TREND MICRO™

9.1 InterScan™ Messaging Security Suite

Patch 1

Administrator's Guide

Comprehensive threat protection at the Internet messaging gateway

for LINUX™

Messaging Security

Document Part No.: MSEM98750/190801

Release Date: December 2021

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

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

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

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

Evaluate this documentation on the following site:

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that InterScan Messaging Security Suite collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Table of Contents

About this Manual

About this Manual xi
What's New xii
Audience xx
InterScan Messaging Security Suite Documentation xxi
Document Conventions xxi

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 Cloud Pre-Filter 1-10
About Spyware/Grayware 1-11
About Web Reputation Services 1-13
About Email Reputation 1-13
About Trend Micro Control Manager 1-16
About Trend Micro Smart Protection 1-19
About Graymail Scanning 1-21
About Command & Control (C&C) Contact Alert Services 1-22

Chapter 2: Getting Started

Opening the IMSS Management Console 2-2
Changing the Management Console Password 2-3
Using Smart Search 2-4
Configuring Proxy Settings 2-4

IMSS Services 2-6
Opening the End-User Quarantine Console 2-7

Chapter 3: Using the Configuration Wizard

Accessing the Configuration Wizard 3-2
Configuring Notification Settings 3-2
Configuring the Update Source 3-4
Configuring LDAP Settings 3-6
Configuring Internal Addresses 3-9
Configuring Control Manager Server Settings 3-10
Activating the Product 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 4-4
Rolling Back a Component Update 4-5
Scheduled Component Updates 4-6

Chapter 5: Getting Started with Cloud Pre-Filter

Understanding Cloud Pre-Filter 5-2
Creating a Cloud Pre-Filter Account 5-5

Chapter 6: Getting Started with ATSE and Virtual Analyzer

Scan Technology 6-2
About Advanced Threat Scan Engine 6-2
About Virtual Analyzer 6-4

Chapter 7: Getting Started with Email Encryption

Understanding Email Encryption 7-2
Using Email Encryption 7-3
Registering for Email Encryption 7-3
Managing Domains 7-4
Registering Domains 7-5

Part II: Configuring IMSS

Chapter 8: Configuring Cloud Pre-Filter

Understanding Cloud Pre-Filter Policies 8-2
Creating a Cloud Pre-Filter Policy 8-3
Verifying Cloud Pre-Filter Works 8-14
Configuring DNS MX Records 8-14
Suggested IMSS Settings When Using Cloud Pre-Filter 8-15
Disabling Cloud Pre-Filter 8-17

Chapter 9: Configuring Sender Filtering Settings

Sender Filtering Service 9-2
Using Email Reputation 9-2
Configuring Sender Filtering 9-4
Displaying Suspicious IP Addresses and Domains 9-17

Chapter 10: Configuring SMTP Settings

Message Transfer Agents 10-2
Enabling SMTP Connections 10-2
Configuring SMTP Routing 10-2
About Message Delivery 10-11

Chapter 11: Configuring Known Hosts Settings

About Known Hosts 11-2
Adding Known Hosts 11-3
Importing Known Hosts 11-4
Exporting Known Hosts 11-4

Chapter 12: Configuring POP3 Settings

Scanning POP3 Messages 12-2
Enabling POP3 Scanning 12-3
Configuring POP3 Settings 12-4
Configuring POP3 Scan Service 12-5

Part III: IMSS Policies

Chapter 13: Managing Policies

About Policies 13-2
How the Policy Manager Works 13-2
Filter Policies that Display in the Policy List 13-4

Chapter 14: Configuring Common Policy Objects

Policy Object Descriptions 14-2
Address Groups 14-2
Using the Keyword & Expression List 14-13
Data Loss Prevention 14-28
Notifications 14-47
Stamps 14-53
DKIM Approved List 14-56
Web Reputation Approved List 14-58

URL Keyword List 14-60

Chapter 15: Configuring Internal Addresses

Configuring Internal Addresses 15-2
Searching for Users or Groups 15-5
Searching for an LDAP User or Group 15-6

Chapter 16: Using Trend Micro Smart Protection

About Trend Micro Smart Protection 16-2
Smart Protection Sources 16-5
Selecting a Scan Method 16-7
Using Web Reputation Services 16-10

Chapter 17: Configuring Policies

Adding Policies 17-2
Specifying a Route 17-2
Specifying Scanning Conditions 17-10
Specifying Actions 17-41
Finalizing a Policy 17-48

Chapter 18: Configuring Encryption Settings

Configuring Encryption Settings 18-2
Encrypting Message Traffic 18-3
Configuring Encryption Policies 18-3

Chapter 19: Configuring Scanning Exceptions

Setting Scan Exceptions 19-2
Configuring Exceptions for Security Settings Violations 19-3
Setting Scan Actions for Security Setting Violations 19-4

Setting Scan Actions for Malformed Messages 19-5
Configuring Exceptions for Encrypted Messages 19-7
Setting Scan Actions for Encrypted Messages 19-8
Setting Scan Actions for Virtual Analyzer Scanning Exceptions 19-9

Chapter 20: Configuring Existing Policies

Modifying Existing Policies 20-2
Policy Example 1 20-5
Policy Example 2 20-10
Using the Asterisk Wildcard 20-15

Part IV: Monitoring the Network

Chapter 21: Monitoring the Network

Monitoring Your Network 21-2
Viewing System Status 21-2

Chapter 22: Dashboard and Widgets

Using the Dashboard 22-2
Understanding Tabs 22-2
Understanding Widgets 22-6

Chapter 23: Reports

Generating Reports 23-2
Managing One-time Reports 23-5
Scheduled Reports 23-8

Chapter 24: Logs

About Logs 24-2

Configuring Log Settings 24-2
Configuring Syslog Settings 24-4
Querying Logs 24-6

Chapter 25: Mail Areas and Queues

About Mail Areas and Queues 25-2
Configuring Quarantine and Archive Settings 25-2
Managing Quarantine Areas 25-4
Managing Archive Areas 25-6
Querying Messages 25-9
Viewing Quarantined Messages 25-15
Viewing Archived Messages 25-17
Viewing Postponed Messages 25-18
Viewing Messages in the Virtual Analyzer Queue 25-19

Chapter 26: Notifications

Event Notifications 26-2
Configuring Delivery Settings 26-2
Configuring Event Criteria and Notification Message 26-5
EUQ Digest 26-8
Configuring a Logon Notice 26-11
Editing Notifications 26-12

Part V: Administering IMSS

Chapter 27: Backing Up, Restoring, and Replicating Settings

Importing and Exporting Settings 27-2
Backing Up IMSS 27-4

Restoring IMSS 27-6
Replicating Settings 27-7
Exporting Debugging Files 27-9

Chapter 28: End-User Quarantine

About EUQ 28-2
EUQ Authentication 28-2
Configuring End-User Quarantine (EUQ) 28-2
Distribution List EUQ Management 28-14
Disabling EUQ 28-16
Managing EUQ Databases 28-17

Chapter 29: Administrative Tasks

Managing Administrator Accounts 29-2
Configuring Connection Settings 29-6
Configuring Database Maintenance Schedule 29-19
Managing Product Licenses 29-20
Activating Products 29-24
Configuring Smart Protection Network Settings 29-26

Chapter 30: Updating and Rescuing the System and Application

Updating the System and Application 30-2

Chapter 31: Troubleshooting and FAQs

Troubleshooting 31-2
Frequently Asked Questions 31-18
Troubleshooting Cloud Pre-Filter 31-36

Appendices

Appendix A: Technical Support

Troubleshooting Resources A-2
Contacting Trend Micro A-4
Sending Suspicious Content to Trend Micro A-5
Other Resources A-6

Appendix B: IMSS Scripts

Using IMSS Scripts B-2

Appendix C: Default Directory Locations

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

Index

Index IN-1

Preface

About this Manual

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

Refer to the *IMSS 9.1 Patch 1 Installation Guide* for information about installing and upgrading IMSS.

Topics include:

- *What's New on page xii*
- *Audience on page xx*
- *InterScan Messaging Security Suite Documentation on page xxi*
- *Document Conventions on page xxi*

What's New

The following tables provide an overview of new features available in IMSS 9.1 Patch 1.

TABLE 1. IMSS 9.1 Patch 1 New Features

NEW FEATURE	DESCRIPTION
URL Analysis	In addition to suspicious files in email messages, IMSS submits suspicious URLs included in email messages (subject, body and attachments) to Virtual Analyzer for further analysis. To protect you from malicious URLs, IMSS first compares URLs in email messages with known malicious URLs in the Web reputation database, and then further analyzes URLs at the time of click. However, untested URLs may pass the first two layers of analysis. IMSS provides enhanced protection by leveraging the URL sandbox available in Virtual Analyzer to perform sandbox simulation and analysis.

TABLE 2. IMSS 9.1 New Features

NEW FEATURE	DESCRIPTION
Cloud Pre-Filter Integration	Cloud Pre-Filter is a hosted email security service that can filter all of your email messages before they reach your network. Pre-filtering your email messages can save you time and money.
Data Loss Prevention	Data Loss Prevention safeguards an organization's confidential and sensitive data-referred to as digital assets-against accidental disclosure and intentional theft.

New Feature	Description
Integration with Virtual Analyzer	Virtual Analyzer is an isolated virtual environment used to manage and analyze samples in Deep Discovery Analyzer. IMSS allows you to define rules to send suspicious messages, including attachments, to Virtual Analyzer for analysis. To achieve better load balancing and failover capabilities, IMSS allows you to add multiple servers for Virtual Analyzer. You can also enable, disable and delete Virtual Analyzer servers on the IMSS management console.
End-User Quarantine Single Sign-on (SSO)	IMSS now allows users to log on once to their domain and then to End-User Quarantine (EUQ) without re-entering their domain name and password.
Dashboard and Widgets	Real-time summaries have been replaced with a dashboard and widgets. This will provide administrators with more flexibility when viewing IMSS data. The **Summary** screen has been renamed **System Status** and appears in the left menu.
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 increase protection against advanced threats that leverage short-lived malicious websites.
Enhanced Smart Protection	IMSS supports both Trend Micro Smart Protection Network and Smart Protection Server as smart protection sources. Smart Protection Servers are supported to localize smart protection services to the corporate network to reduce outbound traffic and optimize efficiency.

New Feature	Description
Social Engineering Attack Protection	Social Engineering Attack Protection detects suspicious behaviors related to social engineering attacks in email messages. When Social Engineering Attack Protection is enabled, the Trend Micro Antispam Engine scans for suspicious behaviors in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information. If the Antispam Engine detects behaviors associated with social engineering attacks, the Antispam Engine returns details about the message to IMSS for further action, policy enforcement, or reporting.
Known Host Support	Known hosts include trusted mail transfer agents (MTAs) and the Cloud Pre-Filter that are deployed before IMSS on your network. IMSS enables you to specify known hosts to exempt them from Sender Filtering and graymail scanning.
Graymail	Graymail refers to solicited bulk email messages that are not spam. IMSS manages graymail separately from common spam to allow administrators to identify graymail messages. IP addresses specified in the graymail exception list bypass scanning.
Multiple LDAP Servers	IMSS supports using more than one LDAP server and has support for more LDAP server types.
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.
Time-of-Click Protection	IMSS provides time-of-click protection against malicious URLs in email messages. If you enable Time-of-Click Protection, IMSS rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious.

New Feature	Description
Connected Threat Defense	Configure IMSS to subscribe to the suspicious object lists on the Trend Micro Control Manager server. Using the Control Manager console, you can specify customized actions for objects detected by the suspicious object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment. Control Manager facilitates the investigation of targeted attacks and advanced threats using suspicious objects. Files and URLs that have the potential to expose systems to danger or loss will be detected.
Report Delivery Through Email	IMSS allows you to send newly generated reports and archived reports through email. Detailed views of reports will be included.
EUQ Distribution List Management	The web-based EUQ service allows end users to manage the spam quarantine of distribution lists that they belong to.
LDAPS Support	IMSS supports LDAP over SSL (LDAPS) that provides users a secure and encrypted channel to communicate with LDAP servers.
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.
EUQ Digest Inline Action Links	IMSS enables users to apply actions to quarantined messages through links in the EUQ digest.

TABLE 3. IMSS 7.1 SP2 New Features

NEW FEATURE	DESCRIPTION
Audit Log Enhancement	Audit logs record various administrator operations and provide a way to query activities of specified administrator accounts. **Note** As an enhanced log category of system events, **Audit log** replaces **Admin activity** on the IMSS management console.
Attachment Keyword Expression enhancement	Keyword expressions configured for IMSS policies are enhanced to apply not only to attachment content but also to attachment names.
Attachment Names Supported by Message Tracking Logs	Message tracking logs include attachment names as a new attribute. Multiple attachment names can be specified to query message tracking logs.
Logon Notice Support	Customizable logon notices are available both on the administrator logon page and End-User Quarantine logon page.

TABLE 4. IMSS 7.1 SP1 New Features

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

New Feature	Description

IPv6 Support	IMSS supports the following IPv6 features in IPv6 networks and proxies:
	• SMTP routing and POP3 connections
	• Trend Micro services:
	  • Web Reputation Services
	  • Product Registration
	  • ActiveUpdate
	  • Smart Feedback
	• Trend Micro Control Manager
	• IP address imports and exports in IPv6 format
	• Notifications
	• Logs and reports with relevant SMTP IPv6 information

Keyword & Expression Enhancements	To improve visibility of triggered keywords and expressions, the entity name (where the keyword expression appears in a message) and the matched expressions now appear in the policy event log query details page. Administrators can also add a description to new keyword expressions for better tracking.
SMTP Authentication Support for End-User Quarantine	SMTP authentication provides users another option for enabling the End-User Quarantine feature.
Email Alias Support	The User Quarantine now has the option to allow end users to retrieve quarantined email messages with alias email addresses.

TABLE 5. IMSS 7.1 New Features

NEW FEATURE	DESCRIPTION
Common Policy Objects	Several information objects that can be used by all policies have been removed from policy creation and given their own areas for configuration: • Address Groups • Keywords & Expressions • Policy Notifications • Stamps • DKIM Approved List • Web Reputation Approved List
Web Reputation	Protect your clients from malicious or suspicious URLs embedded in email messages with Web reputation.
NRS Terminology Change	Network Reputation Service (NRS) has been changed to Email Reputation Service (ERS).
Detection Capability Enhancement	Use DomainKeys Identified Mail (DKIM) enforcement, with the DKIM Approved List, in policies to assist in phishing protection and to reduce the number of false positives regarding domains.
X-Header Support	Insert X-Headers into email messages to track and catalog the messages.
Expanded File Scanning Support	Scanning support for Microsoft® Office 2007 and Adobe® Acrobat® 8 documents.
New Migration Tools	New tools provided to help customers migrating from previous product versions.

TABLE 6. IMSS 7.0 New Features

NEW FEATURE	DESCRIPTION
Multiple Antivirus and Malware Policies	Multiple IMSS policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria.
Centralized Logging and Reporting	A consolidated, detailed report provides top usage statistics and key mail usage data. Centralized logging allows administrators to quickly audit message-related activities.
Centralized Archive and Quarantine Management	An easy way to search multiple IMSS quarantine and archive areas for messages.
Scalable Web End-User Quarantine (Web EUQ)	Multiple Web EUQ services offer end-users the ability to view quarantined email messages that IMSS detected as spam. Together with EUQ notification, IMSS will help lower the cost of helpdesk administrative tasks.
Multiple Spam Prevention Technologies	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 Antispam 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	Detailed logging for all messages tracks and identifies message flow related issues.
Integration with Trend Micro Control Manager™	Perform log queries on Email Reputation Services from Control Manager, in addition to other supported features.

Audience

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

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

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

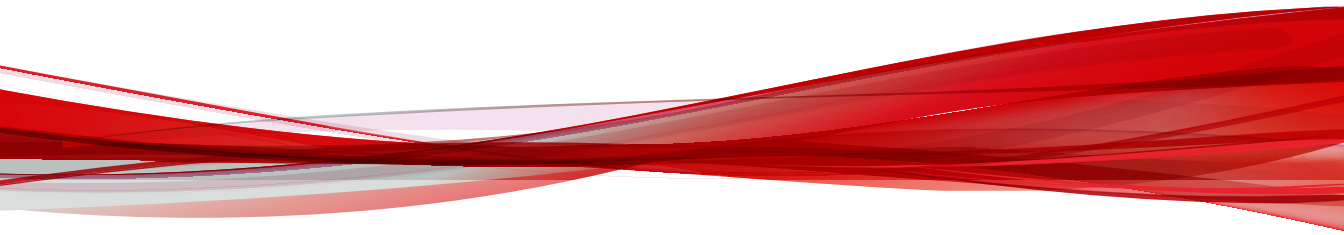
The documentation uses the following conventions:

TABLE 7. 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 antispam capabilities.

Topics include:

- *About InterScan Messaging Security Suite on page 1-2*
- *IMSS Main Features and Benefits on page 1-2*
- *About Cloud Pre-Filter on page 1-10*
- *About Spyware/Grayware on page 1-11*
- *About Web Reputation Services on page 1-13*
- *About Email Reputation on page 1-13*
- *About Trend Micro Control Manager on page 1-16*
- *About Trend Micro Smart Protection on page 1-19*
- *About Graymail Scanning on page 1-21*
- *About Command & Control (C&C) Contact Alert Services on page 1-22*

About InterScan Messaging Security Suite

InterScan Messaging Security Suite (IMSS) 9.1 Patch 1 integrates antivirus, antispam, 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 antispam 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 antispam 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
Cloud-based pre-filtering of messages	Cloud Pre-Filter integrates with IMSS to scan all email traffic before it reaches your network.	Cloud Pre-Filter can stop significant amounts of spam and malicious messages (up to 90% of your total message traffic) from ever reaching your network.
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.
Graymail	Graymail refers to solicited bulk email messages that are not spam. IMSS detects marketing messages and newsletters and social network notifications as graymail.	IMSS manages graymail separately from common spam to allow administrators to identify graymail messages. IP addresses specified in the graymail exception list bypass scanning.
Regulatory compliance	Administrators can meet government regulatory requirements using the new default policy scanning conditions *Compliance templates*.	Compliance templates provide administrators with regulatory compliance. For a detailed list of available templates, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Feature	Descriptions	Benefits
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
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.

Feature	Descriptions	Benefits
Real-time Statistics and Monitor	Administrators can monitor the scan performance and Sender Filtering performance of all IMSS devices (within a group) on the management console.	IMSS provides administrators with an overview of the system that keeps administrators informed on the first sign of mail processing issues. Detailed logging helps administrators proactively manage issues before they become a problem.
Protection against other email threats		
DoS attacks	By flooding a mail server with large attachments, or sending messages that contain multiple viruses or recursively compressed files, individuals with malicious intent can disrupt mail processing.	IMSS allows you to configure the characteristics of messages that you want to stop at the SMTP gateway, thus reducing the chances of a DoS attack.
Malicious email content	Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions.	IMSS allows you to configure the types of messages that are allowed to pass through the SMTP gateway.
Degradation of services	Non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours.	Most companies have acceptable usage policies for their messaging system—IMSS provides tools to enforce and ensure compliance with existing policies.

Feature	Descriptions	Benefits
Legal liability and business integrity	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.
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		

Feature	Descriptions	Benefits
Spyware and other types of grayware	Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see *About Spyware/ Grayware on page 1-11*.	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 antispam features		
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 Sender Filtering, which includes IP Profiler and Email Reputation, IMSS can block spammers at the IP level.

Feature	Descriptions	Benefits
Social Engineering Attack Protection	Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages.	When Social Engineering Attack Protection is enabled, the Trend Micro Antispam Engine scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information. If the Antispam Engine detects behavior associated with social engineering attacks, the Antispam Engine returns details about the message to IMSS for further action, policy enforcement, or reporting.
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.
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 the spam quarantine of their personal accounts and of distribution lists that they belong to. IMSS 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. IMSS also enables users to apply actions to quarantined messages and to add senders to the Approved Senders list through links in the EUQ digest.

Feature	Descriptions	Benefits
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. IMSS allows you to send both one-time and scheduled reports through email.
System availability monitor	A built-in agent monitors the health of your IMSS server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow.	Email and SNMP notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.
POP3 scanning	You can choose to enable or disable POP3 scanning from the management console.	In addition to SMTP traffic, IMSS can also scan POP3 messages at the gateway as messaging clients in your network retrieve them.
Clustered architecture	The current version of IMSS has been designed to make distributed deployment possible.	You can install the various IMSS components on different computers, and some components can exist in multiples. For example, if your messaging volume demands, you can install additional IMSS scanner components on additional servers, all using the same policy services.

Feature	Descriptions	Benefits
Integration with Trend Micro Control Manager™	Trend Micro Control Manager™ (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.
Integration with Virtual Analyzer	IMSS integrates with Virtual Analyzer, which is an isolated virtual environment used to manage and analyze samples in Deep Discovery Analyzer.	IMSS sends suspicious files and URLs to the Virtual Analyzer sandbox environment for simulation. Virtual Analyzer opens files, including password-protected archives and document files, and accesses URLs to test for exploit code, C&C and botnet connections, and other suspicious behaviors or characteristics.
Time-of-Click Protection	IMSS provides time-of-click protection against malicious URLs in email messages.	If you enable Time-of-Click Protection, IMSS rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious.

About Cloud Pre-Filter

Cloud Pre-Filter is a cloud security solution that integrates with IMSS to provide proactive protection in the cloud with the privacy and control of an on-premise virtual appliance.

Cloud Pre-Filter reduces inbound email message volume up to 90% by blocking spam and malware outside your network. Cloud Pre-Filter is integrated with IMSS at the gateway allowing flexible control over sensitive information. And local quarantines ensure your email message stays private. No email message is stored in the cloud. With Cloud Pre-Filter, you can reduce complexity and overhead to realize significant cost savings.

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	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Programs	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Helps hackers enter computers
Remote Access Tools	Helps hackers remotely access and control computers
Password Cracking Applications	Helps 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.

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

About Web Reputation Services

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 antispam protection to the Internet.

About Email Reputation

Trend Micro designed Email reputation 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 for verification against an extensive Reputation Database.

Types of Email Reputation

There are two types of Email reputation: *Standard on page 1-14* and *Advanced on page 1-14*.

Email Reputation: Standard

This service helps block spam by validating requested IP addresses against the Trend Micro reputation database, powered by the Trend Micro Smart Protection Network. This ever-expanding database currently contains over 1 billion IP addresses with reputation ratings based on spamming activity. Trend Micro spam investigators continuously review and update these ratings to ensure accuracy.

Email reputation: Standard is a DNS single-query-based service. Your designated email server makes a DNS query to the standard reputation database server whenever an incoming email message is received from an unknown host. If the host is listed in the standard reputation database, Email reputation reports that email message as spam.

Tip

Trend Micro recommends that you configure IMSS to block, not receive, any email messages from an IP address that is included on the standard reputation database.

Email Reputation: Advanced

Email reputation: Advanced identifies and stops sources of spam while they are in the process of sending millions of messages.

This is a dynamic, real-time antispam solution. To provide this service, Trend Micro continuously monitors network and traffic patterns and immediately updates the dynamic reputation database as new spam sources emerge, often within minutes of the first sign of spam. As evidence of spam activity ceases, the dynamic reputation database is updated accordingly.

Like Email reputation: Standard, Email reputation: Advanced is a DNS query-based service, but two queries can be made to two different databases: the

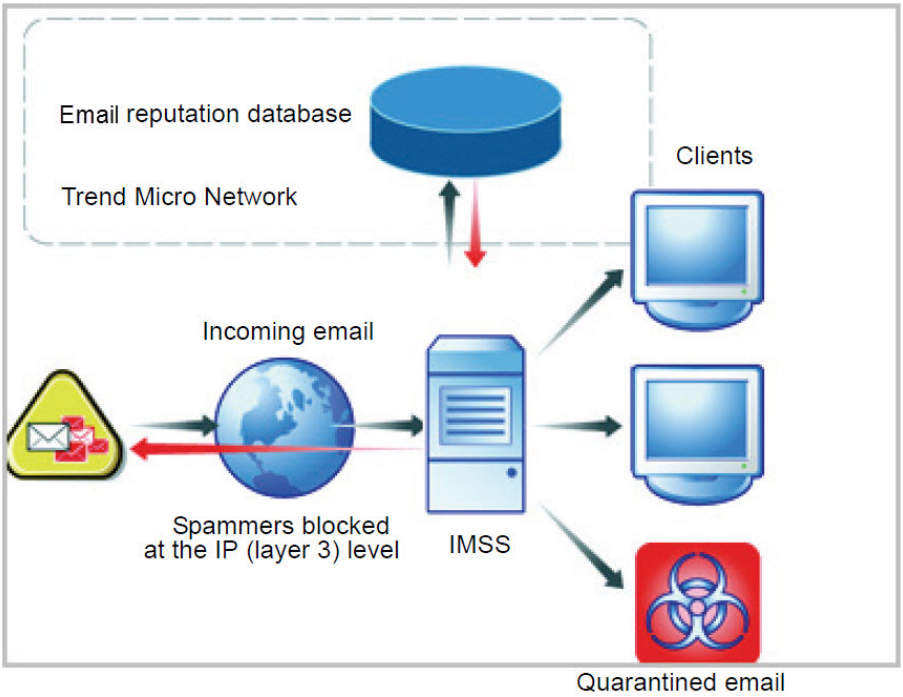
standard reputation database and the dynamic reputation database (a database updated dynamically in real time). These two databases have distinct entries (no overlapping IP addresses), allowing Trend Micro to maintain a very efficient and effective database that can quickly respond to highly dynamic sources of spam. Email reputation: Advanced has blocked more than 80% of total incoming connections (all were malicious) in customer networks. Results will vary depending on how much of your incoming email stream is spam. The more spam you receive, the higher the percentage of blocked connections you will see.

How Email Reputation Technology Works

Trend Micro Email reputation technology is a Domain Name Service (DNS) query-based service. The following process takes place after IMSS receives a connection request from a sending mail server:

1. IMSS records the IP address of the computer requesting the connection.
2. IMSS forwards the IP address to the Trend Micro Email reputation DNS servers and queries the Reputation Database. If the IP address had already been reported as a source of spam, a record of the address will already exist in the database at the time of the query.
3. If a record exists, Email reputation instructs IMSS to permanently or temporarily block the connection request. The decision to block the request depends on the type of spam source, its history, current activity level, and other observed parameters.

The figure below illustrates how Email reputation works.



For more information on the operation of Trend Micro Email reputation, visit https://ers.trendmicro.com/.

About Trend Micro Control Manager

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

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

Control Manager Support

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

TABLE 1-4. Supported Control Manager Features

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

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

Feature	Description	Supported?
Control Manager agent installation/ uninstallation	Install or uninstall IMSS Control Manager agent from Control Manager.	No. IMSS Control Manager agent is automatically installed when you install IMSS. To enable/ disable the agent, do the following from the IMSS management console: 1. Go to **Administration** > **Connections**. 2. Click the **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
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 Graymail Scanning

Graymail refers to solicited bulk email messages that are not spam. IMSS detects marketing messages and newsletters and social network notifications as graymail. IMSS identifies graymail messages in two ways:

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

Note

Note that while IMSS detects these kinds of email messages, these messages are not tagged as spam.

Administrators define the rule criteria to take an action on those email messages. Every graymail message rule has an exception list containing address objects that bypass message filtering. An address object is a single IP address or address range (IPv4 or IPv6), or the Classless Inter-Domain Routing (CIDR) block.

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

The graymail exception list can be exported and imported.

Note

Ensure that IMSS can query external DNS servers for graymail scanning. If you change any DNS server settings, restart the scanner server to load the new settings.

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*
- *Changing the Management Console Password on page 2-3*
- *Using Smart Search on page 2-4*
- *Configuring Proxy Settings on page 2-4*
- *IMSS Services on page 2-6*
- *Opening the End-User Quarantine Console on page 2-7*

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: imss9.1

3. Click **Log On**.

   Note

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

What to do next

To prevent unauthorized changes to your policies, Trend Micro recommends that you set a new logon password immediately after deployment and change the password regularly.

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

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**.

Using Smart Search

Smart Search provides a quick way to navigate to screens on the management console. Specify the name of the screen or the name of a feature in the Smart Search text box and then select an entry from the drop-down list that appears.

Configuring Proxy Settings

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

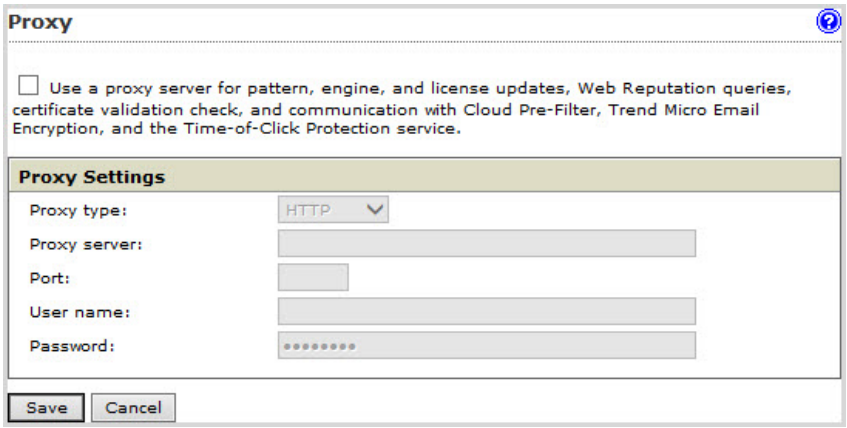
- Component updates (pattern files and scan engines)
- Product license registration
- Web Reputation queries to the Smart Protection Network
- Cloud Pre-Filter service and Smart Feedback
- Trend Micro Email Encryption

- Certificate validation check
- Time-of-Click Protection service

Procedure

1. Go to **Administration** > **Proxy**.

   The **Proxy** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates, Web Reputation queries, certificate validation check, and communication with Cloud Pre-Filter, Trend Micro Email Encryption, and the Time-of-Click Protection service**.

3. Specify the proxy protocol: **HTTP**, **SOCKS4**, or **SOCKS5**.

   Tip

   When using Cloud Pre-Filter, Trend Micro recommends using **HTTP** or **SOCKS5**.

   Certificate validation check only uses **HTTP**.

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 start the EUQ Management Console.

- **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 Management Console**: Acts as 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 **System Status**.

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

Opening the End-User Quarantine Console

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

1. Configured the LDAP settings. See *Configuring LDAP Settings on page 3-6*.
2. Enabled User Quarantine Access. See *Enabling End-User Access on page 28-8*.

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

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

- Primary EUQ service:

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

- Secondary EUQ service:

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

WARNING!

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

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

Logon Name Format

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

TABLE 2-1. EUQ Logon Name Formats

AUTHENTICATION TYPE	LOGON NAME FORMAT

LDAP	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`
	• **Microsoft Active Directory Global Catalog**
	  • Without Kerberos: `user1@domain.com (UPN)` or domain\user1
	  • With Kerberos: `user1@domain.com`
	• **OpenLDAP**: `cn=manager`, `dc=test1`, `dc=com`
	• **Sun iPlanet Directory**: `uid=user1`, `ou=people`, `dc=domain`, `dc=com`

SMTP	Use any valid email address for the logon name. **Note** IMSS supports `auth login`, `auth plain` and `starttls`.

Chapter 3

Using the Configuration Wizard

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

Topics include:

- *Accessing the Configuration Wizard on page 3-2*
- *Configuring Notification Settings on page 3-2*
- *Configuring the Update Source on page 3-4*
- *Configuring LDAP Settings on page 3-6*
- *Configuring Internal Addresses on page 3-9*
- *Configuring Control Manager Server Settings on page 3-10*
- *Activating the Product on page 3-12*
- *Verifying Settings Summary on page 3-13*

Accessing the Configuration Wizard

Access the wizard using one of the following methods:

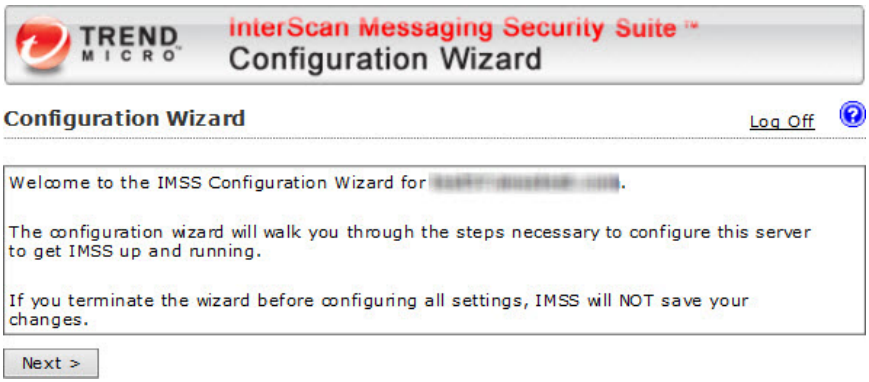
Procedure

- 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.

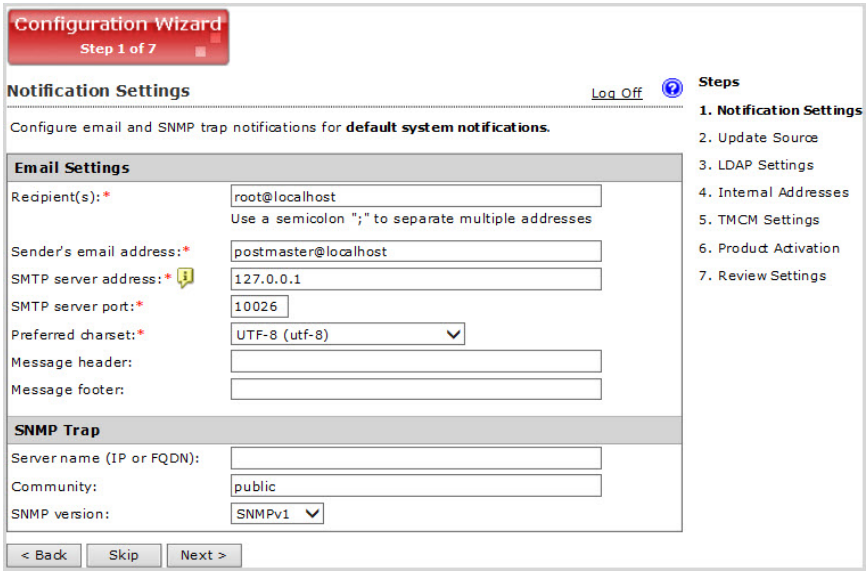


Configuring Notification Settings

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 or IPv6) of the SMTP server that delivers email on the network.
   - **SMTP server port**: Specify the port number that IMSS uses to connect to the SMTP server.
   - **Preferred charset**: IMSS will use this setting to encode the notification messages.
   - **Message header**: Specify the text to appear at the top of the notification.

- **Message footer**: Specify the text to appear at the bottom of the notification.

3. Under **SNMP Trap**, configure the following:

Note

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

- **Server name**: Specify the FQDN or IP address of the SNMP server.
- **Community**: Specify the SNMP server community name.
- **SNMP version**: Select **SNMPv1** or **SNMPv2c**.

Note

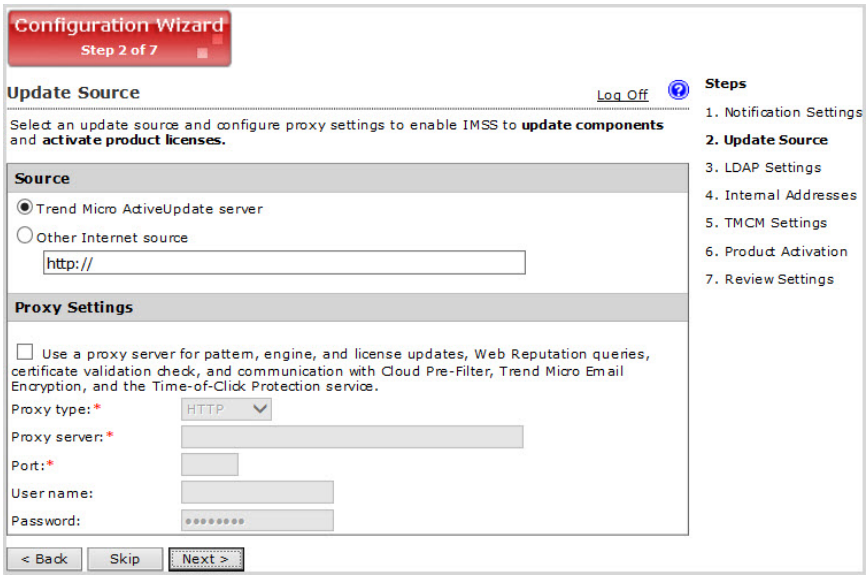
Community is the group that computers and management stations running SNMP belong to. To send the alert message to all SNMP management stations, specify "public" as the community name. For more information, refer to the SNMP documentation.

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://<IP address of Control Manager server or CQDN>/ Tvcs Download/ActiveUpdate/`, if applicable.
Proxy Settings	Select the **Use a proxy server for pattern, engine, and license updates, Web Reputation queries, certificate validation check, and communication with Cloud Pre-Filter, Trend Micro Email Encryption,**

Option	Description
	and the Time-of-Click Protection service check box and configure the proxy type, server name, port, user name, and passwords.

Configuring LDAP Settings

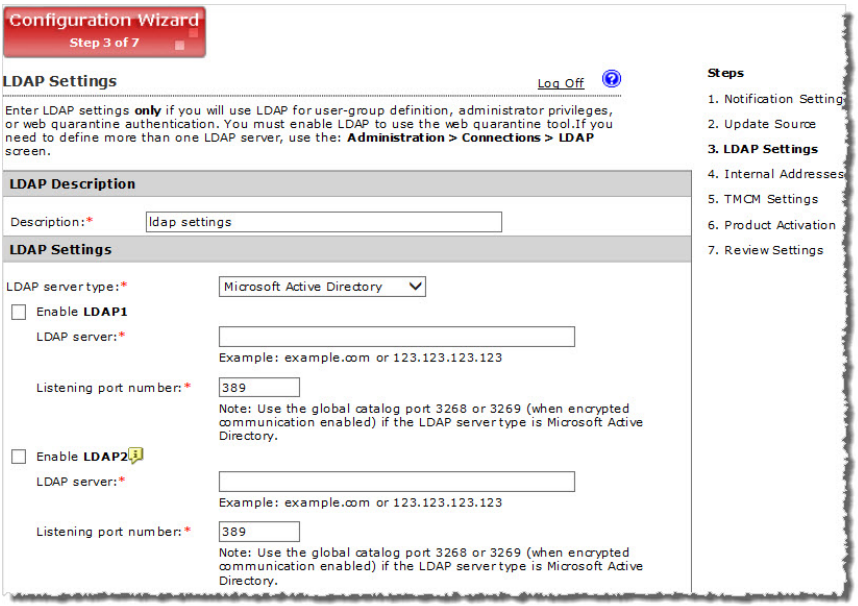
Note

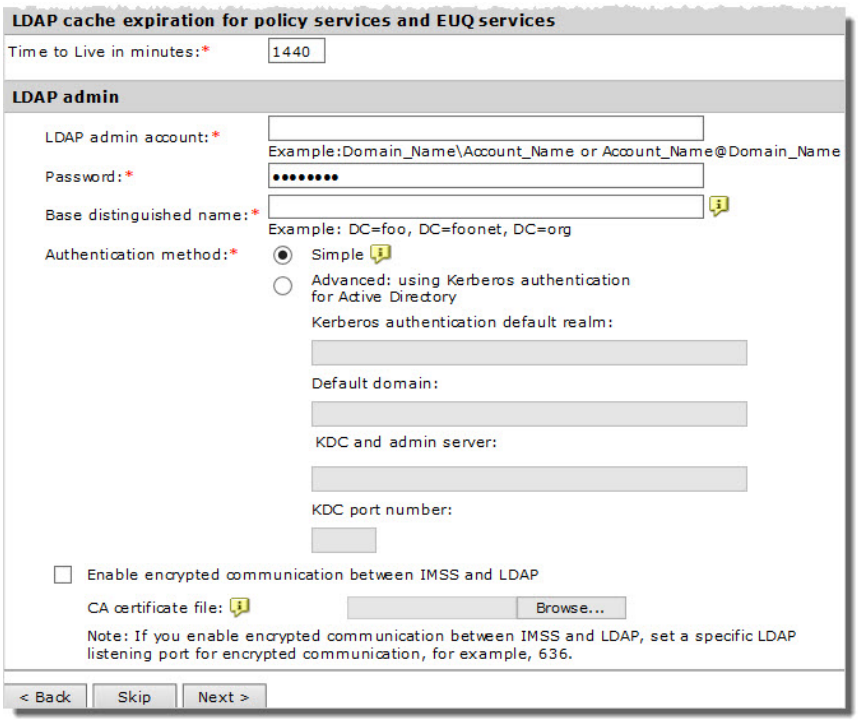
Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or End-User Quarantine authentication.

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**
      - **Microsoft AD Global Catalog**
      - **Open LDAP**
      - **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)
Active Directory Global Catalog	Without Kerberos: `user1@domain.com` (UPN) or `domain\user1` With Kerberos: `user1@domain.com`	dc=domain, dc=com dc=domain1,dc=com (if mutiple unique domains exist)	Simple Advanced (with Kerberos)
OpenLDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com	Simple
Lotus Domino™	user1/domain	Not applicable	Simple

LDAP Server	LDAP Admin Account (examples)	Base Distinguished Name (examples)	Authentication Method
Sun™ iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	uid=user1, ou=people, 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.

g. Select the **Enable encrypted communication between IMSS and LDAP** check box and click **Browse** to upload a CA certificate file to verify the certificate used by the LDAP server.

Configuring Internal Addresses

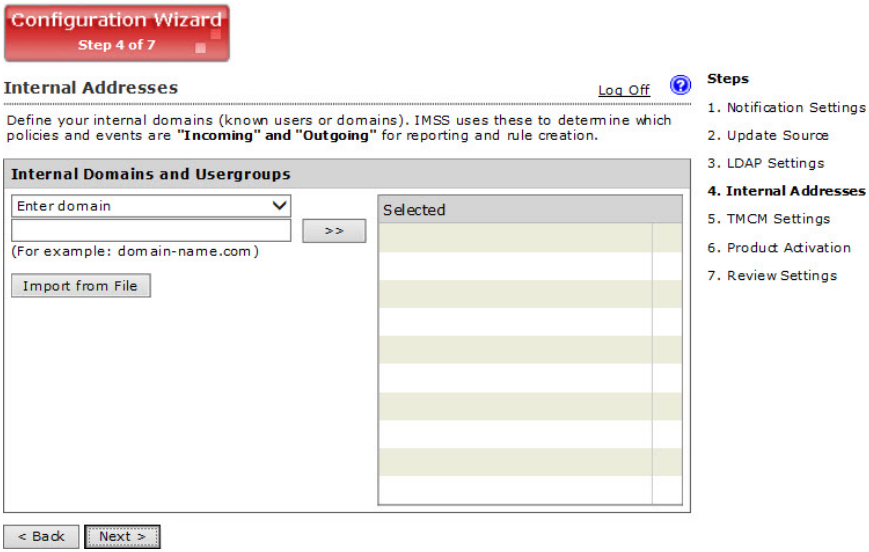
IMSS uses the internal addresses to determine whether a policy or an event is inbound or outbound.

- 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:

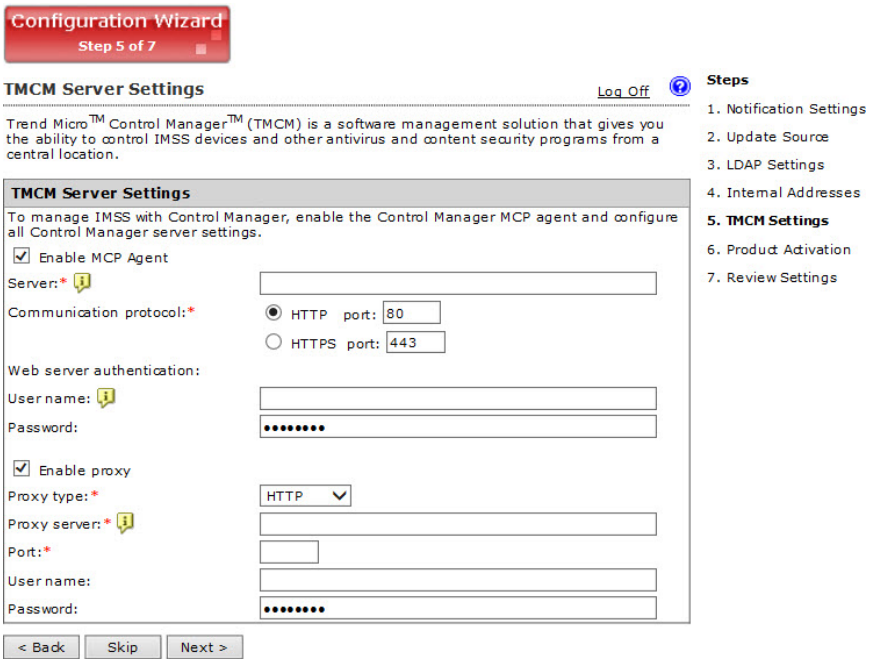
   - Select **Enter domain** from the drop-down list, specify the domain in the text box, and then click **>>**.
   - Select **Search for LDAP groups** from the drop-down list. A screen for selecting the LDAP groups appears. Specify an LDAP group name to search in the text box and click **Search**. The search result appears in the list box. To add it to the **Selected** list, click **>>**.
   - Click the **Import** button to import a text file containing a list of predefined domains.

