to IMSS for server identification.
      - **Secure:** For the specified domain, IMSS requests the certificate from the server. If the common name in the certificate is not equal to or is not a sub-domain of the MTA's domain, the message is blocked.

   d. Specify one of the following from the Cipher grade drop-down list, if any option other than None (Disable) was selected from the Security level drop-down list:

      - **Low:** Communication between IMSS and servers use up to 64-bit encryption.
      - **Medium:** Communication between IMSS and servers use up to 128-bit encryption.
      - **High:** Communication between IMSS and servers use 128-bit or greater encryption.

e. Click **OK**.

Chapter 9

Configuring POP3 Settings

This chapter provides instructions for configuring POP3 settings.

- *Scanning POP3 Messages on page 9-2*
- *Enabling POP3 Scanning on page 9-3*
- *Configuring POP3 Settings on page 9-3*

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.

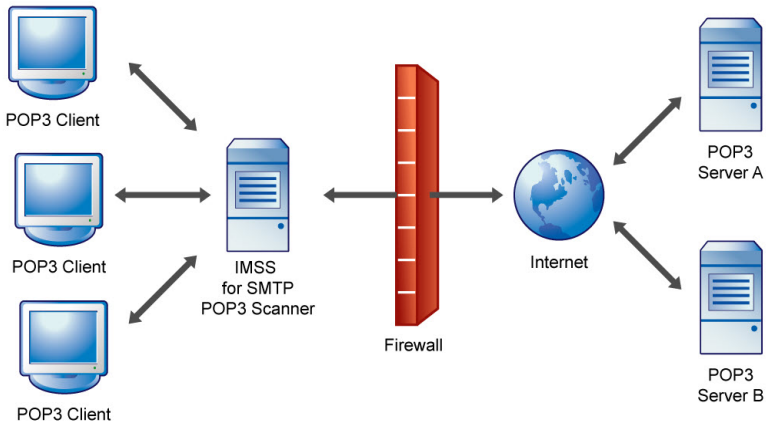


FIGURE 9-1. Scanning POP3 messages

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.

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

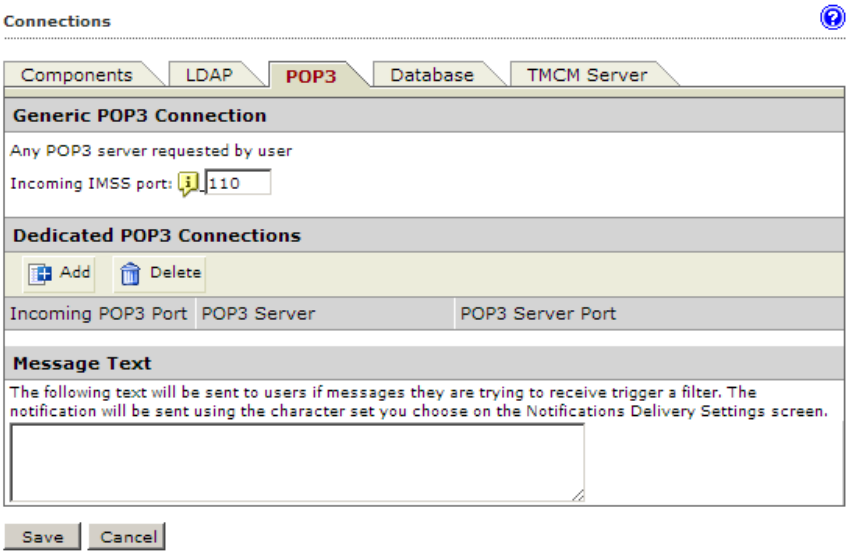
You can specify the IMSS server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection (through the APOP command or using NTLM), you may also set up a dedicated connection and assign a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

Procedure

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

   The **Components** tab appears by default.

2. Click the **POP3** tab.



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 10

Managing Policies

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

Topics include:

- *How the Policy Manager Works on page 10-2*
- *Filter Policies that Display in the Policy List on page 10-3*

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 12-2* 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.

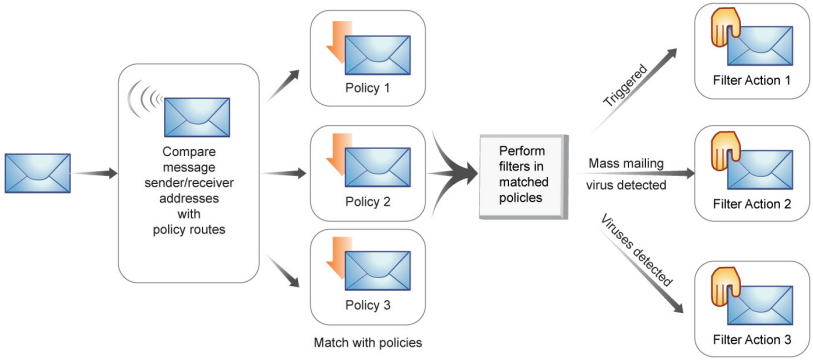


FIGURE 10-1. Simplified policy manager process flow

Note

For more information on how to create a policy, see *Adding Policies on page 13-2*.

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
      - C&C email
      - Spam and phishing email
      - Web Reputation
      - Attachments
      - Content
      - Size
      - Other

   c. Specify the users the policy protects:

      - All Groups
      - [Find user or group]

Chapter 11

Common Policy Objects

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

Topics include:

- *Policy Object Descriptions on page 11-2*
- *Understanding Address Groups on page 11-2*
- *Using BATV Keys on page 11-13*
- *Using the Keyword & Expression List on page 11-17*
- *Using the Notifications List on page 11-23*
- *Using Stamps on page 11-28*
- *Using the DKIM Approved List on page 11-32*
- *Using the Web Reputation Approved List on page 11-33*

Policy Object Descriptions

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

TABLE 11-1. Policy Objects

POLICY OBJECTS	DESCRIPTION
Address Groups	Organize multiple email addresses into a single group.
BATV Keys	Create BATV keys to encode messages that exit IMSS.
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.

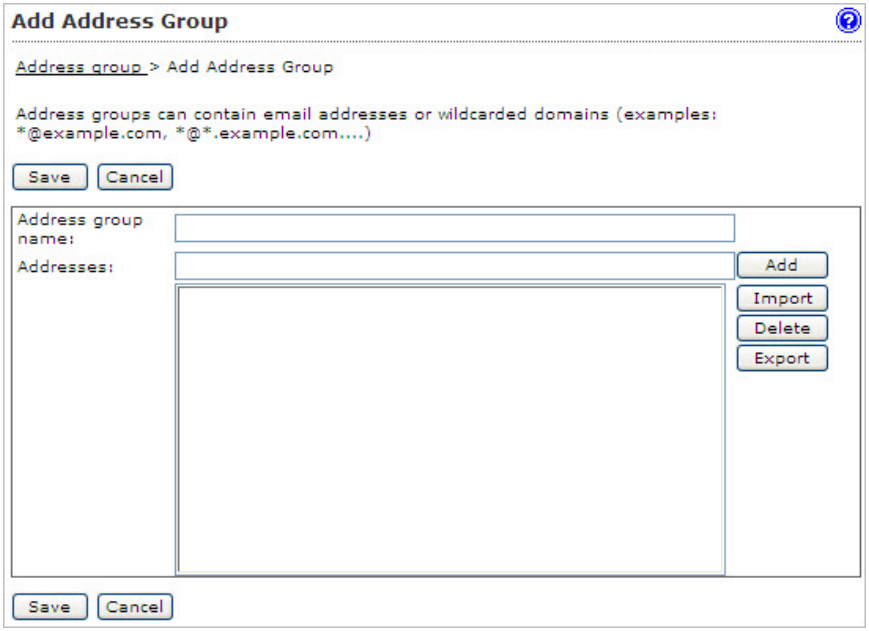
Procedure

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

   The **Address Groups** screen appears.

2. Click **Add**.

   The **Add Address Group** screen appears.



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

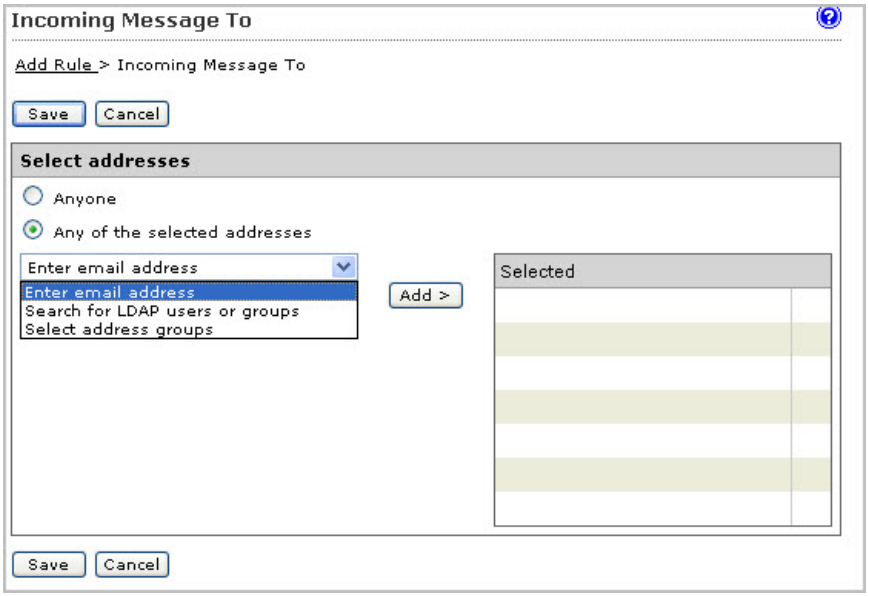
IMSS can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, `*@hr.com`.

Procedure

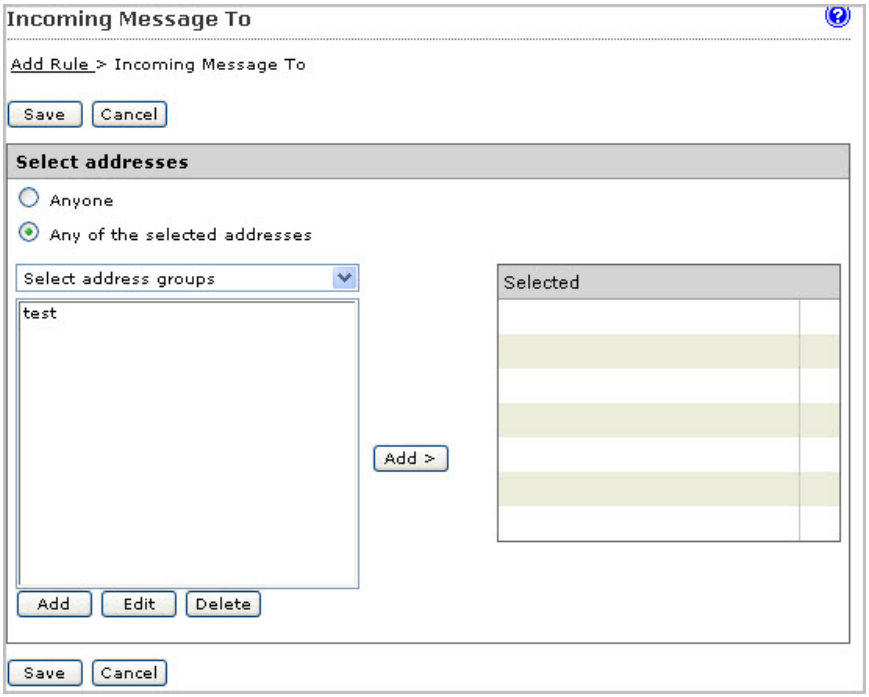
1. Go to **Policy** > **Policy List**.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats.

   The **Step 1: Select Recipients and Senders** screen appears.
4. Click the **Recipients** or **Senders** link.

   The **Select addresses** screen appears.



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



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.

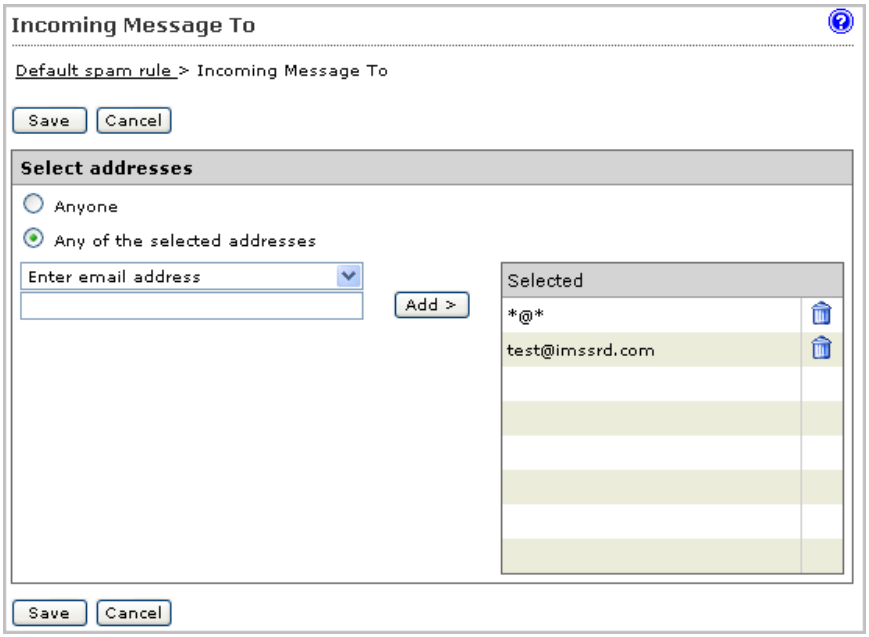
3. To delete an address group:
   a. Select the check box next to an address group.
   b. Click **Delete**.

Editing or Deleting an Address Group from an Existing Policy

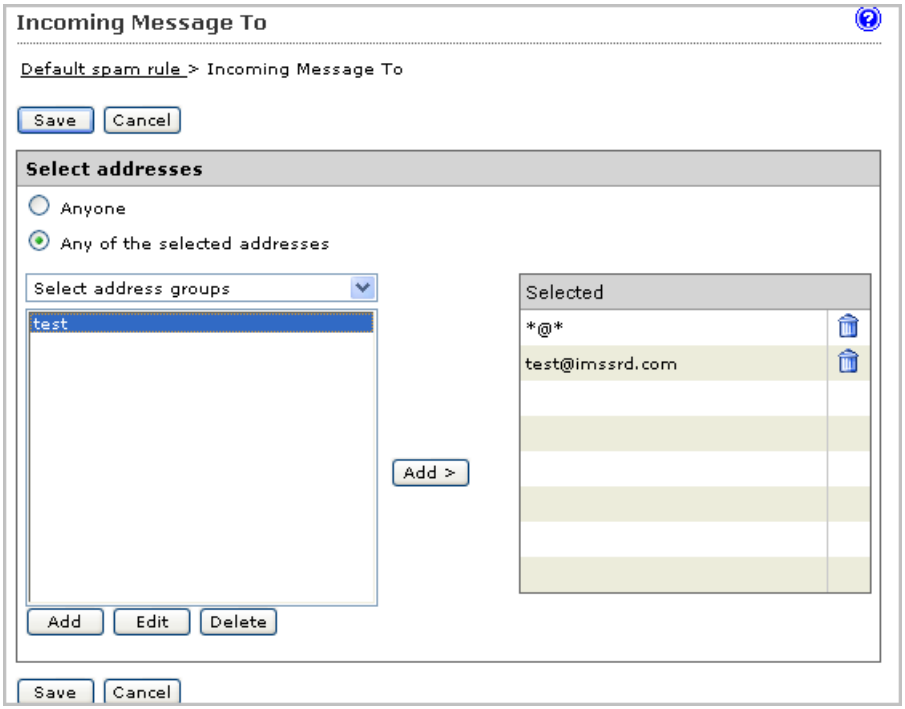
Procedure

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.



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 BATV Keys

BATV keys add another layer of security to messages leaving your network. Use BATV keys to add a token to outgoing messages. The Global Bounce Address Tag Validation (BATV) rule can then perform a specific action on bounced messages that do not have the specified BATV key.

Note

BATV is a new technology. Not all MTAs support the use of BATV keys. Verify your MTA supports the use of BATV keys before using this feature.

You can perform the following from the BATV Key screen:

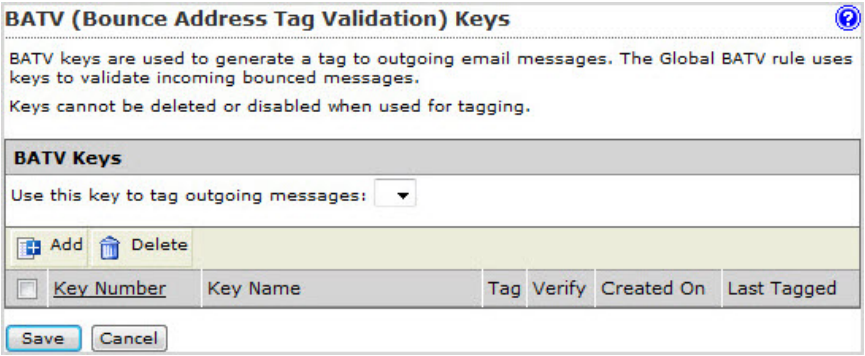
- Add or delete BATV keys
- Enable the BATV key for tagging of messages

Specifying Which BATV Key to Use for Outgoing Messages

Procedure

1. Click **Policy** > **BATV Keys**.

   The **BATV Keys** screen appears.



2. Select a BATV key from the **Use this key to tag outgoing messages** list.

3. Click **Save**.

Adding BATV Keys

Add BATV keys to help in the prevention of bounced messages reaching your end users. The following procedure describes how to specify which BATV key to use for outgoing messages.