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 IPv6) or FQDN.

   c. Next to **Communication protocol**, select **HTTP** or **HTTPS** and specify the corresponding port number.

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

d. Under **Web server authentication**, specify the user name and password for the web server if it requires authentication.

e. If a proxy server is between IMSS and Control Manager, select **Enable proxy**.

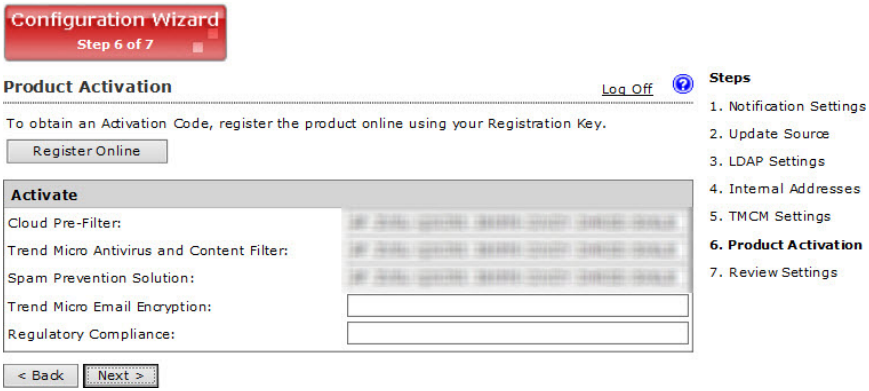
f. Specify the proxy server port number, user name, and password.

Activating the Product

Procedure

1. Click **Next**.

   The **Product Activation** 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**.

   The **Review Settings** screen appears.

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

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

Chapter 4

Updating Components

This chapter explains how to update IMSS components.

Topics include:

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

Updating Engine and Pattern Files

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

The following table provides a list of all IMSS components.

TABLE 4-1. IMSS Components

COMPONENT	DESCRIPTION
Virus Scan Engine	The Virus Scan Engine detects Internet worms, mass-mailers, Trojans, phishing sites, spyware, network exploits and viruses in messages and attachments.
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.

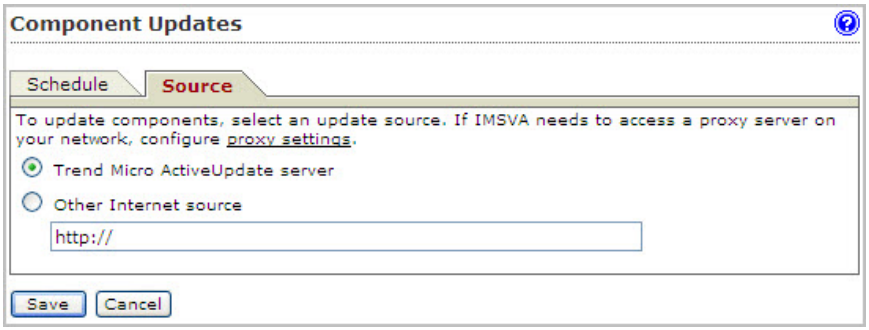
If you did not specify the update source when configuring IMSS using the Configuration Wizard, provide the update source and/or any proxy settings.

Procedure

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

   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. Click **Save**.

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

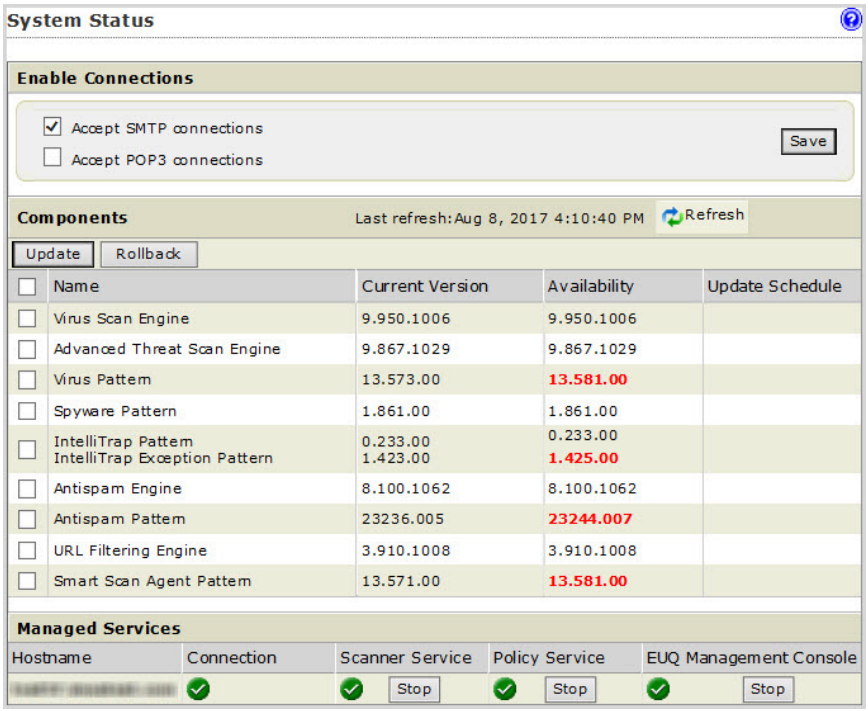
Performing a Manual Update

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 **System Status** 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 **System Status** screen.
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.

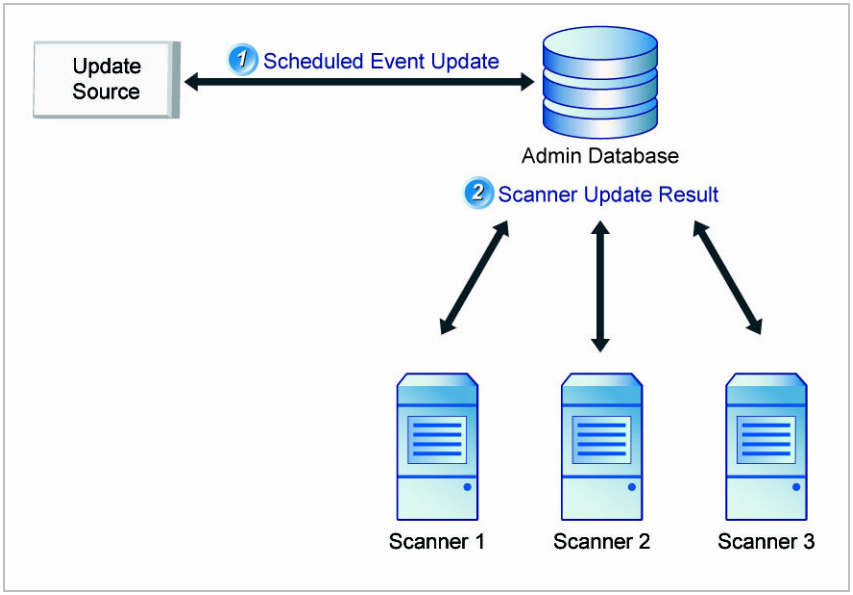


FIGURE 4-1. Scan engine and pattern file updates

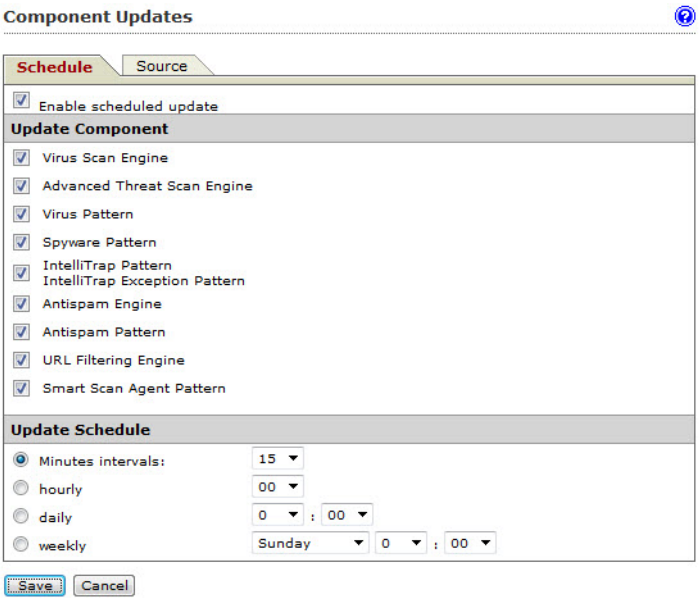
Configuring Scheduled Updates

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** > **Components**.

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

Getting Started with Cloud Pre-Filter

This chapter deals exclusively with Cloud Pre-Filter and how it is used with IMSS.

Topics include:

- *Understanding Cloud Pre-Filter on page 5-2*
- *Creating a Cloud Pre-Filter Account on page 5-5*

Understanding Cloud Pre-Filter

Cloud Pre-Filter service is a managed email security service powered by the Trend Micro Email Security SaaS Solutions. By routing your inbound messages through the service, you can protect your domains against spam, phishing, viruses, and other messaging threats before the threats reach your network.

Mail Flow With and Without Cloud Pre-Filter

Without Cloud Pre-Filter, messages containing viruses, spam, and other malicious threats reach your network directly. These malicious messages waste network bandwidth and staff resources for the administration effort of handling malicious messages.

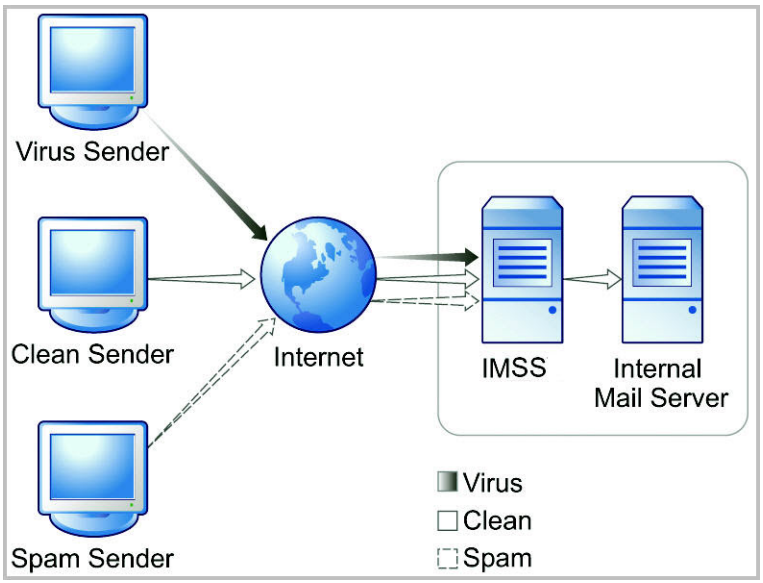


FIGURE 5-1. Mail flow without Cloud Pre-Filter

With Cloud Pre-Filter, you can protect your domains against malicious messages coming from outside your network. Cloud Pre-Filter blocks malicious messages before they reach your network.

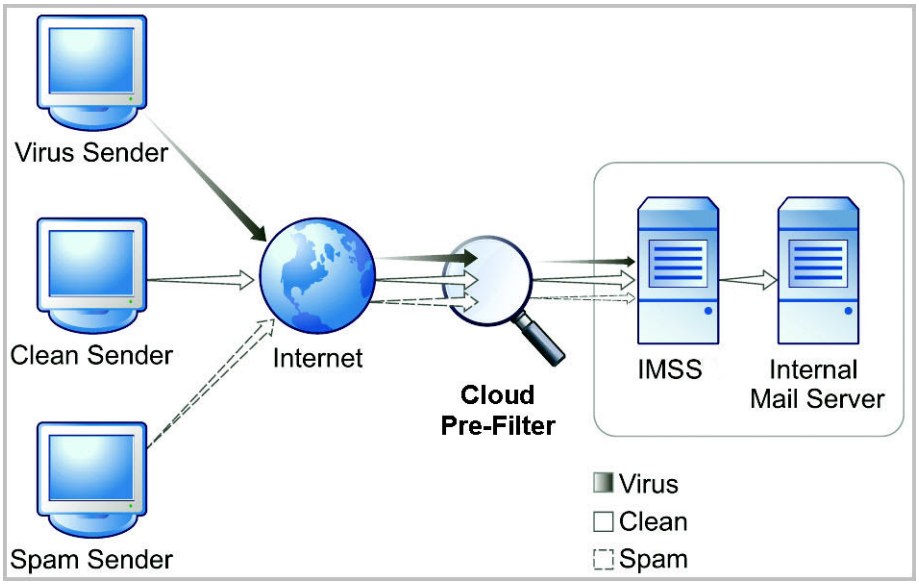


FIGURE 5-2. Mail flow with Cloud Pre-Filter

Cloud Pre-Filter and IMSS Communication

Cloud Pre-Filter uses the SMTP protocol to route messages to IMSS.

IMSS uses an HTTPS connection to communicate with Cloud Pre-Filter for command requests, such as creating an account, managing polices related to an account, and retrieving message tracking and report data.

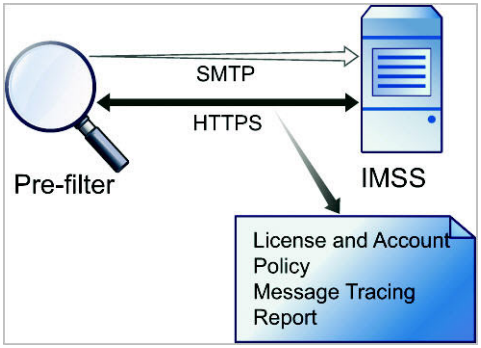


FIGURE 5-3. Cloud Pre-Filter and IMSS

Cloud Pre-Filter Terminology

When referring to Cloud Pre-Filter, the following terminology applies.

TABLE 5-1. Cloud Pre-Filter Terminology

TERM	DESCRIPTION
Account	The Cloud Pre-Filter account is used to manage Cloud Pre-Filter policies. You must create one Cloud Pre-Filter account before you use the Cloud Pre-Filter service. IMSS stores the account information locally after creating an account. IMSS uses the account information to communicate with Cloud Pre-Filter to complete command requests, such as managing Cloud Pre-Filter policies and retrieving message tracking or report data.

Term	Description
Policy	Cloud Pre-Filter policies apply to your domains. You can create only one policy per domain. When the messages sent to the domain reach Cloud Pre-Filter, Cloud Pre-Filter uses the policy for that domain to determine how to scan the messages and how to route the messages to the domain. Cloud Pre-Filter rejects all messages to domains that do not exist in the Cloud Pre-Filter policy list. Cloud Pre-Filter service stores all policies in the cloud.
Inbound Server	Inbound servers of Cloud Pre-Filter are the servers that receive your inbound messages. Cloud Pre-Filter provides the inbound server addresses when you create a domain to change your MX records.

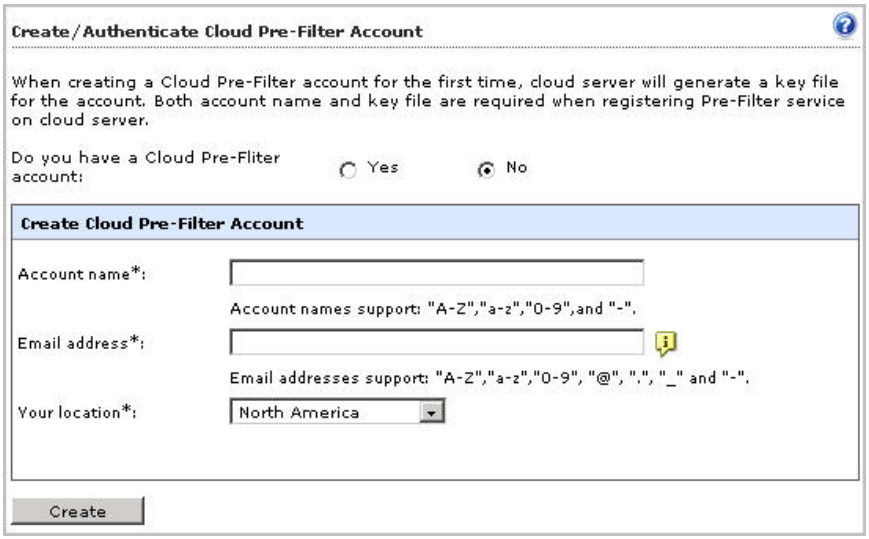
Creating a Cloud Pre-Filter Account

Before you can use Cloud Pre-Filter you must create a Cloud Pre-Filter account.

Procedure

1. Click **Cloud Pre-Filter**.

The **Create/Authenticate Cloud Pre-Filter Account** screen appears.



2. Select **No** next to **Do you have a Cloud Pre-Filter account:**.
3. Specify an account name and email address for the account.
4. Specify your location from the **Your location** list. This setting specifies which of the global Trend Micro data centers you use.
5. Click **Create**.

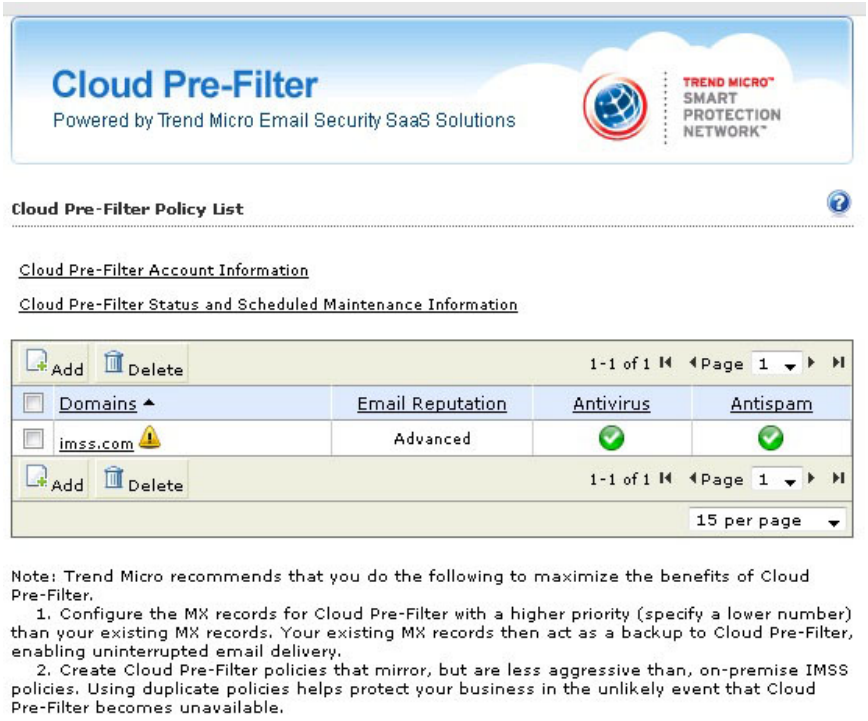
   IMSS generates a key for the Cloud Pre-Filter account.

6. Save this key to a secure location. IMSS uses the key and the user name to authenticate connection to Cloud Pre-Filter.

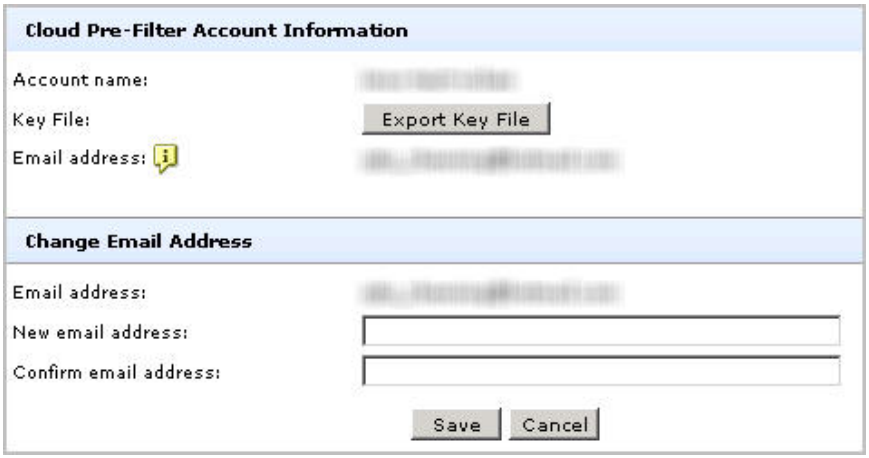
> **Tip**
>
> Trend Micro recommends saving the key file. The key file contains your account password, data center information, and other related settings.

7. Click **Load Cloud Pre-Filter service**.

   The **Cloud Pre-Filter Policy List** screen appears.



8. To view the account information, click **Cloud Pre-Filter Account Information** on the **Cloud Pre-Filter Policy List** screen.


Cloud Pre-Filter Account Information
Account name:
Key File:
Export Key File
Email address:
Change Email Address
Email address:
New email address:
Confirm email address:
Save
Cancel

Chapter 6

Getting Started with ATSE and Virtual Analyzer

This chapter explains how to enable Advanced Threat Scan Engine (ATSE) and configure Virtual Analyzer.

Topics include:

- *Scan Technology on page 6-2*
- *About Advanced Threat Scan Engine on page 6-2*
- *About Virtual Analyzer on page 6-4*

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 6-1. 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 Virtual Analyzer for further analysis. **Note** IMSS integrates with Virtual Analyzer, which is an isolated virtual environment used to manage and analyze samples within Deep Discovery Analyzer.

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. Go 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 Virtual Analyzer

IMSS integrates with Virtual Analyzer in Deep Discovery Analyzer, which is a separately licensed product that provides on-demand analysis of file and URL samples.

IMSS sends suspicious messages, including attachments, to Virtual Analyzer for further analysis. If Virtual Analyzer scanning is enabled for certain attachment file types, messages with those attachments are also sent to Virtual Analyzer. 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.

ATSE Detections and Virtual Analyzer

IMSS leverages ATSE to determine which messages are sent to Virtual Analyzer. 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**, **EXPL** and **AFI MACRO**. If the detection name contains one of these prefixes, IMSS:

- Sends the entire message (including attachments) to Virtual Analyzer for further analysis.
- Determines further action based on the analysis result from Virtual Analyzer.

Virtual Analyzer assigns a risk level to each analyzed message. IMSS queries this risk level approximately 60 seconds after sending the message to Virtual Analyzer. After receiving the risk level, IMSS determines whether the message is a clean message, 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.

Virtual Analyzer Risk Levels and IMSS Security Level Settings

IMSS processes an ATSE-detected message based on the risk level returned by Virtual Analyzer and the security level that you select on the IMSS management console. Possible scenarios are:

- If the returned risk level does not match the security level you select, IMSS determines that the message is a clean message.
- If no risk level is returned, or if the returned risk level is invalid, or if the maximum time allowed for Virtual Analyzer analysis expires, IMSS triggers a Virtual Analyzer scanning exception and logs the detection as a **Probable advanced threat (ATSE)**.
- If the returned risk level matches the security level you select, IMSS performs specified action and logs the detection as an **Analyzed advanced threat (ATSE)**.

  The following table contains the security levels, the corresponding Virtual Analyzer risk levels, and the actions triggered by IMSS.

Tip

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

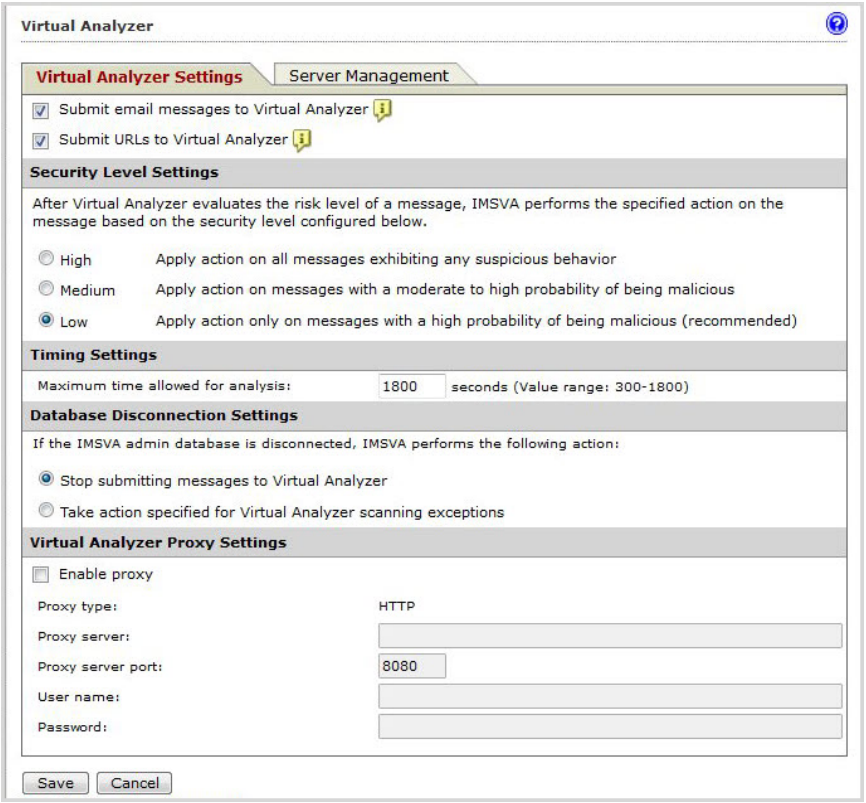
Security Level	Description	Risk Level
High	Apply action on all messages exhibiting any suspicious behavior	• High risk • Medium risk • Low risk
Medium	Apply action on messages with a moderate to high probability if being malicious	• High risk • Medium risk
Low	Apply action only on messages with a high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

Configuring Virtual Analyzer Settings

Procedure

1. Go to **Policy** > **Virtual Analyzer**.

The **Virtual Analyzer Settings** tab appears by default.



2. Select **Submit email messages to Virtual Analyzer**.
3. Select **Submit URLs to Virtual Analyzer**.
4. Configure the **Security Level** settings for the messages that Virtual Analyzer analyzes.

Note

The security level determines the Virtual Analyzer risk level that triggers an action from IMSS. For more information, see *Virtual Analyzer Risk Levels and IMSS Security Level Settings on page 6-5*.

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

5. Set the maximum time allowed for Virtual Analyzer analysis.
6. Select either of the following actions to perform when the IMSS admin database is disconnected:
   - **Stop submitting messages to Virtual Analyzer**
   - **Take action specified for Virtual Analyzer scanning exceptions**
7. Configure the Virtual Analyzer proxy server settings.
   - Proxy server
   - Proxy server port
   - User name
   - Password

Note

IMSS supports only HTTP proxies.

8. Click **Save**.

Note

IMSS can notify you if Virtual Analyzer is unable to return a valid or complete analysis result. For details about notifications, see *Notifications on page 26-1*.

Adding Virtual Analyzer Servers

To achieve better load balancing and failover capabilities, IMSS allows you to add multiple servers for Virtual Analyzer. The round-robin algorithm is used for the servers that have the same preference.

You can also enable, disable and delete Virtual Analyzer servers on the IMSS management console.

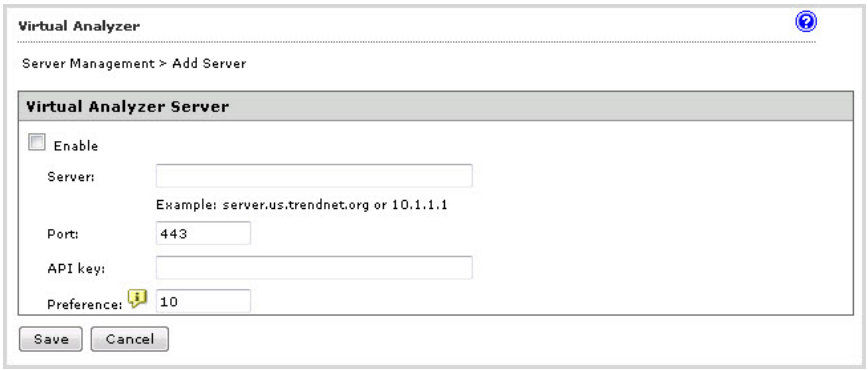
Procedure

1. Go to **Policy** > **Virtual Analyzer**.

   The **Virtual Analyzer Settings** tab appears by default.

2. Click the **Server Management** tab.

3. Click **Add**.



4. Select the **Enable** check box.

5. Specify the server FQDN or IP address, port number, API key and preference value.

Note

Preference represents the priority of Virtual Analyzer servers. The lower the preference value, the higher the priority.

6. Click **Save**.

Chapter 7

Getting Started with Email Encryption

This chapter deals exclusively with Trend Micro Email Encryption and how it is used with IMSS.

Topics include:

- *Understanding Email Encryption on page 7-2*
- *Using Email Encryption on page 7-3*
- *Registering for Email Encryption on page 7-3*
- *Managing Domains on page 7-4*
- *Registering Domains on page 7-5*

Understanding Email Encryption

Trend Micro Email Encryption encrypts messages using Indentity-Based Encryption (IBE). For example, `user1@a.com` sends a message with private information to `user2@b.com`. The domain a.com is registered with IMSS for encryption and decryption. A policy rule enables outgoing messages containing private information to be encrypted. IMSS encrypts the message sent to this `user2@b.com`.

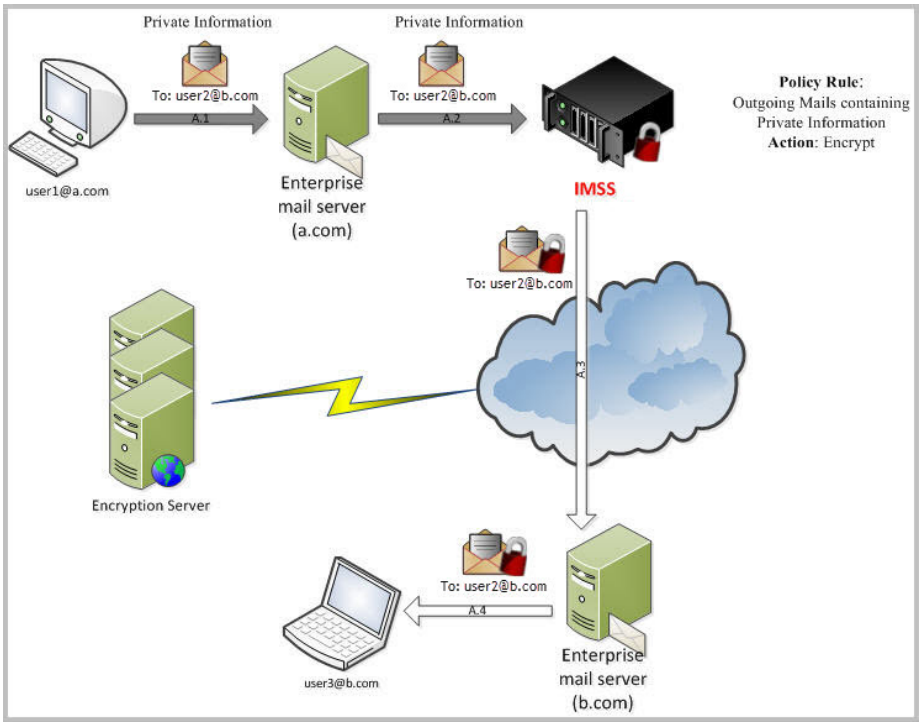


FIGURE 7-1. IMSS Email Encryption

Tip

Before using Trend Micro Email Encryption, Trend Micro recommends that an NTP server is used with IMSS. This ensures standard time and date data for IMSS.

Using Email Encryption

Using Trend Micro Email Encryption requires following these steps:

- **Step 1**: Register IMSS to the encryption service (See *Registering for Email Encryption on page 7-3*)
- **Step 2**: Register domains to the encryption service (See *Registering Domains on page 7-5*)
- **Step 3**: Configure policies to encrypt your messages (See *Adding Policies on page 17-2*)

Registering for Email Encryption

To encrypt messages with Trend Micro Email Encryption technology, IMSS needs to be registered to the Trend Micro Email Encryption Server.

Procedure

1. Go to **Policy** > **Encryption Settings**.

   The Register Trend Micro Email Encryption screen appears.

2. Provide your contact information.

Note

The email address you provide in the contact information is very important for registering your domains to the Email Encryption Server. Key files are sent to the email address you provide. Upload key files to complete the domain ownership process.

The Trend Micro Email Encryption Server team contacts you using the email address. The email address is only used for receiving key files and notifications. The contact email address will not be used for marketing purposes.

You cannot change your contact information unless you have registered at least one domain successfully.

3. Click **Next**.

   Your contact information is sent to the Trend Micro Email Encryption Server.

Note

It may take one or two working days before you receive the information to complete domain ownership verification. If you do not receive a message within 3 working days, contact your sales representative.

What to do next

To change your contact information, click **Change** on the **Gateway Info** tab.

Note

The **Change** button is not enabled until at least one domain has been registered successfully.

Managing Domains

The **Manage Domains** tab enables the administrator to register new domains for use with the IMSS email encryption features. When a domain is

registered with the encryption service, it is permitted to obtain private keys for email addresses on that domain. For example, you want to register `mycompany.org`. After the registration is authorized and completed on the encryption service, IMSS will be able to obtain private keys to decrypt messages to `user01@mycompany.org`, `user02@mycompany.org`, and so on. The security processes and checks to authorize an IMSS domain registration, and will include checking publicly available information that might include contacting the domain registrant.

Note

For security reasons, the person who is the registered owner of the domain will be contacted by the registration team to validate the IMSS registration. Therefore, to register a domain, you must be the owner of, or have the permission of, the owner of the domain name.

You can remove a domain from IMSS by selecting the **[Delete]** link next to the domain. This removes the registration information from the encryption service's database and it will no longer be possible to obtain private keys for email addresses on this domain.

Registering Domains

When registering domains to the Trend Micro Email Encryption Server, messages are sent to the following email addresses to verify ownership of the domains:

- `postmaster@<domain>`
- `webmaster@<domain>`
- the email address returned from a WHOIS lookup for the domain

WARNING!

The postmaster and webmaster accounts must exist and be enabled before domains can be registered.

Trend Micro sends a message to the "Contact Information" email address to verify that the domain exists and that the `postmaster@<domain>` and `webmaster@<domain>` accounts exist and are enabled.

WARNING!

One of the following must respond to the verification message:

- `postmaster@<domain>`
- `webmaster@<domain>`
- the email address returned from a WHOIS lookup for the domain

By design, after a domain is registered, it cannot be re-registered. If a domain has already been registered, subsequent re-registration results in a "domain already registered" error. This is enforced for the purpose of security. If there is a need to reinstall IMSS, backup the database prior to re-installation, and restore it afterwards. This eliminates the need to re-register IMSS and the same domains after re-installation.

Note

IMSS must be registered to the encryption service before any domains can be registered.

The default sender address for your domains will be `postmaster@<domain>`. You can customize the default sender address from the Encryption Settings screen.

The default sender address is used when IMSS tries to encrypt a message, but whose domain is not in the Domain List. IMSS signs these messages with the default sender address.

Registering Domains to the Encryption Service

Procedure

1. Go to the **Policy** > **Encryption Settings** screen.
2. Click the **Domain** tab.
3. Click **Add**.
4. Add the domains you want to protect to the domain list.

   Domains can be manually typed or selected from a list of existing domains. Up to 10 domains can be added at a time.

   Note

   Domains and their sub-domains are treated as unique entries. Sub-domains must be added separately to the domain list.

   Wildcards cannot be used to include sub-domains.

   LDAP groups (entries starting with" LDAP") cannot be added to the domain list.

5. Click **Save**.

   A progress bar appears as the domain information is sent to the Trend Micro Email Encryption Server. A confirmation screen appears that verifies the domain information was received by the Trend Micro Encryption Server.

6. Read the instructions about what to do once you receive the verification key file.
7. Click **Done**.

   The domains appear in the Domain list on the **Domain** tab and a message about the **Domain** tab.

8. If you are the registered owner of the domain, reply to the confirmation message from the Trend Micro Encryption Server. The message is sent

to `postmaster@<domain>` and `webmaster@<domain>`. When your domains are approved, you receive the domain ownership verification key file. You must reply to the confirmation message to prove that you are the owner of the domain.

Note

It may take one or two working days before you receive the key file to register the domain(s) to the encryption service. A key file is sent for each domain that is registered.

If you do not receive a message within 3 working days, contact your sales representative.

9. Once you receive the key file, save it to a secure location.
10. Go to the **Encryption Settings** screen.
11. Click **Browse** and locate the key.
12. Click **Upload**.

    A confirmation message appears when registration completes successfully.

Part II

Configuring IMSS

Chapter 8

Configuring Cloud Pre-Filter

This chapter explains how to configure Cloud Pre-Filter.

Topics include:

- *Understanding Cloud Pre-Filter Policies on page 8-2*
- *Creating a Cloud Pre-Filter Policy on page 8-3*
- *Verifying Cloud Pre-Filter Works on page 8-14*
- *Configuring DNS MX Records on page 8-14*
- *Suggested IMSS Settings When Using Cloud Pre-Filter on page 8-15*
- *Disabling Cloud Pre-Filter on page 8-17*

Understanding Cloud Pre-Filter Policies

The Cloud Pre-Filter service offers policy-based management of your email security. The policy for a domain regulates how each filter is applied to messages sent to the domain.

The following table lists the information that defines each policy.

TABLE 8-1. Cloud Pre-Filter Policies

SECTION	DESCRIPTION
Domain	The domain that will be covered by the policy. With the correct routing settings, all messages to this domain are protected by Cloud Pre-Filter. Each domain must be unique, and only one policy can be applied to a domain.
Valid Recipient	This setting works by comparing the list of users on your LDAP servers to a list of your users on Cloud Pre-Filter. The Cloud Pre-Filter list of your users is generated by synchronizing with your LDAP servers. Use the valid recipient check to block all messages that do not have a recipient on your domain. This prevents malicious messages and spam from reaching your network.
Filter settings	These settings define the following Cloud Pre-Filter filtering options: • Whether a filter is enabled or not • For filters that support this option, how each filtering criterion is applied • For filters that support this option, what filter actions to perform
Destination servers	Destination servers are the inbound mail servers for the domain. These servers receive messages bound for the domain after they are processed by the Cloud Pre-Filter service.
Approved and blocked senders	• **Approved Sender**: Messages from approved senders bypass the Email Reputation service and antispam filters. • **Blocked Sender**: Messages from blocked senders are blocked immediately and never reach your network.

Note

Trend Micro recommends that you create Cloud Pre-Filter policies that mirror, but are less aggressive than, on-premise IMSS policies. Using duplicate policies helps protect your business in the unlikely event that Cloud Pre-Filter becomes unavailable.

Considerations

- Each policy applies to one domain only and only one policy can be created for each domain.
- A policy comprises of a domain, filtering settings, approved and blocked sender lists, and destination servers.
- Review each filter type and assess whether you want to apply it to a domain before saving the policy. The following filters are enabled by default:
  - Email Reputation
  - Antivirus
  - Antispam

Tip

Trend Micro recommends that you have the antivirus and antispam filters enabled and properly configured. Without these filters, the domain is highly vulnerable to large numbers of unwanted mail and infected messages.

Creating a Cloud Pre-Filter Policy

To provide email security services to a domain, create a policy for that domain.

Note

If your network uses a proxy server, verify your proxy settings are correct at **Administration** > **Proxy**, before creating a Cloud Pre-Filter policy.

Creating a Cloud Pre-Filter policy requires the following steps:

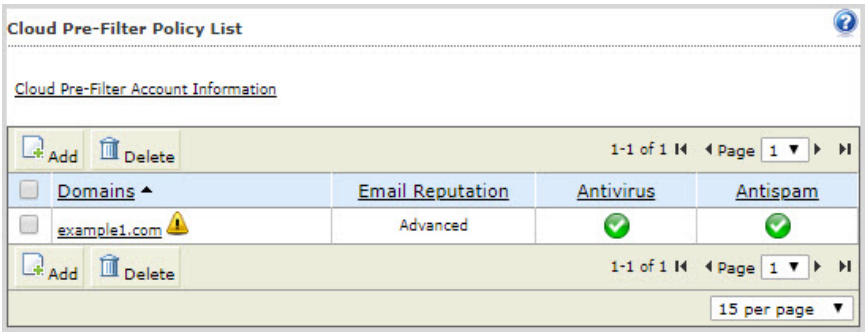
- *Step 1: Domain Settings on page 8-4*
- *Step 2: Configuring Condition Settings on page 8-7*
- *Step 3: Configuring Filter Settings on page 8-11*

Step 1: Domain Settings

Procedure

1. Click **Cloud Pre-Filter**.

   The **Cloud Pre-Filter Policy List** screen appears.



2. Click **Add**.

The **Step 1: Specify Domain and Destination Server** screen appears.

3. Provide the name of the domain to protect.

Note

Specify a domain or subdomain, for example, domain.com or *.domain.com. Top-level domains are not allowed, and only a single level of subdomain matching is supported.

4. Click **Add** under Specify Destination Server.

The **Destination Server** screen appears.

5. Specify the addresses of the domain's actual destination servers to allow Cloud Pre-Filter to relay messages to these servers after processing.

   a. Select one of the following from the **Address Type** drop-down list:

      - **IP address**: IP address of the MTA or IMSS that receives messages from Cloud Pre-Filter
      - **A record**: Hostname Cloud Pre-Filter uses for DNS lookup
      - **MX record**: Mail exchange record Cloud Pre-Filter uses for DNS lookup

      Note

      A policy can only contain one address type for a destination server. An IP address and an A record are considered to be the same type. An MX record is considered to be a different type.

   b. Provide an address for IMSS in the **Address** field.

   c. Provide a port number for communication between IMSS and Trend Micro Email Security SaaS Solutions. The default value is port 25.

d. Provide a value for **Priority** for the destination server.

The Priority option specifies routing priority for the destination servers. Cloud Pre-Filter service will attempt to route messages to servers with higher priority values first. The lower the number, the higher the priority.

You do not need to specify a priority for an **MX record** destination server. The priority for the MX record will be resolved automatically.

6. Click **Add**.

The **Step 1: Specify Domain and Destination Server** screen appears, with IMSS's details in the Destination Server list.

Step 2: Configuring Condition Settings

Approved and Blocked Senders

Messages from Approved Senders are able to bypass the Email Reputation service and antispam filters, while messages from Blocked Senders are prevented from reaching recipients.

Specifying an IP address will block or approve all messages from that IP address.

The approved lists take precedence over the blocked list, the Email Reputation filter, and the antispam filter. All messages from addresses that match the addresses in the approved list are not processed by these filters.

Note

The Approved list from Email Reputation, IP Profiler or spam rules can be imported to the Cloud Pre-Filter Approved list.

Valid Recipients

This feature works by comparing the list of users on your LDAP servers to a list of your users on Cloud Pre-Filter. The Cloud Pre-Filter list of your users is generated by synchronizing with your LDAP servers.

Use the valid recipient check to block all messages that do not have a recipient on your domain. This prevents malicious messages and spam from reaching your network.

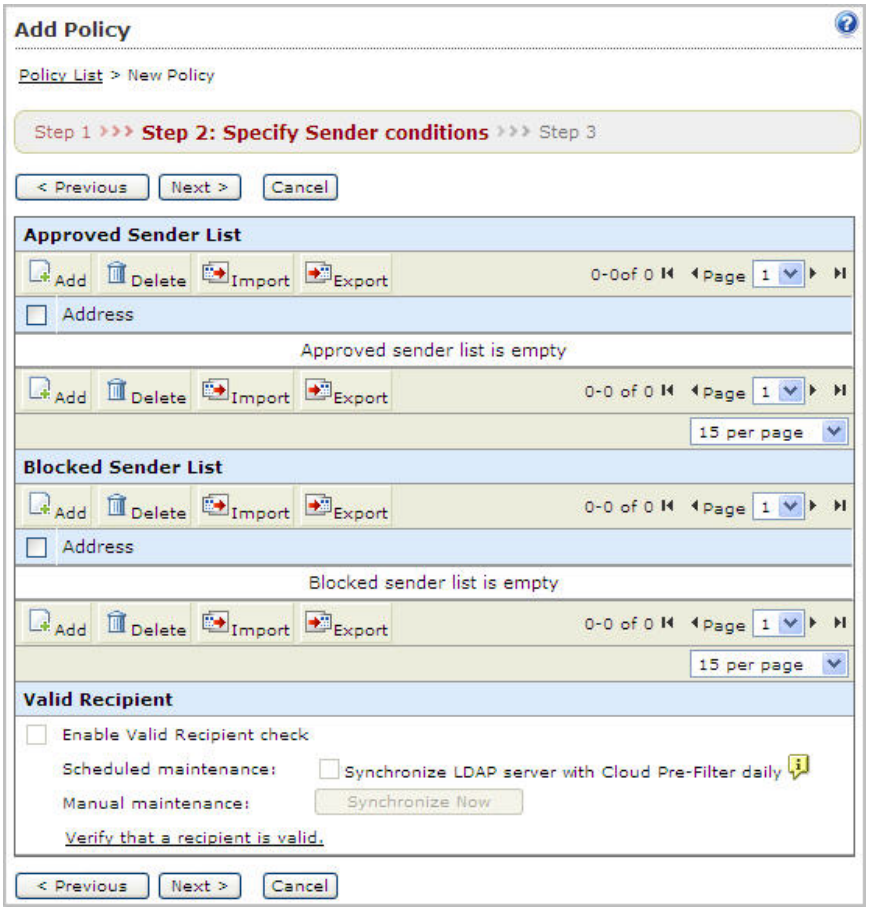
Tip

Trend Micro recommends enabling scheduled synchronization to ensure all valid messages reach your network. LDAP servers must be configured before enabling the valid recipient check and scheduled synchronization.

Procedure

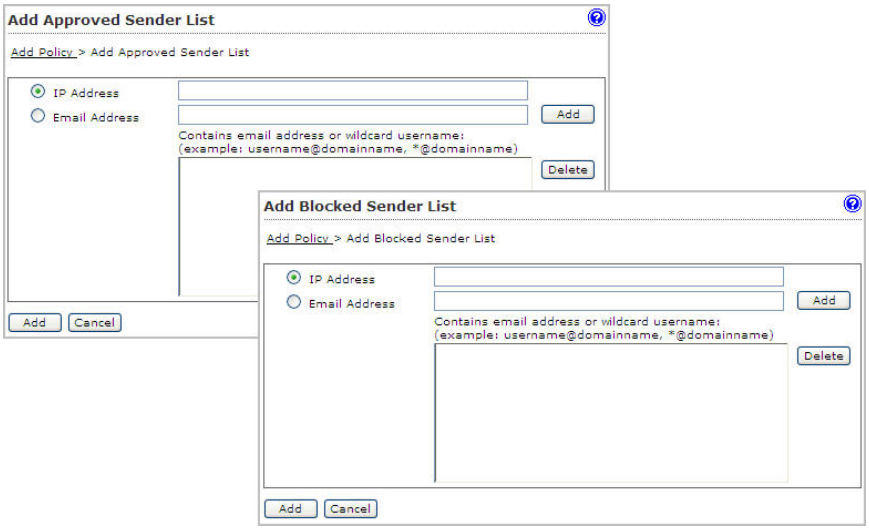
1. Click **Next**.

The **Step 2: Specify Sender conditions** screen appears.



2. Click **Add** to add an entry to the list.

The **Add Approved Sender List** or **Add Blocked Sender List** screen appears.



3. Provide an email address or IP address.
4. Click **Add** beside the IP Address and Email Address fields.

   The entry appears in the list.

WARNING!

The wildcard character * may be used to specify any string in the local-part (local-part@domain.com) of email addresses. Use wildcard characters with caution as they may allow or block messages from a large set of email addresses.

5. Click **Add** under the list.

   The entry appears in the specified list.
6. To import entries to the approved or blocked senders list:
   - When using the import function, use a text file with only one full email or IP address per line.

- When importing sender addresses, ensure that you select the correct import mode. Selecting to replace addresses will delete all existing addresses from the list.

7. Click **Import** for the specified list.

   A dialog box appears.

8. Specify the file to import.

9. Click **Import**.

   The list displays the imported entries.

10. Select **Enable valid recipient check**.

11. Select **Synchronize LDAP server with Cloud Pre-Filter daily**.

Note

Trend Micro recommends enabling scheduled synchronization to ensure all vaild messages reach your network.

After upgrade, the recipient check and scheduled synchronization cannot work properly because the local LDAP cache is empty. You can manually trigger recipient check and scheduled synchronization by clicking **Save & Synchronize** in LDAP settings.

Step 3: Configuring Filter Settings

The Step 3: Select Filter screen contains settings for three filters:

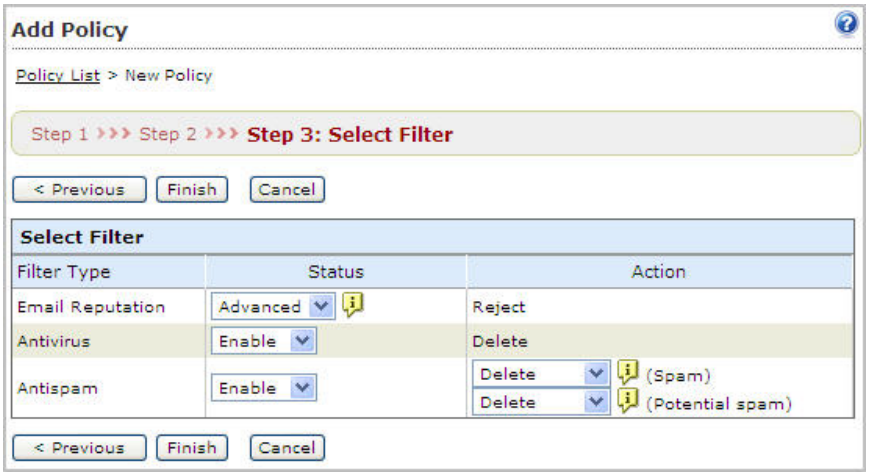
TABLE 8-2. Cloud Pre-Filter Filters

FILTER	DESCRIPTION
Email Reputation	Email Reputation enables you to take advantage of a dynamic and constantly updated email source rating system to block spam and other unwanted messages. Email Reputation blocks messages from source IP addresses whose current reputation ratings are poor. You can choose Email Reputation Advanced or Email Reputation Standard. Email Reputation Standard queries the standard reputation database. Email Reputation Advanced queries the standard reputation database as well as a dynamic database that is updated in real time.
Antivirus	When enabled, the antivirus filter can stop messages containing known and unknown malware code, whether this code is contained in an attachment or embedded in the message body. Messages found to contain malware code are automatically deleted.
Antispam	When enabled, the antispam filter checks messages for spam and phishing characteristics. The filter identifies messages as spam based on the selected catch rate. The antispam filter uses a Web Reputation and spam prevention filter to stop spam from entering your network. The antispam filter can use two approaches when detecting spam: • **Spam**: This setting is very conservative. Almost every "spam" detection is truly an unwanted message. This setting has the following actions: Delete and Quarantine. • **Potential Spam**: This setting is more aggressive. However, there may be some messages marked as "spam" that may be legitimate messages. This setting has the following actions: Delete, Quarantine, and Pass.

Procedure

1. Click **Next**.

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



2. Specify the status for the filters.
3. Specify the action for the filters.

   The filters use the following actions:

   - **Delete**: Deletes the entire message without quarantining it
   - **Quarantine**: Saves a copy of the entire message in the local IMSS quarantine area.

     Administrators can delete or deliver the message after assessing the message.
   - **Reject**: Rejects the message without quarantining it
   - **Pass**: Cloud Pre-Filter performs no action and sends the messages directly to IMSS. IMSS then scans the messages.
4. Click **Finish**.

Cloud Pre-Filter Policy List appears with the domain appearing in the list. The status for the filters display along with the domain.

Verifying Cloud Pre-Filter Works

You can verify that a policy works correctly before activating the policy.

For example:

You want to verify that a policy created for the domain `your-domain.com` processes your email traffic correctly and that Cloud Pre-Filter directs your messages to your IMSS.

To verify the policy works correctly, send a message with a specified sender and recipient account (the recipient's domain should be part of `your-domain.com`) directly to the Cloud Pre-Filter inbound server for `your-domain.com`.

An example Cloud Pre-Filter inbound server address for the policy is `im.emailsecurity.trendmicro.com`.

Send the test message to the inbound server address.

Wait a few minutes after sending the message and query the message tracking logs using Cloud Pre-Filter + IMSS data.

Note

The test message must be sent directly to the Cloud Pre-Filter inbound server for the domain. The Cloud Pre-Filter inbound server addresses for the domain appear on the **Domain** tab for the policy.

Configuring DNS MX Records

After configuring Cloud Pre-Filter settings and verifying that email traffic is delivered from Cloud Pre-Filter to IMSS, add the Cloud Pre-Filter "Inbound

Server Address" to the MX records for your DNS server. The Cloud Pre-Filter host displays under the **Inbound Server Address** section of the **Domain** tab. This is the final step before using Cloud Pre-Filter to scan your email traffic.

WARNING!

You MUST configure your mail delivery (MX) records to route your email traffic through Cloud Pre-Filter. If this step is not completed, your messages will be delivered to your local servers, and not to Cloud Pre-Filter for scanning.

Tip

Trend Micro recommends configuring the MX records for Cloud Pre-Filter with a higher priority (specify a lower number) than your existing MX records. Your existing MX records then act as a backup to Cloud Pre-Filter.

Suggested IMSS Settings When Using Cloud Pre-Filter

Cloud Pre-Filter uses port 9000 as the web service listening port. This port must be open on the firewall for IMSS to connect to Cloud Pre-Filter.

While Cloud Pre-Filter does not impact the deployment of IMSS, Cloud Pre-Filter does impact how you should configure IMSS.

TABLE 8-3. IMSS Recommended Settings When Using Cloud Pre-Filter

SECURITY SERVICE	RECOMMENDED ACTION
Sender Filtering (Email Reputation and IP Profiler)	When Cloud Pre-Filter filters messages for all your domains: **Disable or do not activate Sender Filtering** Cloud Pre-Filter uses Email Reputation to filter all messages before they reach your network. This makes using Sender Filtering (Email Reputation and IP Profiler) redundant.
	When Cloud Pre-Filter filters messages for some of your domains: **Enable and use Sender Filtering (Email Reputation and IP Profiler)** Cloud Pre-Filter is not using Email Reputation to scan all messages before they reach your network. The messages from domains that are not routed through Cloud Pre-Filter may still be malicious.
Spam Prevention Solution (SPS)	IMSS should always use SPS, which means antispam policies should still be created. Cloud Pre-Filter uses a very conservative approach to detect spam. Cloud Pre-Filter does this to lower the risk that a legitimate message is detected as spam. Using antispam policies on IMSS will further reduce the spam reaching your email recipients.
Trend Micro Antivirus and Content Filter	IMSS should always use the Antivirus and Content Filter, which means antivirus policies and content filtering policies should still be created. Cloud Pre-Filter does not support content filtering of messages. Content filtering policies must be created in IMSS. Also, even though Cloud Pre-Filter does filter for viruses, Trend Micro recommends creating antivirus policies.
DKIM	**Cloud Pre-Filter has no impact on DKIM.** Configure and use this feature as your network requires.

Security Service	Recommended Action
Transport Layer Security (TLS)	**Cloud Pre-Filter supports TLS.** If the MTA sending messages to Cloud Pre-Filter supports TLS, the messages are delivered using TLS. When messages reach Cloud Pre-Filter from an inbound server using TLS, Cloud Pre-Filter delivers the message to the destination server using TLS. If the destination server does not support TLS, the message is delivered over SMTP. When messages reach Cloud Pre-Filter from an inbound server that does not use TLS, Cloud Pre-Filter delivers the message to the destination server over SMTP.

Disabling Cloud Pre-Filter

There is no way to disable Cloud Pre-Filter from the IMSS management console. The only way to disable Cloud Pre-Filter is to change the DNS MX record of your domain to point to IMSS or to an MTA and then to IMSS.

Chapter 9

Configuring Sender Filtering Settings

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

Topics include:

- *Sender Filtering Service on page 9-2*
- *Using Email Reputation on page 9-2*
- *Configuring Sender Filtering on page 9-4*
- *Displaying Suspicious IP Addresses and Domains on page 9-17*

Sender Filtering Service

The Sender 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 Sender 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. Sender Filtering should act as the precursor to any application filtering you might use.

Note

Sender 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.

Preparing Your Message Transfer Agent for Use With Email Reputation Services

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

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

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

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

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

https://tmspn.securecloud.com/

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

Note

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

Using the Email Reputation Management Console

Visit the Email reputation management console at https://ers.trendmicro.com/ to access global spam information, view statistics, manage Email reputation settings, and perform administrative tasks.

For details, 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.

Configuring Sender Filtering

To configure Sender Filtering, perform the following steps:

1. *Enabling Email Reputation and IP Profiler on page 9-4*
2. *Adding Approved List Records on page 9-5*
3. *Adding Blocked List Records on page 9-6*
4. *Enabling Sender Filtering Rules on page 9-7*
5. *Configuring Email Reputation on page 9-14*

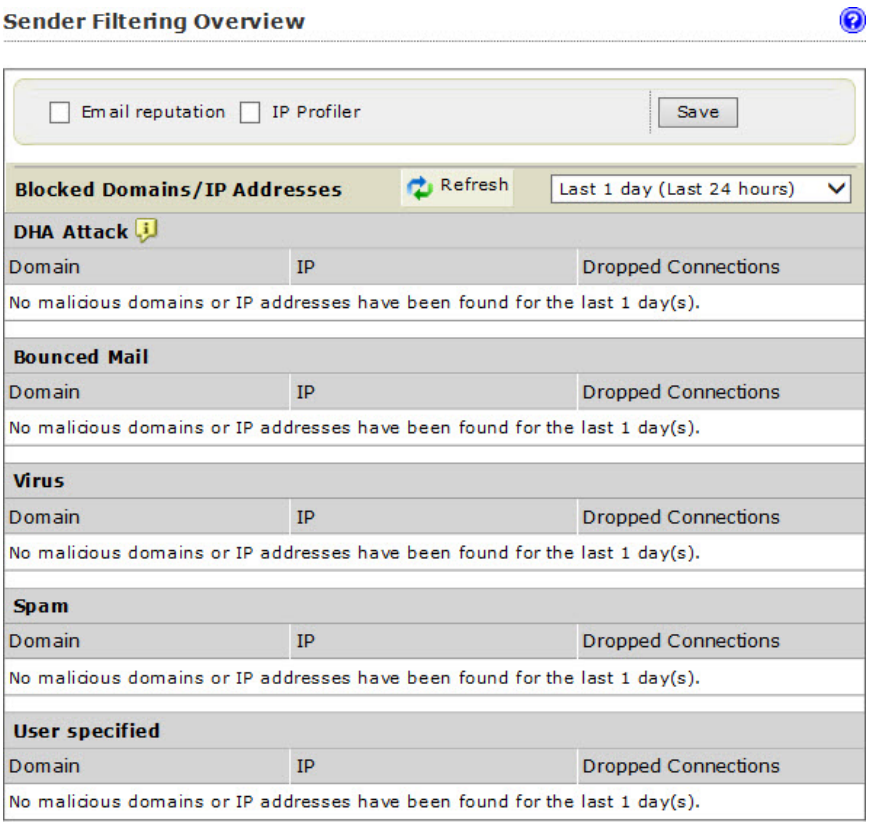
Enabling Email Reputation and IP Profiler

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

Procedure

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

The **Sender Filtering Overview** screen appears.



2. Select the **Email reputation** and **IP Profiler** check boxes as required.
3. Click **Save**.

Adding Approved List Records

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

Procedure

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

   The **Approved List** screen appears.

2. Click **Add**.

   The **Add Approved List Record** 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.

   Note

   By default, the **Scheduled resolution** check box is selected, which means that IMSS will periodically resolve the A record or MX record associated with the domain.

5. Click **Save**.

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

Adding Blocked List Records

IMSS blocks hosts that appear in the Blocked List.

Procedure

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

   The **Blocked List** screen appears.

2. Click **Add**.

   The **Add Blocked List Record** 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. Optional: If you select **Block temporarily**, specify the block duration.
7. Click **Save**.

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

Enabling Sender Filtering Rules

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

- Spam
- Viruses
- DHA attacks
- Bounced mail

WARNING!

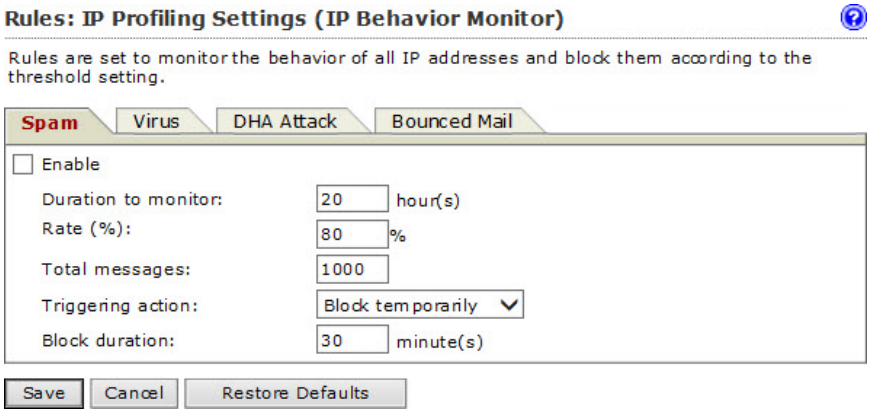
Before enabling sender filtering rules, add all of your email server IP addresses (that send outgoing messages to IMSS) to the Sender Filtering Approved List. To configure the Sender Filtering Approved List, see *Adding Approved List Records on page 9-5*.

Specifying Sender Filtering Spam Settings

Procedure

1. Go to **Sender 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 (%):** The maximum number of allowable messages with spam threats.
   - **Total messages:** 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.

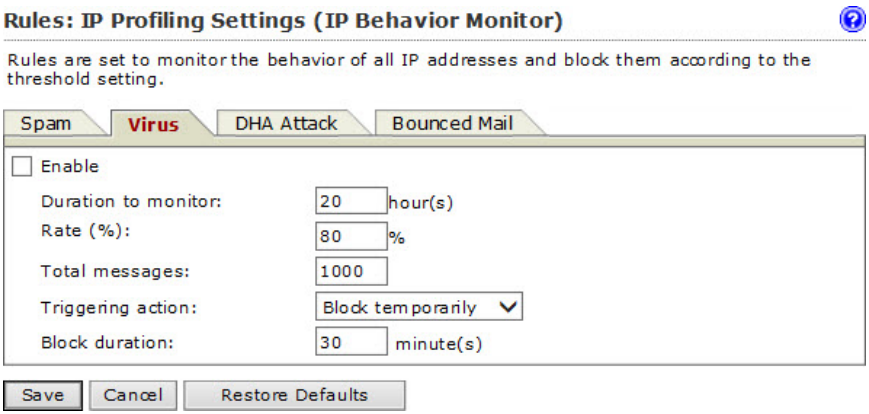
5. Next to **Triggering action**, select one of the following:
   - **Block temporarily:** Block messages from the IP address temporarily and allow the upstream MTA to try again after the block duration ends.
   - **Block permanently:** Never allow another message from the IP address and do not allow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

Specifying Sender Filtering Virus Settings

Procedure

1. Go to **Sender 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 (%):** The maximum number of allowable messages with viruses (the numerator).
   - **Total messages:** 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 temporarily and allow the upstream MTA to try again after the block duration ends.
   - **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.
6. Optional: If you select **Block temporarily**, specify the block duration.
7. Click **Save**.

Specifying Sender Filtering Directory Harvest Attack (DHA) Settings

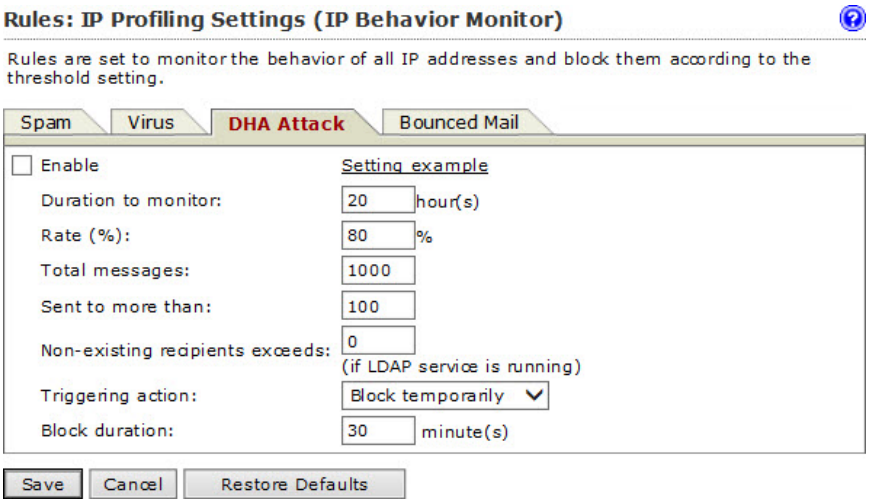
Procedure

1. Go to **Sender 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 (%):** The maximum number of allowable messages with DHA threats (the numerator).
- **Total messages:** The total number of DHA messages out of which the threshold percentage is calculated (the denominator).
- **Sent to more than:** The maximum number of recipients allowed for the threshold value.
- **Non-existing recipients exceeds:** The maximum number of non-existent recipients allowed for the threshold value. DHA attacks often include randomly generated email addresses in the receiver list.

Note

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

Consider the following example.

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

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

Tip

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

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

5. Next to **Triggering action**, select one of the following

- **Block temporarily:** Block messages from the IP address temporarily and allow the upstream MTA to try again after the block duration ends.
- **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.

6. Click **Save**.

Specifying Sender Filtering Bounced Mail Settings

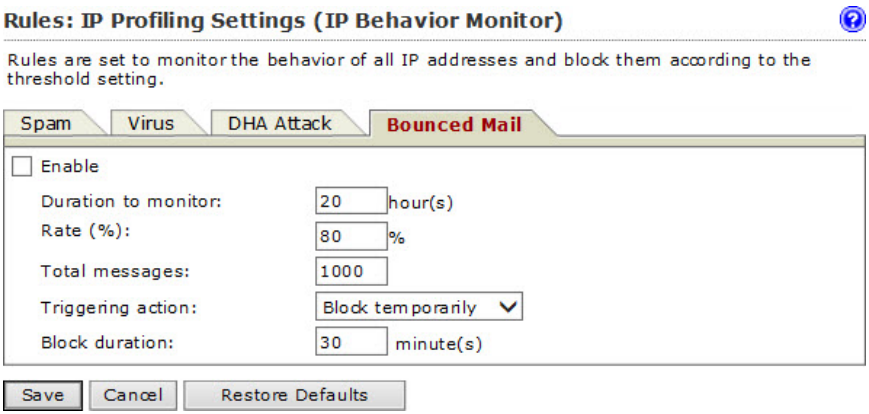
Procedure

1. Go to **Sender 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 (%):** The maximum number of allowable messages signaling bounced mail (the numerator).
- **Total messages:** 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 temporarily and allow the upstream MTA to try again after the block duration ends.
   - **Block permanently:** Never allow another message from the IP address and do not allow the upstream MTA to try again.
6. Optional: If you select **Block temporarily**, specify the block duration.
7. Click **Save**.

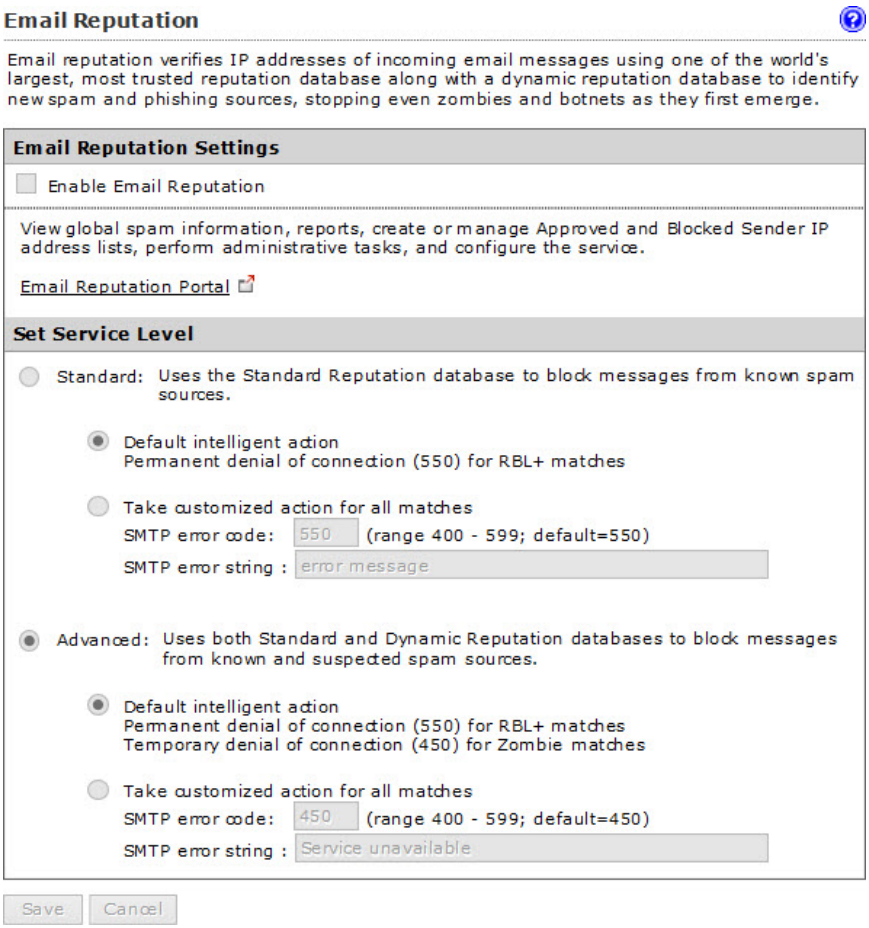
Configuring Email Reputation

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

Procedure

1. Go to **Sender 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.
   - **Take customized action for all matches:**
     - **SMTP error code:** Blocks any connections that have a certain SMTP code. Specify an SMTP code.
     - **SMTP error string:** Specify the message associated with the SMTP error code.

   Advanced:

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

   Note

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

4. Click **Save**.

Displaying Suspicious IP Addresses and Domains

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

Procedure

1. Go to **Sender 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 10

Configuring SMTP Settings

This chapter provides general descriptions on the various configuration tasks that you need to perform to get IMSS up and running.

Topics include:

- *Message Transfer Agents on page 10-2*
- *Enabling SMTP Connections on page 10-2*
- *Configuring SMTP Routing on page 10-2*
- *About Message Delivery on page 10-11*

Message Transfer Agents

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

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

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

Enabling SMTP Connections

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

Procedure

1. Go to **System Status** from the menu.
2. Under **Enable Connections**, select the **Accept SMTP connections** check box.
3. Click **Save**.

Configuring SMTP Routing

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

Note

IMSS 9.1 Patch 1 can communicate to upstream or downstream components in IPv6 networks.

1. *Configuring SMTP Settings on page 10-3*
2. *Configuring Connection Settings on page 10-4*
3. *Specifying Message Rules on page 10-9*
4. *Configuring Message Delivery Settings on page 10-12*

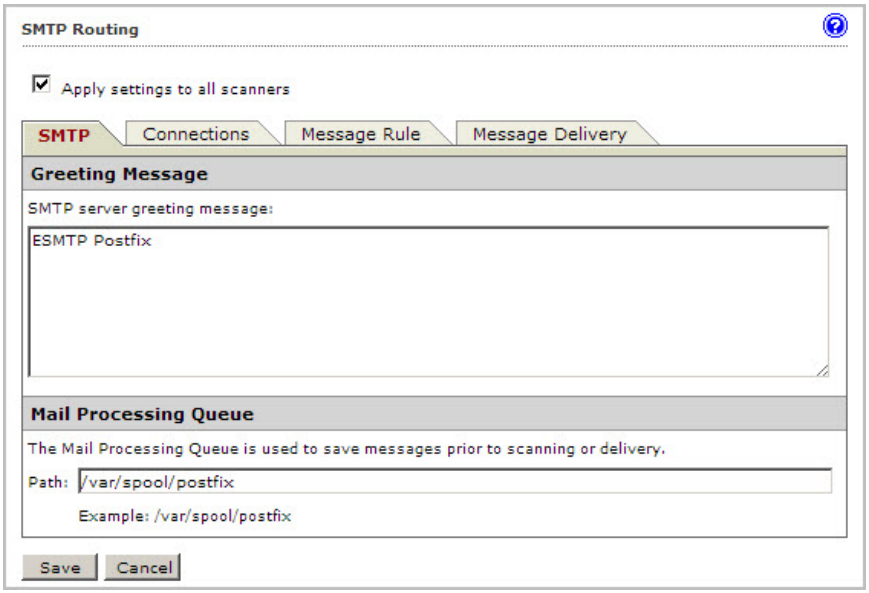
Configuring SMTP Settings

Use the **SMTP Routing** 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 scanning and delivering them.

Procedure

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

The **SMTP Routing** screen appears.



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

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

3. Specify SMTP server **Greeting Message** (displays when a session is created).

4. Specify the **Mail Processing Queue Path**.

5. Click **Save**.

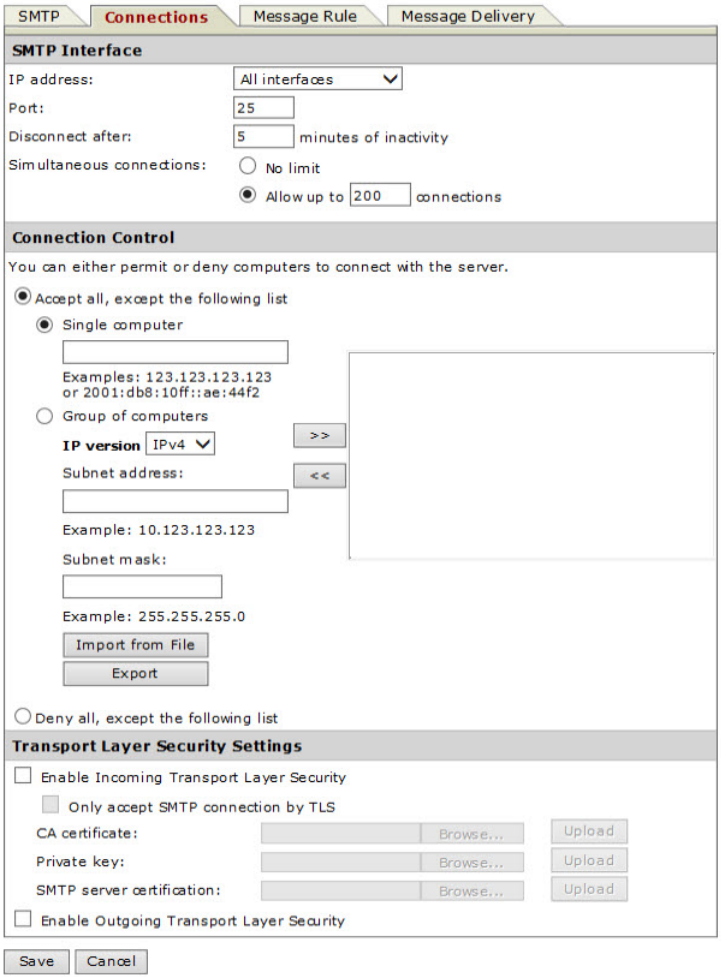
Configuring Connection Settings

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

Procedure

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

   The **Connections** screen appears.



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.

      - **Single computer:** Specify an IP address and then click **>>** to add it to the list.
      - **Group of computers:**

        i. Select the IP version.

           - For IPv4 addresses, specify a subnet address and mask.
           - For IPv6 addresses, specify a subnet address.

        ii. Click **>>** to add the group to the list.

      - **Import from file:** Click to import an IP list from a file. The following shows sample content of an IP list text file:

192.168.1.1

192.168.2.0:255.255.255.0

192.168.3.1:255.255.255.128

192.168.4.100

192.168.5.32:255.255.255.192

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

2001:db8::/32

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

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

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

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

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

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

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

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

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

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

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

  This key must be uploaded to enable a TLS connection.

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

e. Select **Enable Outgoing Transport Layer Security** to protect outbound messages, if desired.

6. Click **Save**.

Configuring Message Rule Settings

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

Email Relay

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

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

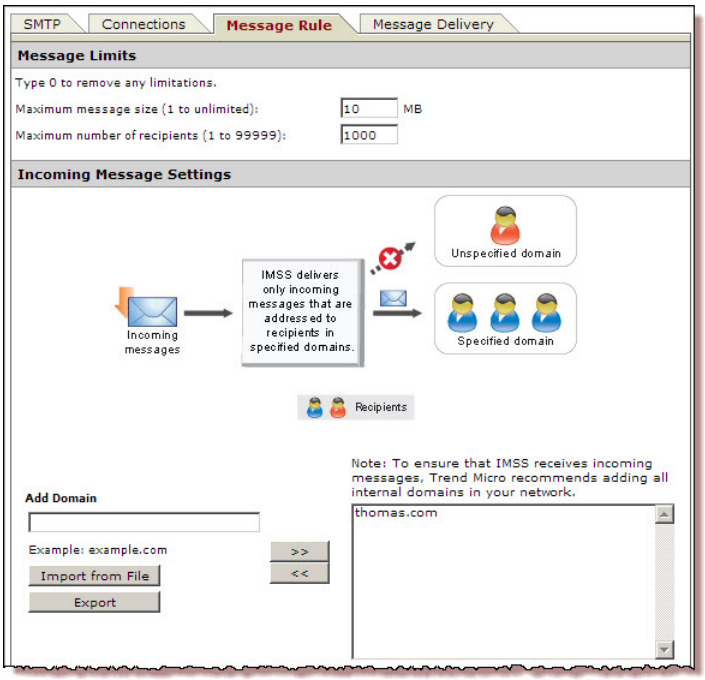
Incoming message settings are different from message delivery domain settings. For more information, see *About Message Delivery on page 10-11*.

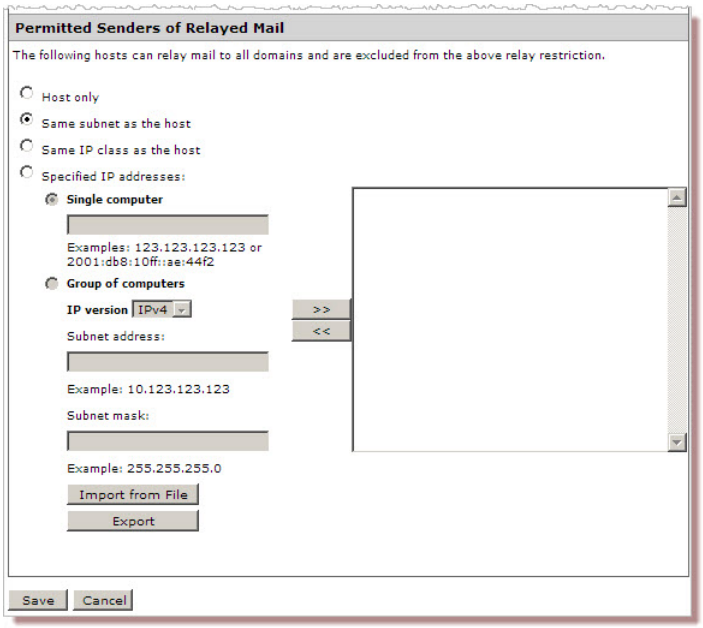
Specifying Message Rules

Procedure

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

   The **Message Rule** screen appears.





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

   - **Maximum message size:** Specify the number of megabytes.
   - **Maximum number of recipients:** Specify the number of recipients from 0 to 99999.

4. Specify the **Incoming Message Settings**.

   IMSS relays the messages to the added domains.

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

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

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

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

6. Click **Save**.

Tip

For security reasons, Trend Micro recommends avoiding open relay when configuring the message rule settings.

About Message Delivery

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

Incoming Message and Message Delivery Domains

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

Incoming message domains

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

Message delivery domains

IMSS delivers messages based on message delivery domains. For example, if the delivery domain includes "domain.com" and the

associated SMTP server 10.10.10.10 on port 25, all email messages sent to "domain.com" will be delivered to the SMTP server 10.10.10.10 using port 25.

Configuring Message Delivery Settings

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

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

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

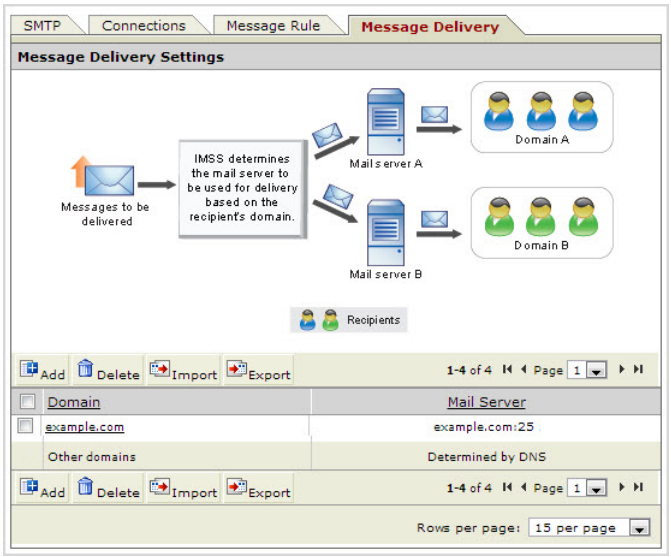
For example, all of the following are valid entries:

- `domain1.com,192.168.1.1:2000`
- `domain2.net,192.168.2.2:1029`
- `domain3.com,smtp.domain3.com:25`
- `domain4.com,mail.domain4.com:2000`
- `domain5.com,[2001:db8:10ff::ae:44f2]:25`

Procedure

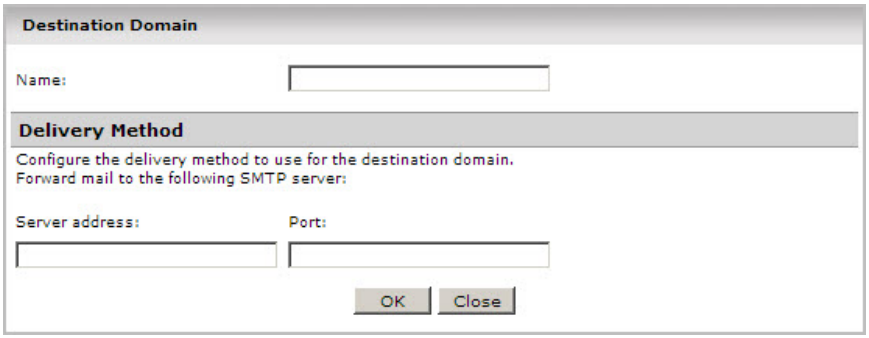
1. Go to **Administration** > **IMSS Configuration** > **SMTP Routing**.
2. Click the **Message Delivery** tab.

The **Message Delivery Settings** screen appears.



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

   The **Destination Domain** screen appears.



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

5. Click **OK**.

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

6. Click **Save**.

Chapter 11

Configuring Known Hosts Settings

This chapter provides general descriptions about known hosts and explains how to add, import, and export known hosts.

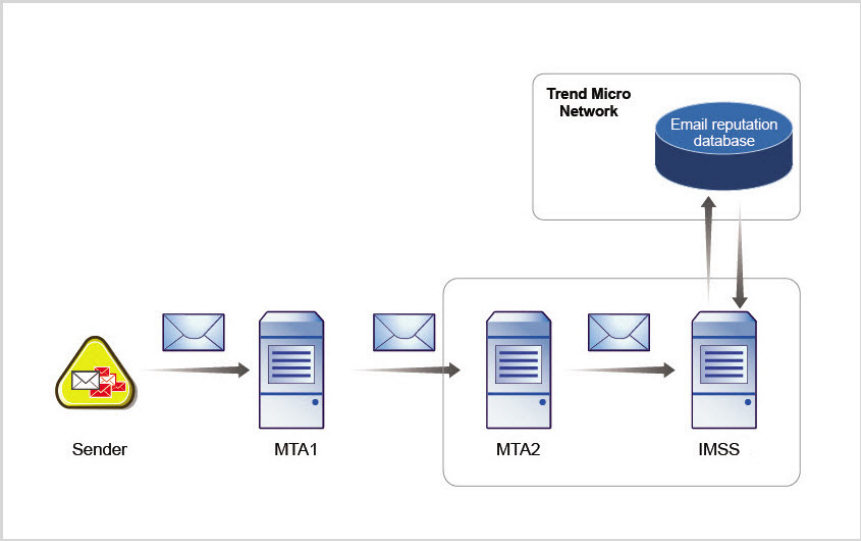
Topics include:

- *About Known Hosts on page 11-2*
- *Adding Known Hosts on page 11-3*
- *Importing Known Hosts on page 11-4*
- *Exporting Known Hosts on page 11-4*

About Known Hosts

Known hosts include trusted mail transfer agents (MTAs) and the Cloud Pre-Filter that are deployed before IMSS on your network. If your IMSS is deployed at the Internet gateway, you do not need to specify known hosts. Use the known host settings in either of the following situations:

- If you have one or multiple MTAs configured upstream from IMSS on your network, enable the known host setting and add these MTAs as known hosts. IMSS then traces the nearest upstream MTA that is not in the known host list and queries its IP address against the email reputation database as well as the IP Profiler approved and blocked lists.



For example, if you have MTA2 configured before IMSS on your network and MTA1 outside your network deployed before MTA2, enable the known host setting and add MTA2 as a known host. IMSS then uses the IP address of MTA1 for query.

- If your IMSS is deployed behind the Cloud Pre-Filter, enable the known host setting. By default, the Cloud Pre-Filter IP address is in the known host list.

If your network has upstream MTAs or the Cloud Pre-Filter deployed before IMSS, use the known host settings for the following reasons:

- IMSS regards all external email messages as coming from these MTAs or the Cloud Pre-Filter and uses their IP addresses for query. All mail traffic routed through these IP addresses will then be considered safe.
- IMSS considers these IP addresses as spam sources since all spam messages come from these addresses before they arrive at IMSS in the mail flow.

Note

IMSS synchronizes Cloud Pre-Filter IP addresses to the known host list at 03:00 a.m. every day. These known hosts will not appear on the management console.

Adding Known Hosts

Procedure

1. Go to **Administration** > **IMSS Configuration** > **Known Hosts**.

   The **Known Hosts** screen appears.

2. Select the **Enable Known Hosts** check box.

3. Specify the IP address and description for the host to add.

   Note

   IMSS supports IPv4 and IPv6 addresses for known hosts. Optionally specify a single IP addresses and subnet addresses.

4. Click **Add**.

   The new host appears in the known host list.

5. Click **Save**.

Importing Known Hosts

Procedure

1. Go to **Administration** > **IMSS Configuration** > **Known Hosts**.

   The **Known Hosts** screen appears.

2. Click **Import**.

   The **Import Known Hosts** dialog box appears.

3. Click **Browse** to locate the file to import.

4. Select one of the following:

   - Merge with current list
   - Overwrite current list

5. Click **Import**.

Note

IMSS can import host addresses from only a text file. Ensure that the text file contains only one IP address or subnet address per line.

Exporting Known Hosts

Procedure

1. Go to **Administration** > **IMSS Configuration** > **Known Hosts**.

   The **Known Hosts** screen appears.

2. Select one or multiple hosts to export.
3. Click **Export**.

Note

IMSS exports only host addresses without description.

Chapter 12

Configuring POP3 Settings

This chapter provides instructions for configuring POP3 settings.

Topics include:

- *Scanning POP3 Messages on page 12-2*
- *Enabling POP3 Scanning on page 12-3*
- *Configuring POP3 Settings on page 12-4*
- *Configuring POP3 Scan Service on page 12-5*

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.

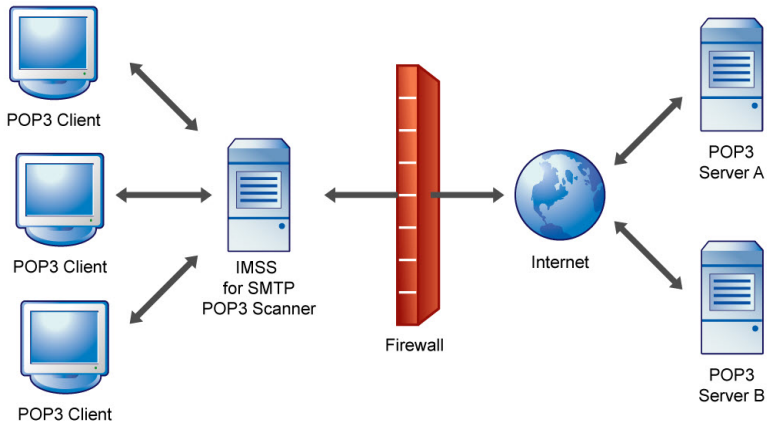


FIGURE 12-1. Scanning POP3 messages

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

You can set up the following connection types:

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

Note

IMSS supports connections to IPv6 POP3 servers.

POP3 Requirements

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

Enabling POP3 Scanning

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

Procedure

1. Go to **System Status**.
2. Under **Enable Connections**, select the **Accept POP3 connections** check box.
3. Click **Save**.