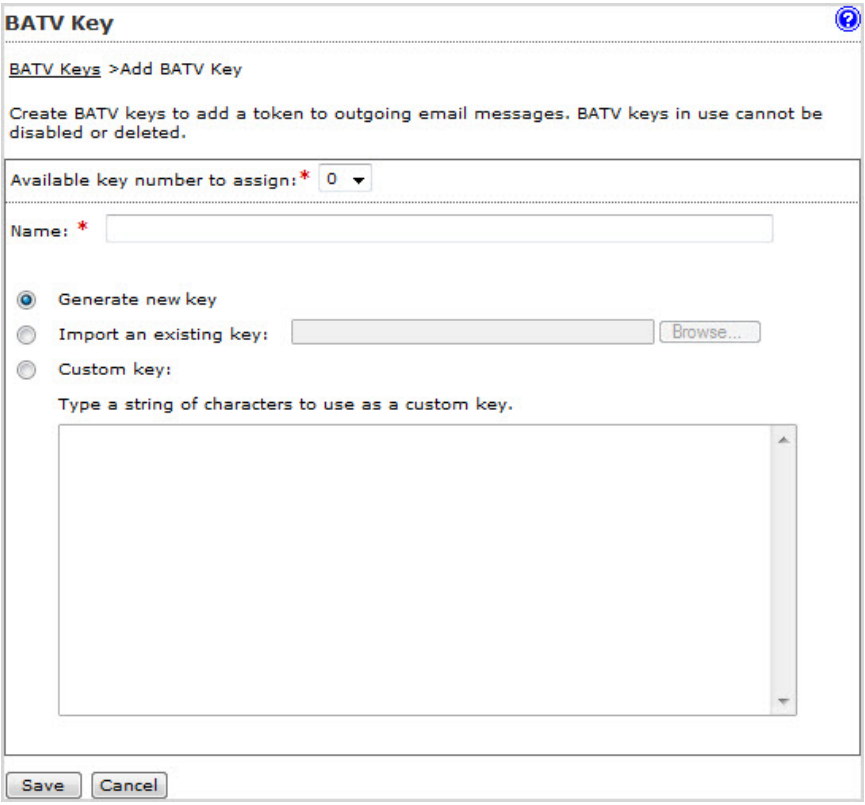
Procedure

1. Click **Policy** > **BATV Keys**.

   The BATV Keys screen appears.

2. Click **Add**.

The **Add BATV Key** screen appears.



3. Select a number from the **Available key number to assign** drop-down box. IMSS uses the number to identify which keys are assigned to tag outgoing messages.

4. Specify a meaningful name for the key in the **Name** field.

5. Select the type of key:

   - **Generate new key**: IMSS generates a new BATV key.

   - **Import an existing key**: Import a BATV key that you are already using in your network.

- **Custom key**: Create a custom key by typing a text string in the area provided.

6. Click **Save**.

   The **BATV Key** screen appears with the key appearing in the BATV Key list.

Viewing BATV Keys

You can perform the following from the View BATV Key screen:

- View the properties of the specified BATV key
- Enable the BATV key for verification
- Edit the BATV key name
- Export the BATV key

Viewing a BATV Key

Procedure

1. Go to **Policy** > **BATV Keys**.

   The BATV Keys screen appears.

2. Click the underlined key name in the **Key Name** column of the BATV Key table.

   The **View BATV Key** screen appears.

3. Select **Enable key for verification** for IMSS to verify that messages are using a valid BATV key.

4. Modify the key name.

Exporting a BATV Key

Procedure

1. Select the type of key:
   a. Click **Export**.

      The **File Download** dialog appears.
   b. Click **Save**.

      The **Save As** dialog appears.
   c. Specify a name and location to save the file.
   d. Click **Save**.
2. Click **Save**. The **BATV Key** screen appears with modifications made to the key appearing in the BATV key list.

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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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:

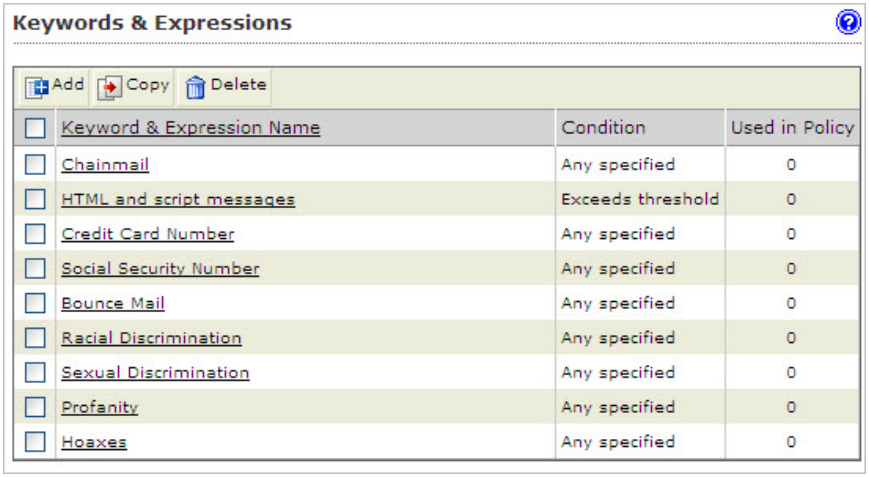
- Note that IMSS follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit http://www.pcre.org/.
- Refer to the predefined expressions for guidance on how to define valid expressions.
- Start with simple expressions. Modify the expressions 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

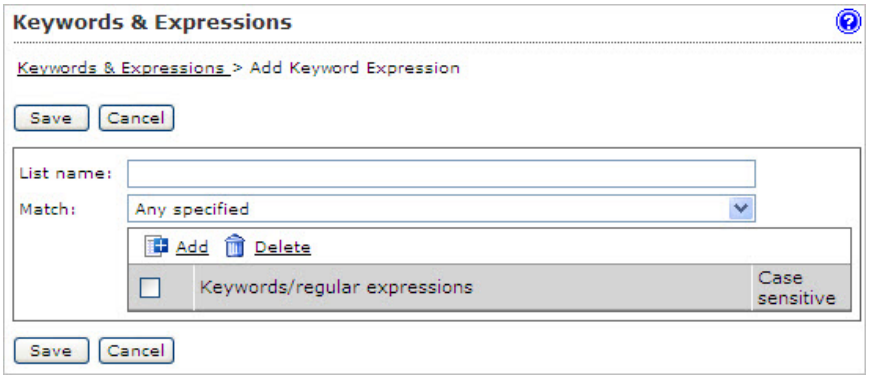
1. Go to **Policy** > **Keywords & Expressions**.

   The **Keywords & Expressions** screen appears.



2. Click **Add**.

   The **Add Keyword Expression** screen appears.



3. Next to **List name**, specify a descriptive name.
4. 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. Specify the keywords. For a partial match, specify the keyword. To specify an exact match, use "`\s`" (without the quotes) before and after the keyword.

      For example:

      - keyword matches "keywords", "akeyword"
      - \skeyword\s matches "keyword" only

   c. Click **Save**.
6. To instruct IMSS to consider the capitalization of message content when it uses the filter, select the check box under **Case sensitive**.
7. 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.

8. 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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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", "akeyword"
   - \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.

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 11-24*.

Sending Policy Notifications

Procedure

1. Create or modify a policy.
   - For information on creating a new rule, see *Adding Policies on page 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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.
3. Add or modify a notification.
4. In the **Available** list, click the notifications you want to enable.
5. 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 **<<**.
6. Click **Save** to continue creating or modifying the policy.

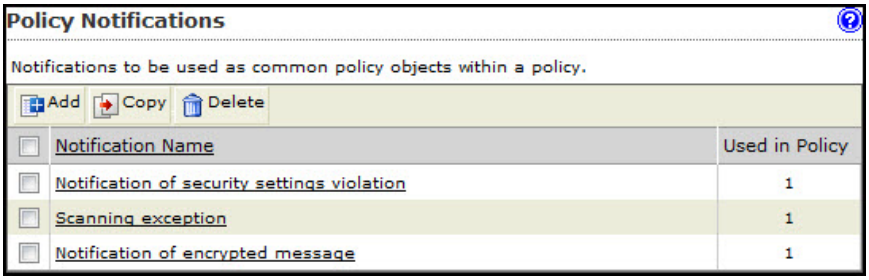
Adding or Modifying Policy Notifications

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

Procedure

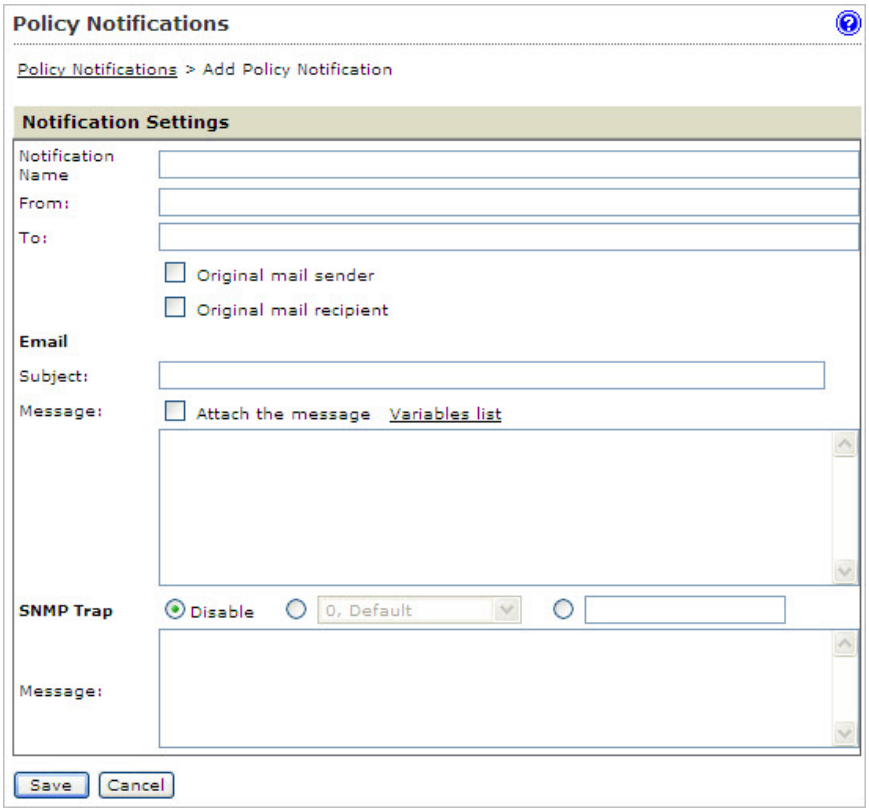
1. Go to **Policy** > **Policy Notifications**.

The **Policy Notifications** screen appears.



2. Click **Add**.

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



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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*
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.

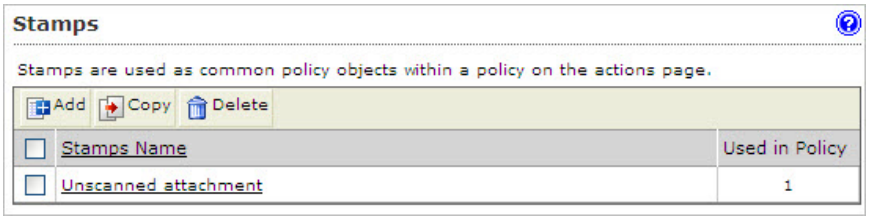
Note

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

Procedure

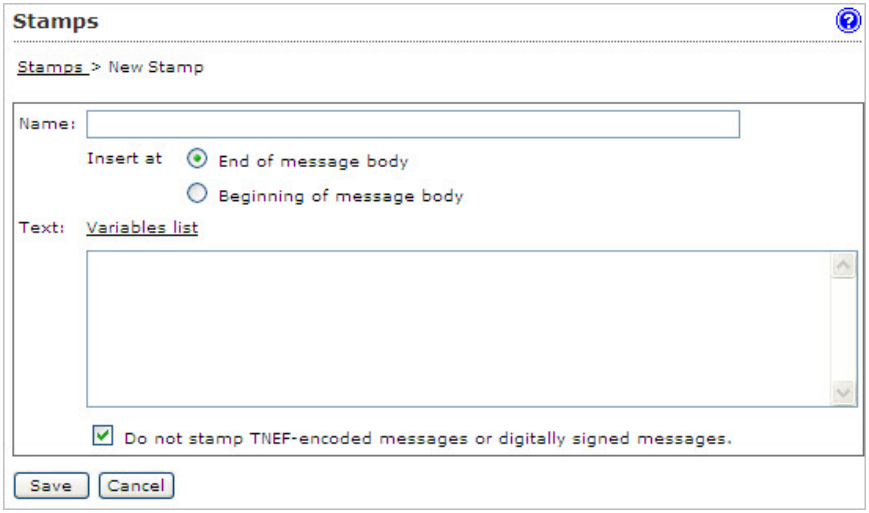
1. Go to **Policy** > **Stamps**.

   The **Stamps** screen appears.



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

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



3. Next to **Name**, specify the name of the stamp

4. Next to **Insert at**, click **End of message body** or **Beginning of message body**.

5. Under **Text**, specify the message. To see the types of variables you can include in the message, click **Variables list**.

6. 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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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

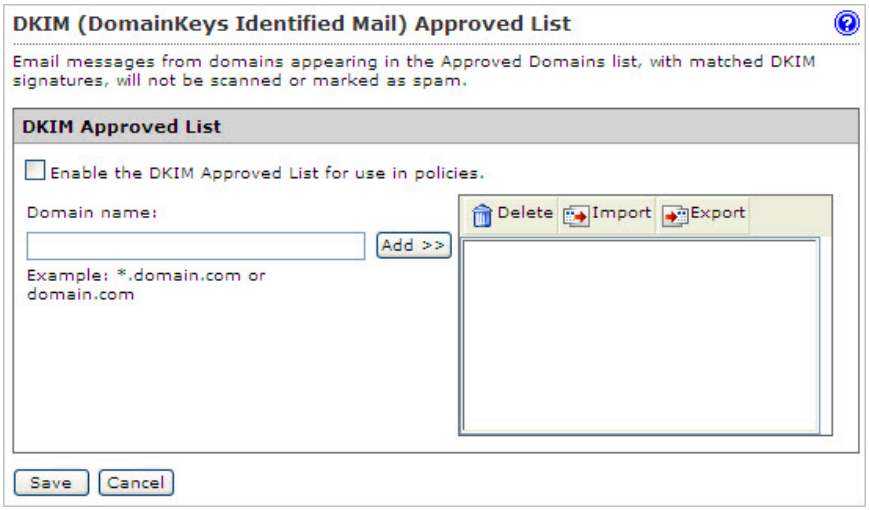
DomainKeys Identified Mail (DKIM) is a signature/cryptography-based email authentication that provides a method for validating a message during its transfer over the Internet. By validating that the message comes from the source it is claiming, IMSS provides spam and phishing protection for your network. 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.



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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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.

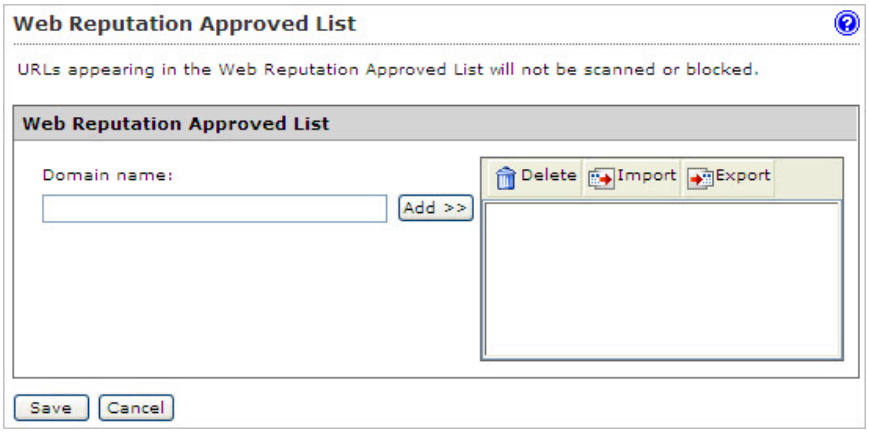
Adding to the Web Reputation Approved List

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.



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 12

Internal Addresses

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

Topics include:

- *Configuring Internal Addresses on page 12-2*
- *Searching for an LDAP User or Group on page 12-6*

Configuring Internal Addresses

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

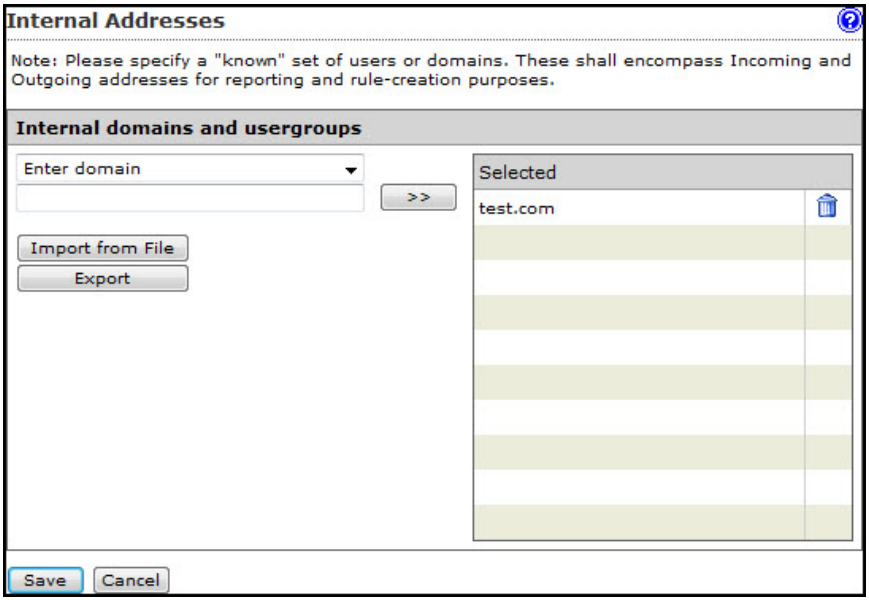
- For incoming messages, specify the recipient's address, which is in range of the internal addresses. For example: internal address is `imsstest.com`, valid recipients include jim@imsstest.com, bob@imsstest.com.
- For outgoing messages, specify the sender's address, which is in range of the internal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



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 12-6*

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.