Configuring POP3 Settings

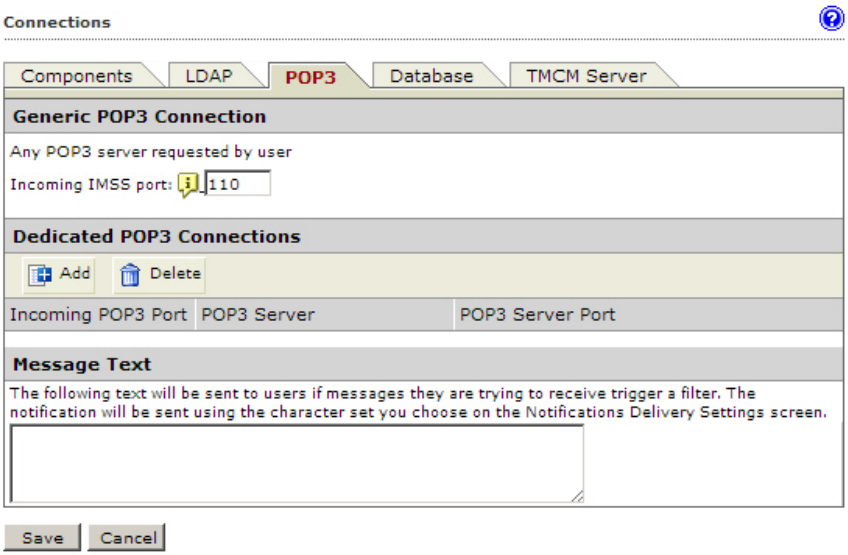
You can specify the IMSS server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection (through the APOP command or using NTLM), you may also set up a dedicated connection and assign a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

Configuring POP3 Scan Service

Procedure

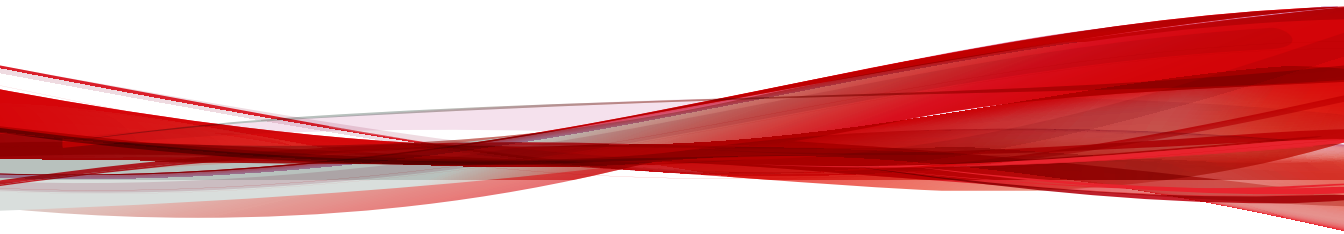
1. Enable POP3 connections.
   a. Go to **System Status**.
   b. Click **Accept POP3 connections** under Enable Connections.
   c. Click **Save**.
2. Configure the POP3 settings.
   For details, see *Configuring POP3 Settings on page 12-4*.
3. Configure the email client.
   - **POP3 server**: IP address of IMSS
   - **POP3 port**: Port specified in IMSS
   - **User account**
     - If you have specified a generic POP3 server: Username#remote_server
     - If you have specified a dedicated POP3 server: Username
   - **Password**: User's password on the remote server

Note

If you have specified a generic POP3 server and the POP3 port is changed at the remote POP3 server, please set the user account format to `username#remote_server#remote_POP3_port`.

Part III

IMSS Policies



Chapter 13

Managing Policies

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

Topics include:

- *About Policies on page 13-2*
- *How the Policy Manager Works on page 13-2*
- *Filter Policies that Display in the Policy List on page 13-4*

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 Sender Filtering.

Note

Before creating a new policy, ensure that you have defined the internal addresses. See *Configuring Internal Addresses on page 15-2* 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, phishing, or social engineering attack 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.

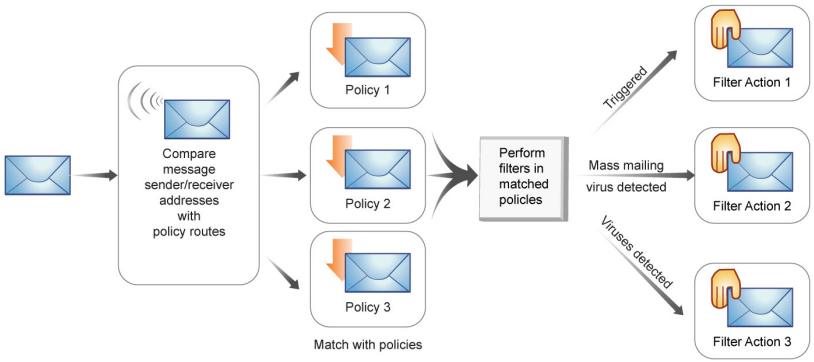


FIGURE 13-1. Simplified policy manager process flow

Note

For more information on how to create a policy, see *Configuring Policies on page 17-1*.

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, phishing and social engineering attack email
      - Graymail
      - Web Reputation
      - Attachments
      - Content

- Compliance
- Size
- Other

c. Specify the users the policy protects:

- All Groups
- [Find user or group]

Chapter 14

Configuring Common Policy Objects

This chapter provides instructions for configuring common policy objects, such as address groups, keywords, expression, compliance templates, notifications, and stamps.

Topics include:

- *Policy Object Descriptions on page 14-2*
- *Address Groups on page 14-2*
- *Using the Keyword & Expression List on page 14-13*
- *Data Loss Prevention on page 14-28*
- *Notifications on page 14-47*
- *Stamps on page 14-53*
- *DKIM Approved List on page 14-56*
- *Web Reputation Approved List on page 14-58*

Policy Object Descriptions

Common policy objects simplify policy management by storing configurations that can be shared across all policies.

TABLE 14-1. Policy Objects

POLICY OBJECTS	DESCRIPTION
Address Groups	Organize multiple email addresses into a single group.
Keywords & Expressions	Create keywords or expressions to prevent information leaks, block spam, or block derogatory messages from entering or moving in your network.
Compliance Templates	Create compliance templates to prevent sensitive data from leaving 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.
URL Keyword List	URLs that contain any of the specified keywords will not be sent to Virtual Analyzer for analysis.

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 apply to them. Defining accurate and complete address groups ensures that the appropriate policies apply to the individuals in those groups.

Creating Address Groups

An address group is a collection of user email addresses in your organization. Create an address group to apply rules to several email

addresses at the same time, rather than applying rules to each address individually.

Create address groups before creating any policies or when specifying the route during policy creation. Optionally, add an address group when modifying an existing policy. Manually create address groups or import them from a text file that contains one email address per line.

Tip

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

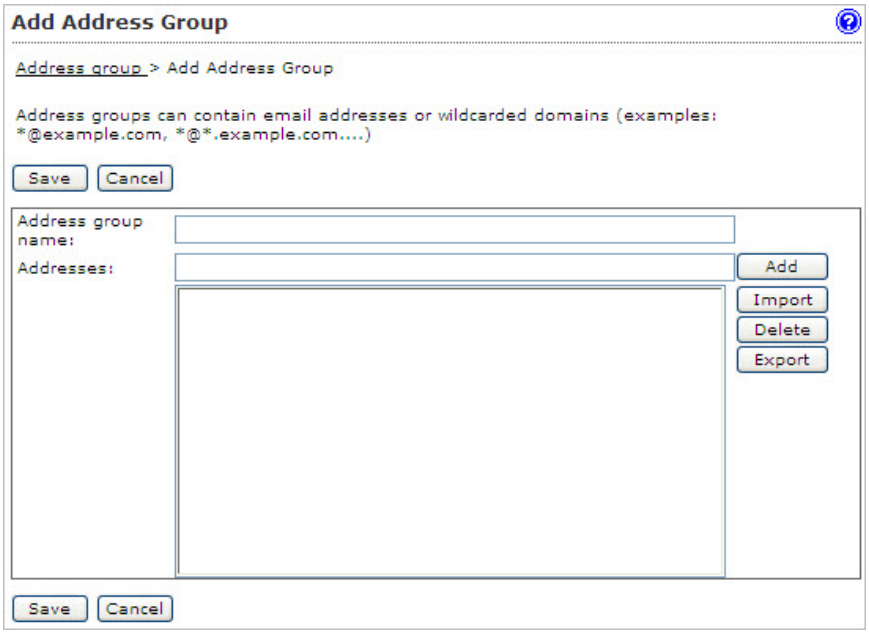
Procedure

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.
4. Do any of the following:
   - **Add an individual address:**
     - Specify an email address and click **Add**. Optionally, 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. Click **Browse** to locate the file to import.

     c. Select one of the following:

- Merge with current list
- Overwrite current list

d. Click **Import**.

Note

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

5. 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

Create an address group when specifying the route during policy creation by adding email addresses individually or importing them from a text file.

Note

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

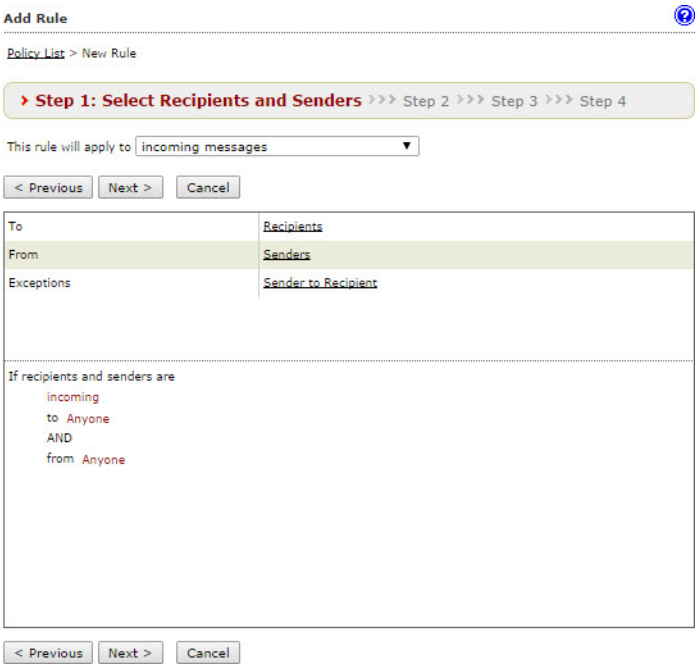
Procedure

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.

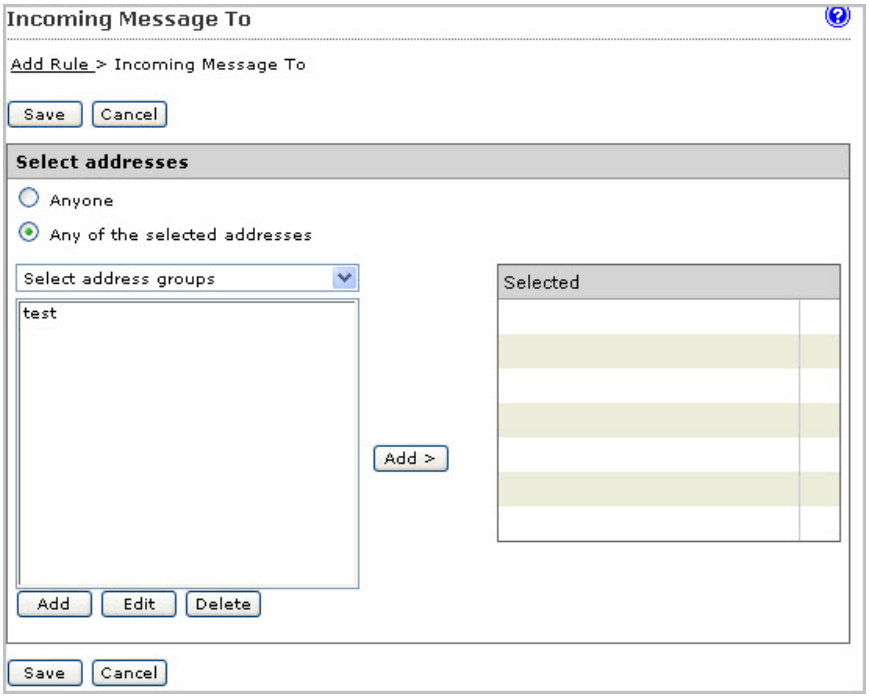
   The **Step 1: Select Recipients and Senders** screen appears.

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.

8. Do one of the following:

   - Add an individual address:

     - Specify an email address and click **Add** to add email addresses individually. Optionally, 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. Click **Browse** to locate the file to import.

c. Select one of the following:

- **Merge with current list**
- **Overwrite current list**

d. Click **Import**.

Note

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

9. Click **Save**.

Editing or Deleting an Address Group

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. Do either of the following

   - 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.

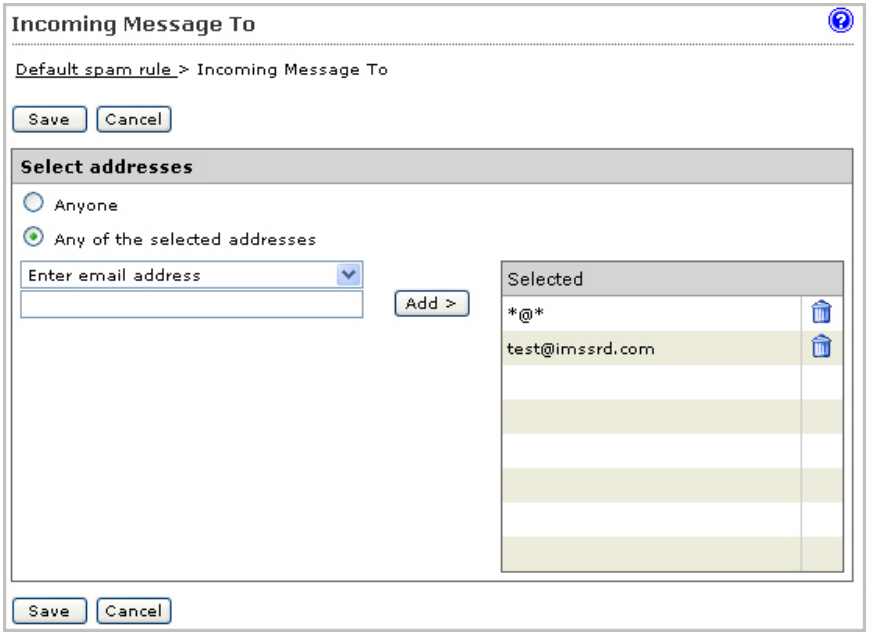
- Delete an address group:
  a. Select the check box next to an address group.
  b. Click **Delete**.

Editing or Deleting an Address Group from an Existing Policy

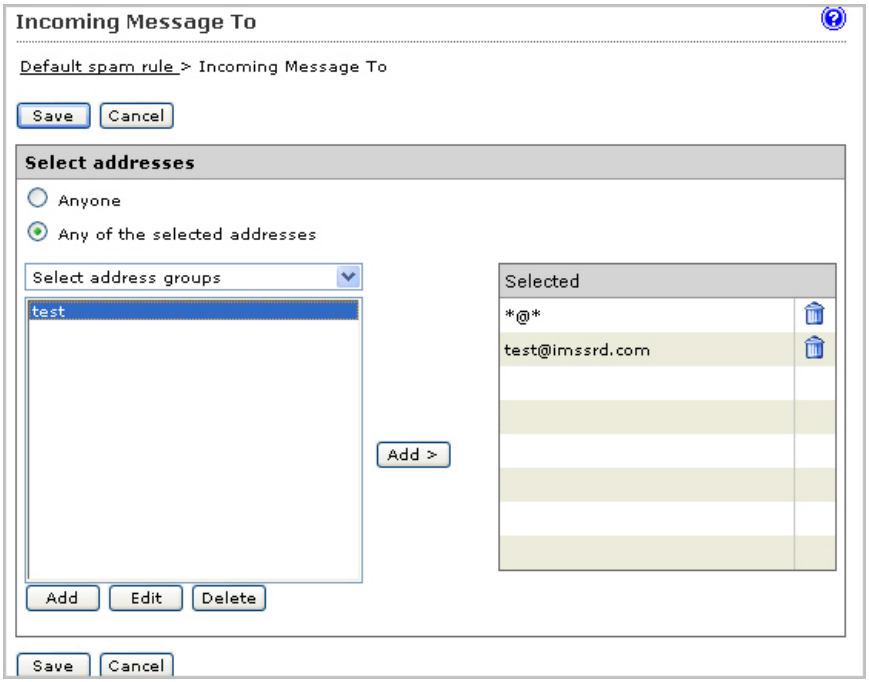
Procedure

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 settings into other IMSS servers. Export address groups from existing policies or from the address group list.

Procedure

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

   The **Address Groups** screen appears.

2. Click the address group to export.

   The **Address Group** screen appears.

3. Click **Export**.

   The **File Download** screen appears.

4. Click **Save**.

   The **Save As dialog** box appears.

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

6. Click **Save**.

Exporting an Address Group from an Existing Policy

Procedure

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

2. Click the link for an existing policy.

3. Click the If recipients and senders are link.

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

   The **Select addresses** screen appears.

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

6. Click **Edit**.

   The **Address Group** screen appears.

7. Click **Export**.

   The **File Download** screen appears.

8. Click **Save**.

   The **Save As** dialog box appears.

9. Specify the name and location to export the address group.
10. Click **Save**.

Using the Keyword & Expression List

Keywords are special words or phrases. Add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. To prevent the transmission of medical certificate files, configure IMSS to block files containing these keywords.

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

IMSS can take action on an email message based on the content of its subject, body, or header. To filter email 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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
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 configuring expressions for the header, select the check boxes next to the header items where the expression applies.
5. Click **Add**.

   The screen for managing keyword expressions appears.
6. Configure the expressions.
7. In the **Available** list, click the expression list 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 keywords and regular expressions to enable IMSS to scan message content. Create keywords or expressions on the **Keywords & Expressions** screen or during policy creation.

Tip

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

When creating expressions:

- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.
- Specify criteria when creating expressions. An expression must meet specified criteria before IMSS subjects it to a policy.

Keywords & Expressions

Each keyword list has built-in conditions that determine if the content triggers a detection. A keyword list must meet specified 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 impact performance. When creating expressions:

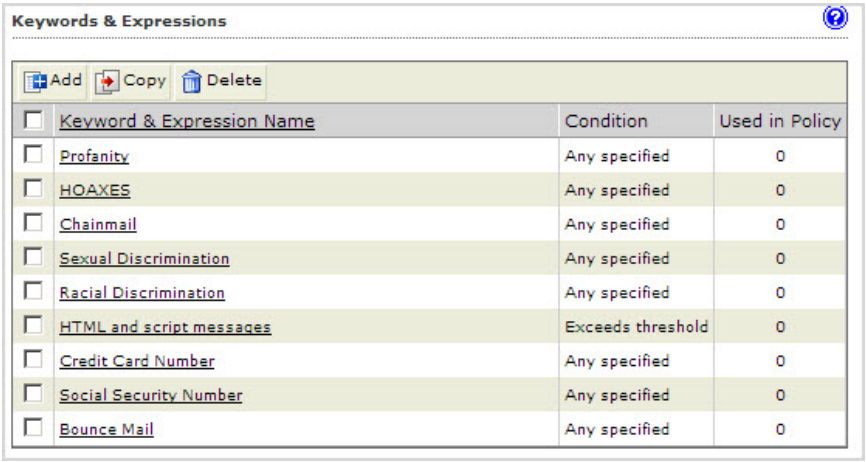
- Note that IMSS follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit http://www.pcre.org/.
- Refer to the predefined expressions for guidance on how to define valid expressions.
- Start with simple expressions. Modify the expressions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

Creating Keywords or Expressions

Procedure

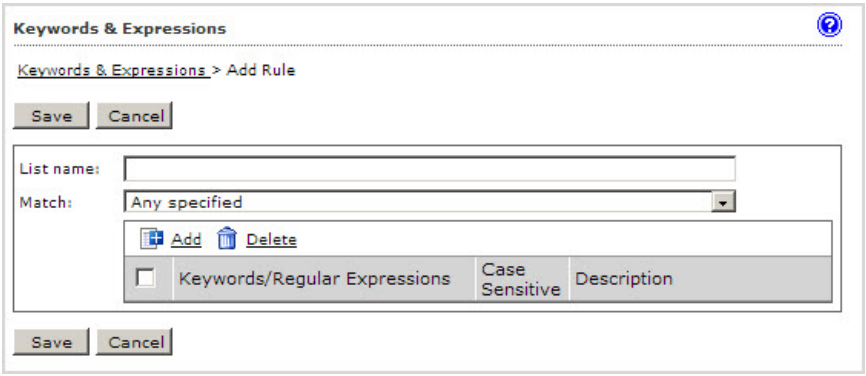
1. Go to **Policy** > **Keywords & Expressions**.

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:

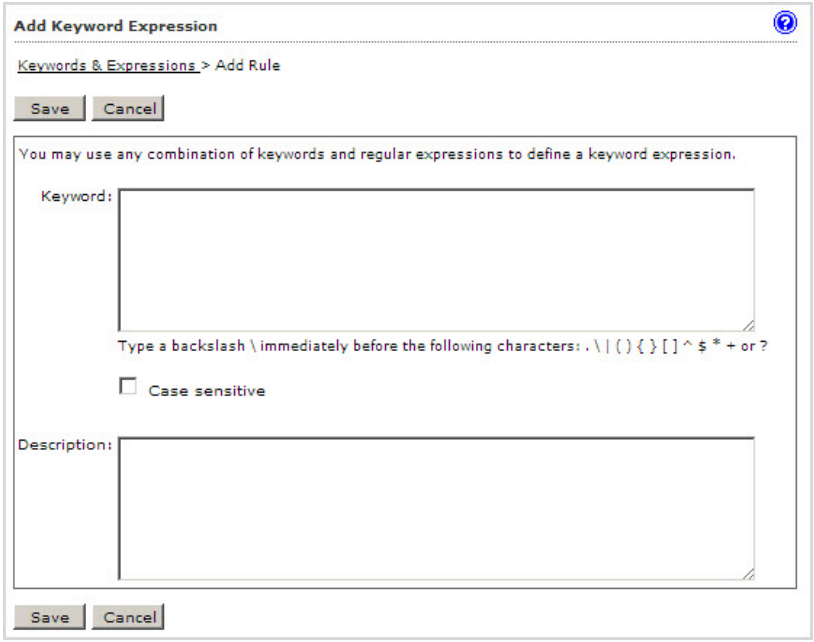
- **Any specified**: Message content matches any of the keywords or expressions in the list.
- **All specified**: Message content matches all keywords or expressions in the list.
- **Not the specified**: Message content does not match any of the keywords or expressions in the list.
- **Only when combined 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. Define the following parameters:

Keyword

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

For example:

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

Case sensitive

Make the keyword expression case sensitive.

Description

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

c. Click **Save**.

6. If you selected **Only when combined score exceeds threshold**:

   a. Specify a threshold in the **Total message score to trigger action** field.

   b. Select a value from the **Score** drop-down box.

7. Click **Save**.

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

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

Procedure

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

   - For information on creating a new rule, see *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.

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, 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. Specify a description for the keywords.
9. 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.
10. Click **Save**.
11. For IMSS to consider the capitalization of message content when it uses the filter, select the check box under **Case sensitive**.

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

About Regular Expressions

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

Tip

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

Characters

Regular Expression	Description
. (dot)	Any character (byte) except newline
x	The character 'x'
\\	The character '\'
\a	The alert (bell) character (ASCII 0x07)

Regular Expression	Description
\b	1. If this meta-symbol is within square brackets [] or by itself, it will be treated as the backspace character (ASCII 0x08). For example, [\b] or \b 2. If this meta-symbol is at the beginning (or end) of a regular expression, it means any matched string of the regular expression must check whether the left (or right) side of the matched string is a boundary. For example: • \bluck > left side must be the boundary • luck\b > right side must be the boundary • \bluck\b > both sides must be the boundary 3. If this meta-symbol appears in the middle of a regular expression, it will cause a syntax error.
\f	The form-feed character (ASCII 0x0C)
\n	The newline (line feed) character (ASCII 0x0A)
\r	The carriage-return character (ASCII 0x0D)
\t	The normal (horizontal) tab character (ASCII 0x09)
\v	The vertical tab character (ASCII 0x0B)
\n	The character with octal value 0n (0 <= n <= 7)
\nn	The character with octal value 0nn (0 <= n <= 7)
\mnn	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh	The character with a hexadecimal value 0xhh, for example, \x20 means the space character

Bracket Expression and Character Classes

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

For example:

Expression	Matches
[abc]	a, b, or c
[a-z]	a through z
[^abc]	Any character except a, b, or c
[[:alpha:]]	Any alphabetic character (see below)

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

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

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

Boundary Matches

Expression	Description
^	Beginning of line
$	End of line

Greedy Quantifiers

Expression	Description
R?	Matches R, once or not at all
R*	Matches R, zero or more times
R+	Matches R, one or more times
R{n}	Matches R, exactly n times
R{n,}	Matches R, at least n times
R{n,m}	Matches R, at least n but no more than m times

R is a regular expression.

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

For example:

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

- 12345abc
- 23455abc

- 3456abc
- 456abc
- 56abc
- 6abc
- abc

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

Logical Operators

Expression	Description
RS	R followed by S (concatenation)
R|S	Either R or S
R/S	An R but only if it is followed by S
(R)	Grouping R

R and S are regular expressions

Shorthand and meta-symbol

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

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

Shorthand	Description
{D}	[0-9]

Shorthand	Description
{L}	[A-Za-z]
{SP}	[(),;\.\\<>@\[\]:]
{NUMBER}	[0-9]+
{WORD}	[A-Za-z]+
{CR}	\r
{LF}	\n
{LWSP}	[\t]
{CRLF}	(\r\n)
{WSP}	[\t\f]+
{ALLC}	.

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

Meta-symbol	Description
\s	[[:space:]]
\S	[^[:space:]]
\d	[[:digit:]]
\D	[^[:digit:]]
\w	[_[:alnum:]]
\W	[^_[:alnum:]]

Literal string and escape character of regular expressions

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

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

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

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

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

Searching for Policies Using an Expression Keyword

Procedure

1. Select the **Policy Search** tab.

2. Next to **Keyword**, specify an expression keyword to search for policies.
3. Click **Query**.

   A list of policies whose expressions contain the specified keyword appear. The associated expression list and expressions are also provided in the list.

Data Loss Prevention

Data Loss Prevention (DLP) safeguards an organization's confidential and sensitive data-referred to as digital assets-against accidental disclosure and intentional theft. DLP allows you to:

- Identify the digital assets to protect
- Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices
- Enforce compliance to established privacy standards

DLP evaluates data against a set of rules defined in policies. Policies determine the data that must be protected from unauthorized transmission and the action that DLP performs when it detects transmission.

Data Identifier Types

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

- **Expressions**: Data that has a certain structure. For details, see *Expressions on page 14-29*.
- **File attributes**: File properties such as file type and file size. For details, see *File Attributes on page 14-35*.
- **Keywords**: A list of special words or phrases. For details, see *Keywords on page 14-38*.

Note

It is not possible to delete a data identifier used in a DLP template. Delete the template before deleting the data identifier.

Expressions

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

You can use predefined and customized expressions. For details, see *Predefined Expressions on page 14-29* and *Customized Expressions on page 14-30*.

Predefined Expressions

IMSS comes with a set of predefined expressions. These expressions cannot be modified or deleted.

IMSS verifies these expressions using pattern matching and mathematical equations. After IMSS matches potentially sensitive data with an expression, the data may also undergo additional validation.

For a complete list of predefined expressions, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Viewing Settings for Predefined Expressions

Note

Predefined expressions cannot be modified or deleted.

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.

2. Click the **Expressions** tab.
3. Click an expression name.
4. View settings in the screen that opens.

Customized Expressions

Create customized expressions if none of the predefined expressions meet your requirements.

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

When creating expressions:

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

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expression on page 14-31*.

Criteria for Customized Expression

TABLE 14-2. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number Expression: [^\d]([0123678]\d{8})[^\d] Characters: 0123456789 Minimum characters: 9 (from 4 to 90) Maximum characters: 9 (from 4 to 90) **Note** Maximum characters must be larger than or equal to minimum characters.

CRITERIA	RULE	EXAMPLE
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] Suffix characters: 0123456789- Number of characters: 5 (from 3 to 90) Minimum characters in the expression: 25 (from 4 to 90) Maximum characters in the expression: 80 (from 4 to 90) **Note** The number of characters in the expression must be within the minimum and maximum limits.

CRITERIA	RULE	EXAMPLE
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] Separator: @ Minimum characters to the left: 3 (from 3 to 90) Maximum characters to the left: 15 (from 4 to 90) Maximum characters to the right: 30 (from 4 to 90) **Note** Maximum characters to the left must be larger than minimum characters to the left. Maximum characters to the right must be larger than maximum characters to the left.

Creating a Customized Expression

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Expressions** tab.
3. Click **Add**.

   A new screen displays.
4. Specify a name for the expression. The name must not exceed 128 bytes in length.

5. Specify a description that does not exceed 255 bytes in length.
6. Specify the expression and set whether it is case-sensitive.
7. Specify the displayed data.

   For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.
8. Select one of the following criteria and configure additional settings for the chosen criteria (see *Criteria for Customized Expression on page 14-31*):
   - None
   - Specific characters
   - Suffix
   - Single-character separator
9. Optional: Select a validator for the expression.

Note

Data units follow semantic rules. Not every 9-digit number is a valid social security number and not every 15- or 16-digit number is a valid credit card number. To reduce false positives, expression validators check if the extracted data units follow these rules.

10. Test the expression against actual data.

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

Note

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

Note

Optionally, copy a predefined expression and edit the copy to create your customized expression.

Importing Customized Expressions

Use this option if you have a properly-formatted `.xml` file containing the expressions. Generate the file by exporting the expressions from either the IMSS server you are currently accessing or from another IMSS server.

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Expressions** tab.
3. Click **Import** and then locate the `.xml` file containing the expressions..
4. Click **Import**.

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

Note

Every customized expression is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the management console.

If the file contains a customized expression that already exists, IMSS overwrites the existing expression. To retain the existing expression, change its internal name before importing the expression file.

File Attributes

File attributes are specific properties of a file. Use two file attributes when defining data identifiers: file type and file size. For example, a software development company may want to limit the sharing of the company's software installation package to the R&D department, whose members are

responsible for the development and testing of the software. In this case, the IMSS administrator can create a policy that blocks the transmission of executable files that are 10 to 40 MB in size to all departments except R&D.

Trend Micro recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files because file attributes, by themselves, are poor identifiers of sensitive files. Continuing the preceding example, third-party software installation packages shared by other departments will most likely be blocked.

For a complete list of supported file types see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Creating a File Attribute List

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **File Attributes** tab.
3. Click **Add**.

   A new screen displays.
4. Specify a name for the file attribute list. The name must not exceed 128 bytes in length.
5. Specify a description that does not exceed 255 bytes in length.
6. Next to **Except flag**, select either of the following:
   - **Except**: The selected file types will be excluded.
   - **Not except**: The selected file types will be included.
7. Select your preferred true file types.
8. If a file type you want to include is not listed, select **File extensions** and then specify the file type's extension. IMSS checks files with the specified extension but does not check their true file types. Guidelines when specifying file extensions:

- Each extension must start with an asterisk (*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file's actual name. For example, `*.pol` matches `12345.pol` and `test.pol`.
- You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (*) to represent two or more characters. See the following examples:

  - `*.*m` matches the following files: `ABC.dem`, `ABC.prm`, `ABC.sdcm`

  - `*.m*r` matches the following files: `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

- Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: `*.do*` matches `abc.doctor_john.jpg` and `abc.donor12.pdf`.
- Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.

9. Specify the minimum and maximum file size in bytes (1 bytes to 2 GB).
10. Click **Save**.

Note

Optionally, copy an existing file attribute list and edit the copy to create another file attribute list.

Importing a File Attribute List

Use this option if you have a properly-formatted `.xml` file containing the file attribute lists. Generate the file by exporting the file attribute lists from either the IMSS server you are currently accessing or from another IMSS server.

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **File Attributes** tab.
3. Click **Import** and then locate the `.xml` file containing the file attribute lists.
4. Click **Import**.

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

Note

Every file attribute list is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the management console.

If the file contains a file attribute list that already exists, IMSS overwrites the existing file attribute list. To retain the existing file attribute list, change its internal name before importing the file attribute file.

Keywords

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. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure IMSS to block files containing these keywords.

Combine commonly used words to form meaningful keywords. For example, combine "end", "read", "if", and "at" to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 14-39* and *Customized Keyword Lists on page 14-40*.

Predefined Keyword Lists

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

For details about the predefined keyword lists in IMSS, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

How Keyword Lists Work

Number of Keywords Condition

Each keyword list contains a condition that requires a certain number of keywords be present in a document before the list will trigger a violation.

The number of keywords condition contains the following values:

- **All**: All of the keywords in the list must be present in the document.
- **Any**: Any one of the keywords in the list must be present in the document.
- **Specific number**: There must be at least the specified number of keywords in the document. If there are more keywords in the document than the number specified, a violation will trigger.

Distance Condition

Some of the lists contain a "distance" condition to determine if a violation is present. "Distance" refers to the amount of characters between the first character of one keyword and the first character of another keyword. Consider the following entry:

F**irst Name:_John_ L**ast Name:_Smith_

The **Forms - First Name, Last Name** list has a "distance" condition of fifty (50) and the commonly used form fields of "First Name" and "Last Name". In the example above, a violation will trigger as the number of characters

between the "F" in First Name and the "L" in Last Name is equal to eighteen (18).

For an example of an entry that would not trigger a violation, consider the following:

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

In this example, the number of characters between the "f" in "first name" and the "l" in "last name" is sixty-one (61). This exceeds the distance threshold and does not trigger a violation.

Customized Keyword Lists

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

A keyword list must meet specified criteria before IMSS subjects it to a DLP policy. Choose one of the following criteria for each keyword list:

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

For details about the criteria rules, see *Customized Keyword List Criteria on page 14-40*.

Customized Keyword List Criteria

TABLE 14-3. Criteria for a Keyword List

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

CRITERIA	RULE
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, the number of characters from the beginning of the first keyword to the beginning of the last keyword must be within <x> characters. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If IMSS detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB###USB The following data does not match the criteria: DISK**********WEB****USB(21 characters between "D" and "U") When deciding on the number of characters, remember that a small number, such as 10, will usually result in faster scanning time but will only cover a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores assigned to keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Creating a Keyword List

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.

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

   A new screen displays.
4. Specify a name for the keyword list. The name must not exceed 128 bytes in length.
5. Specify a description that does not exceed 255 bytes in length.
6. Choose one of the following criteria and configure additional settings for the chosen criteria:
   - **Any keywords**
   - **All keywords**
   - **All keywords within <x> characters**
   - **Combined score for keywords exceeds threshold**
7. To manually add keywords to the list:
   a. Specify a keyword that is 3 to 40 bytes in length and set whether it is case-sensitive.
   b. Click **Add**.
8. To delete keywords, select the keywords and click **Delete**.
9. Click **Save**.

Note

Optionally, copy a predefined keyword list and edit the copy to create your customized keyword list.

Importing a Keyword List

Use this option if you have a properly-formatted `.xml` file containing the keyword lists. Generate the file by exporting the keyword lists from either the IMSS server you are currently accessing or from another IMSS server.

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Data Identifiers**.
2. Click the **Keyword Lists** tab.
3. Click **Import** and then locate the `.xml` file containing the keyword lists.
4. Click **Import**.

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

Note

Every customized keyword list is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the management console.

If the file contains a customized keyword list that already exists, IMSS overwrites the existing keyword list. To retain the existing keyword list, change its internal name before importing the keyword file.

DLP Compliance Templates

A Data Loss Prevention (DLP) compliance template combines DLP data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that meet a certain condition statement will be subject to a DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources personnel to transmit the file through printing so that the printed copy can be signed by an employee. Transmission through all other possible channels, such as email, is blocked.

Optionally create your own templates if you have configured DLP data identifiers. You can also use predefined templates. For details, see *Customized DLP Templates on page 14-44* and *Predefined DLP Templates on page 14-44*.

Note

It is not possible to delete a template used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

Trend Micro comes with a set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

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

Customized DLP Templates

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

For more information and examples on how condition statements and logical operators work, see *Condition Statements and Logical Operators on page 14-44*.

Condition Statements and Logical Operators

IMSS evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage may lead to an erroneous condition statement producing unexpected results.

See the examples in the following table.

TABLE 14-4. Sample Condition Statements

CONDITION STATEMENT	INTERPRETATION AND EXAMPLE
[Data Identifier1] **And** [Data Identifier 2] **Except** [Data Identifier 3]	A file must meet [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].
[Data Identifier 1] **Or** [Data Identifier 2]	A file must meet [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].
Except [Data Identifier 1]	A file must not meet [Data Identifier 1]. For example: A file must not be [a multimedia file].

As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not meet all of the data identifiers in the statement. In most cases, the first data identifier does not have an operator.

Creating a Template

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Compliance Templates**.
2. Click **Add**.

   A new screen displays.
3. Specify a name for the template. The name must not exceed 128 bytes in length.

4. Specify a description that does not exceed 255 bytes in length.
5. Specify a digital asset definition using one of the following:
   - **Expression**: Select **Expression**, select an expression name, and set the number of times the expression must occur before IMSS blocks the message from leaving your network.
   - **Keyword**: Select **Keyword** and select a keyword list. IMSS prevents the transmission of files if they contain keywords in the selected list.
   - **File Attributes**: Select **File Attributes** and select a file attribute list. IMSS prevents the transmission of files if they match the attributes specified in the list.

   Note

   If the **File Attributes** option is not shown, no file attribute list exists. To create a file attribute list, see *Creating a File Attribute List on page 14-36*.
6. Click **+** to add more entries.
7. Select a logical operator for each entry.

   Note

   Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see *Condition Statements and Logical Operators on page 14-44*.
8. Click **Add**.

   The digital asset definition appears in the **Compliance Template Definition** list.
9. Add multiple digital asset definitions if required.
10. Click **Save**.

The compliance template appears in the compliance template list.

Importing Templates

Use this option if you have a properly-formatted `.xml` file containing the templates. Generate the file by exporting the templates from either the IMSS server you are currently accessing or from another IMSS server.

Procedure

1. Go to **Policy** > **Policy Objects** > **DLP Compliance Templates**.
2. Click **Import** and then locate the `.xml` file containing the templates.
3. Click **Import**.

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

   Note

   Every customized template is identified by its **name** field in the `.xml` file. This name is a unique internal name that does not display on the management console.

   If the file contains a customized template that already exists, IMSS overwrites the existing template. To retain the existing template, change its internal name before importing the template file.

Notifications

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 14-49*.

Sending Policy Notifications

Procedure

1. Create or modify a policy.
   - For information on creating a new rule, see *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
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.

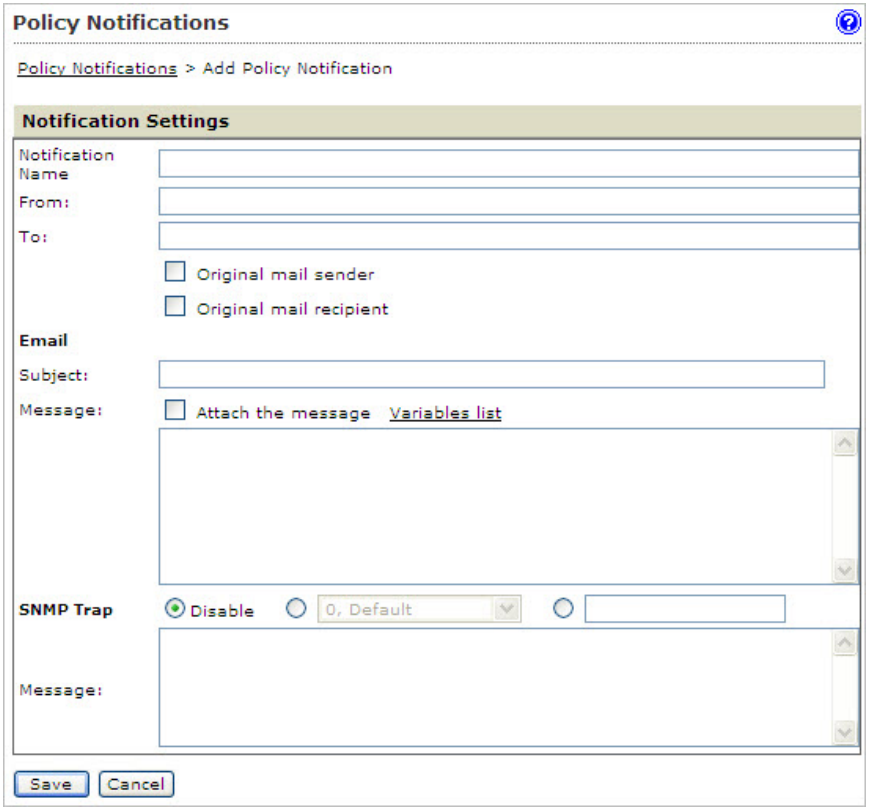
Procedure

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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
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**.

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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
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.

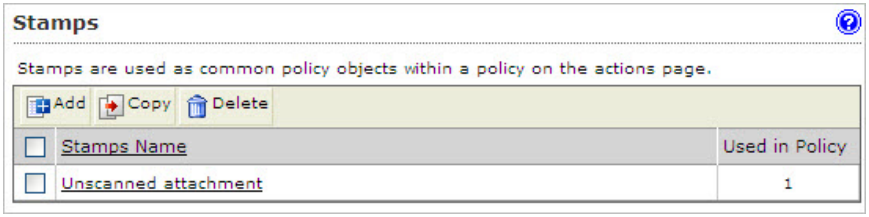
Note

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

Procedure

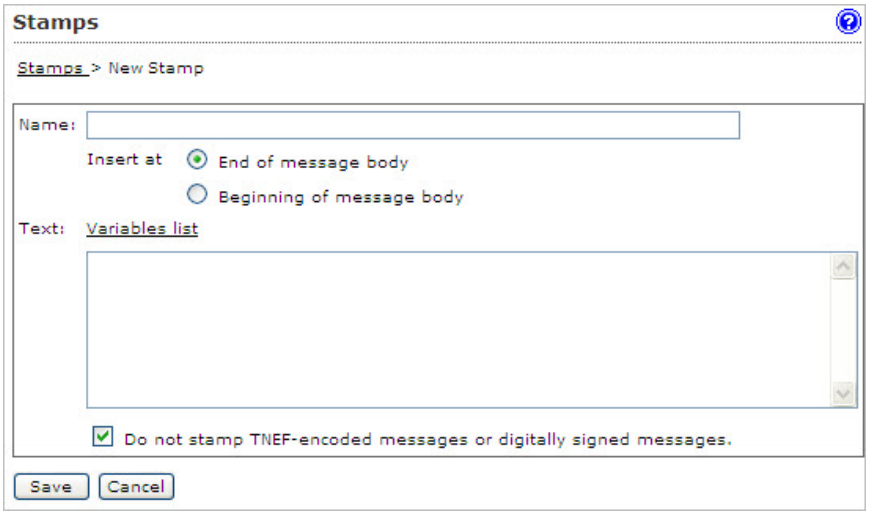
1. Go to **Policy** > **Stamps**.

   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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.

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**.

DKIM Approved List

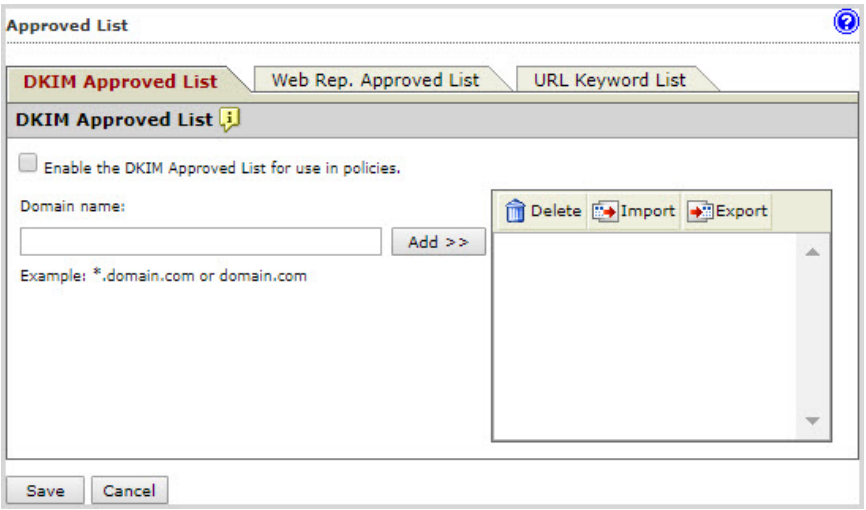
DomainKeys Identified Mail (DKIM) is a signature/cryptography-based email authentication that provides a method for validating a message during its transfer over the Internet. By validating that the message comes from the source it is claiming, IMSS provides spam and phishing protection for your network.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

   The **DKIM Approved List** tab 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. Click **Browse** to locate the file to import.

c. Select one of the following:

- Merge with current list
- Overwrite current list

d. Click **Import**.

4. Click **Save**.

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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
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.