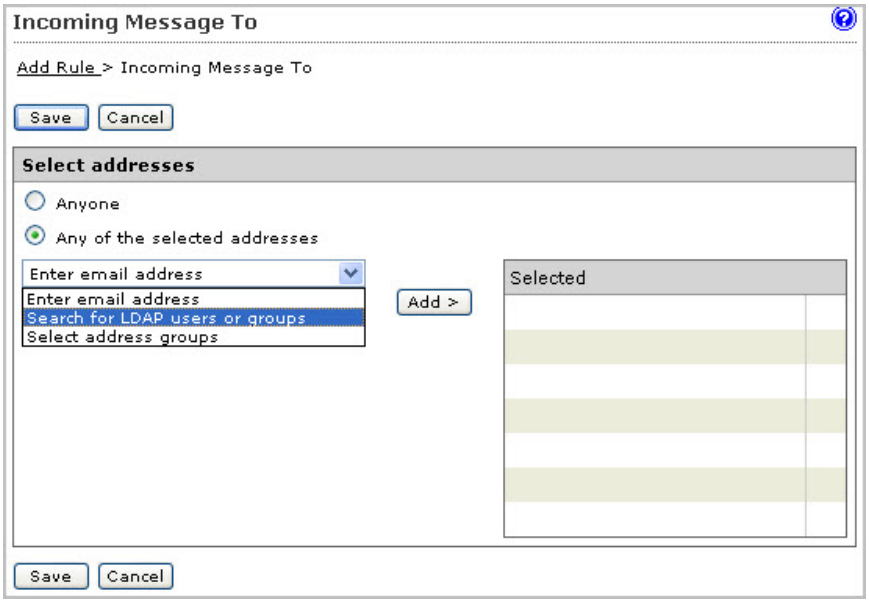
- IBM™ Lotus Domino 8.0 or 8.5
- Microsoft™ Active Directory 2003, 2008 R2, or 2012
- Sun iPlanet Directory 5.2

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

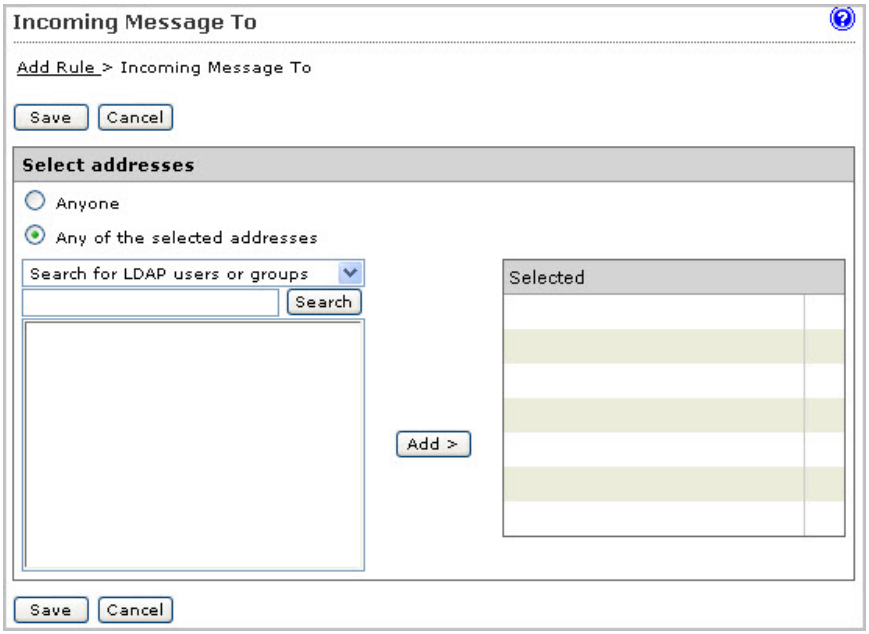
Procedure

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.



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 14-16.*.

b. You can also search for LDAP groups when adding internal addresses. See *Configuring Internal Addresses on page 12-2*.

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 13

Configuring Policies

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

Topics include:

- *Adding Policies on page 13-2*
- *Specifying a Route on page 13-2*
- *Specifying Scanning Conditions on page 13-10*
- *Specifying Actions on page 13-30*
- *Finalizing a Policy on page 13-37*

Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For information, see *Configuring Internal Addresses on page 3-9*.

Creating a policy involves the following steps:

- Step 1: *Specifying a Route on page 13-2*
- Step 2: *Specifying Scanning Conditions on page 13-10*
- Step 3: *Specifying Actions on page 13-30*
- Step 4: *Finalizing a Policy on page 13-37*

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**.

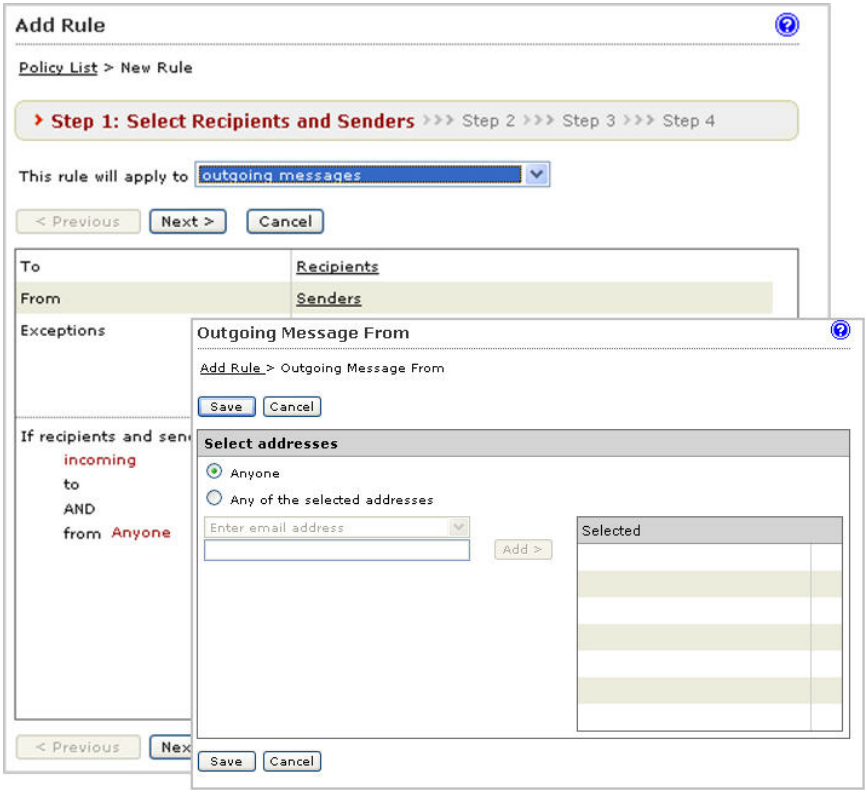
The **Policy List** screen appears.

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, message content, encrypted messages, regulatory compliance, and other attachment criteria.

The **Add Rule** screen appears.



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 14-16*.

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 14-16*.

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 13-1. 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	Select the check box next to one of the following types of file extensions to scan: • **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. **C&C Email**: Scans message headers for email addresses known to be used as C&C callback addresses.

This filter is not triggered if the detected email addresses are found in the **C&C Email Approved List**. For more information, see *Configuring the C&C Email Approved List on page 13-14*.

Note

Selecting **C&C Email** and the filter relation **all conditions matched (AND)** disables the **Spam/Phishing Email** and **Web Reputation** filters.

---

c. **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**

d. **Web Reputation**: Scans URLs in messages to protect against phishing and other malicious websites.

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.

Configuring the C&C Email Approved List

IMSS does not identify messages from senders and recipients in this list as C&C email. The list can contain a maximum of 5,000 entries.

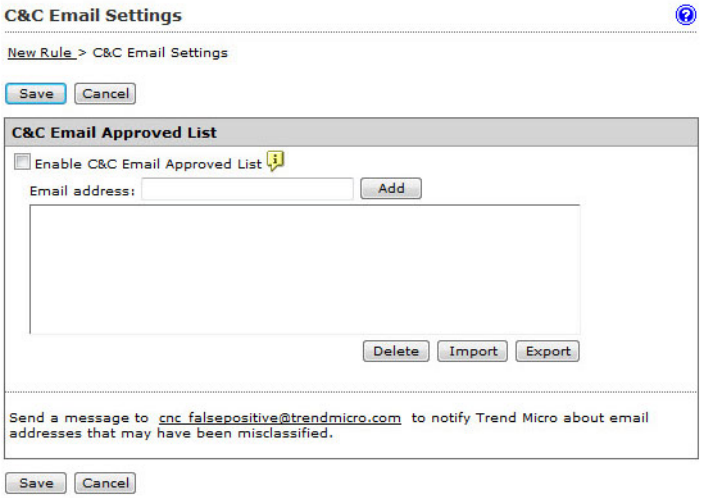
Note

IMSS identifies addresses used in the message header and not the SMTP session.

Procedure

1. On the **Scanning Conditions** screen, select **C&C email settings**.
2. Click **C&C email settings**.

The **C&C Email Settings** screen appears.



3. Select **Enable C&C Email Approved List**.
4. Add email addresses using any of the following methods:
   a. Type an email address in the box then click **Add**.

      The address appears in the list.

      Note

      You can use the asterisk character to add multiple addresses. For details, see *Using the Asterisk Wildcard on page 14-16*.

   b. Import email addresses from a text file on a local host to the IMSS server.

      Note

      Each line in the file should contain only one email address that follows any of the valid formats. IMSS does not import incorrectly formatted email addresses.

      If the list already contains email addresses, choose whether to merge the new entries or overwrite the existing ones.

5. Optional: Export the address list as a text file.
6. Optional: Send a message to cnc_falsepositive@trendmicro.com to notify Trend Micro about email addresses that may have been misclassified.

> **Note**
> For more information, see *Submitting Potentially Misclassified Email Addresses to Trend Micro on page 13-16*.

7. Click **Save**.

Submitting Potentially Misclassified Email Addresses to Trend Micro

Procedure

1. Take screenshots of the management console, error messages, or any notification you receive from IMSS.
2. Create a new email message with the following information:
   - Subject line: [IMSS 7.5] Potentially misclassified email address
   - Email body:
     - Specify the email address.
     - Explain why it is potentially misclassified.
   - Attachments:
     - Screenshots that you took in *Step 1 on page 13-16*.
     - Email message(s) incorrectly identified as malicious

> **Important**
> Do not use the **Forward** command as it deletes essential information from the message header. Instead, send the message as an attachment (`.msg` or `.eml`).

3. Send the email message to: cnc_falsepositive@trendmicro.com.

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 13-18*.

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 13-2*.
- For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.

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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.
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. Optional: Select **Detect URLs that have not been tested by Trend Micro** to increase protection against short-lived websites.

   Note

   Web pages change frequently, and it is difficult to find data or follow a link after the underlying page is modified. Such websites are usually used as vehicles for transporting malware and carrying out phishing attacks.

7. Click **Save**.

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 11-19* 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 13-2*.
   - For information on modifying an existing rule, see *Modifying Existing Policies on page 14-2*.

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(unscanned 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.

   Note

   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 19-2*.
Change recipient	IMSS sends the message to another recipient. Specify the recipient email address and separate multiple recipients with a semicolon (;).
Handoff	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: • 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. **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.

2. Configure **Modify** settings.

OPTION	DESCRIPTION
Insert X-header	Inserts a user-specified message to the header of messages.

Option	Description
Delete attachments	Select an action for IMSS to take: • **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 11-23*.
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 19-2*.
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 19-2*.
Change recipient	IMSS sends the message to another recipient. Specify the recipient email address and separate multiple recipients with a semicolon (;).
Handoff	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: • 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. **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.

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	Select the check box to enable actions if IMSS finds a virus or other malware, and then click one of the following:
	• **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:
	  • **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.
	  • **Delete matching attachment**: Remove only the attachment with viruses/malware.
	  • **Delete all attachments**: Remove all attachments.

Insert X-header	Inserts a user-specified message to the header of messages. **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.
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.
Insert safe stamp for clean mails	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. **Note** The **Insert safe stamp for clean mails** option is not available on the **Special Viruses** tab.
Tag subject	Add text to the subject line of the message. Click Tag subject to edit the tag.

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 11-23*.
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 19-2*.
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.

- **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 13-10*. If IMSS detects spyware/grayware in a message, it takes the actions that are specified here.

Note

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 13-10*.

Note

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

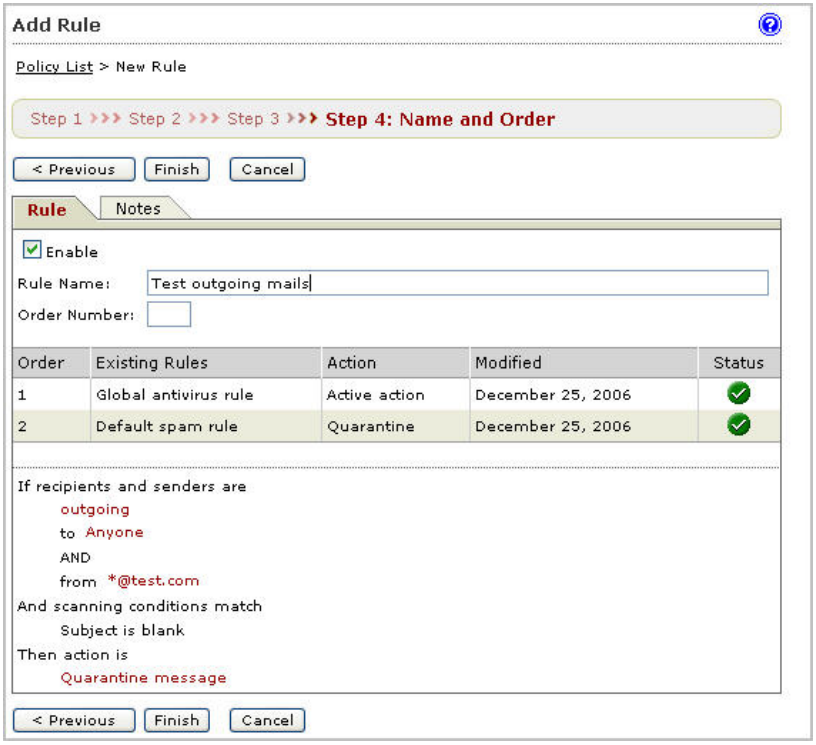
You can enable and disable rules by clicking the buttons.

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.



2. Select the **Enable** check box to activate the rule.
3. Specify a name for the rule in the **Rule Name** field.
4. 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.
5. Click the **Notes** tab.

The **Notes** screen appears.

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 14

Existing Policies

This chapter provides instructions for creating, modifying, and managing InterScan Messaging Security Suite policies.

Topics include:

- *Modifying Existing Policies on page 14-2*
- *Policy Example 1 on page 14-6*
- *Policy Example 2 on page 14-10*
- *Using the Asterisk Wildcard on page 14-16*

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 13-2*.
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)
   - **And** (Global BATV rule)
6. Configure the scan settings. For more information, see the following:
   - For Antivirus and Other rules: *Specifying Scanning Conditions on page 13-10*
   - For the Global DKIM Enforcement rule: *Using the Domain List for the Global DKIM Enforcement Rule on page 14-5*
   - *Using the Domain List for the Global DKIM Enforcement Rule on page 14-5*
7. Click **Edit** for **Then action is**.
8. Configure the action settings.

   For more information, see *Specifying Actions on page 13-30*.

9. Click **Save**.

Using the Domain and Email Exclusion List for the Global BATV Rule

Use the Global BATV rule to prevent bounced mail attacks and minimize backscatter email. IMSS tags the "From" address in messages sent from domains in the Domain List. IMSS does not tag messages from users appearing in the Exclusion List.

Tip

Trend Micro recommends deploying IMSS facing the Internet if you want to enable the Global BATV rule.

When the Global BATV rule is enabled, all messages IMSS delivers to external MTAs contain the BATV tag for bounced mail verification.

IMSS-generated notification messages contain a BATV tag. When the notification messages are delivered to an external MTA and cannot be delivered by that MTA, the returned bounced message will be rejected by IMSS because the message lacks a BATV tag.

For IMSS to accept those notifications, include the notification sender in the BATV Email Exclusion List.

Adding Domains and Email Addresses to the Global BATV Rule

Procedure

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

   The **Policy** screen appears.

2. Click the **BATV rule** link.

The **Policy Summary** screen appears.

3. Click **Edit** in the **And** row.

   The **Scanning Conditions** screen appears.

4. Populate the Domain List.

Option	Description
Manually	Specify a domain name and then 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 Domain 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. Populate the Email Exclusion List.

Option	Description
Manually	Specify an email address and then click **Add**.
Import a list	**Note** When importing a text file for the Email Exclusion List, only one email address should be on each line. a. Click **Import**. The Import Email Exclusion List appears. b. Specify the file path and file name or click **Browse** and locate the file. c. Select one of the following:

Option	Description
	• **Merge with current list** • **Overwrite current list** d. Click **Import**.

6. 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**.

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 14-7*
- *Step 2: Specify the Scanning Conditions on page 14-8*
- *Step 3: Specify the Actions on page 14-8*
- *Step 4: Specify the Priority on page 14-10*

Step 1: Specify the Route

Procedure

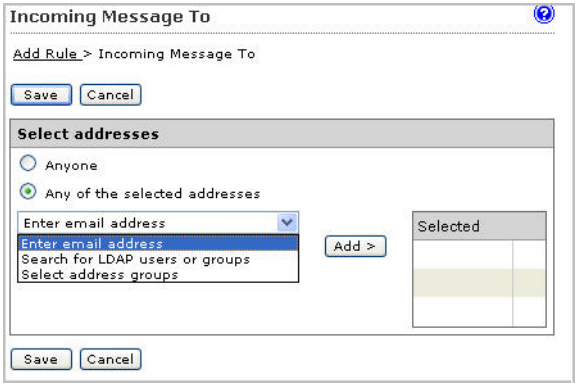
1. Go to **Policy** > **Policy List**.
2. Click **Add**.
3. Select **Other** from the drop-down list.