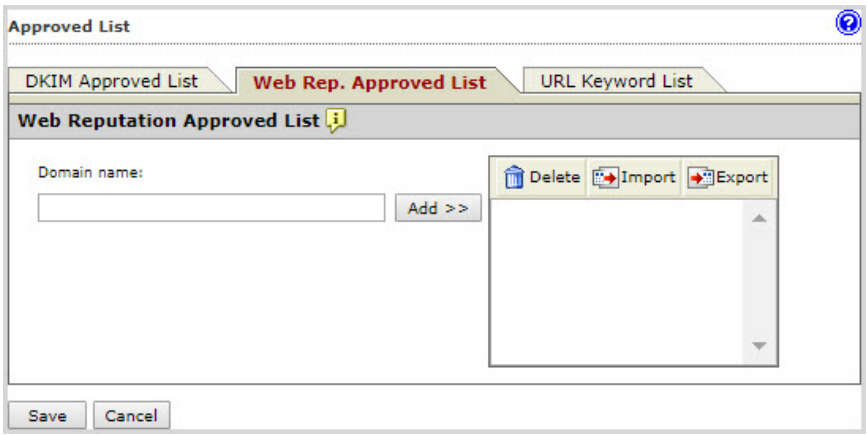
Adding to the Web Reputation Approved List

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** > **Approved List**.
2. Click the **Web Rep. Approved List** tab.

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



3. 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. Click **Browse** to locate the file to import.

c. Select one of the following:

- Merge with current list
- Overwrite current list

d. Click **Import**.

4. Click **Save**.

URL Keyword List

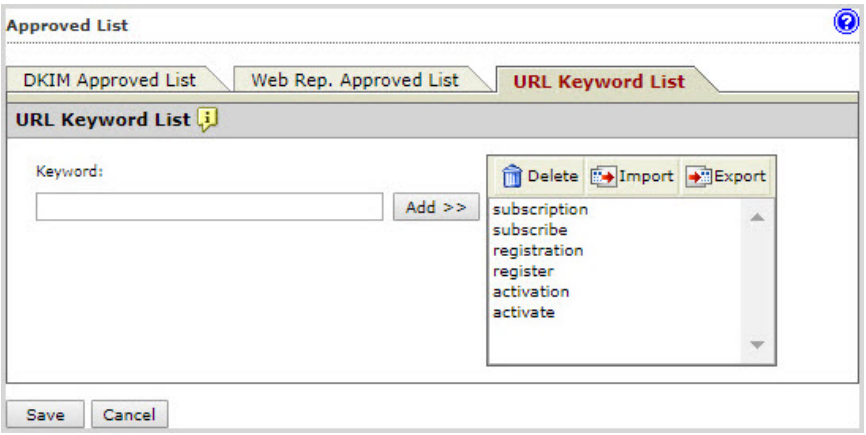
URLs that contain any of the specified keywords are considered one-click URLs and will not be sent to Virtual Analyzer.

Configuring the URL Keyword List

Procedure

1. Go to **Policy** > **Approved List**.
2. Click the **URL Keyword List** tab.

The **URL Keyword List** screen appears.



3. Configure the URL keyword list in one of the following ways:

   Manually:

   a. Specify a keyword, for example, `subscription`.

   b. Click **Add>>**.

   Import a list:

   Note

   URL keywords are not case sensitive.

   Specify one keyword per line.

   a. Click **Import**.

      The **Import Keywords** screen appears.

   b. Click **Browse** to locate the file to import.

   c. Select one of the following:

- Merge with current list
- Overwrite current list

d. Click **Import**.

Chapter 15

Configuring Internal Addresses

This chapter provides instructions for configuring internal addresses.

Topics include:

- *Configuring Internal Addresses on page 15-2*
- *Searching for Users or Groups on page 15-5*
- *Searching for an LDAP User or Group on page 15-6*

Configuring Internal Addresses

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

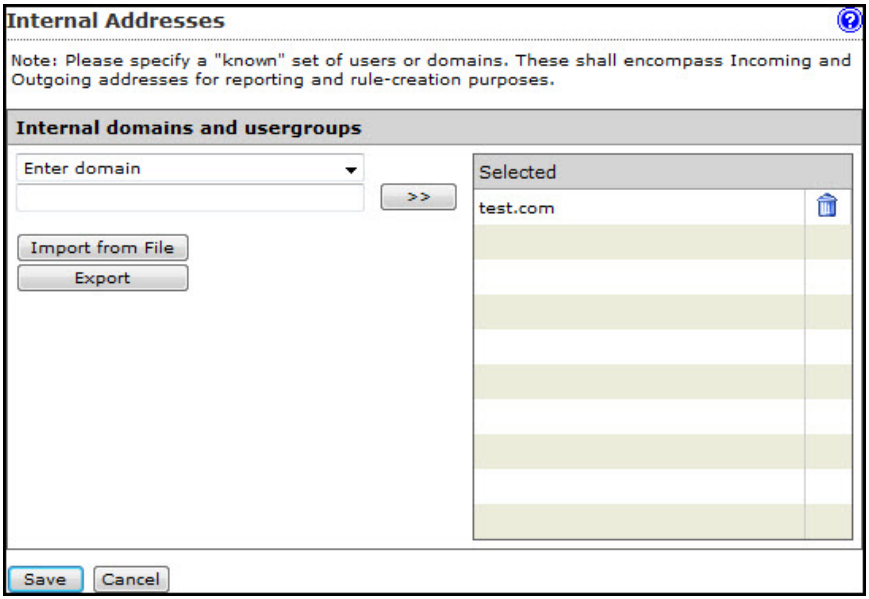
- For incoming messages, specify the recipient's address, which is in range of the internal addresses. For example: internal address is `imsstest.com`, valid recipients include jim@imsstest.com, bob@imsstest.com.
- For outgoing messages, specify the sender's address, which is in range of the internal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

Note

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

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

Tip

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

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

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

Note

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

4. Click **Save**.

Exporting Internal Addresses

Procedure

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

   The **Internal Addresses** screen appears.

2. Click **Export**.

   A **File Download** dialog box appears.

3. Click **Save**.

   A **Save As** dialog box appears.

4. Specify the location and file name.

5. Click **Save**.

Searching for Users or Groups

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

- Email address
- LDAP group
- Address group

Procedure

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

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

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

3. Select one or both check boxes next to **Senders** or **Recipients**.
4. From the drop-down box, select one of the following:
   - **Email address**
   - **LDAP user or group**
   - **Address group**
5. In the text box, specify the key words for which to search.
6. Click **Select**.

Searching for an LDAP User or Group

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

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

- IBM™ Lotus Domino 6.0
- Microsoft™ Active Directory 2000, 2003, 2008 R2, 2012 and 2016
- Sun iPlanet Directory 5.2
- OpenLDAP™ 2.4

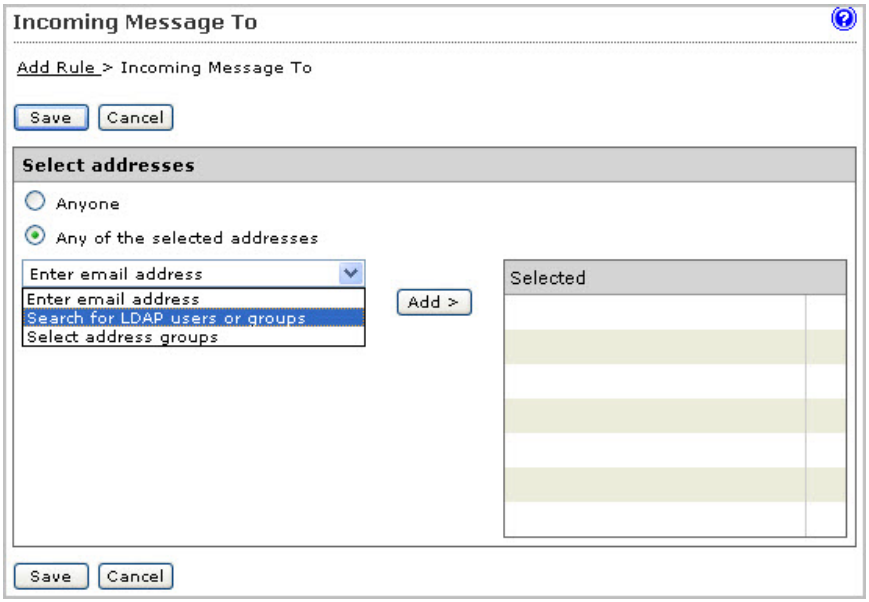
The following steps provide instructions on adding an LDAP user or group when creating a new policy.

Procedure

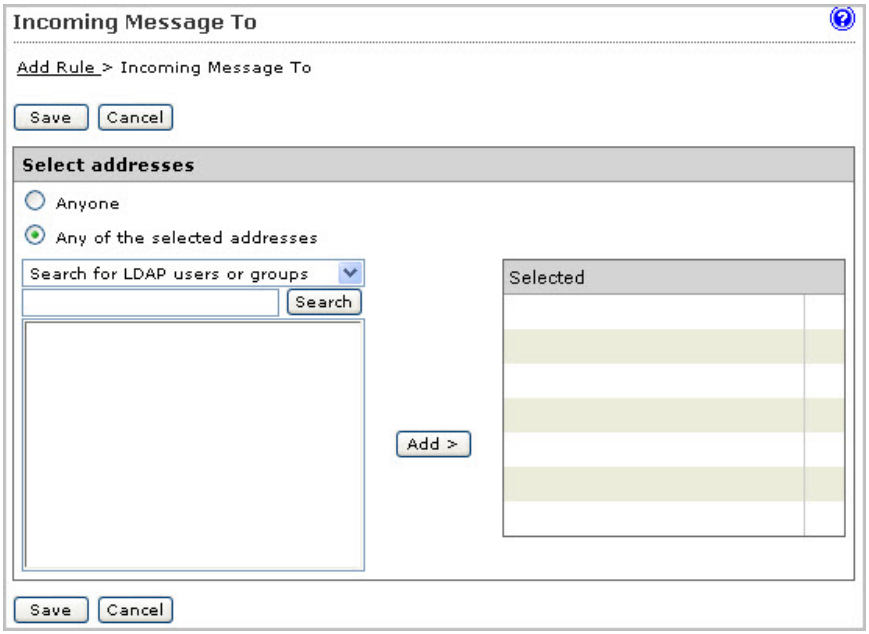
1. Go to **Policy** > **Policy List**.
2. Click **Add**.

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

   The **Select Addresses** screen appears.



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 20-15*..

b. You can also search for LDAP groups when adding internal addresses. See *Configuring Internal Addresses on page 15-2*.

---

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 16

Using Trend Micro Smart Protection

This chapter discusses Trend Micro™ smart protection solutions and describes how to set up the environment required to use the solutions.

- *About Trend Micro Smart Protection on page 1-19*
- *Smart Protection Sources on page 16-5*
- *Selecting a Scan Method on page 16-7*
- *Using Web Reputation Services on page 16-10*

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

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat.

By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in the protection of others. Because the gathered threat information is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Samples of information sent to Trend Micro:

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

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

Tip

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

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Smart Protection Sources

Trend Micro delivers File Reputation Services and Web Reputation Services to IMSS and smart protection sources.

Smart protection sources provide File Reputation Services by hosting the majority of the virus/malware pattern definitions. IMSS clients host the remaining definitions. The client sends scan queries to smart protection sources if its own pattern definitions cannot determine the risk of the file. Smart protection sources determine the risk using identification information.

Smart protection sources provide Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. The client sends web reputation queries to smart protection sources 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 endpoint to determine whether access to the site will be allowed or blocked.

The smart protection source to which the client connects depends on the client's location. Clients can connect to either Trend Micro Smart Protection Network or Smart Protection Server.

Smart Protection Sources Compared

The following table highlights the differences between Smart Protection Network and Smart Protection Server.

TABLE 16-1. Smart Protection Sources Compared

BASIS OF COMPARISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Purpose	Designed and intended to localize smart protection services to the corporate network to optimize efficiency	A globally scaled, Internet-based infrastructure that provides smart protection services to clients who do not have immediate access to their corporate network
Administration	IMSS administrators install and manage these smart protection sources	Trend Micro maintains this source
Pattern update source	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Client connection protocols	HTTP and HTTPS	HTTPS

Adding Smart Protection Servers

Smart Protection Servers localize smart protection services to the corporate network to reduce outbound traffic and optimize efficiency.

You can add, delete, import and export Smart Protection Servers on the IMSS management console. The steps outlined below detail the process to add a Smart Protection Server.

Procedure

1. Go to **Policy** > **Smart Protection**.

   The **Security Risk Scan** tab appears by default.

2. Click the **Local Sources** tab.
3. Click **Add**.

   The **Add Smart Protection Server** screen appears.
4. Specify Smart Protection Server settings.

   a. Specify the server IP address or FQDN.

   b. To use File Reputation Services, select **File Reputation Port** and specify the port number.

   c. To use Web Reputation Services, select **Web Reputation Port** and specify the port number.

   d. Specify the preference value.

   Note

   Preference represents the priority of a Smart Protection Server. The lower the preference value, the higher the priority.
5. Specify the proxy setting.

   a. Select the **Enable** check box to enable the proxy server.

   b. Specify the proxy server IP address or FQDN, port number, user name and password.
6. Click **Test Connection** to verify Smart Protection Server connection.
7. Click **Save**.

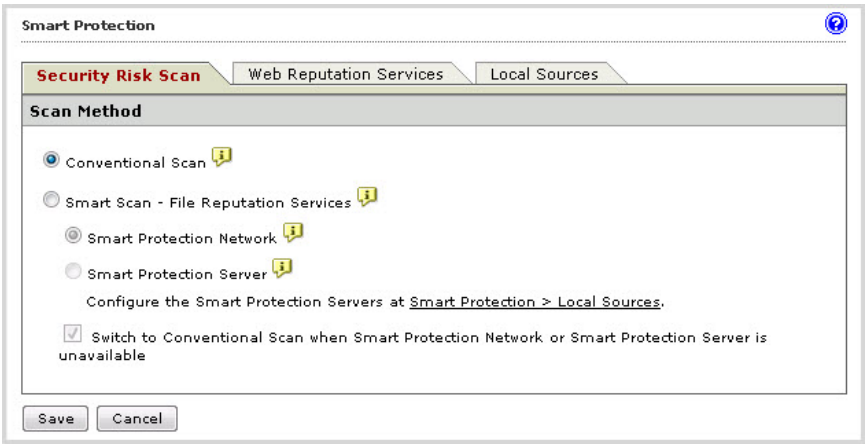
Selecting a Scan Method

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

Procedure

1. Go to **Policy** > **Smart Protection**.

   The **Security Risk Scan** tab appears by default.



2. Select one of the following malware scanning methods.

   - **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.

   - **Smart Scan - File Reputation Services**: 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.

Note

Conventional Scan is the default scan method.

3. If you selected **Smart Scan - File Reputation Services**, select one of the following smart protection sources:

   - **Smart Protection Network**: If you select this option, specify the proxy server setting.
   - **Smart Protection Server**: If you select this option, click the **Local Sources** tab and configure Smart Protection Servers.

Note

IMSS reverts to Conventional Scan when the selected Smart Protection Network or Smart Protection Server is unavailable. IMSS can switch to Conventional Scan only when you have selected **Switch to Conventional Scan when Smart Protection Network or Smart Protection Server is unavailable**.

4. Click **Save**.

Note

If Smart Scan is selected, IMSS attempts to connect to the Smart Protection Network or Smart Protection Server 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.

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

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 24-12*.

You can configure IMSS to send notifications for scan method changes. For details on configuring notifications, see *Configuring Event Criteria and Notification Message on page 26-5*.

Using Web Reputation Services

If you have configured Smart Scan on the **Security Risk Scan** tab, the smart protection environment has been set up, and IMSS is ready to use File Reputation Services. To allow IMSS to use Web Reputation Services, configure web reputation policies.

Procedure

1. Go to **Policy** > **Smart Protection**.

   The **Security Risk Scan** tab appears by default.

2. Click the **Web Reputation Services** tab.

3. Select one of the following smart protection sources:

   - **Smart Protection Network**: If you select this option, go to **Administration** > **Proxy** and configure the proxy setting.
   - **Smart Protection Server**: If you select this option, click the **Local Sources** tab and configure Smart Protection Servers.

Note

IMSS reverts to Smart Protection Network when the selected Smart Protection Server is unavailable. IMSS can switch back to Smart Protection Network only when you have selected **Switch to Smart Protection Network when Smart Protection Server is unavailable**.

If you select the **Do not make external queries to Smart Protection Network** check box, IMSS requests Smart Protection Servers not to make queries outside of the users' environment.

---

4. Click **Save**.

Chapter 17

Configuring Policies

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

Topics include:

- *Adding Policies on page 17-2*
- *Specifying a Route on page 17-2*
- *Specifying Scanning Conditions on page 17-10*
- *Specifying Actions on page 17-41*
- *Finalizing a Policy on page 17-48*

Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For information, see *Configuring Internal Addresses on page 15-2*.

Creating a policy involves the following steps:

- Step 1: *Specifying a Route on page 17-2*
- Step 2: *Specifying Scanning Conditions on page 17-10*
- Step 3: *Specifying Actions on page 17-41*
- Step 4: *Finalizing a Policy on page 17-48*

Tip

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

Specifying a Route

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

Route

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

Route type

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

Adding a Route

Procedure

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

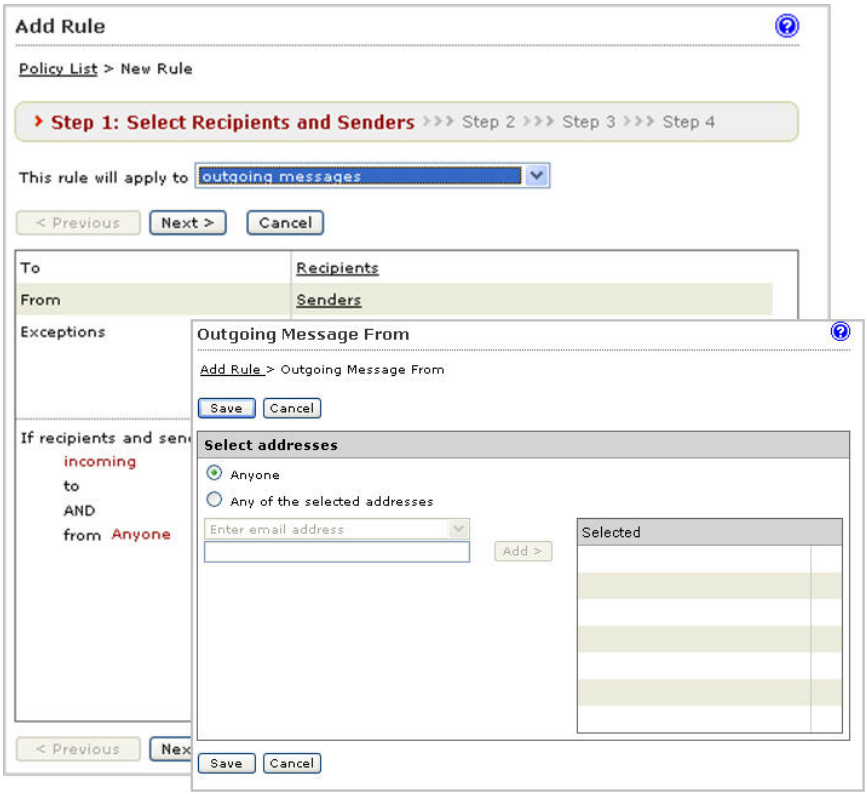
   The **Policy List** screen appears.

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

   - Antivirus
   - Other

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

The **Add Rule** screen appears.



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 20-15*.

   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.

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 20-15*.

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 17-1. 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. **Spam/Phishing Email**: Scans messages identified as spam and phishing messages. Spam messages are generally unsolicited

messages containing mainly advertising content. Phishing messages, on the other hand, originate from senders masquerading as trustworthy entities.

- **Spam detection settings**: Click the link to select a level of spam protection and configure lists for approved and blocked senders and text exemptions.
- **Phishing email**

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

d. **Marketing Messages** : Scans messages against the ERS score to approve certain marketing messages.

e. **Attachment**: Scans messages for file attachments that match the selected criteria, such as attachments with specific extensions or belonging to a certain true file type.

- **Name or extension**: Click the link to configure filter settings for specific file names or extension names.
- **MIME content type**: Click the link to configure filter settings for MIME content types.
- **True file type**: Click the link to configure filter settings for common executable, document, image, media, and compressed files.
- **Size is {>, <, =} {size} {MB, KB, B}**: Select to filter attachments of a size that is more than, less than, or equal to a certain number of bytes, kilobytes, or megabytes. Specify a number that represents the file size.
- **Number is {>, <, =} {number}**: Select to filter the number of attachments that is more than, less than, or equal to a certain number. Specify a number that represents the total number of attachments for each message.

- **Password protected zip files (unscannable files)**: Select to filter password protected zip files that cannot be scanned by IMSS.

f. **Size**: Scans messages that match the specified message size.

- **Message size is {>, <, =} {size} {MB, KB}**: Select to filter messages of a size that is more than, less than, or equal to a certain number of kilobytes, or megabytes. Specify a number that represents the message size.

g. **Content**: Scans messages containing the keyword expressions that match those expressions specified in the subject, body, header, or attachment keyword expressions links.

- **Subject keyword expressions**: Click the link to manage your expression lists.
- **Subject is blank**: Select to filter messages without a subject. Sometimes spam messages do not contain subject lines.
- **Body keyword expressions**: Click the link to manage your expression lists.
- **Header keyword expressions**: Click the link to manage your expression lists. Headers include Subject, To, From, CC, and other headers that you can specify.
- **Attachment keyword expressions**: Click the link to manage your expression lists. Attachments include attachment names and attachment content.

h. **Others**: Scans messages in which the number of recipients match the specified number. Also scans messages that are received within the specified time range.

- **Number of recipients is {>, <, =} {number}**: Select to filter the number of recipients. Specify a number that represents the total number of recipients for each message.

- **Received time range**: Click the link to select a day and time within which a message was received.
- **Encrypted messages**: Select to filter encrypted messages that cannot be decrypted by IMSS.

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.

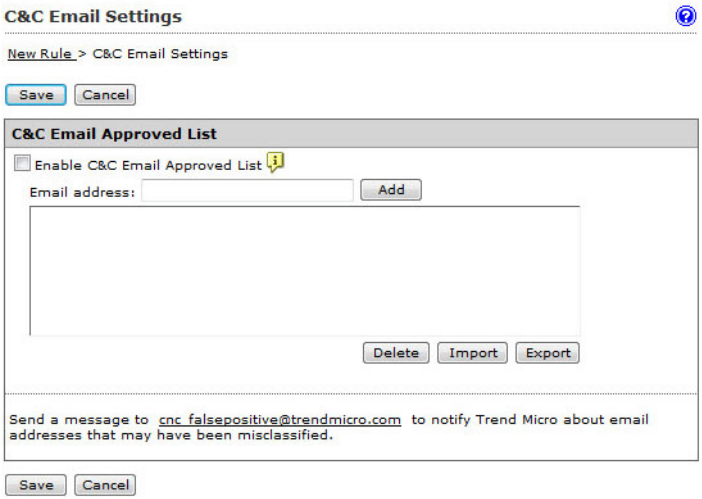
Note

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 20-15*.

   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 17-16*.

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 9.1 Patch 1] 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 17-16*.
  - 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 **Phishing/Social Engineering Attack/Spam** 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 17-19*.

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 Graymail Exceptions

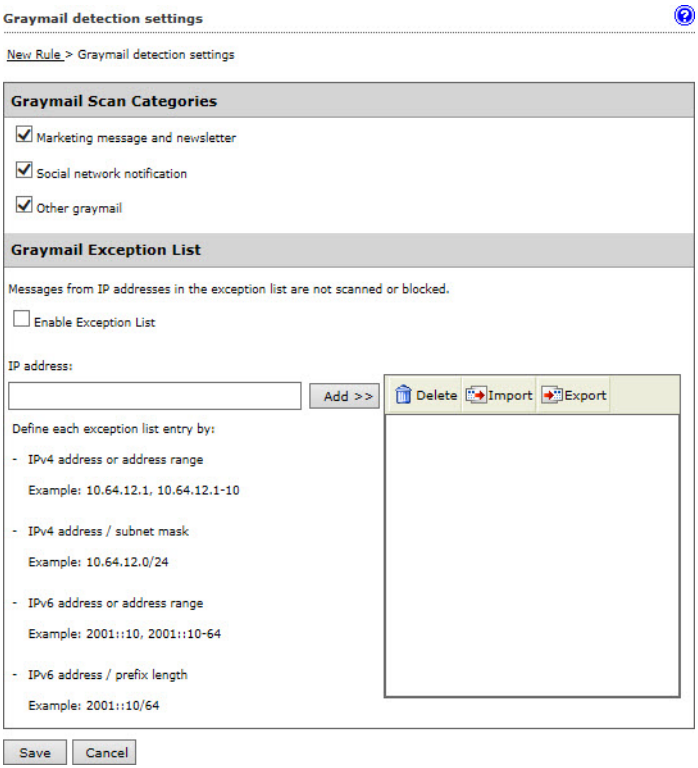
The exception list is a list of IP addresses to ignore when filtering content. Add up to 5,000 IP addresses by either adding individual addresses or by

importing multiple addresses from a text file. The policy takes effect on IP addresses in their order in the list.

Procedure

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
2. Under **Graymail**, click **Graymail detection settings**.

The **Graymail detection settings** screen appears.



3. Select **Enable Exception List**.
4. Add IP addresses using the following methods:
   a. Specify an IP address and then click **Add>>**.

      The IP address appears in the list.

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

      For details, see *Importing Graymail Exceptions on page 17-24*.

5. Optional: Export the IP address list as a text file.
6. Click **Save**.

Importing Graymail Exceptions

Before you begin

Complete configuring graymail exceptions.

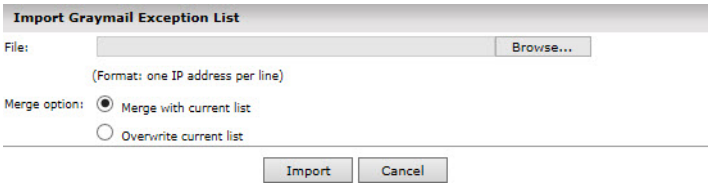
Note

- Each line in the file should contain only one IP address that follows any of the valid formats. IMSS does not import incorrectly formatted IP addresses.
- If the list already contains an IP address that is in the file, the IP address is ignored.
- If the file contains greater than 5,000 IP address, only the first 5,000 are imported.

Procedure

1. In the right pane of the **Graymail Exception List** area, click **Import**.

   The **Import Graymail Exception List** screen appears.



2. Click **Browse** and locate the file.

   Examples of valid input:

IPv4 addresses

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

IPv6 addresses

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

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

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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.

2. Under Web Reputation on the **Scanning Conditions** screen, select the **Web Reputation settings** check box.

3. Click **Next** to continue configuring the policy.

Completing Web Reputation Settings

Procedure

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

   - For information on creating a new rule, see *Configuring Policies on page 17-1*.

   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.

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 the action to take if IMSS detects URLs that have not been tested by Trend Micro.

- **Bypass**: Bypasses email messages that contain the URLs.
- **Apply the policy action**: Applies the action specified in the policy.
- **Submit to Virtual Analyzer**: Submits the URLs to Virtual Analyzer for further analysis.

6. Select **Enable Time-of-Click Protection** and click one of the following:
   - **Apply to URLs that have not been tested by Trend Micro**
   - **Apply to URLs marked by Web Reputation Services with smart flags**
   - **Apply to all URLs**

   Note

   A smart flag is an indicator for rewriting URLs in email messages, which leverages correlation intelligence of Trend Micro Smart Protection Network to detect suspicious and malicious Web threat behaviors.

7. Optional: Select **Apply to URLs in digitally signed messages** if necessary.

   Note

   Enabling Time-of-Click Protection for digitally signed messages is not recommended because digital signatures might be destroyed.

8. 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.
9. Click **Save**.

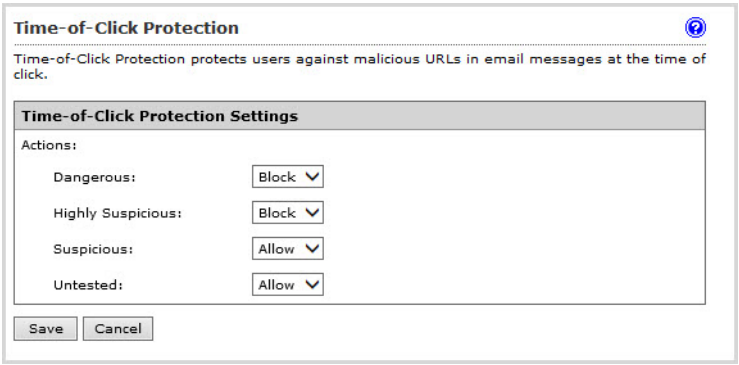
Configuring Time-of-Click Protection Settings

If you enable Time-of-Click Protection, IMSS rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious to protect you.

Procedure

1. Go to **Policy** > **Time-of-Click Protection**.

   The **Time-of-Click Protection** screen appears.



2. Under **Actions**, do the following:

   - **Dangerous**: Select an action (**Allow**, **Warn** or **Block**) to take on dangerous URLs. The default value is **Block**.

     Dangerous URLs are verified to be fraudulent or known sources of threats.

   - **Highly Suspicious**: Select an action (**Allow**, **Warn** or **Block**) to take on highly suspicious URLs. The default value is **Block**.

     Highly suspicious URLs are suspected to be fraudulent or possible sources of threats.

   - **Suspicious**: Select an action (**Allow**, **Warn** or **Block**) to take on suspicious URLs. The default value is **Allow**.

     Suspicious URLs are associated with spam or possibly compromised.

   - **Untested**: Select an action (**Allow**, **Warn** or **Block**) to take on untested URLs. The default value is **Allow**.

While Trend Micro actively tests URLs for safety, users may encounter untested pages when visiting new or less popular websites. Blocking access to untested pages can improve safety but can also prevent access to safe pages.

3. Click **Save**.

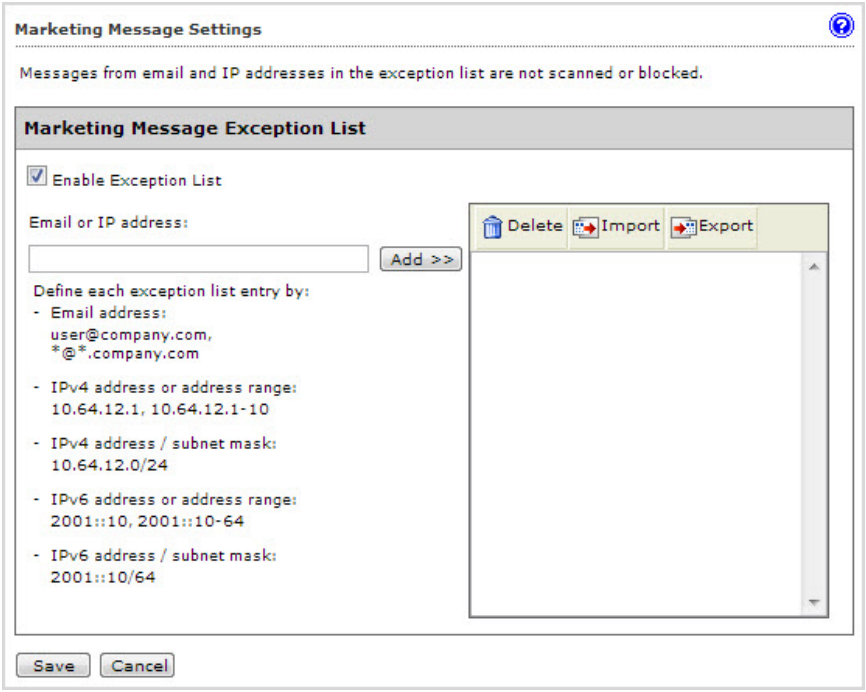
Configuring Marketing Message Exceptions

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

Procedure

1. Create or modify an "Other" (not an Antivirus) policy.
   - For information on creating a new rule, see *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.
2. Under **Marketing Messages**, click **Marketing message settings**.

The **Marketing Message Settings** screen appears.



3. Select **Enable Exception List**.
4. Add email or IP addresses using the following methods:
   a. Specify an email or IP address and then click **Add>>**.

      The address appears in the list.

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

      For details, see *Importing Marketing Email Exceptions on page 17-31*.
5. Optional: Export the address list as a text file.

6. Click **Save**.

Importing Marketing Email Exceptions

Before you begin

Complete *Configuring Marketing Message Exceptions on page 17-29*

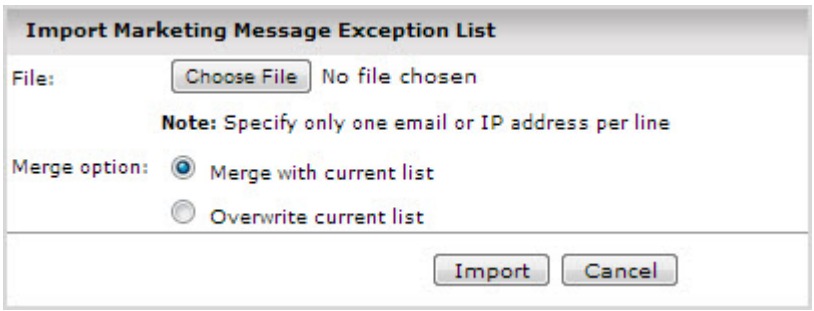
Note

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

Procedure

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

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



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

Examples of valid input:

Email addresses

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

IPv4 addresses

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

IPv6 addresses

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

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

Selecting Scanning Conditions for Attachments

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

Specifying Scanning Conditions for Attachment Names or Extensions

Procedure

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **Name or extension**.
2. Click **Name or extension**.

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

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

Specifying MIME Content Type Scanning Conditions

Procedure

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

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

   Use a semicolon (;) to separate values. You can also use an asterisk wildcard for the MIME type.
6. Click **Save** to continue selecting scanning conditions.

Specifying True File Type Scanning Conditions

Procedure

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

   The **Attachment True File Type** screen appears.
3. Next to **Select**, select one of the following:

- **Selected attachment types**: IMSS takes action on messages with attachments of the selected types.
- **Not the selected attachment types**: IMSS takes action on messages with attachments that are not of the selected types.

4. Select the check boxes next to the true file types to filter.
5. Click **Save** to continue selecting scanning conditions.

Specifying Attachment Size Scanning Conditions

Procedure

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Size is {>, <, =} {size} {MB, KB, B}**.
2. Select the comparison symbol (>, <, =).
3. Specify a number to represent the size.
4. Select Megabytes, Kilobytes, or Bytes (**MB, KB, B**).
5. Continue selecting scanning conditions.

Specifying Attachment Number Scanning Conditions

Procedure

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

Blocking Password Protected Zip Files

Procedure

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

Selecting Scanning Conditions for Message Size

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

Procedure

1. Under **Size** on the scanning conditions selection screen, select the check box next to **Message size is {>, <, =} {size} {MB or KB}**.
2. Select the comparison symbol (>, <, =).
3. Specify a number to represent the size of the message.
4. Select **Megabytes** or **Kilobytes** (**MB** or **KB**).
5. Continue selecting scanning conditions.

Selecting Scanning Conditions for Message Content

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

Procedure

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

   The **Policy** screen appears.

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

   The screen for managing keyword expressions appears.
7. Configure the expressions.
8. In the **Available** list, click the expression list you want to enable.
9. Click **>>**.

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

   To keep an expression list available but temporarily prevent IMSS from using it, click the expression in the selected list, and then click **<<**.
10. Click **Save** to continue to the scanning conditions selection screen.

Specifying Compliance Scanning Conditions

Regulatory compliance for IMSS must be activated before the compliance templates can be used in a policy.

Procedure

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

   The **Policy** screen appears.

2. Create or modify an "Other" (not an Antivirus) policy.

3. Under **Data Loss Prevention**, click **DLP compliance templates**.

   The **DLP Compliance Templates** screen appears.

4. Select the DLP compliance templates you require from the **Available** list.

5. 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 *Configuring Policies on page 17-1*.
   - For information on modifying an existing rule, see *Configuring Existing Policies on page 20-1*.

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.

Setting Scanning Conditions for Spoofed Internal Messages

IMSS blocks all messages if they do not originate from the trusted internal IP address list. This filter triggers only on messages where the sender's and recipient's domains are the same.

Procedure

1. Under **Others** on the scanning conditions selection screen, select the check box next to **Spoofed internal messages**.
2. Click **Spoofed internal messages**.

   The Spoofed Internal Messages screen appears.

   WARNING!

   All edge MTA IP addresses must be added to this list if the feature is enabled. If the IP addresses are not added to the list, all messages from the edge MTAs that are not added will be blocked.
3. Add IP addresses to the Trusted Internal IP List.
4. Click **Save**.

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 to	IMSS puts the message and its attachments into the quarantine area that you select from the drop-down box.
Change recipient to	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.
Delete attachments	Select an action for IMSS to take: • **Delete matching attachment**: Remove only the attachment that matches the attachment scan condition.

Option	Description
	• **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 *Notifications on page 14-47*.
Archive modified to	Archive the message to an archive area.
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 to	IMSS puts the message and its attachments into the quarantine area that you select from the drop-down box.
Change recipient to	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.

Option	Description

	• **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.
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 *Notifications on page 14-47*.
Archive modified to	Archive the message to an archive area.
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. 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.

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

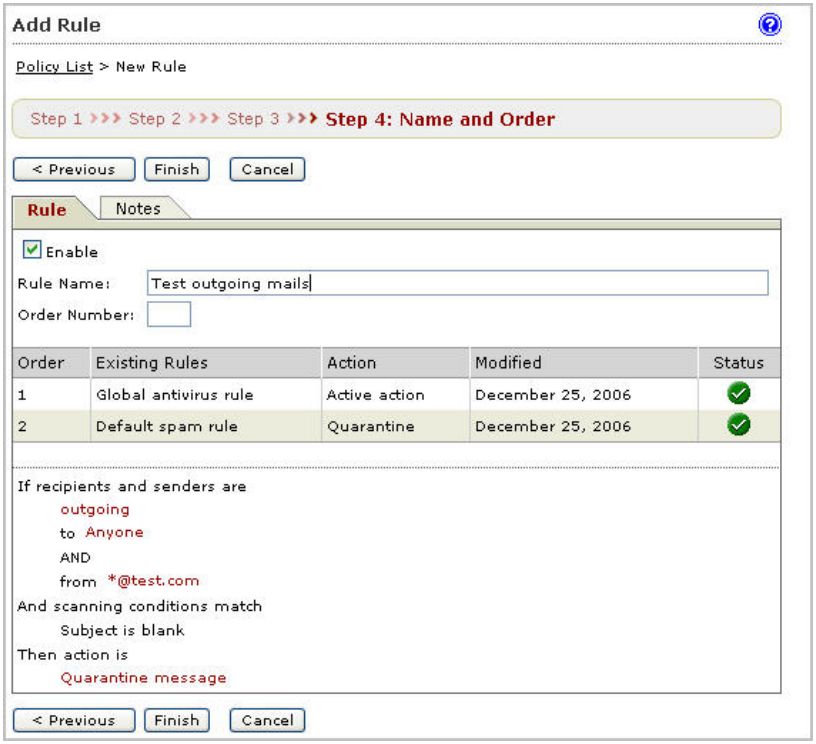
You can enable and disable rules by clicking the buttons.

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 18

Configuring Encryption Settings

This chapter provides instructions for configuring encryption settings for IMSS.

Topics include:

- *Configuring Encryption Settings on page 18-2*
- *Encrypting Message Traffic on page 18-3*
- *Configuring Encryption Policies on page 18-3*

Configuring Encryption Settings

Trend Micro Email Encryption must have your registered domain in order to work. When you register a domain, Trend Micro Email Encryption acquires an encryption key that is unique to your registered and confirmed domain. Without the key, Trend Micro Email Encryption cannot encrypt your message.

Note

In addition to logging in, this email address will be used only for other product related use (example: password resets and registration notifications). It will not be used for marketing purposes, nor sold to any other party. You will not receive spam as a result of registering Encryption for Email.

In distributed environments, the ID that appears on the **Encryption Settings** > **IMSS** tab is shared by the parent IMSS and all child IMSSs.

Encryption Types

There is a difference between the **Encryption exception** rule and the **Unable to decrypt messages** policy rule.

TABLE 18-1. Encryption Types

FEATURE	DESCRIPTION
Encryption exception	This rule triggers when IMSS cannot decrypt or encrypt messages using an Identity-Based Encryption (IBE) algorithm.
Unable to decrypt messages	This rule is used to detect messages encrypted by Pretty Good Privacy (PGP) encryption or Secure/Multipurpose Internet Mail Extensions (S/MIME) encryption. IMSS can decrypt messages encrypted by IBE. However, you must first register a domain to the Trend Micro Email Encryption Server before IMSS is able to decrypt messages from that domain.

Encrypting Message Traffic

Your domains must be registered to the Trend Micro Encryption Email service for email encryption to work. See *Registering Domains to the Encryption Service on page 7-7* for more information.

After configuring encryption settings, IMSS can decrypt and encrypt the messages to protect the message content.

For encrypted message traffic entering your network, IMSS decrypts the messages automatically and scans the messages according to the policy rules you specify. Outgoing messages are re-encrypted after scanning to protect the message content.

Configuring Encryption Policies

IMSS can encrypt plain text message content when you select Encrypt message when specifying scan actions for policies.

If you enable a rule to encrypt incoming messages, registration and support messages from privatepost.com are not encrypted.

Note

Encrypting messages is a terminal action. The message will be delivered to the intended recipient if this action is taken.

After selecting **Encrypt message**, **Deliver the message** is selected automatically and the following selections are not available: **Delete entire message**, **Change recipient to**, and **Postpone delivery to**.

Chapter 19

Configuring Scanning Exceptions

This chapter provides instructions for configuring IMSS scanning exceptions.

Topics include:

- *Setting Scan Exceptions on page 19-2*
- *Configuring Exceptions for Security Settings Violations on page 19-3*
- *Setting Scan Actions for Security Setting Violations on page 19-4*
- *Setting Scan Actions for Malformed Messages on page 19-5*
- *Configuring Exceptions for Encrypted Messages on page 19-7*
- *Setting Scan Actions for Encrypted Messages on page 19-8*
- *Setting Scan Actions for Virtual Analyzer Scanning Exceptions on page 19-9*

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 25-2*.
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. IMSS does not support IPv6 handoff server addresses.

3. Configure **Monitor** settings.

Option	Description
Send policy notifications	Send a notification message to one or more recipients. To select a type of notification, click **Send policy notifications**. For instructions on creating notifications, see *Notifications on page 14-47*.
Archive to	Archive the message to an archive area. For instructions on creating a new archive area, see *Configuring Quarantine and Archive Settings on page 25-2*.
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.
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. IMSS does not support IPv6 handoff server addresses.

3. Configure **Monitor** settings.

Option	Description
Send policy notifications	Send a notification message to one or more recipients. To select a type of notification, click **Send policy notifications**. For instructions on creating notifications, see *Notifications on page 14-47*.
Archive to	Archive the message to an archive area.
BCC	Blind carbon copy the message to another recipient. Specify the recipient's email address and separate multiple addresses with a

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

4. Click **Save**.

Configuring Exceptions for Encrypted Messages

Messages exceeding any of the limits specified on this screen will not be decrypted or encrypted by IMSS.

Procedure

1. Go to **Policy** > **Scanning Exceptions** > **Encryption Exceptions**.
2. To set limits on encrypted or decrypted messages IMSS processes, configure the following:
   - **Encrypted message size exceeds { } MB**: Specify the maximum number of megabytes.
   - **Decrypted message size exceeds { } MB**: Specify the maximum number of megabytes.
   - **Total # recipients exceeds { } recipients**: Specify the maximum number of recipients.
   - **Unable to encrypt outgoing message**: Select this option to trigger IMSS to take action on outgoing messages that IMSS cannot encrypt.
   - **Unable to decrypt outgoing message**: Select this option to trigger IMSS to take action on outgoing messages that IMSS cannot decrypt.
3. Click **Save**.

   The **Scanning Exceptions** screen reappears.

Setting Scan Actions for Encrypted Messages

Procedure

1. Go to **Policy** > **Scanning Exceptions**.
2. Click the **Quarantine and Notify** link for **Encryption exception**.

   The screen for configuring actions appears.
3. Under **Intercept**, click the radio button next to one of the following:
   - **Do not intercept messages**: IMSS does not process the message.
   - **Delete entire message**: Deletes the message and all attachments.
   - **Quarantine to**: 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 25-2*.
   - **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 any more as it is no longer within the control of IMSS.
4. Under **Monitor**, select the check boxes next to any of the following:
   - **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 *Notifications on page 14-47*.

- **Archive to**: Archive the message to an archive area. For instructions on creating a new archive area, see *Configuring Quarantine and Archive Settings on page 25-2*.
- **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.

5. Click **Save**.

Setting Scan Actions for Virtual Analyzer Scanning Exceptions

Procedure

1. Go to **Policy** > **Scanning Exceptions**.
2. Click the **Quarantine and Notify** link for **Virtual Analyzer scanning exceptions**.