   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**.

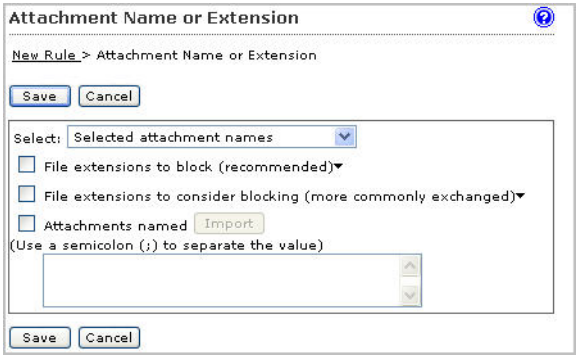
   The **Step 2: Select Scanning Conditions** screen appears.

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.

4. Click **Name or extension**.

   The **Attachment Name or Extension** screen appears.



5. Select the file extensions to block or consider blocking.

6. Click **Save**.

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

Step 3: Specify the Actions

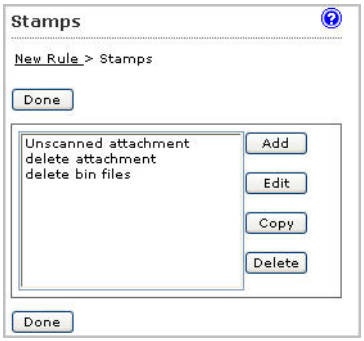
Procedure

1. Click **Next**.

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

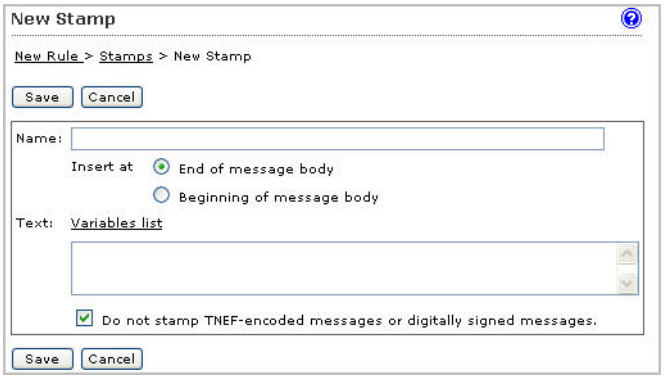
2. Under **Modify**, to enable the **Delete attachment** action, select the check box next to it.
3. Select **Matching attachment** from the drop-down list if it is not already selected.
4. Select the check box next to **Insert stamp in body**.
5. If there is no suitable stamp available from the drop-down 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 14-11*
- *Step 2: Specify the Scanning Conditions on page 14-12*
- *Step 3: Specify the Actions on page 14-15*
- *Step 4: Specify the Priority on page 14-15*

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.

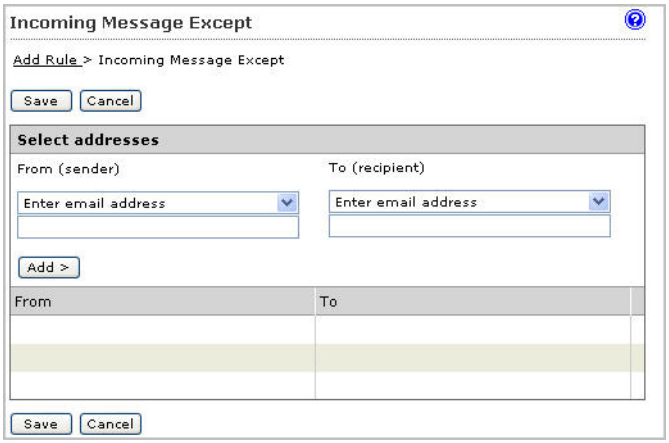
6. Select **Anyone**.

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.

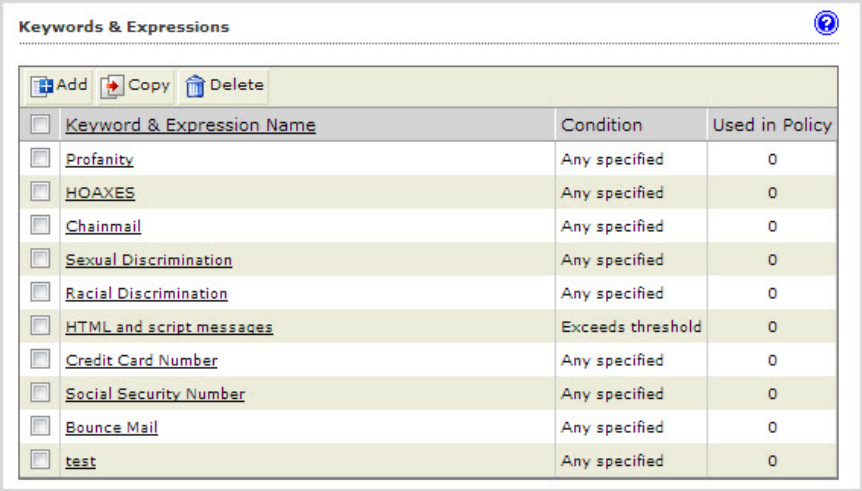
Step 2: Specify the Scanning Conditions

Procedure

1. Click **Next**.

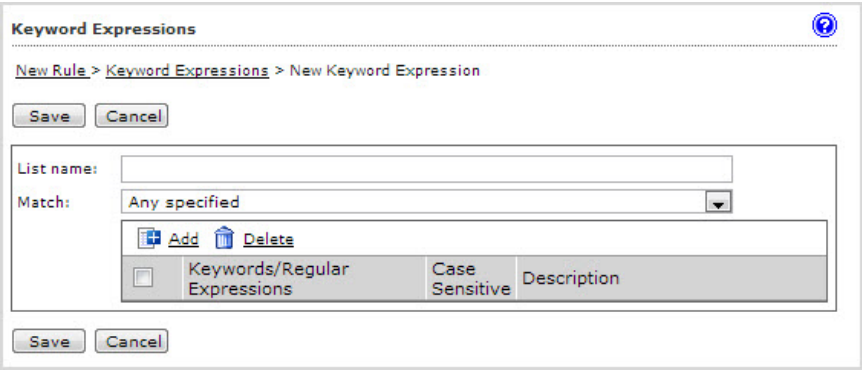
   The **Step 2: Select Scanning Conditions** screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**.

   The **Keyword Expressions** screen appears.



5. If the desired keywords are not available from the existing list, click **Add** to create a new keyword list.

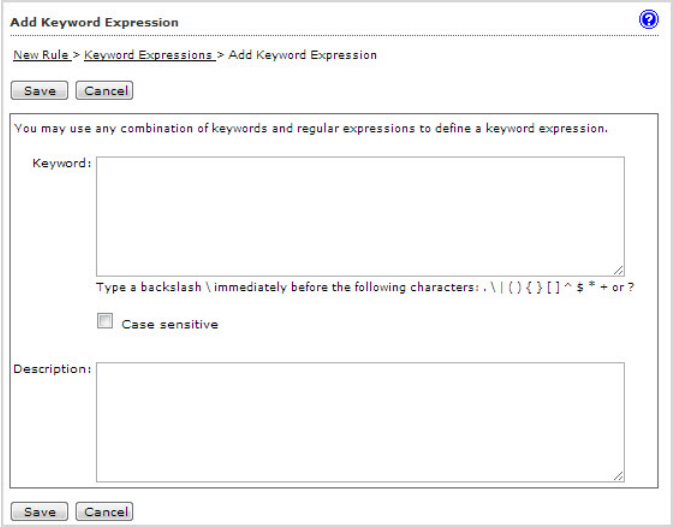
   The **New Keyword Expression** screen appears.



6. Specify the required information.

7. To add an individual keyword expression, click **Add**.

   The **Add Keyword Expressions** screen appears.



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.

10. 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.

11. Select the new list and click **>>** to insert the list into the Selected box.

12. Click **Save**.

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

13. To enable the **Body Keyword Expression** condition, select the check box next to it.

14. Click **Body Keyword Expression**.

    The **Keyword Expressions** screen appears.

15. Select the new keyword list and click **>>** to insert the list into the Selected box.

16. Click **Save**.

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

    Ensure that both the Subject keyword and Body keyword expressions are selected.

Step 3: Specify the Actions

Procedure

1. Click **Next**.

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

2. 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.

Chapter 15

Scanning Exceptions

This chapter provides instructions for managing IMSS scanning exceptions.

Topics include:

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 19-2*.
Handoff	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: • 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.

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 11-23*.
Archive	Archive the message to an archive area. For instructions on creating a new archive area, see *Configuring Quarantine and Archive Settings on page 19-2*.
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 19-2*.
Handoff	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: • 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. **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.

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 11-23*.
Archive	Archive the message to an archive area. For instructions on creating a new archive area, see *Configuring Quarantine and Archive Settings on page 19-2*.
BCC	Blind carbon copy the message to another recipient. Specify the recipient's email address and separate multiple addresses with

Option	Description
	a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

4. Click **Save**.

Part IV

Monitoring the Network

Chapter 16

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 16-2*
- *Viewing System Status on page 16-2*

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: 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: a. Select the check box next to the component to update. b. Click **Update**. To roll back to the previous version of the components: a. Select the check box next to the component to roll back.

OPTION	DESCRIPTION
	b. Click **Rollback**. To refresh the page: • Click **Refresh** to connect to the update source and display the latest component versions in the Availability column.
Managed Server Settings	View other IMSS services registered to this IMSS admin database. To start or stop managed server services: • Click **Start** or **Stop** under the service to change. To unregister managed server services: • 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**. **Note** A managed service could become disconnected for any of the following reasons: • 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.

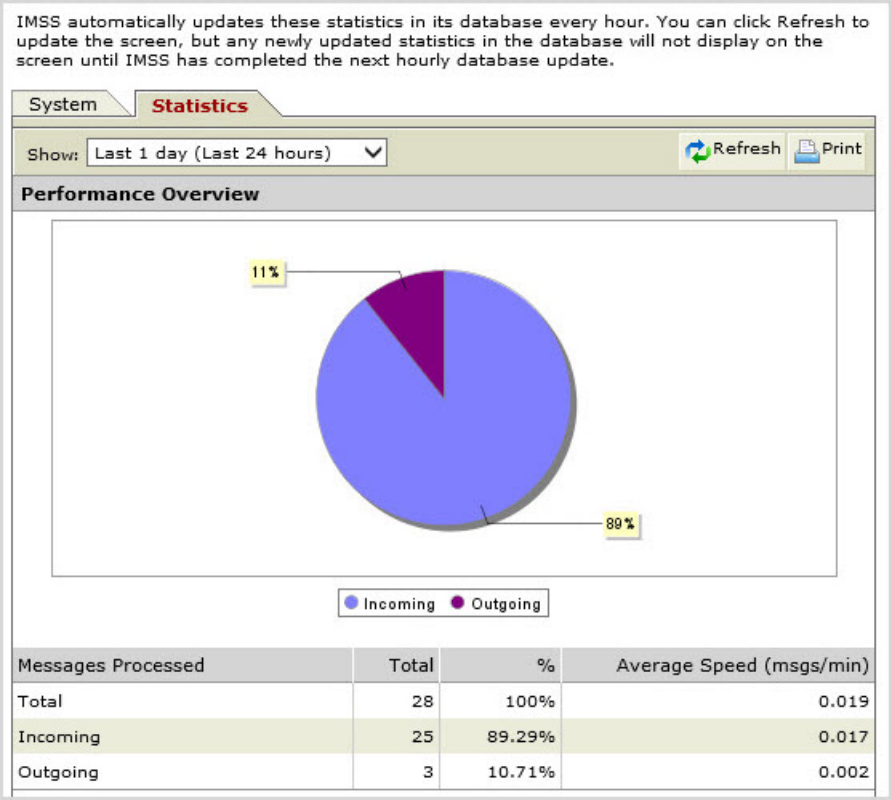
Note

- 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



Messages Processed	Total	%	Average Speed (msgs/min)
Total	28	100%	0.019
Incoming	25	89.29%	0.017
Outgoing	3	10.71%	0.002

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: 17% = 5 / 30

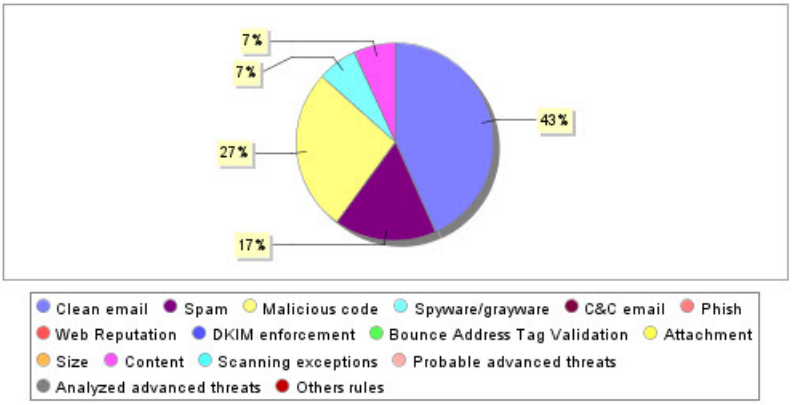
- Table

  Value = Number of messages matching the specific scanning condition divided by the total number of messages processed.

  Example:

  Percentage of spam messages: 17.86% = 5 / 28

Scan Performance



Scanning Conditions	Total	%
Clean email	13	46.43%
Spam	5	17.86%
Malicious code	8	28.57%
Spyware/grayware	2	7.14%
C&C email	0	0%
Phish	0	0%
Web Reputation	0	0%
DKIM enforcement	0	0%
Bounce Address Tag Validation	0	0%
Attachment	0	0%
Size	0	0%
Content	2	7.14%
Scanning exceptions	0	0%
Probable advanced threats	0	0%
Analyzed advanced threats	0	0%
Others rules	0	0%

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:

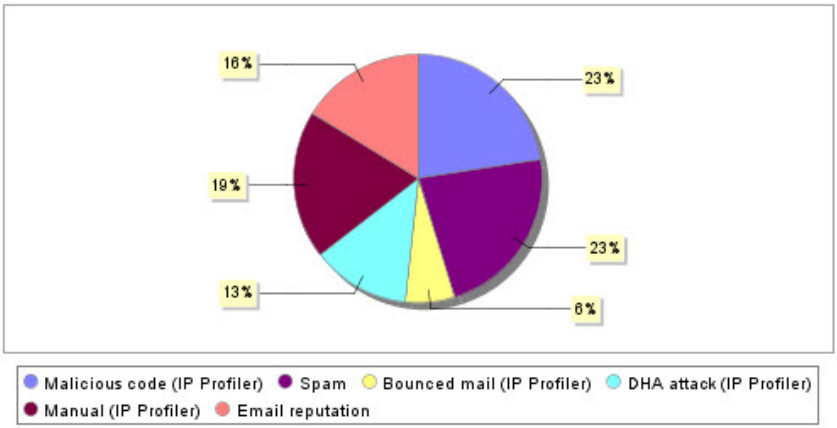
Value = Number of messages matching the specific IP filtering rule divided by the total number of messages blocked by IP Profiler and ERS.

Example:

Total number of messages blocked by IP Profiler and ERS = 12

Percentage of spam messages: 58.33% = 7 / 12

IP Filtering Performance



IP Filtering Type	Total Blocked Connection	Blocked %
Total	12	100%
Spam (IP Profiler)	7	58.33%
Malicious code (IP Profiler)	7	58.33%
DHA attack (IP Profiler)	4	33.33%
Bounced mail (IP Profiler)	2	16.67%
Manual (IP Profiler)	6	50%
Email reputation	5	41.67%

Chapter 17

Reports

This section provides information on generating one time and scheduled reports.

Topics include:

- *Generating Reports on page 17-2*
- *Managing One-time Reports on page 17-4*
- *Accessing Scheduled Reports on page 17-9*

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 17-1. Summary Reports

REPORT CONTENT	DESCRIPTIONS
Policy and traffic summary	Shows the total number and size of incoming and outgoing messages. Also shows the number of messages matching specific scanning conditions.
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.

Report Content	Descriptions
Deep Discovery Advisor analysis summary	Shows the total number of analyzed advanced threats by risk level. **Note** Deep Discovery Advisor may not return a risk level if: • A server or connection error occurs • The attachment's file type is unsupported • Analysis has not been completed

Table 17-2. 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.

Report Content	Descriptions
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 C&C email recipients and senders	Top 10 recipients and senders of C&C email based on the addresses used in the SMTP session

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.

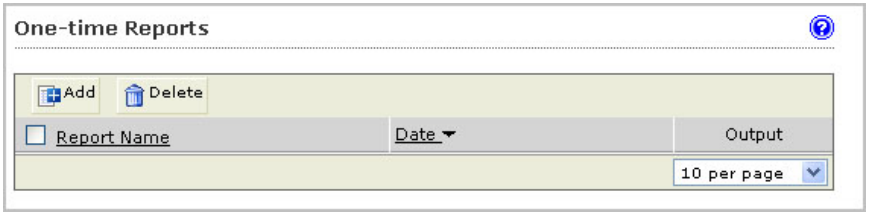
- To delete a report, select the check box next to it and click **Delete**.

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**.