   The screen for configuring actions appears.
3. Under **Intercept**, click the radio button next to one of the following:
   - **Do not intercept messages**: IMSS does not process the message.
   - **Delete entire message**: Deletes the message and all attachments.
   - **Quarantine to**: 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 25-2*.
   - **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 any more as it is no longer within the control of IMSS.

4. Under **Monitor**, select the check boxes next to any of the following:
   - **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 *Notifications on page 14-47*.
   - **Archive to**: Archive the message to an archive area. For instructions on creating a new archive area, see *Configuring Quarantine and Archive Settings on page 25-2*.
   - **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.
5. Click **Save**.

Chapter 20

Configuring Existing Policies

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

Topics include:

- *Modifying Existing Policies on page 20-2*
- *Policy Example 1 on page 20-5*
- *Policy Example 2 on page 20-10*
- *Using the Asterisk Wildcard on page 20-15*

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 17-2*.
5. Click **Edit** for one of the following:
   - **And scanning conditions match** (Antivirus and Other rules)
   - **And domains listed here do not pass DKIM verification.** (Global DKIM rule)
6. Configure the scan settings. For more information, see the following:
   - For Antivirus and Other rules: *Specifying Scanning Conditions on page 17-10*
   - For the Global DKIM Enforcement rule: *Using the Domain List for the Global DKIM Enforcement Rule on page 20-3*
   - *Using the Domain List for the Global DKIM Enforcement Rule on page 20-3*
7. Click **Edit** for **Then action is**.
8. Configure the action settings.

   For more information, see *Specifying Actions on page 17-41*.

9. Click **Save**.

Using the Domain List for the Global DKIM Enforcement Rule

IMSS marks all processed messages as spam from domains appearing in the Domain List that:

- Do not pass DKIM validation
- Do not have a DKIM-Signature

Adding Domains to the Domain List in the Global DKIM Enforcement Rule

Procedure

1. Click **Policy** > **Policy List**.

   The **Policy** screen appears.

2. Click the **Global DKIM Enforcement rule** link.

   The **Policy Summary** screen appears.

3. Click **Edit** in the **And domains listed here do not pass DKIM verification** row.

   The **Scanning Conditions** screen appears.

4. Populate the Domain List in one of the following ways:

   - Manually:

     a. Specify a domain name.

     b. Click **Add**.

   - Import a list:

Note

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

a. Click **Import**. The Import DKIM Enforcement List appears.

b. Specify the file path and file name or click **Browse** and locate the file.

c. Select one of the following:

- **Merge with current list**
- **Overwrite current list**

d. Click **Import**.

5. Click **Save**.

Modifying Recipients and Senders for Existing Rules

Procedure

1. Go to **Policy** > **Policy List**.
2. Click the name of the rule to edit.

   The **Summary [policy name]** screen for the rule appears.
3. Click **Edit** for **If recipients and senders** are.
4. Select the policy route type from the drop-down list next to **This rule will apply** to.

   - **incoming messages**
   - **outgoing messages**
   - **both incoming and outgoing messages**

- **POP3**
- **all messages**

5. Select the recipients and senders:
   - For incoming messages, specify the recipient email address, which is in range of the internal addresses. (Example: internal address is `imsstest.com`, valid recipients include jim@imsstest.com, bob@imsstest.com).
   - For outgoing messages, specify the sender's address, which is in range of the internal addresses. (Example: internal address is `imsstest.com`, valid senders include jim@imsstest.com, bob@imsstest.com).
   - For both incoming and outgoing messages, the rule applies to senders or recipients that match the email address.
   - If you selected POP3, you cannot configure the route. The rule applies to all POP3 routes.
   - If you selected "all messages" for a rule, the rule also applies to messages from any sender to any recipient.
6. Click **Save**.

Policy Example 1

Create a rule to delete attachments with specific file names or extensions and then stamp the affected incoming message with an explanation to the recipients.

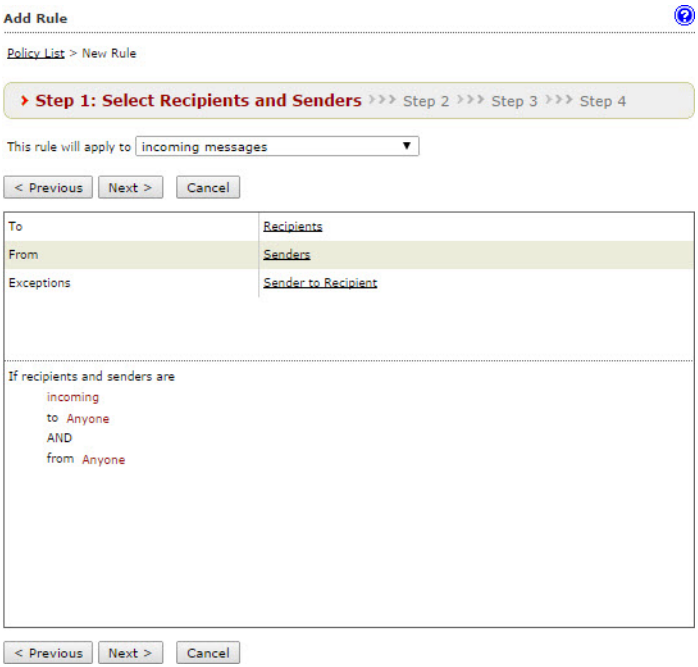
- *Step 1: Specify the Route on page 20-6*
- *Step 2: Specify the Scanning Conditions on page 20-7*
- *Step 3: Specify the Actions on page 20-8*
- *Step 4: Specify the Priority on page 20-9*

Step 1: Specify the Route

Procedure

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

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



4. Next to **This rule will apply to**, select incoming messages from the drop-down list.
5. Click the **Recipients** link.

   The **Select addresses** screen appears.

- To apply this rule to any recipients, select **Anyone**.
- To apply this rule to specific recipients, select **Any of the selected addresses**, and then specify the target email address or group.

6. Click **Save**.

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

Step 2: Specify the Scanning Conditions

Procedure

1. Click **Next**.

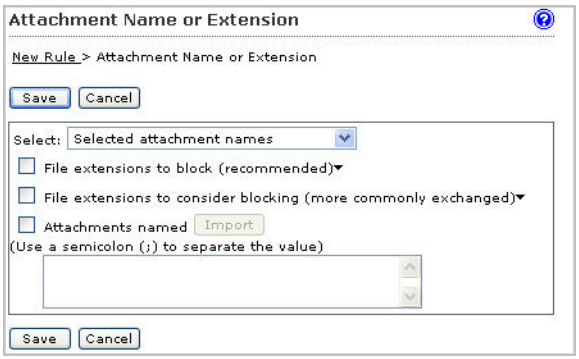
   The **Step 2: Select Scanning Conditions** screen appears.

2. Next to **Take rule action when**, select **any condition matched (OR)**.

3. To enable the **Name or extension** condition, select the check box next to it.

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.

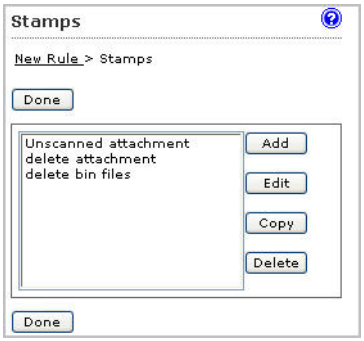
2. Under **Modify**, to enable the **Delete attachment** action, select the check box next to it.

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**.

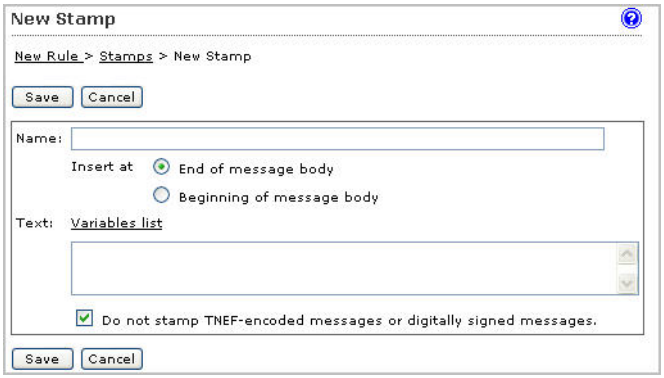
5. If there is no suitable stamp available from the drop-down list, click **Edit**.

   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 20-10*
- *Step 2: Specify the Scanning Conditions on page 20-11*
- *Step 3: Specify the Actions on page 20-15*
- *Step 4: Specify the Priority on page 20-15*

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.

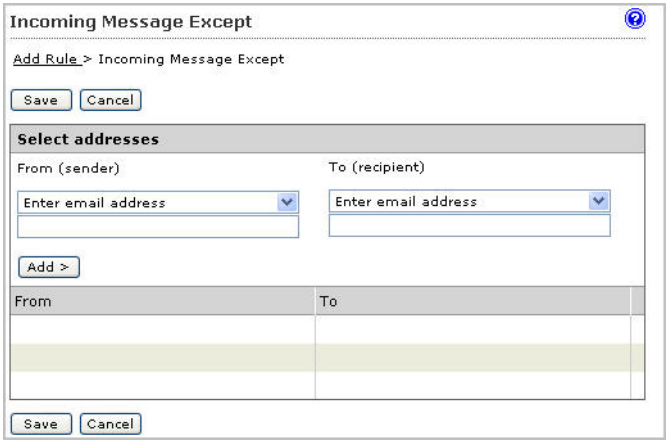
6. Select **Anyone**.

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

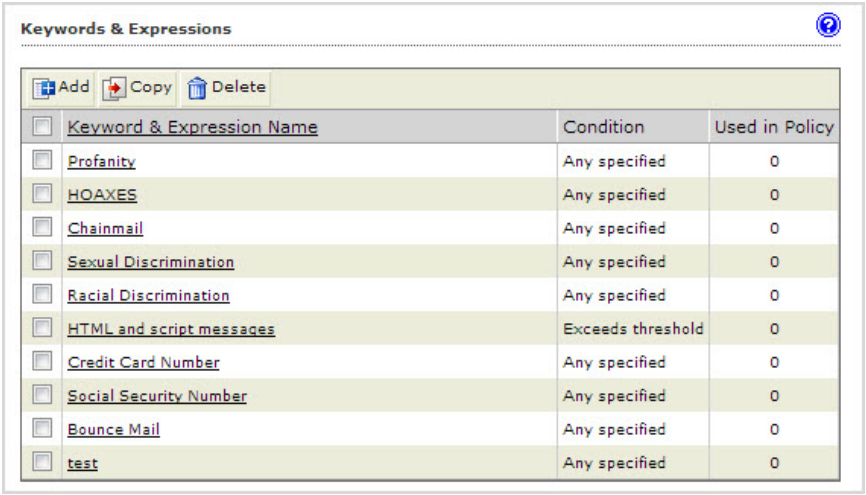
Procedure

1. Click **Next**.

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

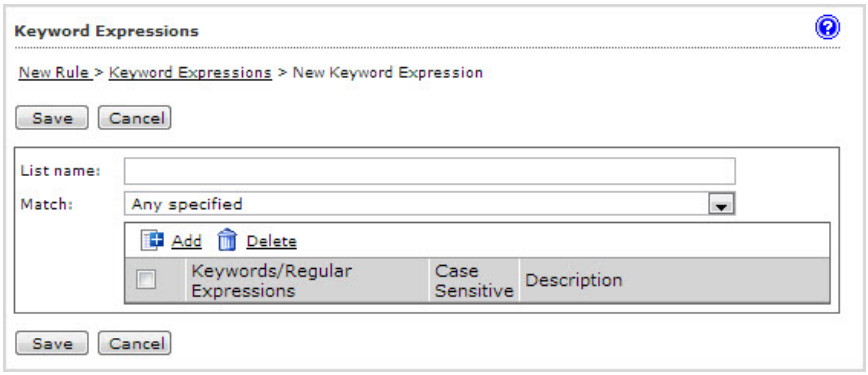
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**.

   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.

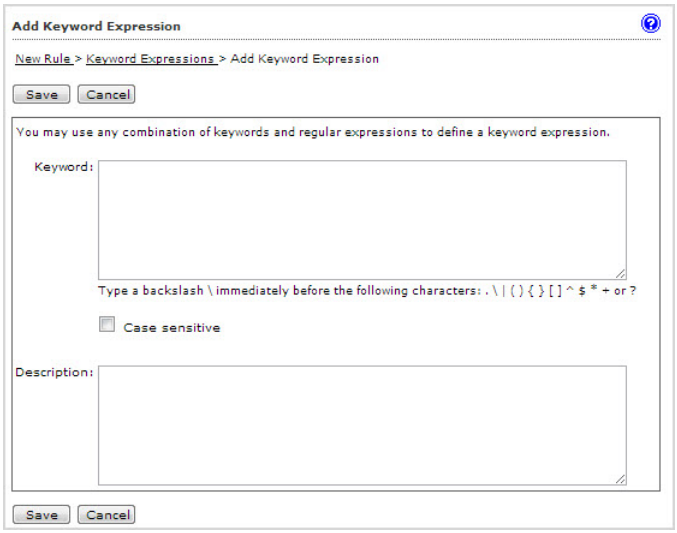
   The **New Keyword Expression** screen appears.



6. Specify the required information.

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

   The **Add Keyword Expression** 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**.

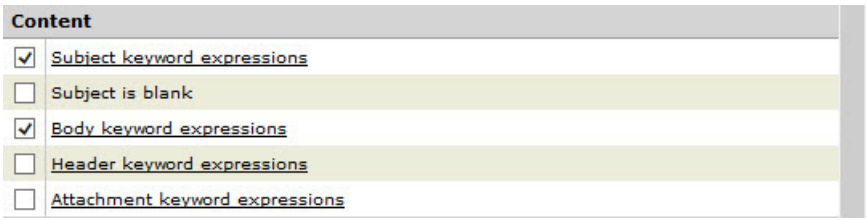
    The **New Keyword Expression** screen re-appears.
11. Select the new list and click **>>** to insert the list into the Selected box.
12. Click **Save**.

    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.

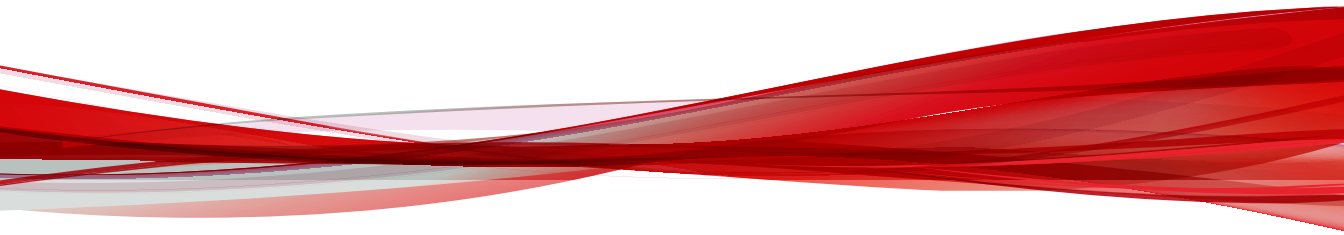
Wildcards in File Names

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.

Part IV

Monitoring the Network



Chapter 21

Monitoring the Network

This section provides you with general instructions on the tasks that you need to perform for day-to-day maintenance.

Topics include:

- *Monitoring Your Network on page 21-2*
- *Viewing System Status on page 21-2*

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 **System Status**.
2. Manage settings.

Option	Description
Enable Connections	View the connections currently enabled (SMTP and POP3). 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. b. Click **Rollback**.

Option	Description
	To refresh the page: • Click **Refresh** to connect to the update source and display the latest component versions in the Availability column.
Managed Services	View other IMSS services registered to this IMSS admin database. To start or stop managed services: • Click **Start** or **Stop** under the service to change. To unregister managed services: • When a managed service is inactive (it is disconnected from the IMSS server), the **Remove** button appears in the Connection column next to the specific service. To remove the managed service from this IMSS server, click **Remove**.  **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.

Chapter 22

Dashboard and Widgets

This chapter provides you with general instructions for using the dashboard and widgets with IMSS.

Topics include:

- *Using the Dashboard on page 22-2*
- *Understanding Tabs on page 22-2*
- *Understanding Widgets on page 22-6*

Using the Dashboard

The IMSS dashboard provides at-a-glance information for the IMSS network. The dashboard is comprised of two components:

- **Tabs:** Allow administrators to create a screen that contains one or more widgets
- **Widgets:** Provide specific information about various security-related events

User Accounts and the Dashboard

Each user account displays it's own dashboard. When a user logs on to IMSS for the first time, the default tabs and the widgets contained within the tabs appear on the dashboard.

Each user account can customize the dashboard, tabs, and widgets for the account's specific needs. Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Understanding Tabs

The IMSS dashboard uses tabs to provide flexibility for administrators. Tabs provide a container for widgets allowing administrators to create their own customized dashboard. The dashboard supports up to 30 tabs per user account.

You can move widgets on tabs by dragging and dropping widgets in various locations on the tab. The layout for a tab determines where you can move the widget.

Note

Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

Default Tabs

The default tabs replace the IMSS Real-Time Statistics screen. All information that was available on the IMSS Real-Time Statistics screen is available through the widgets on the default tabs. The dashboard provides the following default tabs:

- System Overview
- Message Traffic
- Sender Filtering
- Cloud Pre-Filter

Note

Deleting the default tabs permanently removes the tabs from viewing for the user account that removed the tabs. There is no way to recover a deleted tab. Deleting a default tab has no impact on the dashboard for other user accounts.

System Overview Tab

The System Overview tab replaces a portion of the Real-Time Statistics screen. The System Overview tab contains widgets that display system resource usage and queue status information.

TABLE 22-1. System Overview Tab Widgets

WIDGET	DESCRIPTION
System Usage	Displays the system resources used by IMSS on your network.
Mail Queues	Displays the number of messages that just arrived, number of messages ready for delivery, number of messages deferred due to delivery failure, and number of messages kept on hold for later manual delivery.
IMSS Quarantine	Displays the number of quarantined messages and the disk space for each quarantine area.
IMSS Archive	Displays the number of archived messages and the disk space for each archive area.

Message Traffic Tab

The Message Traffic tab replaces a portion of the Real-Time Statistics screen. The Message Traffic tab contains widgets that display message traffic statistics and violations detected by IMSS.

TABLE 22-2. Message Traffic Tab Widgets

WIDGET	DESCRIPTION
IMSS Scan Performance	Displays the number of messages that triggered each type of filter for a given period.
Scanning Conditions	Displays the number of messages that triggered each type of filter and the ratio of these messages compared to the total number of detections.
Messages Processed	Displays the number of incoming and outgoing email traffic.

Sender Filtering Tab

The Sender Filtering tab contains widgets that display all the malicious messages and all the spam blocked by Sender Filtering components.

TABLE 22-3. Sender Filtering Tab Widgets

WIDGET	DESCRIPTION
Sender Filtering Performance	Displays the number of malicious messages and spam blocked by specific Sender Filtering components and the time of blocking.
Sender Filtering Type	Displays the number of malicious messages and spam blocked by specific Sender Filtering components.

Cloud Pre-Filter Tab

The Cloud Pre-Filter tab contains widgets that display Cloud Pre-Filter message traffic and threat detections.

TABLE 22-4. Cloud Pre-Filter Tab Widgets

WIDGET	DESCRIPTION
Cloud Pre-Filter Traffic Summary	Displays the number of messages processed by Cloud Pre-Filter.
Cloud Pre-Filter Violation Types	Displays the number and type of Cloud Pre-Filter message violations.

Adding Tabs

Add tabs to the dashboard to provide a customized information matrix for your IMSS network needs.

Procedure

1. Go to the **Dashboard** screen.
2. Click **New Tab**.

   The **New Tab** screen appears.
3. Specify a meaningful title for the tab in the **Title** field.
4. Select a layout for the tab.

Note

The number of widgets that you can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, you must remove a widget from the tab or create a new tab for the widget.

5. Click **Save**.

   The empty tab appears on the dashboard.

6. Click **Add Widget** to populate the tab with widgets.

Configuring Tab Settings

You can change the default name of a tab using the **Tab Settings** screen.

Procedure

1. Go to the **Dashboard** screen.
2. Click **Tab Settings**.

   The **Tab Settings** screen appears.

3. Specify a meaningful title for the tab in the **Title** field.
4. Click **Save**.

Understanding Widgets

Widgets are the core components for the dashboard. Tabs provide the layout and widgets provide the actual data for the dashboard.

Note

Customizing the dashboard, tabs, or widgets for one user account has no effect on the dashboard, tabs, or widgets for a different user account. Each user account has a completely independent dashboard, tabs, and widgets from every other user account.

In some widgets the total number of messages matching each scanning condition 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.

Using Widgets

Each widget provides targeted security-related information. Widgets can display this information in one of the following ways:

- Bar chart
- Pie chart
- Table

Click the help icon on a widget to view the following types of information:

TABLE 22-5. Widget Help

WIDGET TOPIC	DESCRIPTION
Overview	Provides a description for the widget and how the widget can be used
Widget Data	Detailed information about the data that displays in the widget's table
Configure	Description of settings that are readily visible on the widget
Edit	Description of settings that require clicking the edit icon to modify

Configuring Widgets

Configuring a widget means modifying settings for the widget that are readily visible on the widget. The following table lists some examples of the widget settings administrators can modify.

TABLE 22-6. Configuring Widgets

SETTING	DESCRIPTION
Range	Modify the time range for data that displays: • 1 hour • 6 hours • 12 hours • 24 hours
Data aggregation	Modify the aggregation for the data by specifying all IMSS or a single IMSS.
Display	Modify how the data displays: • Bar chart • Pie chart • Table

Editing Widgets

Editing a widget means modifying settings for the widget that are not readily visible on the widget. Click the edit icon to access these settings. Examples include:

TABLE 22-7. Editing Widgets

SETTING	DESCRIPTION
Title	Modify the name that displays for the widget.

Setting	Description
Others	Some widgets provide settings to modify the amount of data a widget displays (range of entries) or the type of data that displays (security threat type or component type with the product type).

Procedure

1. Go to the **Dashboard** screen.
2. Click the **Edit** icon on the widget. The Edit screen appears.
3. Specify a meaningful title for the widget in the **Title** field.
4. Click **OK**.
5. Specify values for any other settings available on the widget.

   Note

   For more information about "other" settings, check the Help for that specific widget.

6. Click **Save**.

   The widget reloads applying the new settings.

Adding Widgets

The number of widgets that you can add to a tab depends on the layout for the tab. Once the tab contains the maximum number of widgets, you must remove a widget from the tab or create a new tab for the widget.

Procedure

1. Go to any tab on the dashboard.

2. Click **Add Widget**.

   The **Add Widget** screen appears.

3. Click one of the following to filter the widgets that display:

Category	Description
All Widgets	Displays all widgets available
System	Displays only system widgets
Message Traffic	Displays only message traffic widgets
Sender Filtering	Displays only Sender Filtering widgets
Cloud Pre-Filter	Displays only Cloud Pre-Filter widgets

4. Select one or more widgets to add to a tab.

5. Click **Add and Reload**.

Chapter 23

Reports

This chapter provides information on generating one-time and scheduled reports.

Topics include:

- *Generating Reports on page 23-2*
- *Managing One-time Reports on page 23-5*
- *Scheduled Reports on page 23-8*

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 and sending reports to specified recipients through email.

Types of Report Content

You can select from the following types of content to be included in the report:

TABLE 23-1. Cloud Pre-Filter Reports

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

TABLE 23-2. Summary Reports

REPORT CONTENT	DESCRIPTIONS
Policy and traffic summary	Shows the total number and size of incoming and outgoing messages, the number of messages matching specific scanning conditions, and a summary of quarantine events.
Virus and malicious code summary	Shows a summary of the virus message count by actions.
Spam summary	Shows a summary of the total spam message count by antispam engine, Email reputation, IP Profiler, and actions.

Report Content	Descriptions
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 Sender Filtering rules. The latter shows the total sender connections that reached Email reputation and are blocked by Email reputation.
Virtual Analyzer analysis summary	Shows the total number of analyzed advanced threats by risk level. **Note** Virtual Analyzer 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
Time-of-Click Protection summary	Shows the total number of clicks, number of clicks allowed, number of clicks blocked, number of clicks that get users warned and stopped, and number of clicks that get users warned but continued access.

Table 23-3. 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.

Report Content	Descriptions
Top 10 blocked IP addresses for Directory Harvest Attack (DHA)	Top 10 IP addresses ranked by the blocked count for DHA attack.
Top 10 IP addresses ranked by the blocked count for bounced mail attack.	Top 10 IP addresses ranked by the blocked count for bounced mail attack.
Top 10 virus recipients and senders	Top 10 virus recipients and senders ranked by their total received and sent virus message counts.
Top 10 most frequently triggered rules	Top 10 rule names ranked by the number of messages that triggered each rule.
Top 10 spam recipients	Top 10 spam recipient addresses ranked by their total received spam message count.
Top 10 blocked IP addresses by Email reputation	Top 10 blocked IP addresses ranked by the number of connections dropped by Email reputation.
Top 10 blocked IP addresses for spam	Top 10 IP addresses ranked by the blocked count for spam.
Top 10 blocked IP addresses for viruses or malicious code	Top 10 IP addresses ranked by the blocked count for viruses.
Top 10 senders of messages with suspicious URLs	Top 10 sender addresses ranked by their total received messages that contained suspicious URLs.
Top 10 Trend Micro Email Encryption recipients and senders	Top 10 recipients and senders ranked by email encryption violations.
Top 10 compliance recipients and senders	Top 10 recipients and senders ranked by regulatory compliance violations.
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
Top 10 marketing graymail recipients and senders	Top 10 recipients and senders of marketing newsletter email messages

Report Content	Descriptions
Top 10 social network graymail recipients and senders	Top 10 recipients and senders of social networking update email messages

Note

If there is any report record showing the sender "unknown@unknown", ignore it since this is the bounced mail for an undeliverable message.

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**.
- To send a report through email, select the check box next to it and click **Email**.

Note

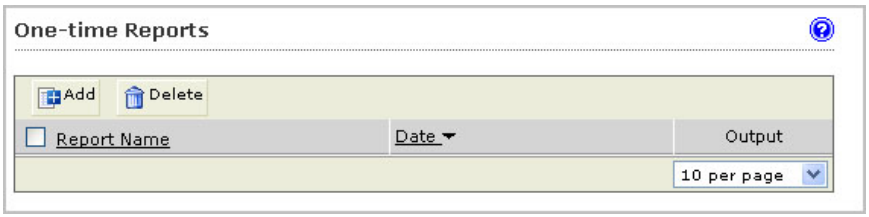
ERS and IP Profiler report content is not available unless you activate those products. For more information on activating ERS and IP Profiler, see *Managing Product Licenses on page 29-20*.

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**.

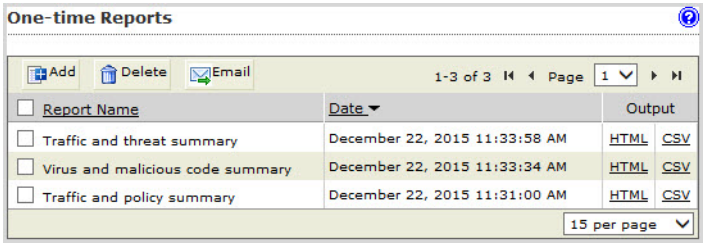
The **Add One-time Report** screen appears. For a list of available reports, see *Generating Reports on page 23-2*.

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.
Delivery Settings	Select to enable the delivery settings for the report.
Sender	Specify the sender email address of the report.
Recipient(s)	Specify the recipients who will receive 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.

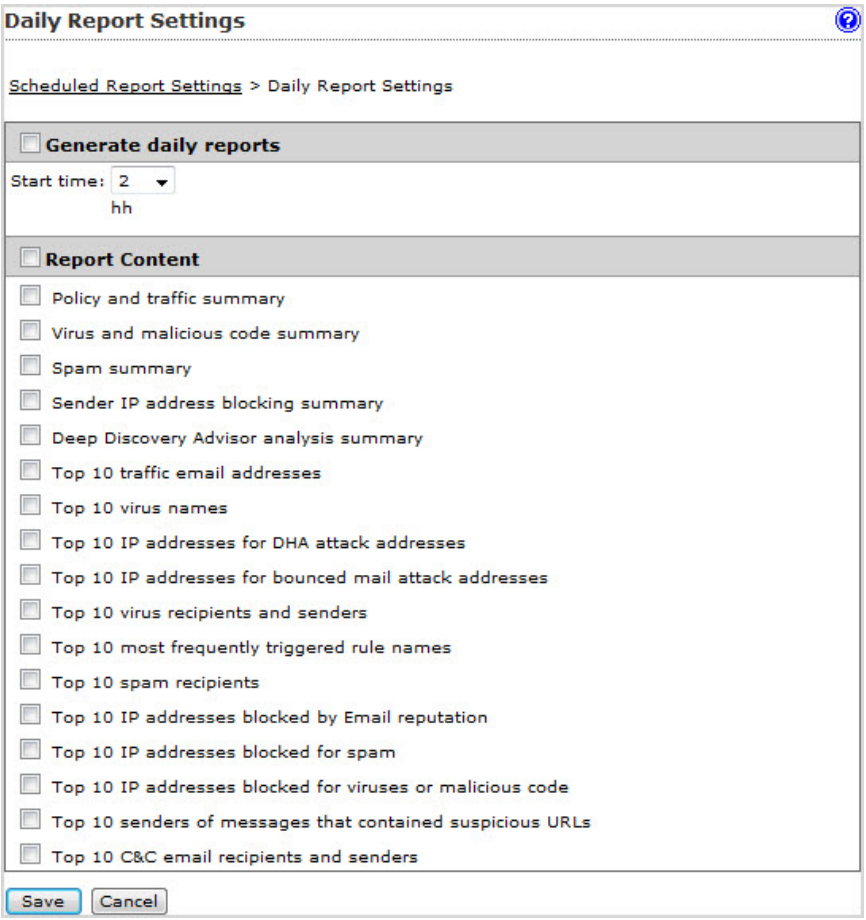
Procedure

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**).



3. Configure the report settings.

   For report options, see *Generating Reports on page 23-2*.

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.

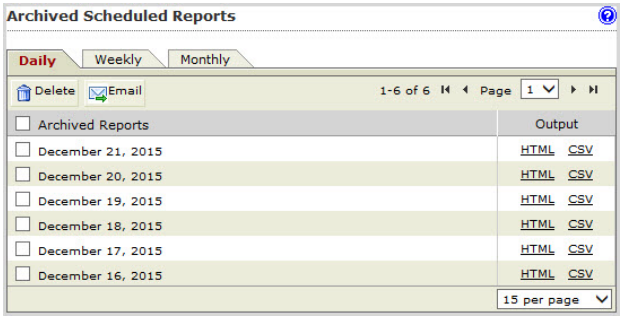
8. After the report generates, see *Accessing Scheduled Reports on page 23-11* for available report options.

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 23-11*.

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**.
- To send a report through email, select the check box next to it and click **Email**.

Chapter 24

Logs

This chapter provides you with general instructions on configuring and querying logs.

Topics include:

- *About Logs on page 24-2*
- *Configuring Log Settings on page 24-2*
- *Querying Logs on page 24-6*

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 24-2*
- **Step 2**: *Querying Logs on page 24-6*

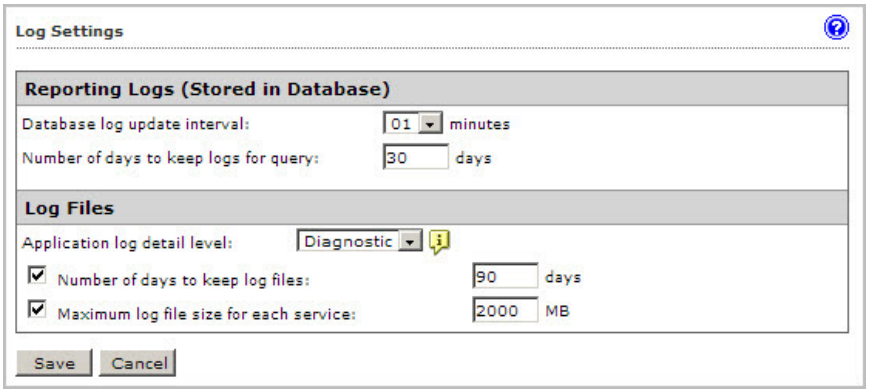
Configuring Log Settings

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 `/opt/trend/imss/log` by default.

  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**.

Configuring Syslog Settings

To provide enterprise-class logging capabilities, IMSS supports sending logs through the syslog protocol to multiple external syslog servers in a structured format. You can send different event log types to multiple syslog servers. On the IMSS management console, you can add, delete, import and export syslog servers.

The following steps describe how to add a syslog server.

Procedure

1. Go to **Logs** > **Syslog Settings**.
2. Click **Add**.

   The **Add Syslog Server** screen appears.
3. In the **Syslog Server Setting** section, select a facility level.

Note

The facility level specifies the source of a message. This lets the configuration file specify that messages from different facilities will be handled differently.

4. In the **Syslog Type** section, select syslog types from the following:

   - **Message tracking**
   - **Policy events**
   - **System events**

     Note

     If you select **System events**, audit logs for the operating system and IMSS are already included.

     Make sure you do not select **local6** if you have selected **System events**.

   - **MTA events**
   - **Sender filtering**
   - **Content scanning**
   - **Administration**

5. In the **Syslog Server** section, specify the IP address, port number and supported protocol of the syslog server and click **Add Syslog Server**.

   The new syslog server appears in the syslog server list within the **Syslog Server** section.

   Note

   You can continue to add more servers, edit the existing servers, and delete servers from the syslog server list.

6. Click **Save**.

The details about each facility level such as the syslog type and server are shown on the **Syslog Settings** screen.

A green check mark appears for each facility level, indicating that the associated syslog server has been enabled. To disable a facility level, click the green check mark.

Querying Logs

You can perform queries on the following types of events or information:

Message tracking
Records message details such as the sender, recipient(s), message size, attachment(s), and the final action that IMSS has taken. The query result also indicates the name and type of the policy rule that was triggered.

System events
Provides details on system events such as scan engine and pattern file updates, scanner service status changes, administrator operations, and errors that IMSS encountered.

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

URL click tracking
Provides details on URL clicks such as the message sender, recipient(s), URL, message ID, and whether the URL is blocked, warned or clicked through.

Quarantine events
Provides details on quarantine events, for example, the percentage of release events in all the quarantine events.

MTA events
Provides connection details of Postfix on the local computer where the central controller is installed.

Sender filtering

Provides the time when IMSS started and stopped blocking messages from the queried IP address or sender 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).

Log Query Behavior

With the inclusion of Cloud Pre-Filter to IMSS, changes in the way that users can query logs have been introduced.

Message Tracking Enhancement

IMSS splits **Message tracking** logs in to:

- **IMSS data only**: These message tracking logs only contain data from IMSS.

  The available query conditions are **Subject**, **Message ID**, **Sender**, **Recipient**, and **Attachment(s)**, and all query conditions can be left blank.

- **Cloud Pre-Filter + IMSS data**: These message tracking logs contain data from the Cloud Pre-Filter and IMSS.

  The available query conditions are **Sender** and **Recipient**, and **Recipient** is mandatory.

IMSS includes hyperlinks for quarantined, archived, and postponed messages in **Message tracking** logs. This provides detailed information about those messages.

Query Behavior

IMSS provides the following log query behavior:

TABLE 24-1. General Query Information

QUERY	IMSS ONLY	IMSS + CLOUD PRE-FILTER
a@a.com	Only the exact match is returned. Result: a@a.com	Displays all messages sent to any variant of "a@a.com", including those with multiple recipients. Result: • za@a.com • a@a.com.us • a@a.com; b@a.com • b@a.com; a@a.com • b@a.com; a@a.com; c@a.com
* in Subject field All other query conditions left blank	Returns **all** messages	Returns approximately **10000** query results
* in Message ID field All other query conditions left blank	Returns **all** messages	Returns approximately **10000** query results

TABLE 24-2. "Sender" Query Information

QUERY	IMSS ONLY	IMSS + CLOUD PRE-FILTER
5!#?	Valid **Sender** value in IMSS, though no results will be returned.	Not supported. User must provide a properly formatted, complete or partial email address.
*test@example.com	Valid **Sender** value in IMSS. Returns: All variations ending with test@example.com	Not supported. The wildcard "*" is not supported in the **Sender** field.

QUERY	IMSS ONLY	IMSS + CLOUD PRE-FILTER
test@example.com	Valid **Sender** value in IMSS. Returns: Only messages sent from test@example.com	Valid **Sender** value in IMSS. Returns: Only messages sent from test@example.com

TABLE 24-3. "Recipient" Query Information

QUERY	IMSS ONLY	IMSS + CLOUD PRE-FILTER
test@example.com	Valid **Recipient** value in IMSS. Returns: Only messages sent to test@example.com	Valid **Recipient** value in IMSS. Returns: Approximately 10000 results sent to all variations of test@example.com (the same as using "*test@example.com*" in IMSS Only data)
*test@example.com	Valid **Recipient** value in IMSS. Returns: All variations ending with test@example.com	Not supported. The wildcard "*" is not supported in the **Recipient** field.
test@example.com*	Valid **Recipient** value in IMSS. Returns: All variations starting with "test@example.com"	Not supported. The wildcard "*" is not supported in the **Recipient** field.

QUERY	IMSS ONLY	IMSS + CLOUD PRE-FILTER
test@example.com	Valid **Recipient** value in IMSS. Returns: All variations of test@example.com	Not supported. The wildcard "*" is not supported in the **Recipient** field. **Tip** Use test@example.com instead.
test@example.com; test2@example.com	Valid **Recipient** value in IMSS. Result: Combined result of querying test@example.com and test2@example.com.	Not supported **Tip** Use "test@example.com" or "test2@example.com"
%^$&^	Valid **Recipient** value in IMSS, though no results will be returned.	Not supported. User must provide a properly formatted, complete or partial email address.

Note

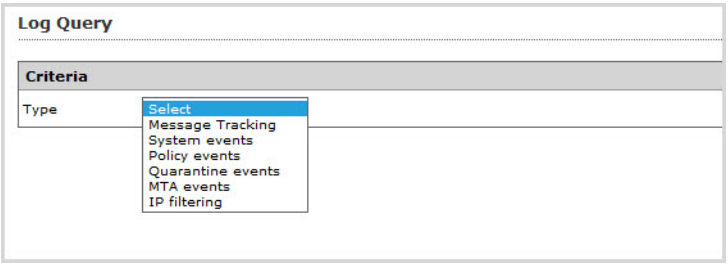
The data `<server name>[127.0.0.1]`, from returned queries, indicates the default DNS server.

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)**
   - **Attachment(s)**

   Note

   Use the asterisk wildcard for partial searches on any field.

5. Click **Display Log**.

   A timestamp, sender, recipient, subject, and last known action appear for each event.

6. Click the timestamp link to see the following information:

   - **Timestamp**

- **Sender**
- **Recipient**
- **Subject**
- **Original size**
- **Attachments**
- **Message ID**
- **Internal ID**
- **Scanner**
- **Final action**
- **Action details**

7. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma-separated value file, click **Export to CSV**.

Querying System Event Logs

Procedure

1. Go to **Logs** > **Query**.
2. Next to **Type**, select **System events**.

   The query screen for system event logs appears.
3. In the second drop-down box next to **Type**, select one of the following:

- **All events**: Displays the timestamp and descriptions for all system events.
- **Updates**: Displays the timestamp of all scan engines and pattern file updates from the ActiveUpdate server to the IMSS admin database.
- **Service status**: Displays the timestamp and descriptions when the scanner service is started or stopped.
- **Audit log**: Displays the timestamp and descriptions for operations performed by specified administrator accounts.

Note

As an enhanced log category of system events, **Audit log** replaces **Admin activity** on the IMSS management console. Audit logs record various administrator operations and provide a way to query activities of specified administrator accounts.

- **Errors**: Displays the timestamp and descriptions for all errors that IMSS encountered.

4. In the third drop-down box next to **Type**, select the server to view.
5. Next to **Dates**, select a date and time range.
6. If you select **Audit log**, specify any administrator account whose configuration changes you want to search for next to **Admin accounts**.

Note

Use semicolons to separate multiple administrator accounts.

7. Next to **Description keywords**, specify any keywords to search for.
8. Click **Display Log**.

   A timestamp, host name, and description appear for each event. If you select **Audit log**, administrator information also appears for each event.

9. Perform any of the additional actions:

- To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
- To sort the table, click the column title.
- To print the query results, click **Print current page**.
- To save the query result to a comma-separated value file, click **Export to CSV**.

Querying Policy Event Logs

Procedure

1. Go to **Logs** > **Query**.
2. Next to **Type**, select **Policy events**.

   The query screen for policy event logs appears.
3. In the second drop-down box next to **Type**, select one of the following items related to the policy and the rules you configured for the policy:
   - **All**
   - **Virus or malicious code**
   - **Advanced persistent threat**
   - **Spyware/grayware**
   - **C&C email**
   - **Spam/phish**
   - **Graymail**
   - **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**
- **Attachment**
- **Size**
- **Content**
- **Compliance**
- **Scanning exceptions**
- **Spam Tagged by Cloud Pre-Filter**
- **Suspicious Objects**
- **Others**

4. Specify any of the following additional information:
   - **Sender**
   - **Recipient(s)**
   - **Rule**
   - **Subject**
   - **Attachment(s)**
   - **Message ID**

   If you leave any text box blank, all results for that item appear.
5. Click **Display Log**. A timestamp, action, rule, and message ID appear for each event.
6. Click the timestamp link to see the following information:

- **Timestamp**
- **Sender**
- **Recipient**
- **Subject**
- **Original size**
- **Violating attachments**
- **Rule type**
- **Rule(s)**
- **Action**
- **Message ID**
- **Internal ID**
- **Reason**
- **Scanner**

7. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
   - To sort the table, click the column title.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma-separated value file, click **Export to CSV**.

Note

- "*A*;*B*" means a string that has A or B.
- "A*;*B" means a string that starts with A or ends with B.
- ";" represents the OR operation.

Querying Quarantine Event Logs

Procedure

1. Go to **Logs** > **Query**.
2. Next to **Type**, select **Quarantine events**.

   The query screen for quarantine event logs appears.
3. Next to **Dates**, select a date and time range.
4. Next to **Rule(s)**, specify any rule name keywords to search for.
5. Click **Display Log**.

   A rule name, quarantine event count, release event count, and release percentage appear for each rule.
6. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
   - To sort the table, click the column title.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma-separated value file, click **Export to CSV**.

Querying URL Click Tracking Logs

Procedure

1. Go to **Logs** > **Query**.
2. Next to **Type**, select **URL click tracking**.

   The query screen for URL click tracking logs appears.
3. Next to **Dates**, select a date and time range.
4. Next to **URL**, specify any URL to search for.
5. Specify any of the following additional information:
   - **Sender**
   - **Recipient(s)**
   - **Message ID**

Note

Each URL click tracking log consists of email message information and URL click information. Email message information, including **Sender**, **Recipient(s)** and **Message ID**, is generated by IMSS, and URL click information, including **Timestamp**, **URL**, **Blocked**, **Warned** and **Clicked Through**, is obtained from the Time-of-Click Protection service. IMSS combines information from the two sources before providing logs for query.

If you find email message related fields shown as not available in query results, the possible reasons are as follows:

- IMSS stores email message information only for a certain period of time, which can be configured in log settings. If a user queries logs whose email message information is outdated but URL click information does not expire without specifying any field, those logs will be shown in query results, but the email message related fields will be regarded as not available. However, if a user queries such logs by specifying any of the email message related fields, those logs will not shown because IMSS cannot match the specified field values.
- Each IMSS server has its own email message information for logs, while URL click tracking logs are generated by Activation Codes. If multiple IMSS servers share one Activation Code, an IMSS server might hold logs whose email message information belongs to other IMSS servers. When a user queries logs on that server, the situation is similar to that described for outdated email message information.

6. Click **Display Log**.

   A click timestamp, message sender, recipient, URL, message ID, and whether the URL is blocked, warned or clicked through appear for each record.

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**.

Querying MTA Event Logs

Procedure

1. Go to **Logs** > **Query**.
2. Next to **Type**, select **MTA events**.

   The query screen for MTA event logs appears.
3. Next to **Dates**, select a date and time range.
4. Click **Display Log**.

   A timestamp and description appear for each event.
5. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the **Results per page** drop-down box on the top of the table.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma-separated value file, click **Export to CSV**.

Querying Sender Filtering Logs

Procedure

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

2. Next to **Type**, select **Sender filtering**.
3. In the second drop-down box next to **Type**, select one of the following items related to Sender Filtering:
   - **All**
   - **ERS**
   - **DHA attack**
   - **Bounced mail**
   - **Virus**
   - **Spam**
   - **Manual**: Refers to the IP addresses that you have specified in the blocked list.
4. Next to **Dates**, select a date and time range.
5. Next to **IP**, provide any IP address to search.
6. Click **Display Log**. Information appears for the time that IMSS both started and stopped blocking each IP address or domain.
7. Perform any of the additional actions:
   - To change the number of items that appears in the list at a time, select a new display value from the drop-down box on the top of the table.
   - To print the query results, click **Print current page**.
   - To save the query result to a comma-separated value file, click **Export to CSV**.