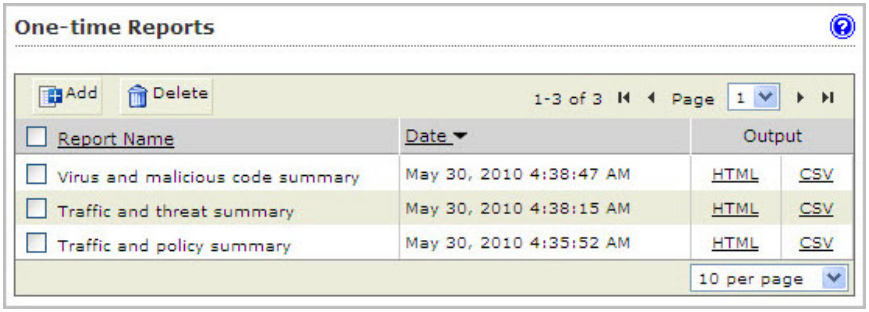
   The **Add One-time Report** screen appears. For a list of available reports, see *Types of Report Content on page 17-2*.

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.

After the report generates, the hyperlinks **HTML** and **CSV** display in the report table.



4. 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.

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**).

Report Content

Summary Reports

- Policy and traffic summary
- Virus and malicious code summary
- Spam summary
- Sender IP address blocking summary
- Deep Discovery Advisor analysis summary

Top 10 Reports

- 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 17-2*.

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.

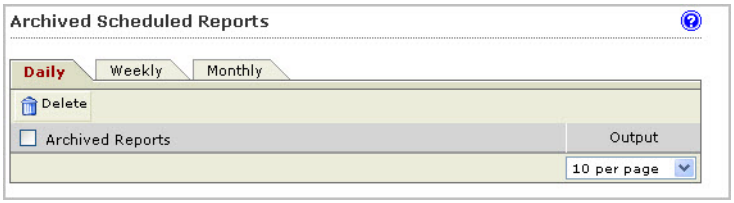
6. Click **Save**.

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 17-9* 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 17-10*.

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 18

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 18-2*
- *Configuring Log Settings on page 18-2*
- *Querying Logs on page 18-4*

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 18-2*
- **Step 2**: *Querying Logs on page 18-4*

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.

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 `IMSS\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 five types of events or information:

Message tracking

Records message details such as the sender, recipient(s), message size, 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

Tracks the time of system events such as user access, modification of rules, registration of MCP agent and so on.

Policy events

Provides details on the policy rules that were triggered, the actions taken, and the message details.

MTA events

Provides connection details of MTA 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).

Note

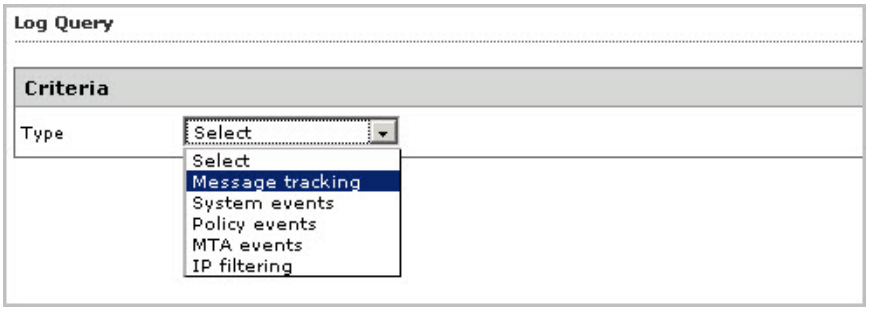
The data `<server name>[127.0.0.1]`, from returned queries, indicates the default DNS server.

Querying Message Tracking Logs

Procedure

1. Go to **Logs** > **Query**.

   The **Log Query** screen appears.



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)**

   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**
   - **Message size**
   - **Message ID**
   - **Scanner**
   - **Scanner that detected the message**
   - **Final action that IMSS took on the message**
   - **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.
   - **Admin activity**: Displays the timestamp and descriptions for major admin activities such as changing IMSS settings, admin account log on and log off.

     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. Next to **Description**, specify any special words to search for.
7. Click **Display Log**.

   A timestamp, component, and description appear for each event.
8. 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**.

Viewing 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**
   - **Probable advanced threats**
   - **Spam/phish**
   - **C&C email**
   - **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.
   - **DKIM enforcement**
   - **Bounce Address Tag Validation**
   - **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**

     Note

     If ATSE is enabled, IMSS adds the **Probable advanced threat** option for **Rule type**. If both ATSE and Deep Discovery Advisor are enabled, IMSS adds the **Probable advanced threat** or **Analyzed advanced threat** option for **Rule type**.

   - **Rule(s)**
   - **Action**

Note

If both ATSE and Deep Discovery Advisor are enabled, IMSS adds an option about the status of Deep Discovery Advisor analysis for **Action**.

- **Message ID**
- **Internal ID**
- **Scanner**

Note

If both ATSE and Deep Discovery Advisor are enabled, IMSS adds **Risk rating** to show the risk level for the entire message received from Deep Discovery Advisor.

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 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. Next to **Message ID**, specify the Message ID to search for.

5. Click **Display Log**.

   A timestamp, action, rule, and message ID appear for each event.

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 **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**
   - **Email reputation**
   - **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 19

Mail Areas and Queues

This chapter provides information about IMSS archive areas and mail queues.

Topics include:

- *About Mail Areas and Queues on page 19-2*
- *Configuring Quarantine and Archive Settings on page 19-2*
- *Managing Quarantine Areas on page 19-4*
- *Managing Archive Areas on page 19-7*
- *Querying Messages on page 19-10*
- *Viewing Quarantined Messages on page 19-15*
- *Viewing Archived Messages on page 19-16*
- *Viewing Deferred Messages on page 19-17*
- *Configuring User Quarantine Access on page 19-18*
- *Adding/Removing an EUQ Database on page 19-21*
- *Removing an EUQ Database on page 19-22*
- *Command-line Options for euqtrans Tool on page 19-23*

About Mail Areas and Queues

IMSS stores messages matching specific policy rule actions in the following areas and queues:

- **Quarantine Area**: Stores messages that you would like to analyze before deciding whether to delete or release to the intended recipient(s).
- **Archive Area**: Stores messages for future reference.
- **Deferred Queue**: Stores messages that IMSS is unable to deliver to the next MTA. IMSS tries to resend the message after 30 minutes and every five minutes thereafter. If IMSS is still unable to deliver the message after 10 retries, the message will be returned to the sender.

Note

In order to use End-User Quarantine, first configure the LDAP settings. For more information, see *Configuring LDAP Settings on page 3-7*.

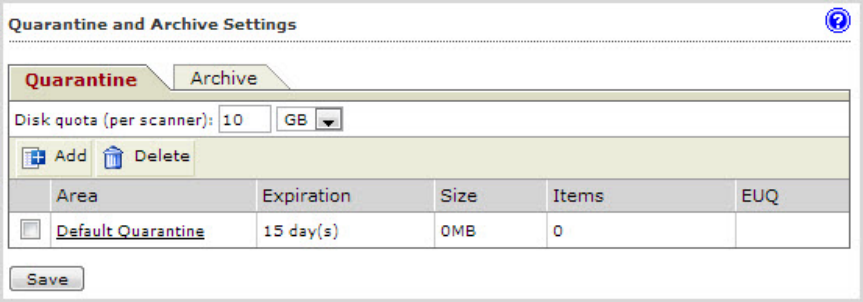
Configuring Quarantine and Archive Settings

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 **Mail Areas & Queues** > **Settings**.

The **Quarantine and Archive Settings** screen appears.



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 .

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 **Mail Areas & Queues** > **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**.

   Note

   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.

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.

7. Click **Save** to return to the **Mail Areas & Queues Management** 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. 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 **Archives** screen.

7. Click **Done** to continue selecting actions.

8. 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 **Mail Areas & Queues** > **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**.

Note

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. 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.

8. Click **Save** to return to the **Mail Areas & Queues Management** screen.

9. Click **Save**.

Querying Messages

You can perform a query on quarantined, archived, or deferred messages before deciding which action to perform. After viewing the message details, you can 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 **Mail Areas & Queues** > **Query**.

   The **Mail Areas & Queues Management** screen appears. The **Quarantine** tab displays by default. If it does not display, click **Quarantine**.

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 **Mail Areas & Queues** > **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.

Querying Deferred Messages

Procedure

1. Navigate to **Mail Areas & Queues** > **Query**.

   The **Quarantine** tab displays by default.
2. Click the **Deferred** tab.
3. Under **Criteria**, configure the following:
   - **Search**: Select the scanner that scanned the message.

- **Dates**: Select a date and time range.

4. Specify values for the following:
   - **Sender**
   - **Recipient(s)**
   - **Message ID**
   - **Reason**
5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, the reason for deferring the message, the host (or device), and the next retry time.
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 postponed message, click the **Timestamp** for the item. The message and all of its details appears.
8. To resend any message, click the check box next to it in the query result table, and then click **Retry**.
9. To delete any message, click the check box next to it in the query result table, and then click **Delete**.
10. To delete any message and send a non-delivery report (NDR) message, click the check box next to the message in the query result table, and then click **Delete with NDR**.

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.

Viewing Deferred Messages

All messages that IMSS defers can be queried and viewed.

Procedure

1. After you perform a query for deferred messages, click the timestamp for the deferred item in the query result table. The query screen appears showing the following information:
   - **Timestamp**
   - **Sender**
   - **Recipient**
   - **Host**
   - **Message ID**

   Each recipient and corresponding reason or the message's delivery history appear at the bottom of the screen.

2. Perform any of the additional actions:

- To change the number of items that appears on a page at one time, select a new display value from the **Display** drop-down box on the upper right of the list.
- To move to another page, select a number from the drop-down box to the right, or click one of the arrow icons.

3. Click any of the following buttons:
   - **Back to List**: Return to the query screen.
   - **Retry**: Resend the message to its original recipients.
   - **Delete**: Delete the message.
   - **Delete with NDR**: Delete the message and send a message to the recipient informing them of the deferred message.

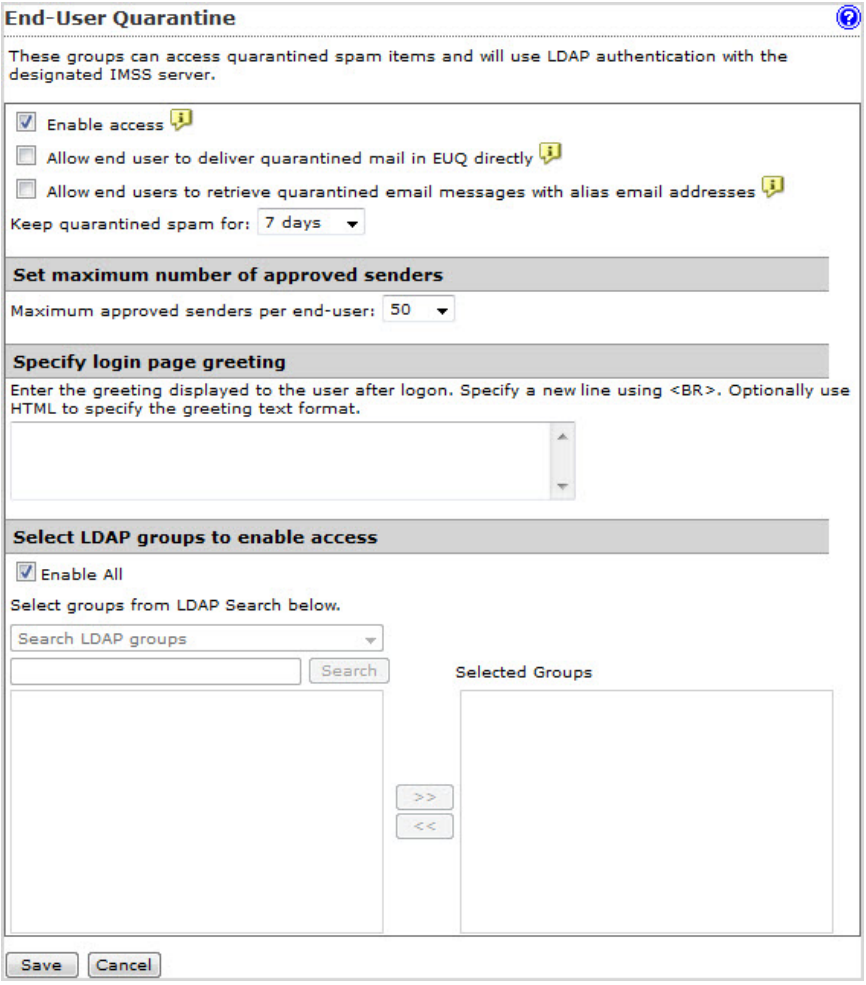
Configuring User Quarantine Access

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**.

The **End-User Quarantine** screen appears.



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**.

Note

When enabling user quarantine access for an LDAP group, you can use wildcards in 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, *A* are all allowed. If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A, *A* are not allowed.

Adding/Removing 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

Alternatively, you may choose to reduce the number of EUQ databases.

Adding an EUQ Database

Perform the following to add an EUQ database.

- **Step 1**: *Registering an EUQ Database on page 19-21*
- **Step 2**: *Rebuilding End-User Data on page 19-22*

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**.

Rebuilding End-User Data

To retain the original end-user's data, run the `euqtrans` script from the `<IMSS>\bin` directory of the Central Controller to re-balance the EUQ databases. This script does the following:

- Transfer the Approved List
- Transfer information about the quarantined emails

Note

If you do not run the `euqtrans` script after adding the new EUQ Database, some previously quarantined mail messages may not be available to the end users.

Removing an EUQ Database

Perform the following to remove an EUQ database.

- **Step 1**: *Unregistering an EUQ Database on page 19-23*

- **Step 2**: *Rebuilding End-User Data on page 19-23*

Unregistering an EUQ Database

You can unregister but not delete the EUQ database from the system through the web management console. Unregistering a database means that the database will still exist, but it will not be used by IMSS.

Procedure

1. Go to **Administration** > **IMSS Configuration** > **Connections** from the menu.

   The **Components** tab appears by default.

2. Click the **Database** tab.
3. Select the check box next to the unwanted EUQ database server.
4. Click **Unregister**.
5. Click **OK** to confirm the unregistration.

Rebuilding End-User Data

Run the `euqtrans` script from the `<IMSS>\bin` directory of the Central Controller to move the Approved Senders List and information about the quarantined mail messages from this database to other databases and re-balance the other databases.

Command-line Options for euqtrans Tool

The following table explains the command-line options for the `euqtrans` script.

TABLE 19-1. 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 20

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 20-2*
- *Configuring Delivery Settings on page 20-3*
- *Configuring Event Criteria and Notification Message on page 20-5*
- *EUQ Digest on page 20-7*
- *Editing Notifications on page 20-8*

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 20-1. 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 4-7*.
Scanner Update Result	Alerts you when IMSS is unable to update the engine or pattern files on any scanner.
Deep Discovery Advisor Settings	Alerts you when Deep Discovery Advisor analysis is incomplete or invalid.
Smart Scan Event	Alerts you when IMSS reverts to Conventional Scan after an unsuccessful attempt to connect to the Smart Protection Network.

Configuring Delivery Settings

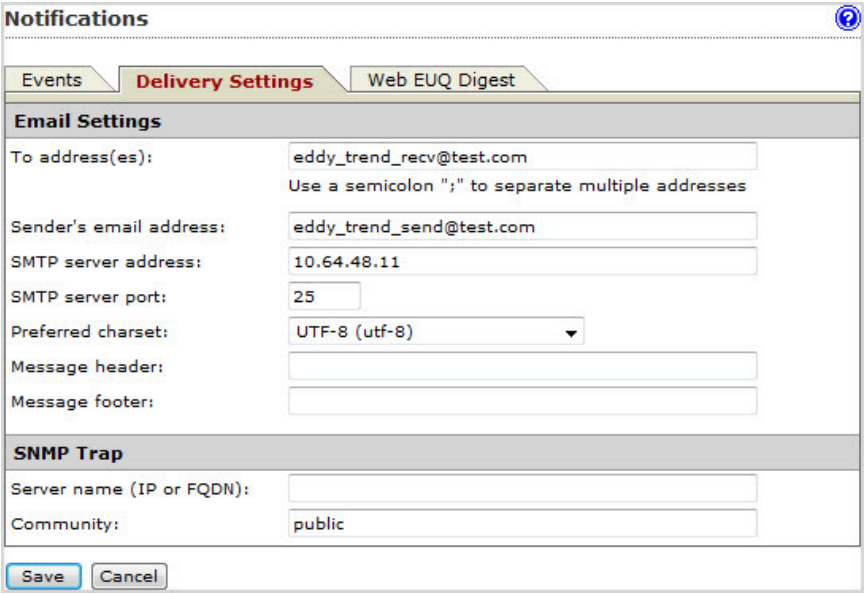
The delivery settings allow you to specify email and SNMP trap settings to deliver system and policy event notification messages.

Procedure

1. Go to **Administration** > **Notifications**.

   The **Events** tab appears by default.

2. Click the **Delivery Settings** tab.



3. Under **Email Settings**, configure the following:

   - **To address(es)**: 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	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. **Note** SNMP servers do not support IPv6-formatted addresses.
Community	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.

5. Click **Save**.

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

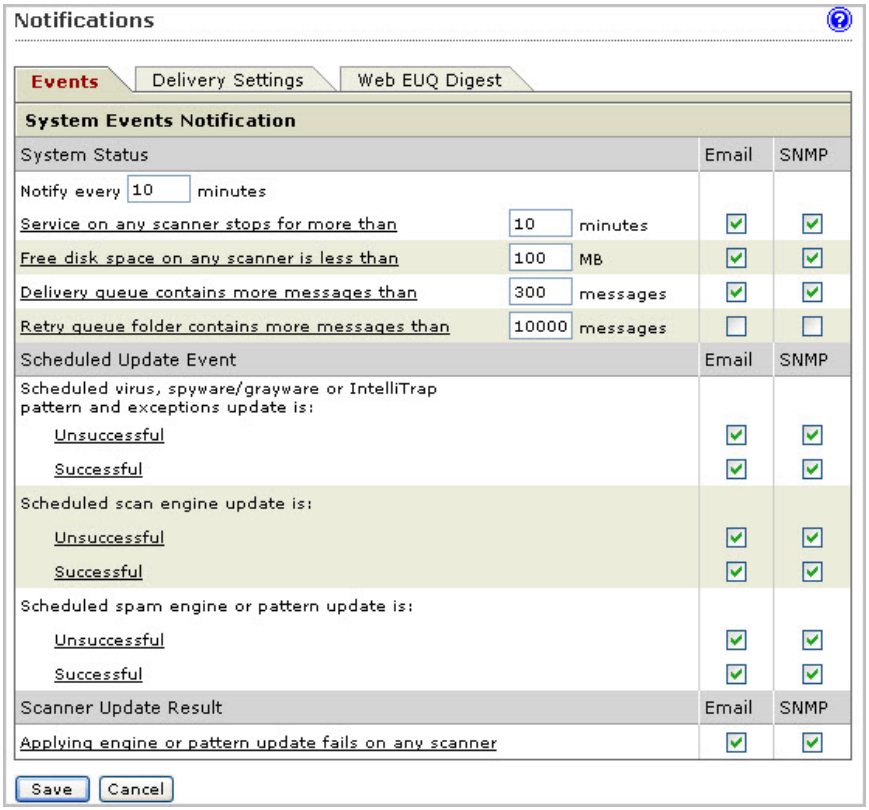
Configuring Event Criteria and Notification Message

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.



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.
   - **Scan queue contains more than**: Specify the number of messages.

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 **Deep Discovery Advisor Settings**, click the **Message analysis is incomplete or invalid** link to edit the notification.

   This notification describes the breakdown in communication between IMSS and Deep Discovery Advisor. IMSS may send this notification because of:

   - A file or database operation error
   - A client, server, or network connection error
   - An invalid analysis report

6. 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.

7. Select the **Email** and/or **SNMP** check boxes according to how you would like to receive the notification.
8. 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**.

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 21

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 21-2*
- *Backing Up IMSS on page 21-3*
- *Restoring Settings with the Backup Database on page 21-6*
- *Replicating Settings on page 21-10*

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 7.5 server . You can also replicate a configuration across several IMSS 7.5 servers by importing the same configuration file into the desired servers.

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.
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

IMSS stores all configuration settings in the admin database (default database "imss"). This section describes how to back up the configurations in the admin database, as well as how to restore all settings.

Backing Up the Admin Database

Procedure

1. Log on as the database administrator:
   a. Open SQL Query Analyzer (for example, SQL 2000 server).
   b. Connect to the database server where the IMSS admin database is installed.

c. Log on as user "sa".

2. Create a backup database named `imss_bak` by running the following SQL script:

```
USE master
GO
IF EXISTS (SELECT * FROM   master..sysdatabases
WHERE  name = 'imss_bak')
DROP DATABASE imss_bak
GO
CREATE DATABASE imss_bak
GO
```

3. Back up configuration tables to the backup database `imss_bak` by running the following SQL scripts:

```
SELECT * into imss_bak..tb_global_setting
FROM imss..tb_global_setting
SELECT * into imss_bak..tb_named_obj
FROM imss..tb_named_obj
SELECT * into imss_bak..tb_entity
FROM imss..tb_entity
SELECT * into imss_bak..tb_policy
FROM imss..tb_policy
SELECT * into imss_bak..tb_rule
FROM imss..tb_rule
SELECT * into imss_bak..tb_scanning_exceptions
FROM imss..tb_scanning_exceptions
SELECT * into imss_bak..tb_version_number
FROM imss..tb_version_number
SELECT * into imss_bak..tb_entity_rule
FROM imss..tb_entity_rule
SELECT * into imss_bak..tb_named_obj_rule
FROM imss..tb_named_obj_rule
SELECT * into imss_bak..tb_report_tickets
FROM imss..tb_report_tickets
SELECT * into imss_bak..tb_euq_entity
FROM imss..tb_euq_entity
SELECT * into imss_bak..t_foxhuntersetting
FROM imss..t_foxhuntersetting
```

```
SELECT * into imss_bak..t_type_setting
FROM imss..t_type_setting
SELECT * into imss_bak..tb_administrator
FROM imss..tb_administrator
SELECT * into imss_bak..tb_inter_addr
FROM imss..tb_inter_addr
SELECT * into imss_bak..tb_named_obj_scan_exception
FROM imss..tb_named_obj_scan_exception
SELECT * into imss_bak..tb_report_setting
FROM imss..tb_report_setting
SELECT * into imss_bak..tb_mta_config
FROM imss..tb_mta_config
SELECT * into imss_bak..t_iprule
FROM imss..t_iprule
SELECT * into imss_bak..t_manual_domain
FROM imss..t_manual_domain
SELECT * into imss_bak..tb_component_list
FROM imss..tb_component_list
GO
```

4. Back up the `imss_bak` database by running the following SQL script:

```
BACKUP DATABASE imss_bak TO DISK= 'c:\imss_bak.bak'
GO
```

Note

If you encounter "Operating System Error 5", create a folder named `backup` on disk C where the IMSS admin database is installed and then run the following SQL script:

```
BACKUP DATABASE imss_bak TO DISK= 'c:\backup\imss_bak.bak'
GO
```

Deleting a Backup Database

Procedure

- Drop the database `imss_bak` by running the following SQL script:

```
drop database imss_bak
go
```

Restoring Settings with the Backup Database

Procedure

1. Log on as database administrator:
   a. Open an SQL Query Analyzer.
   b. Log on as sa.
2. Restore the `imss_bak` file by executing the following SQL script:

```
Use master
GO
RESTORE DATABASE imss_bak FROM DISK = 'c:\imss_bak.bak'
GO
```

3. Stop all IMSS related services.
4. Delete the configuration tables in the IMSS database by running the following SQL script:

```
USE imss
GO
DELETE FROM tb_global_setting
DELETE FROM tb_component_list
DELETE FROM t_manual_domain
DELETE FROM t_iprule
DELETE FROM tb_mta_config
DELETE FROM tb_report_setting
DELETE FROM tb_named_obj_scan_exception
DELETE FROM tb_inter_addr
DELETE FROM tb_administrator
```

```
DELETE FROM t_type_setting
DELETE FROM t_foxhuntersetting
DELETE FROM tb_euq_entity
DELETE FROM tb_report_tickets
DELETE FROM tb_named_obj_rule
DELETE FROM tb_entity_rule
DELETE FROM tb_version_number
DELETE FROM tb_scanning_exceptions
DELETE FROM tb_rule
DELETE FROM tb_policy
DELETE FROM tb_entity
DELETE FROM tb_named_obj
GO
```

5. Copy configuration tables from the backup database `imss_bak` by running the following SQL scripts:

```
INSERT INTO imss..tb_global_setting
SELECT *
FROM imss_bak..tb_global_setting
GO
SET IDENTITY_INSERT imss..tb_named_obj on
GO
INSERT INTO imss..tb_named_obj(id,type,name,
content,msg_count,msg_size )
SELECT * FROM imss_bak..tb_named_obj
GO
SET IDENTITY_INSERT imss..tb_named_obj off
GO
SET IDENTITY_INSERT imss..tb_entity on
GO
INSERT INTO imss..tb_entity(entity_id,entity_type,
entity_name, root_entity)
SELECT * FROM imss_bak..tb_entity
SET IDENTITY_INSERT imss..tb_entity off
GO
SET IDENTITY_INSERT imss..tb_policy on
GO
INSERT INTO imss..tb_policy
(policy_id,policy_name,policy_type,is_enable,
is_default,is_hidden,create_by,modify_by,
```

```
creation_time,last_modified_time)
SELECT * FROM imss_bak..tb_policy
GO
SET IDENTITY_INSERT imss..tb_policy off
GO
SET IDENTITY_INSERT imss..tb_rule on
GO
INSERT INTO imss..tb_rule( rule_id, policy_id,
version_number, rule_name, active_time, rule_type,
display_action, has_multi_actions,
has_virus_filter, has_spam_filter,
has_attachment_filter, has_content_filter,
has_size_filter, has_time_range_filter,
has_other_filter, note, rule_value, rule_order,
has_wrs_filter)
SELECT * FROM imss_bak..tb_rule
GO
SET IDENTITY_INSERT imss..tb_rule off
GO
INSERT INTO imss..tb_scanning_exceptions
SELECT * FROM imss_bak..tb_scanning_exceptions
GO
INSERT INTO imss..tb_version_number
SELECT * FROM imss_bak..tb_version_number
GO
INSERT INTO imss..tb_entity_rule
SELECT * FROM imss_bak..tb_entity_rule
GO
INSERT INTO imss..tb_named_obj_rule
SELECT * FROM imss_bak..tb_named_obj_rule
GO
SET IDENTITY_INSERT imss..tb_report_tickets on
GO
INSERT INTO imss..tb_report_tickets( ticket_id,
admin_id, report_type, request_timestamp,
report_name, report_status, scanner_name,
report_item, report_start_day, reset_column,
time_start, time_end, run_today, isenabled )
SELECT * FROM imss_bak..tb_report_tickets
SET IDENTITY_INSERT imss..tb_report_tickets off
GO
SET IDENTITY_INSERT imss..tb_euq_entity on
```

```
GO
INSERT INTO imss..tb_euq_entity(entity_id,entity_name)
SELECT * FROM imss_bak..tb_euq_entity
GO
    SET IDENTITY_INSERT imss..tb_euq_entity off
GO
INSERT INTO imss..t_foxhuntersetting
SELECT * FROM imss_bak..t_foxhuntersetting
INSERT INTO imss..t_type_setting
SELECT * FROM imss_bak..t_type_setting
SET IDENTITY_INSERT imss..tb_administrator on
GO
INSERT INTO imss..tb_administrator( admin_id,
admin_name, enabled, using_imss_auth,
own_root_entity, md5_digest, summary_permission,
policy_permission, ipfiltering_permission,
reports_permission, logs_permission,
quarantines_permission, system_permission )
SELECT * FROM imss_bak..tb_administrator
GO
SET IDENTITY_INSERT imss..tb_administrator off
GO
INSERT INTO imss..tb_inter_addr
SELECT * FROM imss_bak..tb_inter_addr
GO
INSERT INTO imss..tb_named_obj_scan_exception
SELECT * FROM imss_bak..tb_named_obj_scan_exception
GO
INSERT INTO imss..tb_report_setting
SELECT * FROM imss_bak..tb_report_setting
GO
INSERT INTO imss..tb_mta_config
SELECT * FROM imss_bak..tb_mta_config
GO
INSERT INTO imss..t_iprule
SELECT * FROM imss_bak..t_iprule
GO
INSERT INTO imss..t_manual_domain
SELECT * FROM imss_bak..t_manual_domain
GO
SET IDENTITY_INSERT imss..tb_component_list on
GO
```

```
INSERT INTO imss..tb_component_list( scanner_id,
scanner_name, ip_addr, daemon, policy, euq, nrs,
ipprofiler, euq_port, admin_cmd, app_ver)
SELECT * FROM imss_bak..tb_component_list
GO
SET IDENTITY_INSERT imss..tb_component_list off
GO
```

6. Start all IMSS 7.5 services.

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 21-3*.

- **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.

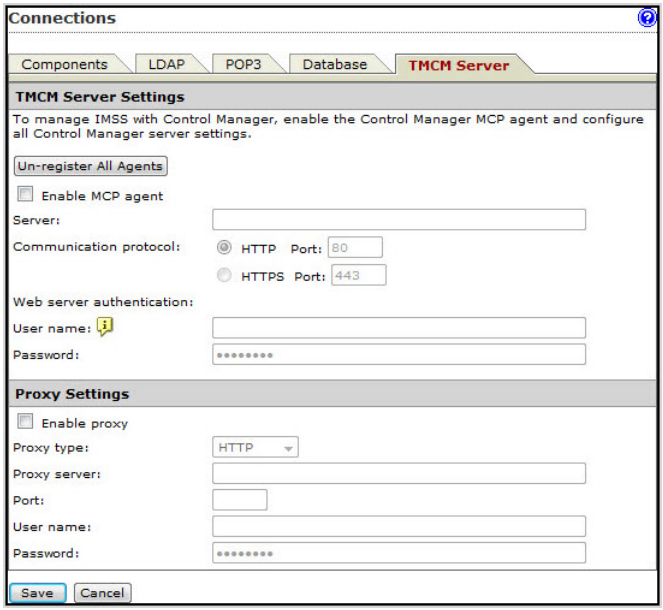
Procedure

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

   The **Components** tab appears by default.

2. Click the **TMCM Server** tab.

   The **TMCM Server Settings** screen appears.



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 22

Using End-User Quarantine

This chapter explains how to use End-User Quarantine (EUQ).

Topics include:

- *About EUQ on page 22-2*
- *EUQ Authentication on page 22-2*
- *Configuring End-User Quarantine (EUQ) on page 22-2*
- *Disabling EUQ on page 22-8*

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 3-7*.

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. *Configuring and Enabling LDAP on page 22-3*
2. *Enabling EUQ on page 22-4*
3. *Starting the EUQ Service on page 22-5*
4. *Enabling End-User Access on page 22-6*

5. *Opening the End-User Quarantine Management Console Remotely on page 22-7*

Configuring and Enabling LDAP

You must configure and enable LDAP to use EUQ.

Procedure

1. You can configure and enable LDAP settings in the following ways:
   - Go to **Administration** > **IMSS Configuration** > **Connections** from the menu, then click the **LDAP** tab.
   - Go to **Administration** > **IMSS Configuration** > **Configuration Wizard** from the menu.
2. Configure the options under **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.
3. 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.
4. Configure the options under **LDAP admin** .
   a. 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 22-1. 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

b. 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.

5. Click **Save**.

Enabling EUQ

After configuring LDAP settings, enable and configure EUQ settings.

Enabling EUQ requires one of the following authentication methods:

- LDAP

For details about EUQ authentication, see *EUQ Authentication on page 22-2*.

Procedure

1. Go to **Administration** > **End-User Quarantine**.

   The **User Quarantine Access** screen appears.

2. Select **Enable access**.

   Note

   After enabling EUQ, the EUQ service starts automatically. To manually start the service, see *Starting the EUQ Service on page 22-5*.

3. 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 22-5*.

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 **EUQ Service**

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 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.

Procedure

1. Go to **Administration** > **End-User Quarantine**.

   The **End-User Quarantine** screen appears.

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.

6. Select the maximum number of approved senders for each end-user.

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**.

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 22-2. EUQ Logon Name Formats

AUTHENTICATION TYPE	LOGON NAME FORMAT

LDAP	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.
	• **Domino**: user1/domain
	• **Microsoft Active Directory**
	  • 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`

Disabling EUQ

Before disabling EUQ, inform your users that they should manage their quarantined spam.

Procedure

1. Go to **Administration** > **End-User Quarantine**.
2. Deselect the **Enable access** check box.
3. Click **Save**.

Chapter 23

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 23-2*
- *Configuring Connection Settings on page 23-6*

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.

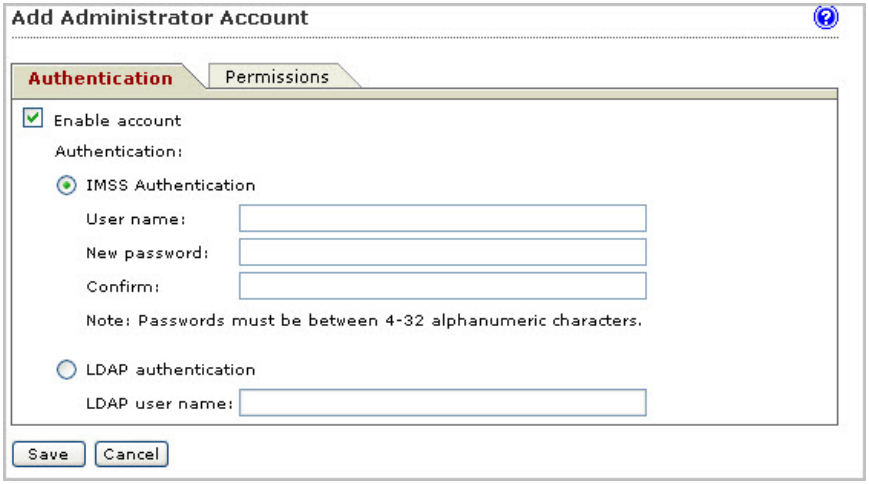
Procedure

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.



3. Specify authentication settings:

   a. Select **Enable account**.

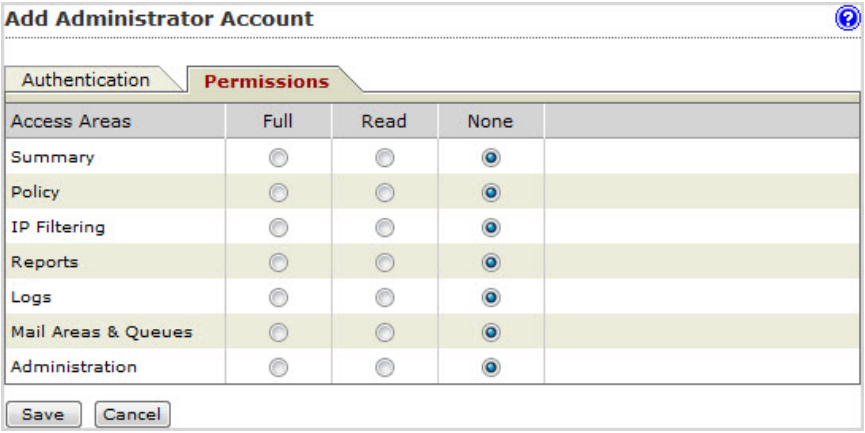
   b. Select an authentication type:

      - **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.



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.