Chapter 25

Mail Areas and Queues

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

Topics include:

- *About Mail Areas and Queues on page 25-2*
- *Configuring Quarantine and Archive Settings on page 25-2*
- *Managing Quarantine Areas on page 25-4*
- *Managing Archive Areas on page 25-6*
- *Querying Messages on page 25-9*
- *Viewing Quarantined Messages on page 25-15*
- *Viewing Archived Messages on page 25-17*
- *Viewing Postponed Messages on page 25-18*
- *Viewing Messages in the Virtual Analyzer Queue on page 25-19*

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.
- **Postponed Queue**: Stores messages that will be delivered at a specified time.
- **Virtual Analyzer Queue**: Stores messages that IMSS submits to Virtual Analyzer before IMSS receives message analysis results.

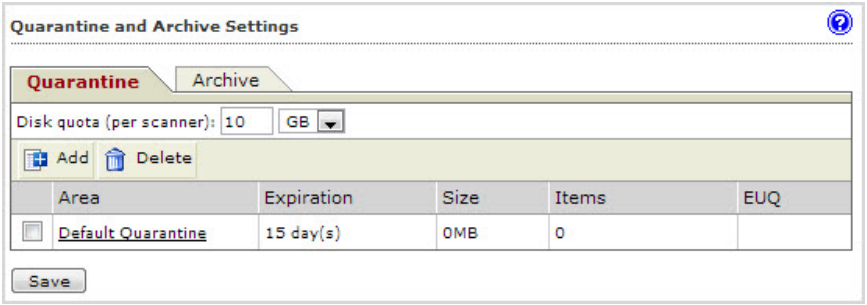
Configuring Quarantine and Archive Settings

Quarantine and archive settings allow you to manage quarantine and archive areas and allocate the amount of disk space per scanner for storing quarantined or archived messages.

Procedure

1. Go to **Quarantine & Archive** > **Settings**.

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



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.

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 messages that do not violate virus, phishing, Web Reputation, advanced threat, and social engineering attack rules or violate virtual analyzer scanning exceptions, to the EUQ database (for this area only)** to automatically save messages to the EUQ database.

Note

After selecting **Synchronize all messages that do not violate virus, phishing, Web Reputation, advanced threat, and social engineering attack rules or violate virtual analyzer scanning exceptions, 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 Query** 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 **Quarantine and Archive Settings** screen.
8. Click **Save**.

Managing Archive Areas

IMSS can archive messages on the server in the following directory:

```
$IMSS_HOME/queue/archive
```

Managing the Archive from the Actions Screen of a Policy Rule

If you are configuring the actions for a rule, do the following:

Procedure

1. Click **Edit** next to **Archive modified to** under **Monitor** actions.

   The **Archives** screen appears showing the available quarantine areas.

2. Do one of the following:

   - To add a new archive area, click **Add**.
   - To modify an existing archive area, click the area name and then click **Edit**.

   An edit screen appears.

3. Next to **Name**, specify the name of the archive area.

4. To automatically delete archived messages after a certain number of days, next to **Delete messages older than**, specify the number of days from 1 to 60.

   This number represents the number of days after which IMSS deletes the archived messages. The value is exclusive. For example, if you specify 15, IMSS deletes the archived messages on the 16th day.

5. Click **Save** to return to the **Archives** screen.

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

7. To archive messages, select the radio button next to **Archive modified to** under **Monitor** and select the desired archive area from the drop-down box.

Managing the Archive Settings

Procedure

1. Go to **Quarantine & Archive** > **Settings**.

   The **Quarantine and Archive Settings** screen appears with the **Quarantine** tab displayed by default.

2. Click the **Archive** tab.

3. Next to **Disk quota per scanner service**, do the following:

   a. Specify the maximum size for the area.

   b. Select **MB** or **GB**.

   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. Click **Save** to return to the **Quarantine and Archive Settings** screen.
8. Click **Save**.

Querying Messages

You can perform a query on quarantined and archived messages before deciding which action to perform. After viewing the message details, you can choose to release or delete archived messages from IMSS.

Tip

Trend Micro recommends quarantining items that could pose a risk to your network, such as messages and attachments that violate antivirus rules. Before you resend any quarantined message, make sure that it does not pose a threat to your network.

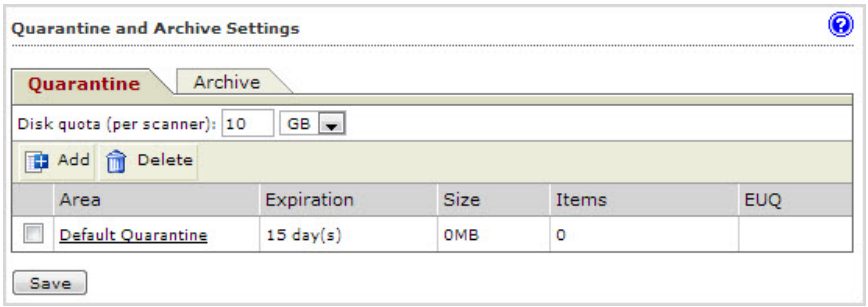
Trend Micro recommends archiving only items that you want to reference later.

Querying the Quarantine Areas

Procedure

1. Go to **Quarantine & Archive** > **Query**.

   The **Quarantine and Archive Query** screen appears. The **Quarantine** tab displays by default. If it does not display, click **Quarantine**.



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 violating 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 violating attachment names if you have specified **Attachment** as a scanning condition. However, if the number of attachments in the message exceeds the maximum number specified in condition, the attachment name will not be shown.

Querying the Archive Areas

Procedure

1. Go to **Quarantine & Archive** > **Query**.

   The **Quarantine** tab displays by default.

2. Click the **Archive** tab.

3. Under **Criteria**, configure the following:

- **Search**: Select the archive area, the reason the message was archived, and the scanner that scans the message.
- **Dates**: Select a time range.

4. Specify values for the following:
   - **Sender**
   - **Subject**
   - **Recipient(s)**
   - **Attachment(s)**
   - **Rule**
   - **Message ID**

Note

When querying a message containing multiple recipients or violating 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 violating 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 Postponed Messages

Procedure

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

   The **Quarantine** tab displays by default.

2. Click the **Postpone** tab.

3. Under **Criteria**, configure the following:

   - **Search**: Select the reason and device.
   - **Dates**: Select a date and time range.

4. Specify values for the following:

   - **Sender**
   - **Subject**
   - **Recipient(s)**
   - **Violating Attachment(s)**
   - **Rule**

- **Internal ID**

5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject, and reason for postponing 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 postponed message, click the **Timestamp** for the item. The message and all of its details appear.
8. To resend any message, click the check box next to it in the query result table, and then click **Release**.
9. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

Querying Messages in the Virtual Analyzer Queue

Procedure

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

   The **Quarantine** tab displays by default.
2. Click the **Virtual Analyzer** tab.
3. Under **Criteria**, configure the following:
   - **Search**: Select the device.

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

4. Specify values for the following:
   - **Sender**
   - **Recipient(s)**
   - **Subject**
5. Click **Display Log**.

   The results appear at the bottom of the screen.
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 message in the Virtual Analyzer queue, click the **Timestamp** for the item. The message and all of its details appear.
8. To release a message from Virtual Analyzer scanning, click the check box next to it in the query result table, and then click **Release**.

Note

Trend Micro does not recommend releasing suspicious messages from Virtual Analyzer scanning. Doing so could put your network at risk.

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 an 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 recommends not 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 an 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 Postponed Messages

All messages that IMSS postpones can be queried and viewed.

Procedure

1. After you perform a query for postponed messages, click the timestamp for an item in the query result table. The query screen appears showing the following information:
   - **Timestamp**
   - **Sender**
   - **Reason**
   - **Recipient**
   - **Rules**
   - **Subject**
   - **Scanner**
   - **Original Size**
   - **Message ID**
   - **Internal ID**

- **Attachments**

If ATSE is enabled, IMSS also displays the following information:

- **Reason**: **Probable advanced threat**

If both ATSE and Virtual Analyzer are enabled, IMSS also displays the following information:

- **Reason**: **Probable advanced threat** or **Analyzed advanced threat**
- **Virtual Analyzer Status**: Status of Virtual Analyzer analysis

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.
   - **Release**: Resend the message to its original recipients.
   - **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 Messages in the Virtual Analyzer Queue

Email messages IMSS submits to Virtual Analyzer are stored in the Virtual Analyzer queue while pending analysis or being analyzed. All messages in the Virtual Analyzer queue can be queried and viewed.

Note

Once IMSS receives the analysis result for an email message, this message will be removed from the Virtual Analyzer queue.

Procedure

1. After you perform a query for messages in the Virtual Analyzer queue, click the timestamp for an item in the query result table. The query screen appears showing the following information:
   - **Timestamp**
   - **Message ID**
   - **Sender**
   - **Recipient**
   - **Rules**
   - **Attachments**
   - **Subject**
   - **Scanner**
   - **Original Size**
   - **Internal ID**
   - **Submission**
   - **Query Time**
   - **Attempts**
   - **Expiration**
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.
   - **Release**: Release the message from Virtual Analyzer scanning. IMSS may continue to scan the message if any other scanning condition is met.

Chapter 26

Notifications

This chapter provides you with general instructions on notifications in IMSS.

Topics include:

- *Event Notifications on page 26-2*
- *Configuring Delivery Settings on page 26-2*
- *Configuring Event Criteria and Notification Message on page 26-5*
- *EUQ Digest on page 26-8*
- *Configuring a Logon Notice on page 26-11*
- *Editing Notifications on page 26-12*

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 26-1. 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.
Scanner Update Result	Alerts you when IMSS is unable to update the engine or pattern files on any scanner.
Virtual Analyzer Settings	Alerts you when Virtual Analyzer analysis is incomplete or invalid.
Smart Protection Event	Alerts you when IMSS reverts to Conventional Scan or is unable to use smart protection services or local sources.

Configuring Delivery Settings

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

Note

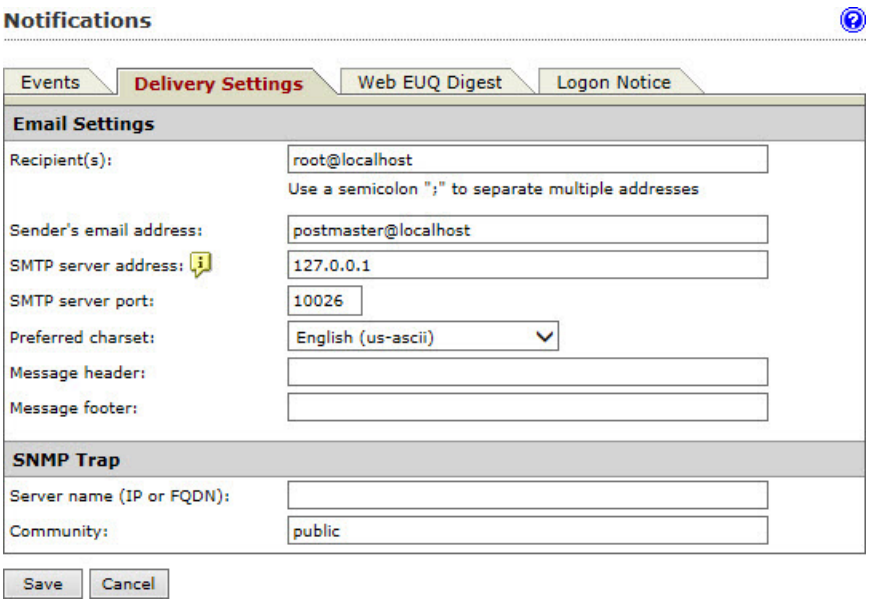
IMSS 9.1 Patch 1 supports sending notifications to IPv6 servers.

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:

   - **Recipient(s)**: Specify the recipient email addresses.
   - **Sender's email address**: Specify the email address to appear as the sender.
   - **SMTP server address**: Specify the Fully Qualified Domain Name (FQDN) or the IP address of the SMTP server that delivers email on the network.
   - **SMTP server port**: Specify the port number that IMSS uses to connect to the SMTP server.

- **Preferred charset**: IMSS will use this setting to encode the notification messages.
- **Message header**: Specify the text to appear at the top of the notification.
- **Message footer**: Specify the text to appear at the bottom of the notification.

4. Under **SNMP Trap**, configure the following:
   - Server name
   - Community
   - SNMP version

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.
SNMP version	Select either of the following: • **SNMPv1** • **SNMPv2c** For more information, refer to the SNMP documentation.

5. Click **Save**.

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

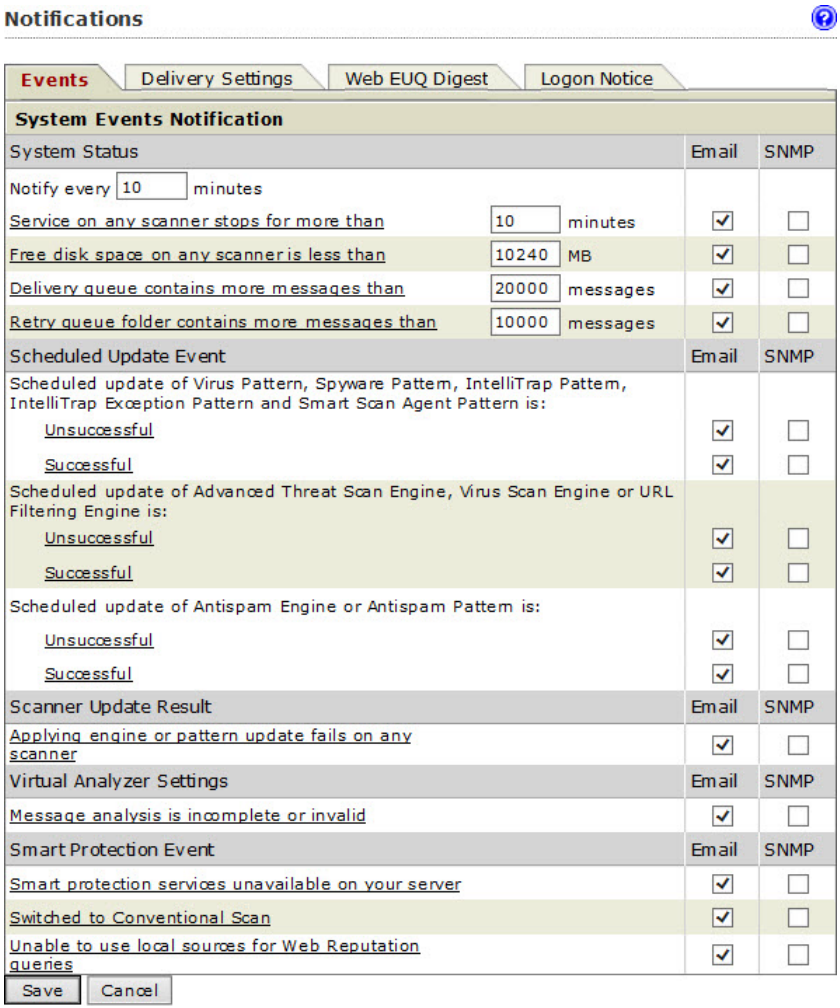
Configuring Event Criteria and Notification Message

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

Note

The notifications **Delivery queue contains more messages than** and **Retry queue folder contains more messages than** only function when IMSS runs with Postfix.

3. Under **Scheduled Update Event**, click the **Unsuccessful** and **Successful** links to edit notifications for component updates.

   Scheduled Update Event is the event in which the latest engine and pattern files from the Update Source are updated onto the IMSS admin database.

4. Under **Scanner Update Results**, click the **Applying engine or pattern update fails on any scanner** link to edit the notification.

   Scanner Update Results are the results of updating the latest engine and pattern files from the IMSS admin database onto the scanners.

5. Under **Virtual Analyzer Settings**, click the **Message analysis is incomplete or invalid** link to edit the notification.

   This notification describes the breakdown in communication between IMSS and Virtual Analyzer. 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 Protection Event**, click the following links to edit notifications:
   - **Smart protection services unavailable on your server**
   - **Switched to Conventional Scan**
   - **Unable to use local sources for Web Reputation queries**
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
- **Inline action links**: Links that users can click to apply actions to quarantined messages and to add senders to the **Approved Senders** list

Note

Inline action links display only if you enable this feature.

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 to send EUQ digests every day from the drop-down boxes.
   - **Weekly**: Select the day and time to send EUQ digests every week 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. Select **Enable inline action** to allow users to apply actions from the EUQ digest.
7. Click **Save**.

Inline Action Links

IMSS enables users to apply actions to quarantined messages through links in the EUQ digest. Users can select any of the following actions by clicking the corresponding link.

- Delete: Deletes the message and all attachments.
- Release: Releases the message from quarantine. IMSS may scan the message again or deliver it to the original recipients.

Note

If you enabled the **Control the 'auto-add' approved Sender behavior when end user reprocess a message** feature, IMSS automatically adds senders of released messages to the **Approved Senders** list.

- Add sender to Approved list: Prevents IMSS from identifying messages from this sender as spam.

IMSS automatically deletes messages after a period that you specify. You can also manually delete and release messages from the IMSS management console. Users cannot select actions for messages that have been deleted or released.

Important

Trend Micro does not recommend forwarding notifications. Inline action links remain active in forwarded messages.

Configuring a Logon Notice

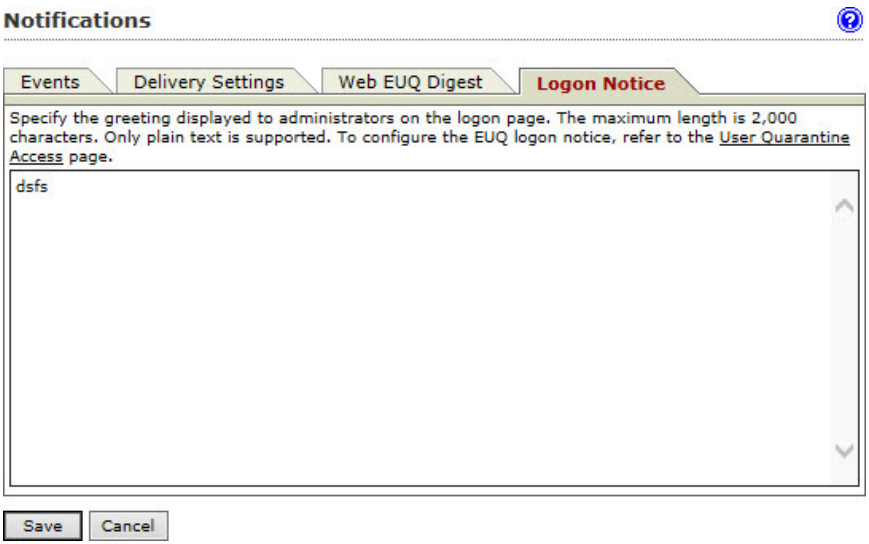
A logon notice is a customizable message displayed to administrators on the logon page.

Procedure

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

   The **Events** tab displays by default.

2. Click **Logon Notice**.



3. Specify a logon notice that will be displayed to administrators.
4. Click **Save**.

Editing Notifications

Procedure

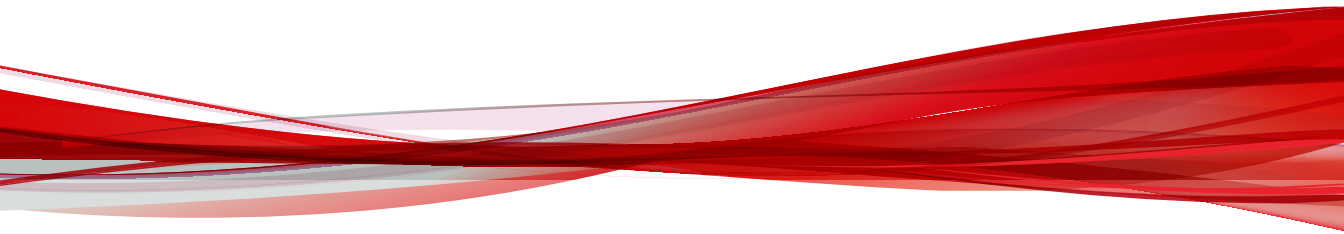
1. Go to **Administration** > **Notifications**.
2. Click the notification to edit.

   The edit screen for that notification appears.
3. Specify the subject and message, or SNMP message.

   To see a list of variables to include in the notification, click **Variables list**.
4. Click **Save**.

Part V

Administering IMSS



Chapter 27

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 27-2*
- *Backing Up IMSS on page 27-4*
- *Restoring IMSS on page 27-6*
- *Replicating Settings on page 27-7*
- *Exporting Debugging Files on page 27-9*

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 9.1 Patch 1 server . You can also replicate a configuration across several IMSS 9.1 Patch 1 servers by importing the same configuration file into the desired servers.

Important

Only the following configurations are compatible with IMSS Linux 9.1 Patch 1. Other configurations are not supported.

- IMSS Linux 7.1 Service Pack 2 Patch 1
- IMSS Linux 9.1

Note

IMSS 9.1 Patch 1 recognizes addresses imported in IPv6 format, and can export addresses in IPv6 format. However, you must manually import or export `imss.ini` settings.

Exporting Configuration Files

During export, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any IMSS services.
- Register/unregister any EUQ database to/from IMSS.
- Start other export or import tasks.

Procedure

1. Go to **Administration** > **Import/Export**.

2. Click **Export**.
3. When the dialog box appears, click **Save** and save it to your computer.
4. To return to the **Import/Export** screen, click **Return**.

Importing Configuration Files

During import, do not:

- Access other management console screens or modify any settings.
- Perform any database operations.
- Start/stop any IMSS services.
- Register/unregister any EUQ database to/from IMSS.
- Start other export or import tasks.

Procedure

1. Log on to the IMSS management console.
2. Click **System Status**.
3. Verify that no services are starting or stopping. If services are starting or stopping, wait until the operation has completed.
4. Go to **Administration** > **Import/Export**.
5. Under **Import Configuration Files**, click **Browse...** and locate the file.

Note

When importing IMSS Linux configurations, the imported configuration file must be from an IMSS Linux build number that is equal to or older than the current build number.

6. 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.

Note

The End-User Quarantine feature is disabled after migration or upgrade. To use this feature, manually enable it after importing configuration files. For details, see *Enabling EUQ on page 28-3*.

Backing Up IMSS

After you have installed IMSS and configured the required settings, it is always prudent to create backups of the settings so that you can restore IMSS quickly in the event of a system failure.

You can choose to perform a full or minimal backup of IMSS as follows:

- **Full**: Backs up all IMSS local configuration and binary files stored in `/opt/trend` and database-related files in `/var/imss`.
- **Minimal**: Backs up only IMSS configuration settings stored in `/opt/trend/imss/config`.

Note

1. 1. The backup and restore instructions in this manual are targeted at the all-in-one deployment of IMSS. In the case of distributed deployment, you need to back up the following:
    a. The database files or tables on the computer(s) where you installed the databases.
    b. The local binary and configuration files on every computer where you installed IMSS components.
2. If you perform a minimal backup, you may need to install previous hot fixes, patches, or service packs after restoring IMSS.

Performing a Full Backup

Procedure

1. Stop all IMSS-related processes:

   `/opt/trend/imss/script/imssstop.sh stop`

2. Stop Postfix.
3. Back up the folder `/opt/trend/ and /var/imss/`.
4. Back up all Postfix configuration files under `/etc/postfix`.

   For example, `main.cf`, `master.cf`, `allowAccessList`, `denyAccessList`.

5. Start Postfix.
6. Start all IMSS-related processes:

   `/opt/trend/imss/script/imssstart.sh`

Performing a Minimal Backup

Procedure

1. Stop all IMSS-related processes.

   For details, see *Performing a Full Backup on page 27-5*.

2. Stop Postfix.
3. Back up the `/opt/trend/imss/config` folder.
4. Back up the folder `/ect/postfix`.
5. Back up all database tables.
6. Start Postfix.
7. Start all IMSS-related processes.

For details, see *Performing a Full Backup on page 27-5*.

Restoring IMSS

In the event of a system failure, you can restore IMSS depending on whether you have performed a full or minimal backup previously.

Performing a Full Restoration

Procedure

1. Install a new IMSS server on one computer, ensuring that the IP address, database user name, and password are the same as the original.
2. Stop all IMSS-related processes. For details, see *Performing a Full Backup on page 27-5*.
3. Stop Postfix.
4. Restore the folders `/var/imss/` and `/opt/trend/` using the previous backup.
5. Restore Postfix configuration files.
6. Start Postfix.
7. Start all IMSS-related processes. For details, see *Performing a Full Backup on page 27-5*.

Performing a Minimal Restoration

Procedure

1. Install a new IMSS server on one computer, ensuring that the IP address, database user name, and password are the same as the original.

2. Stop all IMSS-related processes. For details, see *Performing a Full Backup on page 27-5*.
3. Stop Postfix.
4. Restore the `/opt/trend/imss/config/` folder using the previous backup.
5. Restore Postfix configuration files.
6. Import the previous database table backup into the new database.
7. Start all IMSS-related processes. For details, see *Performing a Full Backup on page 27-5*.

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.
- **Step 2**: Enable the MCP agent.
- **Step 3**: Replicate settings from the Control Manager management console.

Enabling MCP 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.

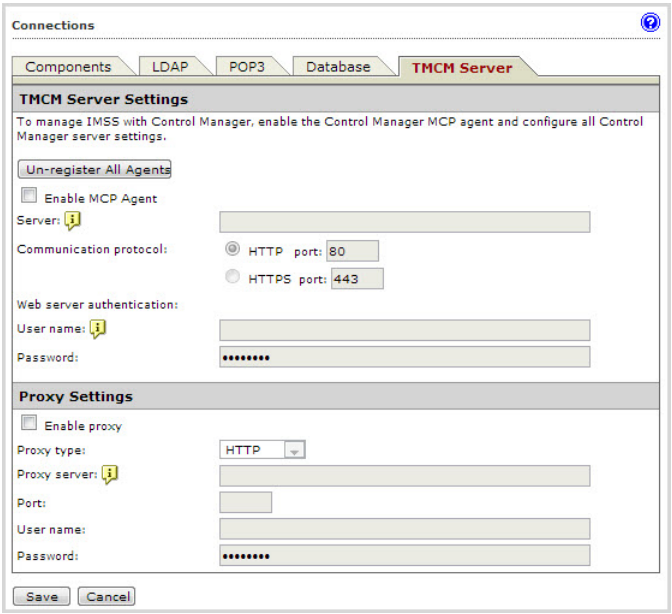
Procedure

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.

Exporting Debugging Files

If you need to analyze the debug files for troubleshooting purposes, you can export debug logs for up to the past two days for the parent device or any device that is registered to the parent device.

Note

The debug logs are contained in a password protected zip file. The default password for the file is `trend`.

Procedure

1. Go to **Administration** > **Import/Export**.
2. Click the **Export Debugging Files** tab.
3. Next to **Scanner**, select a device.
4. Select the number of days to export.
5. Click **Export**.

   The process might take 10 minutes to 1 hour or more depending on the total log file size.

Note

If you want to change the debug log path in the `imss.ini` file, make sure you also add the new log path to the `ExInterface_IMSS.ini` file in `/opt/sharon/imss/cdt/ExInterface`. Therefore, IMSS can collect debug logs from the new path.

Chapter 28

End-User Quarantine

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

Topics include:

- *About EUQ on page 28-2*
- *EUQ Authentication on page 28-2*
- *Configuring End-User Quarantine (EUQ) on page 28-2*
- *Distribution List EUQ Management on page 28-14*
- *Disabling EUQ on page 28-16*
- *Managing EUQ Databases on page 28-17*

About EUQ

IMSS provides web-based EUQ to improve spam management. The web-based EUQ service allows end users to manage the spam quarantine of their personal accounts. Messages that are determined to be spam are quarantined. These messages are indexed into a database by the EUQ agent and are then available for end users to review, delete, or approve for delivery.

You can specify the period to keep messages in the quarantine. IMSS automatically deletes messages that are not released from quarantine. Deleted messages cannot be recovered.

EUQ Authentication

Enabling EUQ requires one of the following authentication methods:

- **LDAP authentication**: Before enabling EUQ, configure LDAP settings using any of the following ways:
  - Go to **Administration** > **IMSS Configuration** > **Connections**, then click the **LDAP** tab.
  - Go to **Administration** > **IMSS Configuration** > **Configuration Wizard**. For details, see *Configuring LDAP Settings on page 3-6*.
- **SMTP authentication**: Specify recipient domains and server addresses on the **EUQ Authentication** screen during the enabling process.

Configuring End-User Quarantine (EUQ)

To allow end-users to access quarantined spam items that IMSS might have misidentified as spam, do the following:

1. *Enabling EUQ on page 28-3*
2. *Configuring SMTP Server Settings on page 28-5*

3. *Starting or Stopping the EUQ Management Console on page 28-7*
4. *Enabling End-User Access on page 28-8*
5. *Opening the End-User Quarantine Management Console Remotely on page 28-13*

Enabling EUQ

Enabling EUQ requires one of the following authentication methods:

- LDAP
- SMTP

For information about EUQ authentication, see *EUQ Authentication on page 28-2*.

Procedure

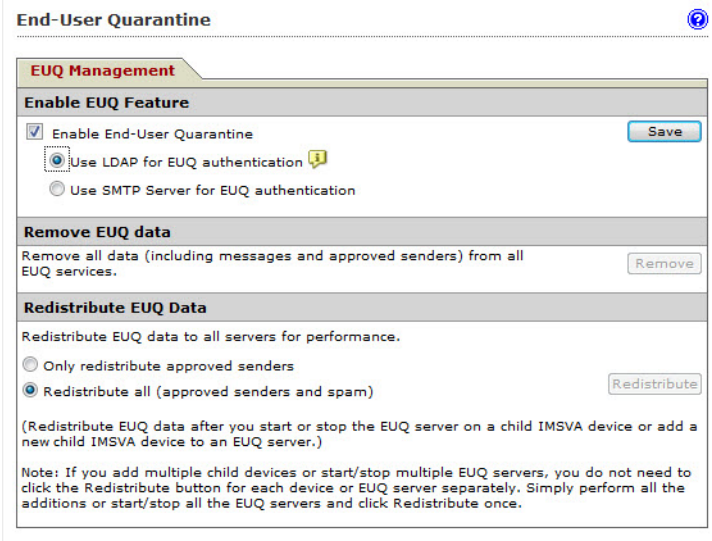
1. Go to **Administration** > **End-User Quarantine**.

   The **EUQ Management** tab appears.

2. Select **Enable End-User Quarantine**.
3. Select an authentication method.

   - **Use LDAP for EUQ authentication**: This option is disabled if LDAP settings are not configured. If LDAP settings are configured, this is the default authentication method.
   - **Use SMTP Server for authentication**: When selected, the SMTP settings section appears. Specify recipient domains and server

addresses. For more information, see *Configuring SMTP Server Settings on page 28-5*.



4. Click **Save**.

   The EUQ service automatically starts.

Note

Your settings will not be saved automatically. To avoid losing your information, do not navigate away from the page without clicking **Save**.

The EUQ service automatically starts. To manually start the EUQ management console, see *Starting or Stopping the EUQ Management Console on page 28-7*.

Configuring SMTP Server Settings

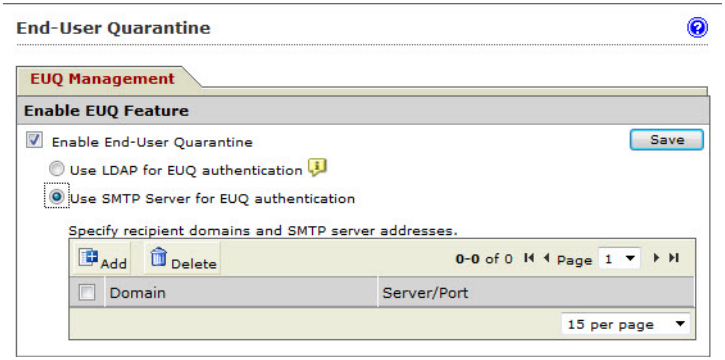
Procedure

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

   The **EUQ Management** tab appears.

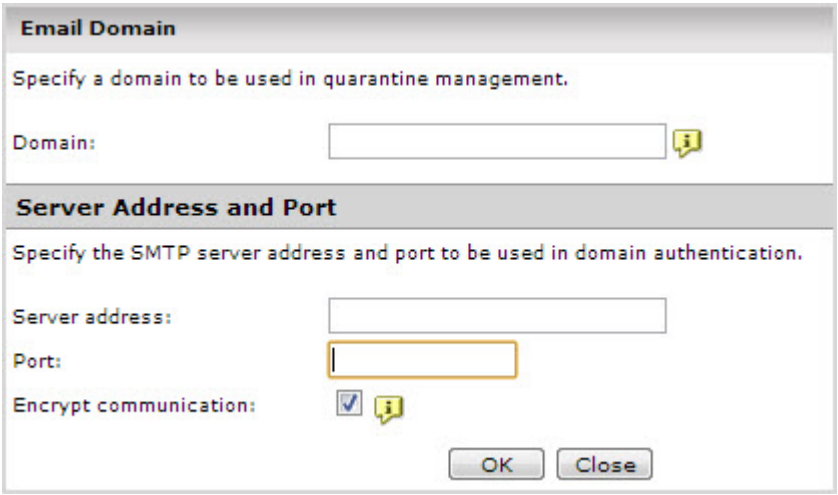
2. Select **Use SMTP Server for EUQ authentication**.

   The SMTP settings section appears.



3. Click **Add**.

The **SMTP Server Configuration** screen appears.



4. Specify the following information:

   - **Email Domain**: Indicates a domain that will be used to access the EUQ console. IMSS uses the recipient's domain to determine the SMTP server to be used for authentication.

     Note

     You can use the following formats to specify domains:

     - company.com
     - *.company.com: Any subdomain of company.com
     - *: Any domain

     A domain can only be listed once. Only unique domains will be added to the list.

   - **Server Address and Port**: Indicates the server address and port that will be used to assign the server address for the destination domain.

Note

Use the default port 25 or specify a different port.

Only one SMTP server can be assigned to a domain. However, more than one domain can be mapped to an SMTP server.

5. Click **OK**.

   The information appears in the SMTP settings table.

Starting or Stopping the EUQ Management Console

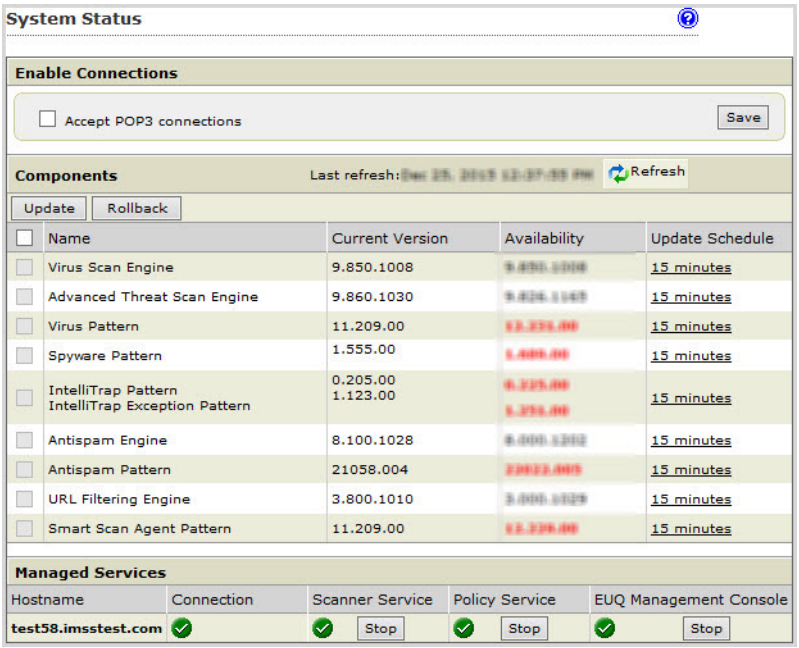
You can manually start or stop the EUQ management console.

Procedure

1. Go to **System Status**.

   The **System Status** screen appears.

In the **Managed Services** table, a green check mark appears under **EUQ Management Console**, indicating that the EUQ management console is active.



2. Click **Stop**.

   After a moment, the EUQ management console stops.

3. Click **Start** under **EUQ Management Console**.

   After a moment, the EUQ management console starts.

Enabling End-User Access

Enable end user access to allow the users to access quarantined spam items that IMSS might have misidentified as spam. The clients use LDAP or SMTP authentication to access the IMSS EUQ service.

Note

To allow users to manage messages on the EUQ management console, add their individual and distribution list email addresses to the list of users on your LDAP server.

When using SMTP authentication, you do not need to configure LDAP settings.

Procedure

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

   The **EUQ Management** tab appears.

2. Click the **User Quarantine Access** tab.

The **User Quarantine Access** screen appears. The displayed screen depends on the authentication method you selected during the enabling process.

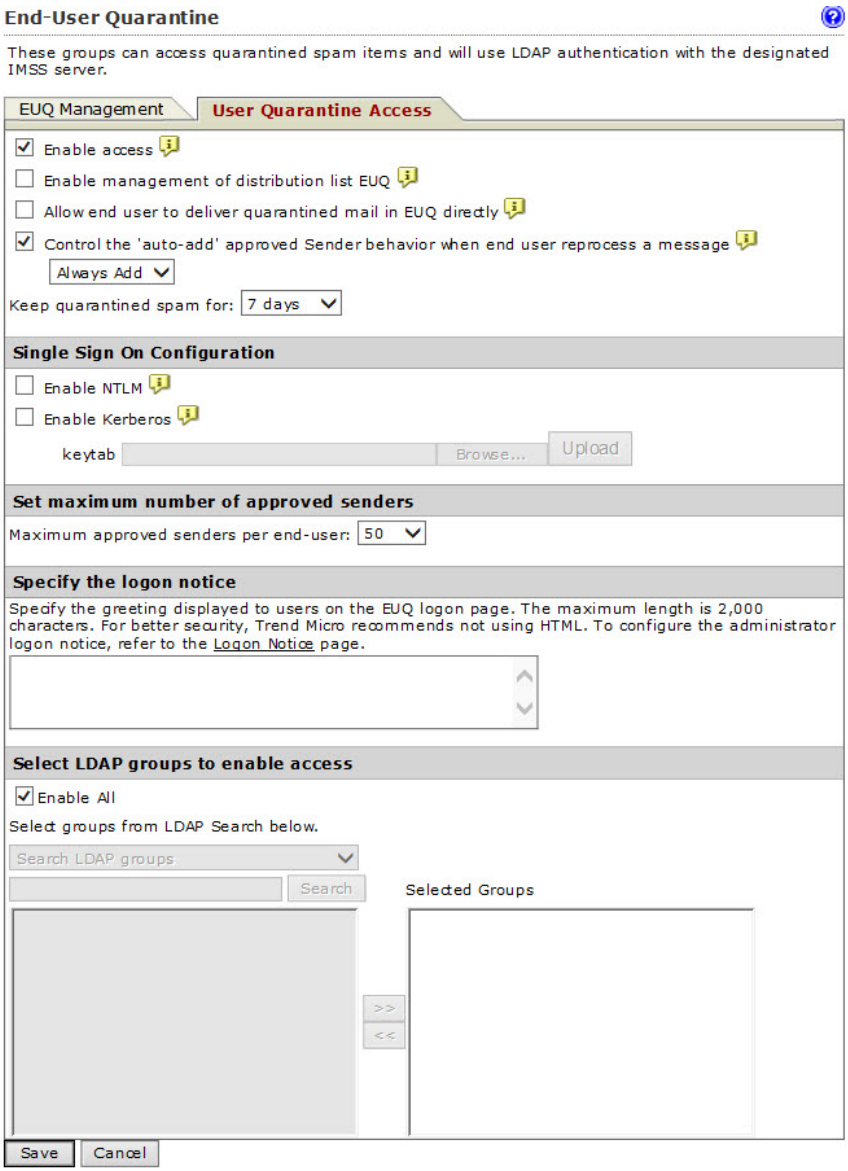


FIGURE 28-1. LDAP authentication

3. Select **Enable access**.
4. Select **Enable management of distribution list EUQ** to allow users to manage the EUQ of distribution lists that they belong to.
5. 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.
6. Select **Control the "auto-add" approved sender behavior when an end user reprocesses a message** and select a value from the drop-down list.
7. Select **Enable NTLM** to allow end users single sign-on access the EUQ management console using the NTLM authentication protocol.
8. To enable Kerberos single sign-on:
   a. Select **Enable Kerberos** to allow end users single sign-on access to the EUQ management console using Kerberos authentication protocol.
   b. Create a new user account in your domain for the host on which IMSS is installed.
   c. On the Active Directory domain controller, use the following command to generate a keytab file for IMSS:

      ```
      C:\>ktpass.exe -out filename -princ HTTP/instance@REALM
      -mapuser account -ptype KRB5_NT_PRINCIPAL -pass password
      ```

      Where:

      `filename` is where the generated keytab file will be stored. For example, `C:\test.keytab`.

      `instance` is the hostname of the computer where IMSS is installed. For example, `imss.test.com`.

      `REALM` is the uppercase name of the realm you want to authenticate with, normally the same with the domain name on DNS server. For example, `TEST.COM`.

      `account` is the account created for IMSS. For example, `user@test.com`.

`password` is the password of the account.

d. Click **Browse...** to locate the generated keytab file.

e. Click **Upload** to upload the keytab file to IMSS.

If `ktpass.exe` is not found, you can install support tools using the Windows server installation CD/DVD or download the file from the Microsoft website.

If Kerberos single sign-on is enabled, use the hostname for IMSS when accessing the EUQ management console.

9. Select the number of days to keep quarantined spam.

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

11. Specify a logon notice that appears on the user's browser when he/she starts to access the quarantined messages.

12. Under Select LDAP groups, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.

13. 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.