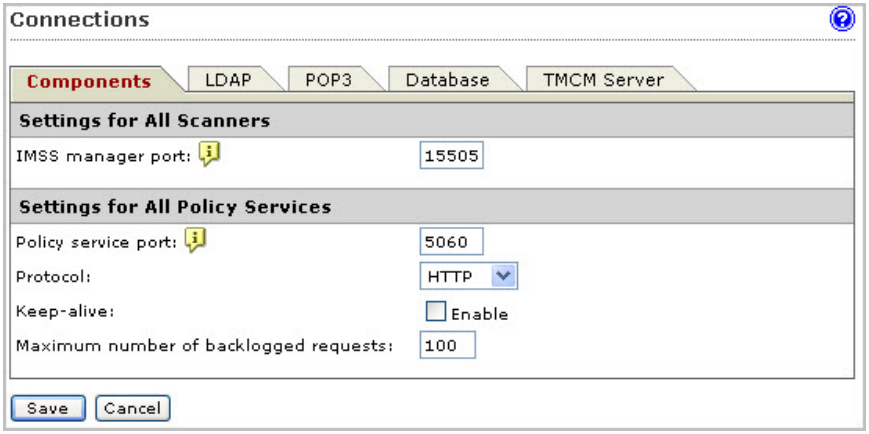
Configuring Connection Settings

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.



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** > **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 23-1. 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.

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 TMCM Settings

To use Trend Micro Control Manager (TMCM) 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 **TMCM Server** tab.

3. Under **TMCM 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.
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.

OPTION	DESCRIPTION
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 **TMCM 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 23-16*.

Component Descriptions

IMSS can use the following components:

Component	Description
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
IP Filtering Service	Automatically blocks known spam senders. IP Filtering includes the following: • **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: • **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-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 24

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 24-2*
- *Frequently Asked Questions on page 24-12*
- *Support Information on page 24-35*

Troubleshooting

For common issues that you might encounter when configuring or administering IMSS, see *Troubleshooting Issues on page 24-2*. 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.	The target port is not in the firewall approved list. Open the ports as shown in *IMSS Ports on page 24-8* in the firewall. If you are unable to access the management console, do the following: 1. Start the database service. 2. If you are still unable to access the management console, restart the IMSS management console from the System Service Manager.
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 imssps daemon is running but refusing connections.	If the imssps 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
Unable to activate products (Antivirus/eManager, SPS, Email Reputation, IP Filtering) or update components	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. **To verify your DNS server settings:** • Use the following command: `nslookup licenseupdate.trendmicro.com` The command should return the IP address of the Trend Micro license update server. 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. **To verify your proxy settings from the management console:** 1. Go to **Administration** > **Updates**. The **Schedule** tab displays by default. 2. Click the **Source** tab. 3. Configure the proxy settings. 4. Click **Save**.
Email notifications do not properly display.	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. **To modify the character set:** 1. Go to **Administration** > **Notifications** > **Delivery Settings**. 2. 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.	A managed server could become disconnected for any of the following reasons: • The scanner was removed from your network. • The IMSS manager service has stopped. • Network connection issue has occurred. Check your firewall settings for the Manager Service listening port.
When viewing detailed information for quarantined or archived messages, attachment information is sometimes not available.	IMSS records attachment information only when the triggered rule is for an attachment. Check the reason why IMSS quarantined the message.
IMSS does not receive email messages.	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.	Web Reputation needs to query the Trend Micro Web Reputation servers. Verify the HTTP connectivity from the IMSS scanner to the external network. For Web Reputation issues, check the `wrsagent.*` files under the `{Installation_Path}\imss\log` folder.
The IMSS Monitor does not display the correct information on Windows x64 platforms.	IMSS is a 32-bit program. When installing on a 64-bit operating system, use the commands `perfmon.msc -32` or `mmc /32 perfmon.msc` to start 32-bit compatibility mode for IMSS Monitor.

Issue	Description and Resolution
Cannot add an IMSS Monitor	Verify that the IMSS SMTP Service is running. The IMSS Monitor is only available when the service starts. You can check the status from the Services console, or use the following command to start it: `net start TmImssMTA`
The Performance System Monitor cannot record IMSS 7.5 objects on 64-bit platforms.	Change the performance service image path to a 32-bit version by importing `$ProductDir\bin\SysmonLog_WOW.reg` into the registry. To change the performance service image path to a 64-bit version, import `$ProductDir\bin\SysmonLog_64B.reg` into the system registry.
End-User Quarantine Issues	
Unable to access the EUQ management console	Do the following: 1. Verify that you are using the correct URL and port number. To view the console from another computer on the network, type the following URLs: • Primary EUQ service: `https://<target server IP address>:8447` • Secondary EUQ service: `https://<target server IP address>:8446` 2. Verify that the system time of each EUQ service on your network is synchronized. The first instance of the EUQ service, the primary EUQ service, runs Apache Web Server (httpd) while listening on port 8447 (HTTPS). 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: `https://{Primary EUQ Service IP address}:8447/`

Issue	Description and Resolution
Users are unable to log on to EUQ management console	Do the following: 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: 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 22-8*.. 4. If the issue persists even after verifying the above settings, do the following: 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 `imssuieuq.yyyymmdd` located in `C:Program Files\Trend Micro\IMSS\logs` to Trend Micro's technical support.

Issue	Description and Resolution
The EUQ digest does not correctly display quarantined message information.	Verify that the correct character set is selected: 1. Go to **Administration** > **Notifications** > **Delivery Settings**. 2. Next to **Preferred charset**, select the character set that will properly display the digest information.
Some quarantined messages are not appearing on the EUQ management console	On the EUQ management console, users can only access the quarantined messages if the administrator configures EUQ to allow access. **To make quarantine areas visible to end users:** 1. Go to **Mail Areas & Queues** > **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 messages that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only)**. 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. End users cannot access malicious messages.
Cannot enable LDAP with Kerberos authentication.	Kerberos protocol requires time synchronization between the Kerberos server and IMSS. Synchronize the date/time for all computers with IMSS. Check whether the DNS server is configured correctly.
IP Filtering Issues	

Issue	Description and Resolution
FoxDNS is not functioning.	Verify that the BIND service is running: 1. Check the BIND service status from the System Services console. 2. Start the service if it is not running.
Email Reputation does not work after being enabled from the management console.	Email Reputation may not work due to the following reasons: • IP Filtering Servicewas not activated. Email Reputation shares the same Activation Code with IP Filtering Service. If IP Filtering Service was not activated, activate IP Filtering Service and then activate Email Reputation. • 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. Activate IP Filtering Service and confirm IMSS can access the Internet.
IP profiler does not block IP addresses in the Blocked List.	The changes require about one (1) minute to take effect. Wait one (1) minute before checking the list again.
Blocked IP address does not display in the Overview page	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. View the **Overview** page after an hour.

IMSS Ports

The following table outlines all ports used by IMSS in their default configuration.

TABLE 24-1. IMSS Ports

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
25	The MTA service port. The mail server will listen at this port to accept messages. This port must be opened at the firewall, or the server is not able to accept mails.	Go to **Administration** > **IMSS Configuration** > **SMTP Routing** > **Connections**.
110	IMSS scanner generic POP3 port. The scanner uses this port to accept POP3 request and scan POP3 mails for all POP3 servers.	Go to **Administration** > **IMSS Configuration** > **Configuration** > **Connections** > **POP3**.
5060	Policy Server listening port. The scanner will connect to this port to query matched rules for every message.	Go to **Administration** > **IMSS Configuration** > **Connections** > **Components**.
8005	IMSS management console server (Tomcat) management port that can handle Tomcat management command.	`{IMSS}\UI\adminUI\conf\server.xml: Server\port`
8009	EUQ management console Tomcat AJP port. This port is used to perform load balancing between several Tomcat servers and the Apache HTTP server.	`{IMSS}\UI\euqUI\conf\server.xml: Server\Service\Connector (protocol=AJP\1.3)\port`
8015	Tomcat management port that can handle Tomcat management command.	`{IMSS}\UI\euqUI\conf\server.xml:Server\port`
8445	Management console listening port. You need to open this port to log on to the management console using a web browser.	Tomcat listen port: `{IMSS}\UI\adminUI\conf\server.xml: Server\Service\Connector\port`

Port Number	Component and Role	Configuration Location
8446	EUQ service listening port.	`{IMSS}\UI\euqUI\conf\server.xml:Server\Service\Connector\port`
8447	EUQ service listening port with load balance.	`{IMSS}\UI\euqUI\conf\EUQ.conf:Listen\VirtualHost\ServerName`
10024	IMSS scanner reprocessing port. Messages released from the central quarantine area in the admin database and from the EUQ database will be sent to this port for reprocessing.	`imss.ini\[Socket_3]\proxy_port`
10026	The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated byIMSS.) All messages sent to this port will not be scanned by IMSS. Due to security considerations, the port is only bound at IMSS server's loopback interface (127.0.0.1). It is therefore not accessible from other computers. You are not required to open this port at the firewall.	`tsmtpd.ini`

Port Number	Component and Role	Configuration Location
15505	IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the management console. The manager also provides quarantine/archive query results to the management console and the EUQ management console through this port.	Go to **Administration** > **IMSS Configuration** > **Connections** > **Components**.
IMSS uses the following ports when you enable related service:		
389	LDAP server listening port.	Go to **Administration** > **IMSS Configuration** > **Connections** > **LDAP**.
80	Microsoft IIS HTTP listening port. Use this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	Go to **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server**.
443	Microsoft IIS HTTPS listening port. Use this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	Go to **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server**.
465	The MTA TLS service port.	Go to **Administration** > **IMSS Configuration** > **TLS Settings**.
88	KDC port for Kerberos realm.	Not configurable on the IMSS server.

Port Number	Component and Role	Configuration Location
53	The Bind service listening port. **WARNING!** Do not modify the port number.	Not configurable on the IMSS server.

Frequently Asked Questions

This section answers various Frequently Asked Questions.

Mail Transfer Agent

How do I modify the MTA configuration file?

Changes are applied to the local MTA component after you restart the component.

Procedure

1. Open and edit the MTA configuration file.

   ```
   %IMSS_HOME%\config\tsmtpd.ini
   ```

2. Using the command line interface, stop and restart the scanner and MTA components to apply the changes:

   ```
   net stop TmImssScan
   net stop TmImssMTA
   net start TmImssMTA
   net start TmImssScan
   ```

3. Check that the settings are applied to the MTA component.

How does IMSS process a partial email messages?

IMSS rejects partial email as a malformed message if `BypassMessagePartial=no` in the `imss.ini file` (default setting).

If the key is set to yes, IMSS will bypass the partial mails. Trend Micro does not recommend changing the item `BypassMessagePartial` to `yes` as this may cause virus leak.

How do I replace a self-signed MTA SSL certification?

Do the following:

Procedure

1. Write a configuration file. For more information, see

   http://www.openssl.org/docs/apps/req.html

2. Run the following command:

   ```
   openssl req -new -x509 -days 1460 -nodes -config
   tsmtpd.cfg -out tsmtpd.pem -keyout tsmtpd.pem
   ```

3. Upload `tsmtpd.pem` from the web management console.

4. The OpenSSL utility command line. For more information go to the following website:

   http://www.openssl.org/docs/apps/req.html

Is the SMTP AUTH feature for "Domain-based relay" and "Default relay" supported? If yes, which authentication method does IMSS support?

IMSS supports the CRAM-MD5, PLAIN and LOGIN SMTP AUTH authentication methods for "Domain-based relay" and "Default relay". However, you cannot configure the settings from the web management console. To configure the settings, set <auth>=1 to use the AUTH function and manually edit tsmtpd.ini as follows:

Syntax:

```
[SmtpClient]
# for Domain-based delivery
RelayHostCount=1
RelayHost0=trend.com:guid0
D_guid0]
UseMethod=1
SmartHostCount=1
SmartHost0=<hostname_or_ip>:<port>:<auth>:<username>:<password>
# for Default delivery
[DefaultRelay]
UseMethod=1
SmartHostCount=1
SmartHost0=<hostname_or_ip>:<port>:<auth>:<username>:<password>
```

Example:

```
[SmtpClient]
# for Domain-based delivery
RelayHostCount=1
RelayHost0=trend.com:guid0
[D_guid0]
UseMethod=1
SmartHostCount=1
SmartHost0=192.168.1.1:25:1:user1:@trend.com:
!CRYPT!66AE674C2079B2CD00CAB0D02E765970
# for Default delivery
[DefaultRelay]
UseMethod=1
```

```
SmartHostCount=1
SmartHost0=192.168.1.2:25:1:user2@trend.com:
!CRYPT!66AE674C2079B2CD00CAB0D02E765970
```

Note

Type the following command to encrypt the password before adding the encrypted password into `tsmtpd.ini`:

```
C:\Program Files\Trend Micro\IMSS\bin\password.exe <password
text>
```

SMTP Settings

Is IMSS an open relay mail server by default?

No, IMSS is not an open relay mail server by default. However, some administrative tools may incorrectly report that IMSS is an open relaymail server as IMSS allows some special characters such as the percent mark (%) and exclamatory mark (!) in email addresses. This causes some third-party administrative tools to misidentify IMSS as an open relay because some old UNIX mail server implementations treat such characters embedded in an email address as tricky source routings. You may do one of the following to prevent IMSS from being misidentified as an open relay mail server:

- Apply the settings to all IMSS servers under one central database

  If you have deployed IMSS in a distributed environment, run the following SQL statements to add new settings to the **tb_mta_config** table in the central database:

```
insert into tb_mta_config(section, name, value, inifile)
values ( 'SmtpServer', ' RestrictInDomain', '1', 'tsmtpd.ini');
```

```
insert into tb_mta_config (section, name, value, inifile)
values ( 'SmtpServer', ' RestrictInDomainMeta', ' !#$%', 'tsmtpd.ini'
```

- Apply the settings to one IMSS server

Edit `tsmtpd.ini` (located in `IMSS_INSTALL_ROOT\config\`) and remove the comments for the following keys:

```
RestrictInDomain=1
```

```
RestrictInDomainMeta=!#$%
```

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:

Procedure

1. Backup the configuration tables.
   a. Log on as database administrator.
      i. Open SQL Query Analyzer.
      ii. Log on as `sa`.
   b. Back up the IMSS database as follows:

```
BACKUP DATABASE imss TO DISK='c:\imss.bak'
GO
```

2. Restore the configuration tables.

a. Log on as database administrator.

   i. Open SQL Query Analyzer.

   ii. Log on as `sa`.

b. Restore the IMSS database as follows:

```
Use masterGO
RESTORE DATABASE imss FROM DISK=':\imss.bak'
GO
```

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.

IP Profiler

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.

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.

Is the LDAP service mandatory for analyzing whether an incoming traffic is a form of DHA attack?

Yes, the LDAP service is required for analyzing whether incoming traffic is a form of DHA attack.

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 24-2. Search for email addresses

EXAMPLE	DESCRIPTION
*	Valid representation of all email addresses.

EXAMPLE	DESCRIPTION
@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 24-3. 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** inIMSS 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.

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. Go to **Control Panel** > **Administrative Tools** > **Services** and stop all services in the following sequence:

   a. `Trend Micro IMSS Web Console`

   b. `Trend Micro IMSS IPProfiler`

   c. `Trend Micro IMSS Task Services`

   d. `Trend Micro IMSS CMAgent Service`

   e. `Trend Micro IMSS Policy Service`

   f. `Trend Micro IMSS Scan Service`

   g. `Trend Micro IMSS SMTP Service`

   h. `Trend Micro IMSS Manager`

2. Change the server IP address.

3. Change the IP address in `ODBC.ini` and `EUQ.ini` in the IMSS configuration folder.

4. Change the database URL and user name/password in `%IMSS_HOME%\ui\adminUI\webapps\ROOT\WEB-INF\struts-config-common.xml`

5. 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 management console URL.

6. Modify your SQL Server's IP settings and restart your Microsoft SQL Server services.
7. Go to **Control Panel** > **Administrative Tools** > **Services** and restart all services in the following sequence:

   a. `Trend Micro IMSS Manager`

   b. `Trend Micro IMSS SMTP Service`

   c. `Trend Micro IMSS Scan Service`

   d. `Trend Micro IMSS Policy Service`

   e. `Trend Micro IMSS CMAgent Service`

   f. `Trend Micro IMSS Task Services`

   g. `Trend Micro IMSS IPProfiler`

   h. `Trend Micro IMSS Web Console`

Changing the IP address for a Scanner

New IP addresses for scanner are automatically updated in the `tb_component_list` by the IMSS service TmImssManager when the service restarts. To update the IP address on the scanner, restart the TmImssManager service.

Changing the IP address for the Central Controller

Procedure

1. Restart the IMSS service `TmImssManager`.
2. Specify the new IP address of the central controller in the`[cmagent]/ConfigUrl` parameter in the **tb_global_setting** table.

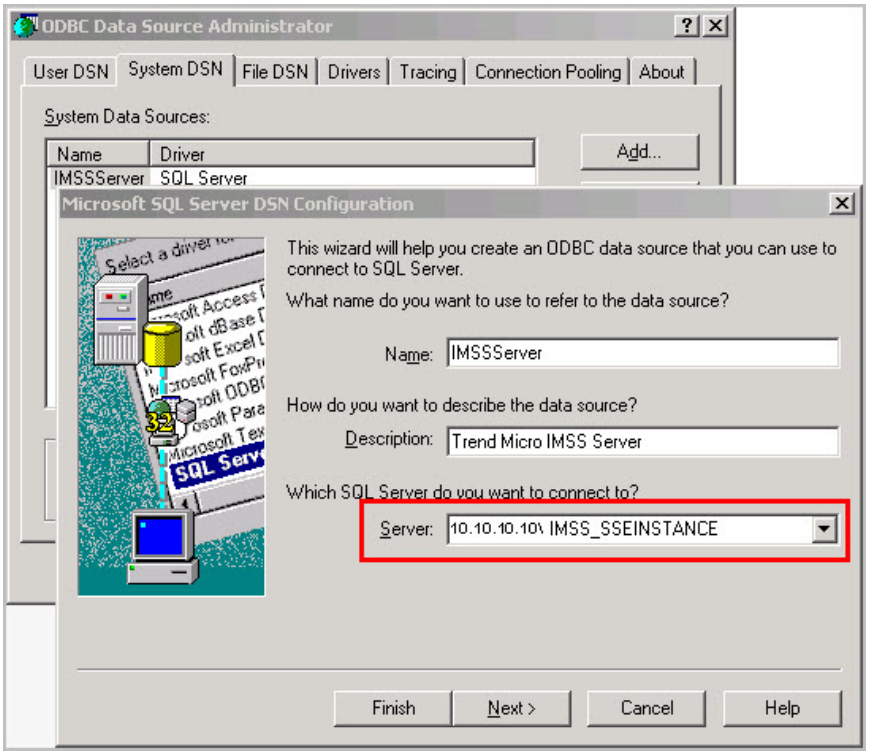
3. If IP Profiler was installed:
   - Restart the BIND Service (ISC BIND) on the central controller.
   - Update the IP address for the `[SmtpServer]/IPProfilerDNSServerIP` parameter in the `tsmtpd.ini` file on each scanner.
4. Restart the SMTP service on each scanner to use the new IP Profiler DNS server IP address.
5. Change the IP address, for web management console access, to the new IP address in the `adminui` file. The file is located in the IMSS installation directory.

Changing the IP address of the admin database

Procedure

1. Stop all IMSS components.
2. On all scanners and EUQ servers, set the server parameter to the new IP address of the database server in the ODBC System DSN settings.

Modify the setting from the **ODBC Data Source Administrator** dialog box, located at **Start** > **Administrative Tools** > **Data Sources (ODBC)**.



Note

On 64-bit platforms, run `%systemdrive%\Windows\SysWOW64\Odbcad32.exe` to change the DSN Setting for IMSS.

3. On all scanners and EUQ servers, set the ServerName parameter to the new IP address of the database server in the odbc.ini file, located at IMSS\config\.

4. On the central controller, set the database URL to the new IP address of the database server in the `struts-config-common.xml` file, located at `IMSS\ui`

`\adminUI\webapps\ROOT\WEB-INF\`. To change the setting, locate the string similar to the following and modify the IP address:

```
<set-property

property="url"

value="jdbc:sqlserver://10.100.10.31;DatabaseName=imss" />
```

5. On all servers, start all IMSS components.

Changing the IP address of primary EUQ servers

Procedure

1. Change the "ServerName" to the new IP address in the `EUQ.conf` file, located at `<IMSS Install Path>\UI\euqui\conf\`.
2. Change the IP address in the following files to the new IP address:
   - `euqbalance`
   - `euqui`

   Both files are located in the IMSS installation directory.
3. Set the `admin_cmd` parameter in `tb_global_setting` for the primary EUQ server to 12288.
4. Restart the IMSS manager on the primary EUQ server. This changes the IP address in the `tb_component_list` to the new IP address, updates the load balance configuration, and restarts the TmImssEuqLoadBalancer service.
5. Restart the EUQ service on the primary EUQ server.

Changing the IP address of secondary EUQ servers

Procedure

1. Change the IP address in the `euqui` file to the new IP address. The file is located in the IMSS installation directory.
2. Restart the IMSS manager on the secondary EUQ server. This changes the IP address in the `tb_component_list` to the new IP address.
3. Set the admin_cmd parameter in tb_global_setting for the primary EUQ server to 12288.
4. Restart the IMSS manager on the primary EUQ server to update the `worker.properties` configuration file.

Removing or adding EUQ servers into an IMSS group

The Setup program notifies the IMSS manager service on the primary EUQ server to update the load-balancing configuration for Apache. The IMSS manager service on the Primary EUQ Server detects the `admin_cmd` command and updates the workers.properties configuration file to include or remove an EUQ server in / from the pool of EUQ servers used by Apache to distribute the End User requests.

Adding an EUQ database

Use the IMSS web management console or Setup program to add a new EUQ database. Once installation completes, use the euqtrans.bat script, from the `<IMSS>\bin` directory of the central controller, to re-balance the EUQ databases.

Removing an EUQ database

Procedure

1. Use the IMSS web management console to unregister (not delete) the EUQ database.

2. Run the `euqtrans.bat` script to move the Approved Sender list and quarantined message information to another database, and re-balance the databases based on the new deployment.

Changing the EUQ database IP address

Procedure

1. Change the IP address in the `euq.ini` file to the new IP address. The file is located at `<IMSS>\config\`.
2. Use the IMSS web management console to change the IP address of the EUQ database to the new IP address for the database.

   After configuring the EUQ Database Settings, IMSS automatically informs all the services to restart. On restart, the services automatically check for updated EUQ database connection settings from the `tb_euq_db_info` table and updates the local ODBC User DSN settings in the Windows registry.

How does IMSS process a partial message?

The key `BypassMessagePartial` in theIMSS 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=C:\Program Files\Trend Micro\IMSS\log
event_log_path=C:\Program Files\Trend Micro\IMSS\log
policy_evt_log_path=C:\Program Files\Trend Micro\IMSS\log
```

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).

Support Information

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.

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users. After one year, users must purchase renewal maintenance. To get help or to submit feedback, feel free to contact Trend Micro any time.

- Get a list of the worldwide support offices at:
  http://esupport.trendmicro.com
- Get the latest Trend Micro product documentation at:
  http://docs.trendmicro.com

In the United States, reach Trend Micro representatives 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

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.

TrendLabs

TrendLabs℠ 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

Security Intelligence

Comprehensive security information is available at the Trend Micro website.

http://www.trendmicro.com/vinfo

Security information includes:

- List of malware and malicious mobile code currently active or "in the wild"
- Computer malware hoaxes
- Internet threat advisories
- Malware weekly report

- Threat Encyclopedia, which includes a comprehensive list of names and symptoms for known malware, spam, malicious URLs, and known vulnerabilities, plus write-ups on web attacks and online trends.

Download Center

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

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

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

http://esupport.trendmicro.com/solution/en-us/1055473.aspx

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Appendix A

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 A-2*
- *eManager, Virus, and Program Logs on page A-3*
- *Temporary Folder on page A-3*
- *Notification Pickup Folder on page A-4*

Default Mail Queues

The following table shows the various mail directories that store the mail messages managed by IMSS.

TABLE A-1. Default IMSS Mail Locations

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_malform= `C:\Program Files\Trend Micro\IMSS\queue\malform`		Stores malformed messages.
queue_archive= `C:\Program Files\Trend Micro\IMSS\queue\archive`		Stores archived messages.
queue_quarantine = `C:\Program Files\Trend Micro\IMSS\queue\quarantine`		Stores quarantined messages.
queue_notify= `C:\Program Files\Trend Micro\IMSS\queue\notify`	queue_notify_big= `C:\Program Files\Trend Micro\IMSS\queue\notifybig`	Stores notification messages.
queue_postpone= `C:\Program Files\Trend Micro\IMSS\queue\postpone`	queue_postpone_big= `C:\Program Files\Trend Micro\IMSS\queue\postponebig`	Stores postponed messages.
queue_deliver= `C:\Program Files\Trend Micro\IMSS\queue\deliver`	queue_deliver_big= `C:\Program Files\Trend Micro\IMSS\queue\deliverbig`	Stores messages for final delivery.

Queues for Regular Mails	Queues for Large Mails	Descriptions
mailqueuedir= `C:\Program Files\Trend Micro\IMSS\mque`		Stores messages that will be handled by the IMSS MTA.
queue_reprocess= `C:\Program Files\Trend Micro\IMSS\queue \reprocess`	queue_reprocess_big= `C:\Program Files\Trend Micro\IMSS\queue \reprocessbig`	Stores messages pending reprocessing.
queue_handoff= `C:\Program Files\Trend Micro\IMSS\queue \handoff`	queue_handoff_big= `C:\Program Files\Trend Micro\IMSS\queue \handoffbig`	Stores messages pending handoff.
queue_undeliverable= `C:\Program Files\Trend Micro\IMSS\queue \undeliverable`		Stores undeliverable messages.
queue_unnotify= `C:\Program Files\Trend Micro\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:

`C:\Program Files\Trend Micro\IMSS\log`

Temporary Folder

IMSS stores all application-generated temporary files in the temporary folder:

```
C:\Program Files\Trend Micro\IMSS\temp
```

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:

```
C:\Program Files\Trend Micro\IMSS\queue\notify\
```

and

```
C:\Program Files\Trend Micro\IMSS\queue\notifybig
```

Configuring the SMTP Notification Server

For details, see *Configuring SMTP Routing on page 7-2*.

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, 23-19
    product, 23-20
add
    administrator accounts, 23-2
address group
    add, 11-5
    delete, 11-8
    edit, 11-8
address groups
    examples of, 11-2
    understand, 11-2
administrator accounts
    add, 23-2
    delete, 23-5
    edit, 23-5
    manage, 23-2
Advanced Threat Scan Engine, 5-2
adware, 1-10
antivirus rule, 13-10
APOP, 9-3
approved list
    add hosts, 6-10
approved senders list
    configure, 13-18
archive
    configure settings, 19-2
archive areas
    manage, 19-7
archived messages
    view, 19-16
asterisk wildcard
    use, 14-16
attachment size
    scanning conditions, 13-25
audience, xiii

B

back up
    IMSS, 21-3
blocked list
    add hosts, 6-10
blocked senders list
    configure, 13-18
bounced mail settings
    configure, 6-16

C

C&C email, 13-12
change
    web console password, 2-5
Command & Control (C&C) Contact Alert Services, 1-17
component update, 4-7
configuration wizard, xiii
Configuration Wizard
    accessing, 3-2
configure
    approved senders list, 13-18
    archive settings, 19-2
    blocked senders list, 13-18
    connection settings, 7-3, 23-6
    Control Manager server settings, 3-10
    delivery settings, 20-3
    Direct Harvest Attack (DHA) settings, 6-14
    Email reputation, 6-17

expressions, 11-19
internal addresses, 3-9, 12-2
IP Filtering, 6-8
IP Filtering bounced mail settings, 6-16
IP Filtering spam settings, 6-11
IP Filtering virus settings, 6-13
LDAP settings, 3-7, 23-7
log settings, 18-2
Messaged Delivery settings, 7-10
Message Rule settings, 7-6
notification messages, 20-5
notification settings, 3-3
other scanning exceptions scan actions, 15-5
POP3 settings, 9-3, 23-10
product settings, 3-12
quarantine settings, 19-2
route, 13-7
scan exceptions, 15-2
scheduled reports, 17-7
security setting violation exceptions, 15-3
security setting violation scan actions, 15-4
SMTP routing, 3-2, 7-2
SMTP settings, 7-2
spam text exemption rules, 13-20
TMCM settings, 23-13
update source, 3-5
User Quarantine Access, 19-18
Web EUQ Digest settings, 20-7
configure event criteria, 20-5
connection settings
configure, 7-3, 23-6
Control Manager
enable agent, 21-10
replicate settings, 21-11
see Trend Micro Control Manager, 1-12
Control Manager server settings
configure, 3-10
Conventional scan, 2-10

D

Deep Discovery Advisor, 5-4
deferred messages
view, 19-17
delete
address group, 11-8
administrator accounts, 23-5
delivery settings
configure, 20-3
dialers, 1-10
Direct Harvest Attack (DHA) settings
configure, 6-14
display
domains, 6-20
suspicious IP addresses, 6-20
documentation, xiv
domains
display, 6-20

E

edit
address group, 11-8
administrator accounts, 23-5
email relay, 7-6
Email reputation, xii
Administration Console, 6-3
configure, 6-17
enable, 6-8
email threats
spam, 1-5
unproductive messages, 1-5

enable
Control Manager agent, 21-10
Email reputation, 6-8
End-User Access, 22-6
EUQ, 22-4
IP Profiler, 6-8
IP Profiler rules, 6-11
POP3 scanning, 9-3
End-User Access
enable, 22-6
ERS
using, 6-2
EUQ, 22-2
authentication, 22-2
disable, 22-8
enable, 22-4
open the console, 22-7
start, 22-5
web console, 22-7
Web console, 2-7
event criteria
configure, 20-5
event notifications, 20-2
export notes, 21-2
expression lists
manage, 11-17
expressions
configure, 11-19

F

FAQ
ERS, 24-18
EUQ, 24-21
IMSS components, 24-16
IP Profiler, 24-18
mail areas, 24-19
queues, 24-19
File Reputation Services, 1-15
filtering, how it works, 1-7
filters
examples of, 11-2

G

generate
reports, 17-2

H

hacking tools, 1-10

I

import notes, 21-2
IMSS
about, 1-2
backing up, 21-3
restore, 21-6
internal addresses
configure, 3-9, 12-2
IP Filtering
configure, 6-8
configure bounced mail settings, 6-16
configure Direct Harvest Attack (DHA) settings, 6-14
configure spam settings, 6-11
configure virus settings, 6-13
IP Filtering Service
about, 6-2
IP Profiler, xii
enable, 6-8
enable rules, 6-11

J

joke program, 1-10

L

LDAP settings

configure, 3-7, 23-7
LDAP User or Group
search for, 12-6
license
activate, 23-19
renew, 23-19
logs, 18-2
configure settings, 18-2
query, 18-4
query IP filtering, 18-11
query message tracking, 18-5
query MTA event, 18-10
query policy event, 18-8
query system event, 18-6

M

manage
administrator accounts, 23-2
expression lists, 11-17
notifications list, 11-23
one-time reports, 17-4
policies, 10-1
product licenses, 23-16
manual update, 4-5
mass mailing viruses
pattern, 1-6
message delivery, 7-10
Message Delivery settings
configure, 7-10
Message Rule settings
configure, 7-6
message size
scanning conditions, 13-26
MIME content type
scanning conditions, 13-24
MTA features, opportunistic TLS, xiii

N

new features, x
notes
export, 21-2
import, 21-2
notification messages
configure, 20-5
notifications
event, 20-2
notification settings
configure, 3-3
notifications list
manage, 11-23

O

one-time reports
manage, 17-4
online help, xiv
other rule, 13-11

P

password
Web console, 2-5
password cracking applications, 1-10
pattern files
update, 4-2
permitted senders, 7-9
policies
add, 13-2
example 1, 14-6
finalize, 13-37
manage, 10-1
policy notification
add, 11-24
edit, 11-24
POP3 messages
scan, 9-2

POP3 scanning
enable, 9-3
POP3 settings
configure, 9-3, 23-10
product licenses
manage, 23-16
view, 23-17
product services, 2-6
product settings
configure, 3-12

Q

quarantine
configure settings, 19-2
quarantine and archive, 19-2
quarantine areas
manage, 19-4
quarantined messages
view, 19-15
query
archive areas, 19-12
deferred messages, 19-13
IP filtering logs, 18-11
logs, 18-4
messages, 19-10
MTA event logs, 18-10
policy event logs, 18-8
quarantine areas, 19-10
system event logs, 18-6

R

readme file, xiv
remote access tools, 1-10
renew
license, 23-19
replicating settings, 21-10
reports
content, 17-2
generate, 17-2
manage one-time, 17-4
scheduled reports, 17-7, 17-10
restore
IMSS, 21-6
roll back
components, 4-6
route
configure, 13-7
specify, 13-2

S

scan
POP3 messages, 9-2
SMTP messages, 7-1
scan actions
configure other scanning exceptions
settings, 15-5
scan engine
update, 4-2
scan exceptions
configure, 15-2
Scan methods, 2-9
scanning conditions, 13-25
attachment names, 13-23
attachment number, 13-26
attachments, 13-23
attachment size, 13-25
extensions, 13-23
message size, 13-26
MIME content type, 13-24
spam, 13-17
specify, 13-10
true file type, 13-25
scheduled reports
access, 17-7

configure, 17-7
use, 17-10
scheduled updates, 4-8
security risks
spyware/grayware, 1-9
security setting violations
configure exceptions, 15-3
configure scan actions, 15-4
services, 2-6
IP Filtering Service, 6-2
Smart Protection, 1-15
Smart Protection Network, 1-16
Smart Scan, 2-9
SMTP
notification server, A-4
SMTP messages
scan, 7-1
SMTP routing, 7-2
configure, 3-2, 7-2
SMTP settings
configure, 7-2
spam prevention, xii
spam settings
configure, 6-11
spam text exemption rules
configure, 13-20
specify
actions, 13-30
route, 13-2
scanning conditions, 13-10
update source, 4-3
spyware/grayware, 1-9
adware, 1-10
dialers, 1-10
entering the network, 1-10
hacking tools, 1-10
joke program, 1-10
password cracking applications, 1-10
remote access tools, 1-10
risks and threats, 1-10
start
EUQ, 22-5
support
knowledge base, 24-35
resolve issues faster, 24-36
technical support, 24-36
TrendLabs, 24-37
suspicious IP addresses
display, 6-20
System Status screen, 16-2

T

tag subject
add, 13-36
technical support, 24-36
TMCM settings
configure, 23-13
TrendLabs, 24-37
Trend Micro Control Manager, 1-12
agent, 1-12
server, 1-12
troubleshooting, 24-2
activating products, 24-3
email notifications, 24-3
EUQ quarantined messages, 24-7
EUQ web console access, 24-6
imssps daemon, 24-2
IP Filtering, 24-7
Web EUQ digest, 24-7
true file type, 13-25

U

update

automatically, 4-8
manually, 4-5
pattern files, 4-2
scan engine, 4-2
update source
configure, 3-5
specify, 4-3
User Quarantine Access
configure, 19-18

V

view
archived messages, 19-16
deferred messages, 19-17
product licenses, 23-17
quarantined messages, 19-15
virus settings
configure, 6-13

W

web console password
change, 2-5
Web EUQ Digest
configure settings, 20-7
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: MSEM76206/131030