14. 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
```

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 28-1. 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`
	• **Microsoft Active Directory Global Catalog**
	  • Without Kerberos: `user1@domain.com (UPN)` or domain\user1
	  • With Kerberos: `user1@domain.com`
	• **OpenLDAP**: `cn=manager, dc=test1, dc=com`
	• **Sun iPlanet Directory**: `uid=user1, ou=people, dc=domain, dc=com`

SMTP	Use any valid email address for the logon name. **Note** IMSS supports `auth login`, `auth plain` and `starttls`.

Distribution List EUQ Management

IMSS enables users to manage the EUQ of distribution lists that they belong to.

Note

Note: You can enable distribution list EUQ management only when using LDAP authentication.

This feature supports the following LDAP server types:

- Domino
- Microsoft Active Directory
- Microsoft AD Global Catalog

When a user requests management rights, IMSS sends a notification to the distribution list address. The notification contains the following information:

- Requesting user's address
- Distribution list address
- Unique, single-use authentication code
- Authentication code expiration date

Note

Authentication codes expire after five minutes by default. To specify a new expiration period, add the following section in the `imss.ini` file:

```
[EUQ]
expired_interval=5
```

Only one user can manage the EUQ at any given time. IMSS forces the current user to log off if another user:

- Requests management rights
- Chooses to force the current user to log off

Managing Distribution List EUQ

Provide the following instructions to the user.

Note

The **Distribution List EUQ Management** link displays only if you enable this feature.

Procedure

1. Log on to your personal Email Quarantine.
2. Click **Distribution List EUQ Management**.

   A new screen appears.
3. Specify the email address of the distribution list.
4. Click **Next**.

   A new screen appears and the system sends a notification to the distribution list.
5. Specify the authentication code provided in the notification.

   The authentication code can be used only:

   - By the requesting user
   - Once
   - Before the specified expiration date
6. Click **Log On**.

Disabling EUQ

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

Procedure

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

   The **EUQ Management** screen appears.
2. Clear the **End-User Quarantine** check box.

3. Optional: Remove all EUQ data from each device to save disk space. To do so, click **Remove** on the **EUQ Management** tab.

4. Click **Save**.

Managing EUQ Databases

By default, IMSS installs an EUQ database on the IMSS server. The default EUQ database name is **imsseuq**, user name is **sa**, and password is **postgreSQL**.

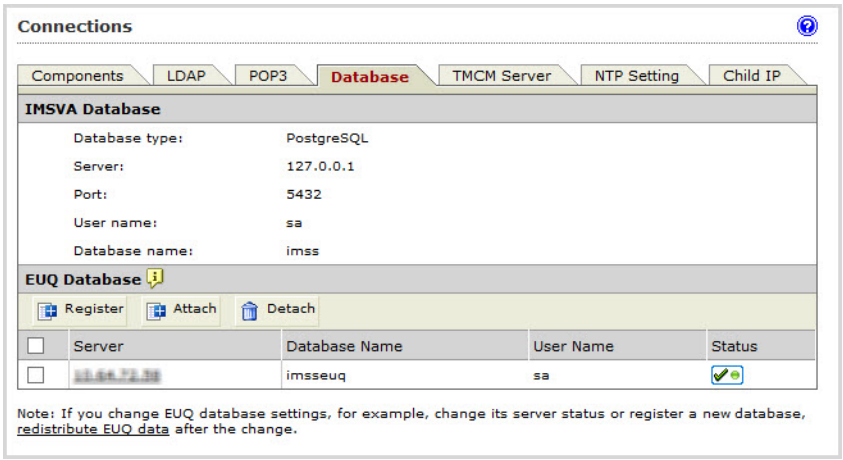
In addition, you can manually register, attach, disable and detach EUQ databases if necessary.

Procedure

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

   The **Components** tab displays by default.

2. Click the **Database** tab.



3. To register an EUQ database to IMSS, click **Register** under **EUQ Database**. Type the EUQ database server IP address, port number, administrator user name, password and database name.

   Note

   The administrator account you use for registering and attaching EUQ databases must have the superuser role.

4. To attach an EUQ database, click **Attach**. Type the EUQ database server IP address, port number, administrator user name, password and database name.

   Note

   The attach function is used to restore a detached database. Make sure that the database you want to attach has an initialized schema.

5. To detach an EUQ database from IMSS, disable the database, select the check box next to a database, and then click **Detach**.

   Note

   The detach function will remove a database from the EUQ database list. It is used to stop an EUQ database.

   You can attach the database again if necessary. Detaching the database does not delete or otherwise affect the actual database server; IMSS just stops using the database.

6. To disable an EUQ database, click the green check mark for that database in the **Status** column.

   Note

   The disable function is used to temporarily stop an EUQ database. For example, you can stop an EUQ database for maintenance for a certain period of time.

What to do next

Redistribute data among multiple EUQ-enabled devices in a group to improve EUQ performance. Redistribute data:

- After you register, attache or disable a database
- Before you use the command line interface to remove an EUQ-enabled device

Tip

Trend Micro recommends that you do the following after redistributing EUQ data:

- Verify that the newly added approved senders are still available.
- Instruct end users not to add approved senders to the list while you are adding a child device and redistributing EUQ.

Chapter 29

Administrative Tasks

This chapter explains how to perform important administrative tasks, such as managing accounts, configuring connection settings, and managing product licenses.

Topics include:

- *Managing Administrator Accounts on page 29-2*
- *Configuring Connection Settings on page 29-6*
- *Configuring Database Maintenance Schedule on page 29-19*
- *Managing Product Licenses on page 29-20*
- *Activating Products on page 29-24*
- *Configuring Smart Protection Network Settings on page 29-26*

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.

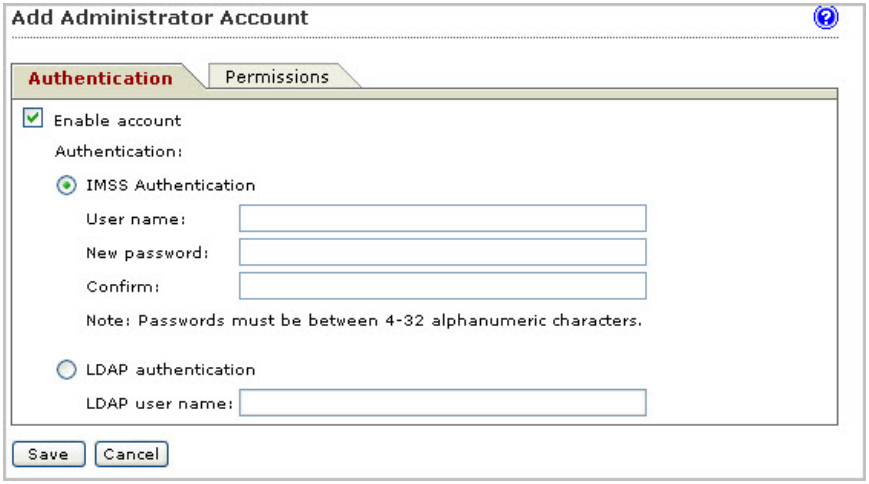
Procedure

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:

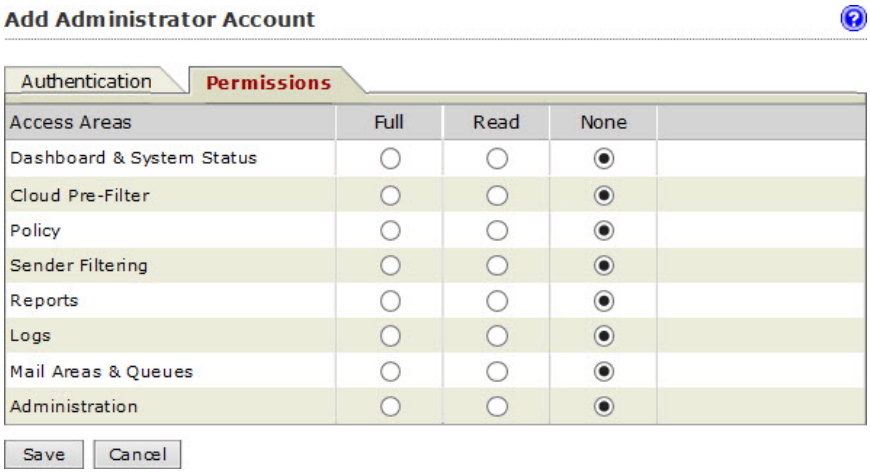
   a. Select **Enable account**.

   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:

      - **Dashboard & System Status**
      - **Cloud Pre-Filter**
      - **Policy**
      - **Sender 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.

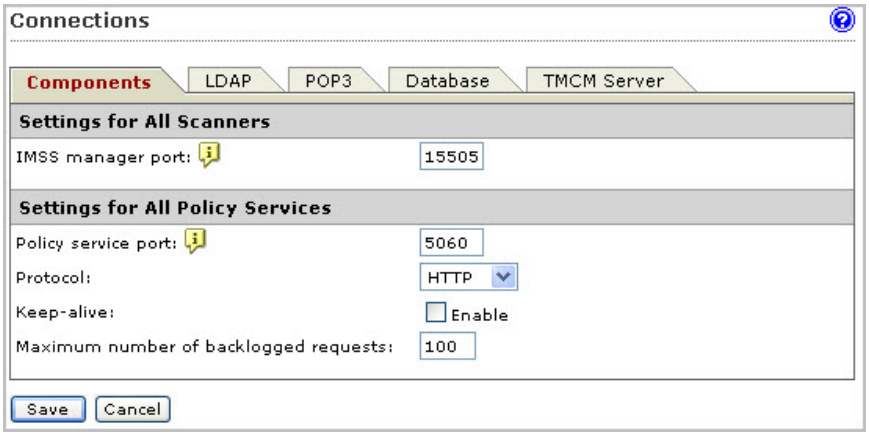
Configuring Connection Settings

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 **System Status** page. Furthermore, any changes will not take effect on the managed service(s).

3. Under **Settings for All Policy Services**, configure the following:

   - **Policy service port**: Specify the port number that IMSS uses to communicate with policy services. The default port number that the policy service uses to communicate with IMSS is 5060.
   - **Protocol**: Select the type of protocol the scanner uses to communicate with the policy service (HTTP or HTTPS).
   - **Keep-alive**: Select the check box to enhance policy retrieval by maintaining a constantly active connection between the scanner and policy services.
   - **Maximum number of backlogged requests**: Specify a number that represents the maximum number of requests IMSS will preserve until it can process them later.

4. Click **Save**.

About LDAP Settings

Configure LDAP settings for user-group definition, administrator privileges, or end-user quarantine authentication.

If the LDAP settings on the **Administration** > **Connections** > **LDAP** screen are not configured, the following LDAP related features will not work:

- **Policy** > **Internal Addresses** > **[Search for LDAP groups]**
- **Policy** > **[any rule]** > **[Sender to Recipient]** > **[Search for LDAP user and groups]**

- **Administration** > **End-User Quarantine** > **User Quarantine Access** > **[Select LDAP groups to enable access]**
- **Administration** > **Admin Accounts** > **Add** > **[LDAP authentication]**

LDAP Server Types

TABLE 29-1. 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)
Active Directory Global Catalog	Without Kerberos: user1@domain.com (UPN) or domain \user1 With Kerberos: user1@domain.com	dc=domain, dc=com dc=domain1,dc=com (if mutiple unique domains exist)	Simple Advanced (with Kerberos)
OpenLDAP	cn=manager, dc=test1, dc=com	dc=test1, dc=com	Simple
Lotus Domino	user1/domain	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	Simple

Configuring LDAP Settings

Procedure

1. Go to one of the following to access the **LDAP** tab:
   - **Administration** > **IMSS Configuration** > **Connections | LDAP**
   - **Administration** > **IMSS Configuration** > **Configuration Wizard | Step 6: LDAP Settings**
2. Click **Add**.

   The **LDAP Settings** screen appears.
3. Specify a meaningful description for the LDAP server.
4. Next to **LDAP server type**, select the type of LDAP servers on your network:
   - **Domino**
   - **Microsoft Active Directory**
   - **Microsoft AD Global Catalog**
   - **OpenLDAP**
   - **Sun iPlanet Directory**
5. Next to **Enable LDAP 1**, select the check box.
6. Next to **LDAP server**, specify the server name or IP address.
7. Next to **Listening port number**, specify the port number that the LDAP server uses to listen to access requests.
8. Configure the settings under **LDAP 2** if necessary.
9. 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.

10. Under **LDAP admin**, specify the administrator account, the corresponding password and the base distinguished name.

    Refer to *LDAP Server Types on page 29-8* for assistance.

11. 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.

12. Select the **Enable encrypted communication between IMSS and LDAP** check box and click **Browse** to upload a CA certificate file to verify the certificate used by the LDAP server.

13. Click **Add**.

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

Note

Only Active Directory and Active Directory Global Catalog support Kerberos Authentication.

14. Under **LDAP Email Address Attribute**, select the LDAP attribute from which IMSS retrieves user email addresses.
    - **mail**: This is the default LDAP attribute that stores email addresses.
    - **proxyAddresses**: This is the recommended attribute to choose if you use Microsoft Exchange Server.
    - **Other attribute**: Specify an LDAP attribute that stores email addresses.
15. Click **Save & Synchronize**.

Enabling and Disabling LDAP Servers

LDAP servers can be enabled or disabled depending on the requirements for your network.

Procedure

1. Go to **Administration** > **IMSS Configuration** > **Connections** > **LDAP** to access the LDAP tab.
2. Click a server that you want to enable or disable in the LDAP server table.

   The **LDAP Settings** screen appears.
3. Under **LDAP server type**, select or clear the **Enable LDAP 1** and **Enable LDAP 2** check boxes to enable or disable the LDAP server.

   Note

   LDAP 1 and LDAP 2 refers to backup servers for each other. If you select only one check box, the LDAP server status is enabled, but its backup server is not enabled.
4. Click **Save**.

Configuring POP3 Settings

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as your clients retrieve them.

Tip

To use the POP3 message filter, enable **Accept POP3 connection** from **System Status** screen. This option is not selected by default.

Procedure

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

   The **Components** tab displays by default.

2. Click the **POP3** tab.

3. To configure a connection from unknown POP3 servers on the Internet, specify the port number IMSS uses for incoming POP3 connections under **Generic POP3 Connection**.

4. To configure connections from specific POP3 servers, do the following:

   a. Click **Add** under **Dedicated POP3 Connections**.

      The **Dedicated POP3 Connection** window appears.

   b. Specify the port IMSS uses for incoming POP3 connections, the POP3 server IP address, and the POP3 server port number.

   c. Click **OK**.

   d. To modify an existing connection, click the connection name.

5. Under **Message Text**, modify the message that IMSS sends to users if messages that they are trying to receive trigger a filter and are quarantined or deleted.

6. Click **Save**.

Note

The incoming port on your scanners must be idle or the IMSS daemon might not function properly.

Configuring POP3 Generic Services

For a generic POP3 service, the POP3 client logs on using the USER command and specifies the actual POP3 server and optional port number along with the user's name using the UserServerSeparator character to separate the values.

Example 1: To connect user "User1" to server "Server1", and the UserServerSeparator character is "#", the client issues the following USER command:

```
USER User1#Server1
```

Example 2: To connect to port 2000 on Server1, the following command is used:

```
USER User1#Server1#2000
```

Note

If you do not specify a port number, IMSS uses the default value of 110.

The following example shows how to configure generic POP3 settings for Outlook:

Procedure

1. Specify the POP3 server address with IMSS scanner IP `192.168.11.147`.
2. Specify user name `test123#192.168.11.252`.
3. Set POP3 port to `110`.

Configuring POP3 Dedicated Services

For a POP3 dedicated service, the POP3 service always connects to a specific POP3 server. IMSS uses this service for a POP3 logon and for any type of logon using the AUTH command. For this service, a separate port on the proxy has to be set up for each specific POP3 server that any client might want to connect.

The following example shows how to configure dedicated POP3 settings in Microsoft Outlook:

Procedure

1. Specify the POP3 server address with IMSS scanner IP `192.168.11.147`.
2. Specify user name `test123`.
3. Set the POP3 port to `1100`, which is the port that the IMSS dedicated POP3 service is listening on.

Configuring Database Settings

Configure the database connection settings so IMSS can save messages and data.

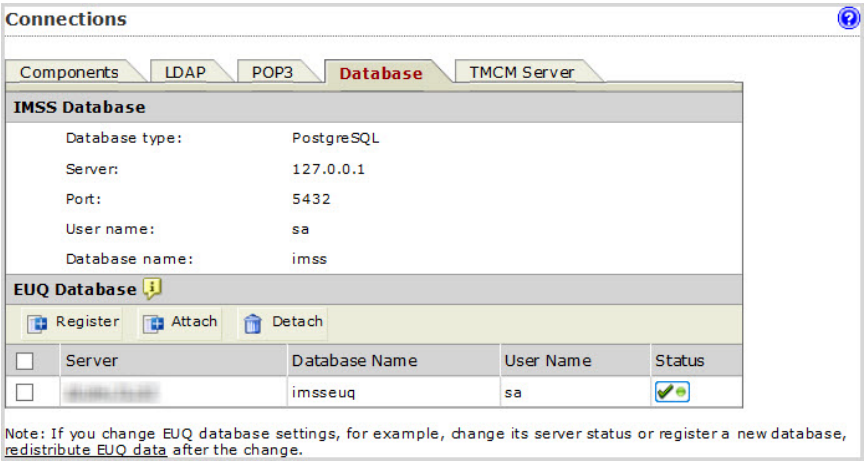
Procedure

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

   The **Components** tab displays by default.

2. Click the **Database** tab.

The IMSS admin database type, server IP address, port number, user name and database name appear at the top of the table.



3. Under **EUQ Database**, perform operations to manage EUQ databases as required.

Note

For detailed operations, see *Managing EUQ Databases on page 28-17*.

Configuring TMCM Settings

To use Trend Micro Control Manager (TMCM) 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.

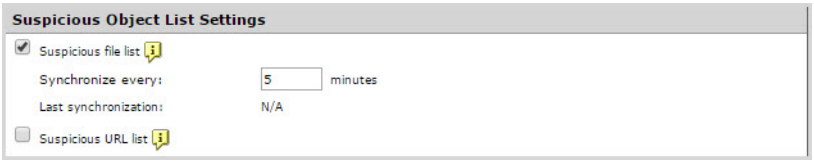
4. Under **Proxy Settings**, specify the following parameters:

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.
Port	Specify the port for the proxy server.
User name	Specify the user name to access the proxy server.

Option	Description
Password	Specify the password for the user name.

5. Under **Suspicious Object List Settings**, do the following:

   - If you want IMSS to detect suspicious files, select the **Suspicious file list** check box and specify the interval to synchronize the suspicious file list from Control Manager. The default synchronization interval is 5 minutes, and the minimum interval is 1 minute.



   - If you want IMSS to detect suspicious URLs, select the **Suspicious URL list** check box.

> **Note**
>
> IMSS detects suspicious URLs based on Web Reputation Services available through Smart Protection Servers. Make sure you have properly configured Web Reputation settings and Smart Protection Servers.

6. 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.

Note

In addition, make sure that your Control Manager version is Version 6.0 Service Pack 3 Patch 3 Hotfix 3611 or later and the Smart Protection Server version is 3.0 Patch 1 or later.

Providing IMSS Logon Credentials in Control Manager

To make your settings effective, provide your IMSS logon credentials for authentication on the Control Manager management console.

Procedure

1. Log on to the Control Manager management console.
2. Go to **Administration** > **Manager Servers**.
3. Next to **Server Type**, select **InterScan Messaging Security Virtual Appliance**.
4. Find your IMSS server and click the **Edit** icon in the **Actions** column.

   The **Edit Server** screen appears.
5. Under **Authentication**, provide your IMSS logon credentials.

   Note

   Trend Micro recommends that you create a separate administrator account other than the default "admin" account for Control Manager to manage IMSS. The account is required for authentication on the Control Manager management console.
6. Click **Save**.

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.

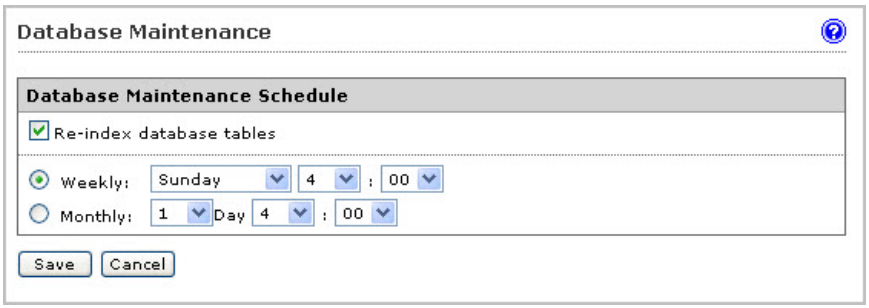
Configuring Database Maintenance Schedule

You may want to re-index the IMSS database tables if you encounter slow performance when performing queries. As re-indexing can impact the scanner performance, Trend Micro recommends that you do this during off-peak hours.

Procedure

1. Go to **Administration** > **Database Maintenance**.

   The **Database Maintenance Schedule** screen appears.



2. Select the **Re-index database tables** check box.

3. Select the weekly or monthly schedule from the drop-down boxes.
4. Click **Save**.

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.

Component Descriptions

IMSS can use the following components:

Component	Description
Cloud Pre-Filter	Provides message approved and blocked list filters and scanning for spam, viruses, and other threats before the messages reach your network.
Trend Micro Antivirus and Content Filter	Basic scanning and filtering functionality. You can think of this product as the IMSS program itself.
Spam Prevention Solution (SPS)	A built-in filter that helps IMSS identify content typically found in spam.

Component	Description
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.
Trend Micro Email Encryption	Trend Micro Email Encryption integrates with IMSS to encrypt and decrypt messages and to block messages that cannot be decrypted. Trend Micro Email Encryption is not available in the IMSS Linux solution.
Regulatory Compliance	Compliance templates provide administrators with regulatory compliance. For a detailed list of available templates, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

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.

4. Click **Hide Notifications for Inactive Components** on the top of license summary to hide notifications for inactivate components.

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** 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-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.

Configuring Smart Protection Network Settings

Enable Trend Micro Smart Feedback to share threat information with the Trend Micro Smart Protection Network. This provides better protection for your network because Trend Micro is able to quickly identify and address new threats.

Note

Email Reputation, File Reputation, and Web Reputation are all part of the Smart Protection Network.

Procedure

1. Go to **Administration** > **Smart Protection Network**.

   The **Smart Protection Network Settings** screen appears.

2. Select **Enable Trend Micro Smart Feedback**.

3. Click **Save**.

Chapter 30

Updating and Rescuing the System and Application

This chapter explains how to update and rescue the system and application files when Trend Micro releases patches, service packs, and other updates.

Topics include:

- *Updating the System and Application on page 30-2*

Updating the System and Application

When new operating system and application files become available from Trend Micro, deploy them to a parent IMSS device and all of its child devices. By default, child devices will be updated before the parent device.

Topics include:

- *Updating the System and Application on page 30-2*

Uploading a New System or Application File

Procedure

1. Go to **Administration** > **Updates** > **System & Applications**.
2. Under **Upload**, click **Browse** and locate the file.
3. Click **Upload**.

   After the file finishes uploading, the package type, build number, and title appear under **Latest uploaded package**.

Deploying the System or Application File

Procedure

1. Select the check boxes next to the devices to which you want to deploy the update.
2. Click **Update**.
3. Accept the license agreement.

   After an operating system update or upgrade, IMSS reboots. An application upgrade might force IMSS to automatically reboot.

4. If IMSS rebooted, wait for it to start up and log on again.
5. Go to **Administration** > **Updates** > **System & Applications** to view the summary screen.

Note

a. During an update, do not modify any other settings. If you are updating several devices, you can click **Cancel** to stop the update of the next device.

b. If you have applied some patches on a child device, and later unregister this child device from the parent device, IMSS automatically rescues the system and application files, but you need to re-apply the patches again.

If a device check box is grayed out, you cannot deploy the files to the device because the device:

- Already has the updated files.
- Has more up-to-date files than the ones you are trying to deploy.
- Is a child device and the patch requires you to upload the files and deploy them to the parent first, or vice versa.

Viewing the Update History for Any Device or Rolling Back an Update

Procedure

1. Under **Host Name**, click the name of the device you want to view.

   A summary screen appears showing the updates and related log information.

2. To remove an update, click **Rollback**.

   You can only roll back the latest application updates.

3. To go back to the main screen, click **OK**.

Chapter 31

Troubleshooting and FAQs

This chapter explains how to troubleshoot common IMSS issues.

Topics include:

- *Troubleshooting on page 31-2*
- *Frequently Asked Questions on page 31-18*
- *Troubleshooting Cloud Pre-Filter on page 31-36*

Troubleshooting

This section helps to resolve common issues that you might encounter when configuring or administering IMSS. 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

General

Troubleshooting Management Console or Component Access

The target port is not in the firewall approved list. Open the ports as shown in *IMSS Ports on page 31-15* in the firewall.

If you are unable to access the management console, do the following:

Procedure

1. If the management console URL is not a trusted site in Internet Explorer, add the URL to the trusted sites.
2. Start the database process, `dbctl.sh`, before starting the Central Controller process, `S99ADMINUI`.
3. If you are still unable to access the management console, restart the Central Controller process, `S99ADMINUI`.

   For more details, see *IMSS Scripts on page B-1*.

Troubleshooting the IMSSPS Daemon

If the imssps daemon is running, the policy service is working.

Procedure

1. Check the connection between the policy service and scanner service.
2. Verify your LDAP settings.

Troubleshooting Product Activation or Component Updates

This procedure explains how to troubleshoot activating products (Antivirus/eManager, SPS, Email Reputation, Sender 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.

Procedure

- Verify your DNS server settings with the following command:

  ```
  nslookup licenseupdate.trendmicro.com
  ```

  The command should return the IP address of your IMSS 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.

- Verify your proxy settings from the management console.

  a. Go to **Administration** > **Updates**.

     The **Schedule** tab displays by default.

  b. Click the **Source** tab.

  c. Configure the proxy settings.

  d. Click **Save**.

Troubleshooting Email Notifications

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:

Procedure

1. Go to **Administration** > **Notifications** > **Delivery Settings**.
2. Next to **Preferred Charset**, select the character set in which the messages will be encoded.

Troubleshooting Message Log Queries

IMSS scanner records the log with local time.

Procedure

- To query message logs, synchronize the date/time on all computers with IMSS.

Troubleshooting 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.

Procedure

- Check your firewall settings for the Manager Service listening port.

Troubleshooting Attachment Information

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.

Procedure

- Check the reason why IMSS quarantined the message.

Troubleshooting Not Receiving Email Messages

Procedure

- Check if the IMSS scanner service and SMTP service are running.
- Check if a different application is using the required port. Free up port 25.

Troubleshooting Services Not Running

Procedure

1. Start the database before starting IMSS services.
2. Restart all IMSS services.

Troubleshooting Scan Time After Enabling Web Reputation

Web Reputation needs to query the Trend Micro Web Reputation servers.

Procedure

1. Verify the HTTP connectivity from the IMSS scanner to the external network.
2. For Web Reputation issues, check the `wrsagent.*` files under the `{Installation_Path}\imss\log` folder.

End-User Quarantine Issues

Troubleshooting EUQ Access

To view the console from another computer on the network, go to:

Procedure

- Verify that you are using the correct URL and port number.

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

Troubleshooting User Access to EUQ

Procedure

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 2-8*.

4. Ensure the LDAP 1 and LDAP 2 servers are synchronized. If a user's account exists only on one of the LDAP servers, users will not be able to consistently log on to the EUQ management console. IMSS uses LDAP2 servers as backup for LDAP 1 servers.

5. If the issue persists even after verifying the above settings, send the log file to Trend Micro.

Troubleshooting EUQ Using NTLM SSO

This procedure explains how to troubleshoot users unable to log on to EUQ management console using NTLM single sign-on (SSO).

Note

Logging on to the EUQ management console using SSO requires that LMCapabilityLevel of Active Directory is configured to support NTLMv1.

Procedure

1. Configure the LMCapabilityLevel.

   a. Go to **Start** > **Run** and type `secpol.msc`.

b. Go to **Security Settings** > **Local Policies** > **Security Options** > **Network security: LAN Manager authentication level** > **Local Security Setting**.

c. Select **Send LM & NTLM responses** and save.

2. Enable the LDAP1 or LDAP2 servers and specify them as in use for Active Directory (IP or domain name or FQDN).

3. Verify that the endpoint operating system supports (and enables) NTLMv1 in LMcapabilityLevel settings.

   - Using Firefox: The `about:config` link is configured to add the NTLM trusted host list.
   - Using Internet Explorer: The EUQ management console is added to the internal site list.
   - Using Internet Explorer: The Windows integrated authentication setting in Internet Explorer is enabled.

Troubleshooting EUQ Digest Message Display

The EUQ digest may not correctly display quarantined message information if the correct character set is not selected.

Procedure

1. Go to **Administration** > **Notifications** > **Delivery Settings**.
2. Next to **Preferred charset**, select the character set that will properly display the digest information.

Troubleshooting Messages Appearing on EUQ

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:

Procedure

1. Go to **Quarantine & Archive** > **Settings**.
2. Click the link of the quarantine area that you want to synchronize to EUQ.
3. Select the check box next to **Synchronize all spam and email messages, that do not violate virus, phishing, or Web reputation rules, to the EUQ database (for this area only). This allows end users to view and manage the messages from the EUQ Web console**.

   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.

Troubleshooting LDAP with Kerberos Authentication

Kerberos protocol requires time synchronization between the Kerberos server and IMSS.

Procedure

1. Synchronize the date/time for all computers with IMSS.
2. Check whether the DNS server is configured correctly.

Troubleshooting Kerberos SSO to EUQ

Logging on to the EUQ management console using SSO requires the following:

Procedure

1. Verify that LDAP1 or LDAP2 servers are enabled and specified as in use for Active Directory (IP address or domain name or FQDN).
2. Verify that the DNS server is configured for IMSS contains the record of the Kerberos service.
3. Verify that the endpoint operating system supports (and enables) Kerberos authentication:
   - Time should be synchronized between IMSS and the Kerberos authentication service.
   - Using FireFox: The `about:config` link is configured to add the negotiate-auth trusted url list.
   - Using Internet Explorer: The EUQ management console is added to the internal site list.
   - The Windows integrated authentication setting in Internet Explorer is enabled.
   - Using Windows Vista or above, use the hostname as the instance when generating a keytab file.
4. Verify that only one EUQ management console instance is mapped to one user account. If the instance is mapped to more than one user, SSO will not work.
5. If EUQ is deployed in a parent-child deployment, verify that you are using the parent device's 8447 port to access EUQ. SSO will not work if a child's port is used.
6. Verify that the account provided on the LDAP Settings screen has permission to look up all accounts for authentication.

Sender Filtering Issues

Troubleshooting FoxyProxy Startup

There are several reasons why FoxProxy might not start. To find out the reason, view the IP Profiler logs.

Procedure

1. Go to the directory where IP Profiler is installed (by default: `/opt/trend/imss/config`).
2. Open foxproxy.ini.
3. Change the value for `log_level` to 4.
4. Restart FoxProxy by typing the following:

   ```
   /opt/trend/imss/script/foxproxyd restart
   ```

5. Open the log file by typing the following:

   ```
   /opt/trend/imss/log/foxproxy-general.****
   ```

Troubleshooting FoxyProxy Connectivity

Procedure

1. Verify that FoxProxy is running and that it binds on the configured port (port 25 by default).

Troubleshooting FoxyProxy Message Processing Speed

When FoxProxy receives messages, it performs a DNS query on FoxDNS. If Bind is not running, FoxProxy continues to wait until the DNS query times out.

Procedure

- Verify that the bind service is running on the computer where FoxDNS is installed:

  a. Type the following command:

  ```
  ps -ef | grep named
  ```

  b. Start the service if it is not running.

Troubleshooting Viewing FoxyProxy Blocked Connections

Every five (5) minutes, FoxProxy sends information about blocked connections to the IMSS server.

Wait for at least five minutes before viewing the connection information.

To change this time value:

Procedure

1. Open `foxproxy.ini`.
2. Modify the value for `report_send_interval`.
3. Restart FoxProxy by typing the following:

   ```
   /opt/trend/imss/script/foxproxyd restart
   ```

Troubleshooting FoxDNS

Verify that the BIND service is running:

Procedure

1. Specify the following command:

   ```
   ps -ef | grep named
   ```

2. Start the service if it is not running.

Troubleshooting IP Profiler Logs

The following IP Profiler-related log files are in the IMSS admin database:

- foxmsg.****
- foxnullmsg.****
- foxreport.****

This procedure explains how to verify that the log files exist.

Procedure

1. Go to the log directory where IMSS is installed (by default: `/opt/trend/imss/log/`).
2. If the files are not present, use the following command to check if imssmgr is running:

   ```
   ps –ef | grep imssmgr
   ```

3. Check if FoxProxy is running:

   ```
   ps –ef |grep foxproxy
   ```

4. Verify that IP Profiler is enabled. In the table `t_foxhuntersetting`, the following should exist:

   ```
   record: 'Type' = 1 and 'enable' = TRUE
   ```

Troubleshooting Email Reputation After Enabling the Management Console

Email Reputation may not work due to the following reasons:

- Email Reputation has not been activated.

- 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.

Procedure

1. Activate Email Reputation and confirm IMSS can access the Internet.

Troubleshooting SMTP Routing and Postfix

This procedure explains the MTA settings on the **SMTP Routing** management console screen are not being written into the Postfix configuration files.

By default, the settings on the SMTP routing screen will not be automatically applied to Postfix on each scanner.

To apply the settings to all scanners:

Procedure

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

   The **SMTP Routing** screen appears.

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

3. Click **Save**.

4. After a few minutes, the IMSS manager process on each scanner synchronizes the settings to Postfix. To restart the IMSS manager immediately, use the command:

   ```
   /opt/trend/imss/script/S99MANAGER restart
   ```

5. If the process above does not work, check the local configuration file `/opt/trend/imss/config/imss.ini` to verify the `enable_postset_thd` key is set to **yes** or is blank.

Troubleshooting IP Profiler Blocked List

The changes require about one (1) minute to take effect.

Procedure

1. Wait one (1) minute before checking the list again.

Troubleshooting Blocked IP Addresses in 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.

Procedure

1. View the **Overview** page after an hour.

IMSS Ports

The following tables outline all ports used by IMSS in their default configuration.

TABLE 31-1. 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**.

Port Number	Component and Role	Configuration Location
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** > **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**.
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`
8445	Management console listening port. You need to open this port to log on to the management console using a web browser.	Apache listen port: `{IMSS}\UI\php\conf\widget.conf: Listen\VirtualHost`
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`
10025	IMSS scanner SMTP service listening port.	`imss.ini\[socket_1]\proxy_port`

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
10026	The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSS.) 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.	`IMSS_HOME/postfix/etc/ postfix/ master.cf`
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.	Not configurable on the IMSS server.
IMSS uses the following ports when you enable related service:		
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.

Postfix MTA Settings

If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally?

To control all the Postfix computers from the web management console, enable the **Apply settings to all scanners** option. Choose **Administrator** > **SMTP Routing** > **SMTP** from the menu.

Can I make an exception on the settings for some Postfix instances separately?

To make an exception for some Postfix settings, search for the key "detach_key_postfix" in `imss.ini`, and add the keys that you do not want to apply from the web management console. For example:

```
detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory
```

The parameters above will not be overwritten by any settings that you configure through the web console. You can modify `main.cf` manually.

Note

"`{Parameter1:{Parameter2}:…::{Parameter n}`" means you can use one or more parameters by separating them using colons.

You can find the parameter names in the table `tb_postfixconfig` from the database, under the column fieldname.

WARNING!

Use extreme caution when modifying the configuration file.

IMSS Components

How can I set up and maintain the database?

The following commands can help you maintain the database:

Note

Before you use SQL commands such as `ex`, `psql`, `pgdump`, and `pgrestore`, run the `source /IMSS_install_path/imss/script/pg.rc` command first. For example, run `source /opt/trend/imss/script/pg.rc`.

In addition, to connect to a database server running Red Hat Enterprise Linux 7, add `-h 127.0.0.1` to the command line. For example, run `/opt/trend/imss/PostgreSQL/bin/psql -h 127.0.0.1 -U sa -d imss`.

- `pg_dump -d imss -U sa > YYMMDD.HHMMSS.backup`: Back up the database.
- `psql -U sa -d imss < ./YYMMDD.HHMMSS.backup`: Retrieve the latest data if errors occur.
- `vacuum`: Clean up the database on tables that are frequently accessed or on tables that have large amounts of data. Use this command when email traffic is low or when the device is not connected to your network.
- `vacuumfull`: Clean up the entire database when the database is not being heavily utilized or when the device is not connected to your network.
- `redirect_stderr= and log_rotate_***=`: Turn on these options in postgresql.conf to redirect old database log entries to the system log, which is rotatable. You can name the log file to start with a dash “-”.

Email Reputation

How do I configure Email reputation not to 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 **Sender Filtering** > **Approved List**.
3. Add the IP addresses or domains that you do not want blocked to the Approved List.

IP Profiler

How can I purge the FoxProxy log?

A log purge program exists in the IP Profiler installation directory (by default: `/opt/trend/imss/bin/TmFoxPurgeLog`).

The settings about log purge function are in the configuration file `foxproxy.ini`. The keys are as follows:

- log_purge
- log_purge_unit

- log_purge_num

Which process monitors FoxProxy's status? Which process rescues it when it shuts down?

FoxProxy is a multiple-process program. The main process only monitors child processes. If child processes are stopped, the main process rescues them. The FoxProxy main process is monitored by imssmgr. If the main process is stopped, imssmgr rescues it.

Which process/component performs DNS queries?

The DNS queries are performed directly by FoxProxy.

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 Sender Filtering Suspicious IP screen also display the connection information of blocked IP addresses?

The **Sender 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?

No. IMSS installs a new BIND server, and the IP Profiler can use only that build-in BIND server.

When does IMSS 9.1 Patch 1 send an email message to "Foxhunter_proxy@domain"?

IMSS sends an email message to "Foxhunter_proxy@domain" under the following three conditions:

- When FoxProxy receives an "Incomplete" message.
- When FoxProxy receives a "Null" message.
- When FoxProxy rejects a connection, it will send a statistics mail every 5 minutes. You can configure the time interval by modifying the `report_send_interval` (unit in seconds) setting in `foxproxy.ini`.

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

Technically, LDAP service is not required. The DHA rule of IMSS relies on the result returned from Postfix, which in turn passes the result to FoxProxy, a sub-module of IP Profiler, for analysis. The LDAP server is just one of the many means by which Postfix checks for the existence of a recipient's mailbox.

Mail Areas & Queues

Can I use special characters to perform queries?

Yes, you can use the following special characters to perform queries:

- **Asterisk (*):** Used as a wildcard character to search for characters. You can use the asterisk (*) to search for email addresses or file names.

  To search for email addresses, refer to the following examples:

TABLE 31-2. Search for email addresses

EXAMPLE	DESCRIPTION
*	Valid representation of all email addresses.
@domain.tld, name@.tld	Valid representation of the whole name or the domain (not the top level domain (TLD)).
@.tld	Valid representation of both the name and the domain (not the TLD).

To search for file names, refer to the following examples:

TABLE 31-3. 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.

Why are some users unable to use Kerberos SSO?

Users who are bound to SPN (Service Principal Name) cannot use Kerberos SSO.

Spam Protection Service

How is the spam catch rate determined?

Specify a threshold value between 3.0 and 10.0 for IMSS to classify a message as spam. A high threshold value means that a message must be very "spam-like" to be classified as spam (this decreases the spam catch rate but reduces

the likelihood of false positives). A lower threshold value means that a message only needs to be slightly "spam-like" to be classified as spam (this increases the spam catch rate and may lead to more false positives).

ActiveUpdate

How do I roll back a pattern file?

Click the **Rollback** button on the **System Status** screen.

Control Manager

How do I verify that IMSS is registered to Control Manager? Unregistered from Control Manager?

There are three ways to verify:

- From the Control Manager management console
- From the OS shell
- From the IMSS management console

Verifying that IMSS is registered from the Control Manager management console

Procedure

1. Log on to the Control Manager management console.
2. Click **Products**.

   The **Product Directory** screen appears.
3. Check the Product Directory **Local Folder** for IMSS.

Verifying that IMSS is registered from the OS shell

Procedure

1. Log on to the OS shell.
2. Type the following command:

   ```
   /opt/trend/imss/script/S99CMAGENT isregistered
   ```

Verifying that IMSS is registered from IMSS management console

Procedure

1. Log on to the IMSS web console.
2. Go to **Administration** > **Connections** > **TMCM Server**.
3. Check the **Connections Status**.

LDAP

I cannot add an LDAP server using the correct admin account. Why?

First, verify that the LDAP server can be connected to IMSS. Next, verify the LDAP server type and logon name format are configured correctly.

Active Directory 2008 cannot use Kerberos authentication. Why?

First, verify that the DNS server is configured correctly. Then check the ServicePrincipalName of Active Directory 2008 Kerberos. If the ServicePrincipalName has changed, modify the value in `/opt/trend/imss/config/imss.ini`.

For example:

```
[LDAP-Setting]

server-spn=ad2008@domain.com
```

I use Sun iPlanet as my LDAP server, but my accounts are not synchronizing correctly to Cloud Pre-Filter. Why?

If you have more that 2000 account on Sun iPlanet LDAP server you need to make some changes to the Sun iPlanet LDAP server. Increase the value of "nsslapd-lookthroughlimit" on the **Directory Server** > **Directory** > **cn=config** > **Plugins** > **ldbm database** > **config** > **General Editor** screen.

Other FAQs

Can the IP address for IMSS or IMSS components be changed?

Yes.

Changing the IP Address for IMSS (Central Controller + Scanner)

Procedure

1. Stop all IMSS services by running the `$IMSS_Home/imss/script/imssstop.sh stop` command or stop the services individually.

   For more information on IMSS scripts, see *IMSS Scripts on page B-1*.

2. Change the server IP address.

3. Start the database service if it is installed on this server. If IMSS installed the database use the following command:

   ```
   $IMSS_Home/imss/script/dbctl.sh start
   ```

4. Change the IP address in the `odbc.ini` and `euqodbc.ini` files. The files are located in the IMSS configuration folder: `$IMSS_Home/imss/config/`.

5. Change the following database data:

   tb_component_list
   Specify the computer name and all scanner IP addresses.

   tb_euq_db_info
   Specify the EUQ database computer settings.

   tb_global_setting
   In section [cmagent] name [ConfigUrl], change the web console URL.

6. Start all IMSS services with the following command:

   ```
   $IMSS_Home/imss/script/imssstart.sh
   ```

How does IMSS process a partial message?

The key `BypassMessagePartial` in 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=/opt/trend/imss/log
event_log_path=/opt/trend/imss/log
policy_evt_log_path=/opt/trend/imss/log
```

Can IMSS 9.1 Patch 1 configure its own relay restrictions if a third-party upstream server is not installed?

No. IMSS 9.1 cannot configure its own relay restrictions as it does not have its own MTA on the Linux platform. You can only configure relay restrictions using a third-party MTA.

How can I modify the Access Control List (ACL) for the IMSS scanner?

You can modify the following settings in `imss.ini`.

- Add the target IP address to the parameter `smtp_allow_client_ip`.
- Alternatively, disable ACL check by setting `open_to_all_connections=yes`.
- To ensure that other computers are able to connect to the scanner, insert the target IP addresses in the parameter `proxy_smtp_server_ip`.

For more details, refer to the comments in `imss.ini`.

Why are messages from some senders always received as attachments? Why is the message body replaced by the disclaimer or stamp?

When the character set of the stamp is different from the character set of the message content, IMSS will encounter issues inserting the stamp into the message body after scanning the message. In this situation, IMSS will create a new message, insert the stamp into the message body, and attach the original message. The message content, however, will not be changed.

How can I specify a keyword expression to represent a blank header for matching fields such as "From", "To", or "Subject" when creating rules with the content filter?

If you are going to use a regular keyword expression to represent a blank header, Trend Micro recommends that you use "^(\s)*$" (without the quotation marks). The expression "^(\s)*$" (without the quotation marks) represents a blank header or whitespace characters.

For example, if you want to check if a message's **From** header is blank, edit a rule's scanning condition as follows:

Procedure

1. Go to **Policy** > **Policy List**.
2. Click the link for an existing rule to edit the rule.
3. Click **And scanning conditions match**.
4. Click **Header keyword expressions** under the **Content** section.
5. Click **Add** to create a new keyword expression.
6. Add the content as "^(\s)*$"" (without the quotation marks).

Why does the message size scan condition not work for encrypted messages?

IMSS treats encrypted messages as a special type of message. Most scan conditions do not apply. IMSS requires the use of the encrypted message scan condition to scan or perform actions on encrypted messages.

Troubleshooting Cloud Pre-Filter

Unable to Connect to Cloud Pre-Filter

If you cannot connect to Cloud Pre-filter, try the following:

- If there is a firewall on your test segment, verify that the firewall allows access through port 9000. Port 9000 is the default port that Cloud Pre-Filter uses to connect to the Cloud service. Open port 9000 if the firewall does not allow connection to the port.
- If you do not use a proxy server for connection to Cloud Pre-Filter, use the following command from IMSS to verify that IMSS can connect to Cloud Pre-Filter:

  ```
  telnet ws.emailsecurity.trendmicro.com 9000
  ```

- If you use a proxy server to connect to Cloud Pre-Filter, verify the proxy server allows access through port 9000.

Unable to Receive Messages from Cloud Pre-Filter

If you can connect to Cloud Pre-Filter but cannot receive the messages, verify the status of Cloud Pre-Filter by clicking the **Cloud Pre-Filter Status and Scheduled Maintenance Information** link on the **Cloud Pre-Filter Policy List** screen.

Appendices

Appendices

Appendix A

Technical Support

This appendix explains various Trend Micro resources and technical support information.

Topics include:

- *Troubleshooting Resources on page A-2*
- *Contacting Trend Micro on page A-4*
- *Sending Suspicious Content to Trend Micro on page A-5*
- *Other Resources on page A-6*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cyber security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to http://www.trendmicro.com/us/security-intelligence/index.html to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version

- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Email Reputation Services

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

https://ers.trendmicro.com/

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

http://esupport.trendmicro.com/solution/en-us/1036097.aspx

Web Reputation Services

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

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

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

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Download Center

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

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

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

TrendLabs

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

Appendix B

IMSS Scripts

This appendix provides you with a list of IMSS scripts and their respective parameters that you can invoke from the command line.

Topic includes:

- *Using IMSS Scripts on page B-2*

Using IMSS Scripts

IMSS scripts provide a convenient and alternative means of performing administrative tasks from the command line.

The following table lists the IMSS scripts, the respective parameters and the functions that the scripts perform.

Note

All scripts listed in the table are located in:

`/$IMSS_Home/imss/script`

TABLE B-1. IMSS Scripts

SCRIPT	PARAMETERS	DESCRIPTION
dbctl.sh	start / stop / status / reload / restart	Postgres database service
db_maintain.sh	{vacuum|reindex|analyze|all} [vacuum] - Vacuum admin db and all euq db. [reindex] - Reindex admin db and all euq db. [analyze] - Analyze admin db and all euq db. [all] - Vacuum && Reindex && Analyze.	Used by S99SCHEDULED for database maintenance. **Note** Do not run this script on its own.
euqtrans	all / approved sender	Transfers EUQ database data or approved senders
forceUpdate.sh	DBDSN username password	Notifies the policy server to reload the policy settings
foxproxyd	start / stop / restart	IP Profiler service

Script	Parameters	Description
ibe_server.sh	start / stop / restart	Trend Micro Email Encryption service
imssctl.sh	start / stop / stop_others / restart / restart_others / status	Controls all IMSS services
imssstop.sh	stop	Forces all IMSS services to stop.
imssstart.sh		Start all IMSS services
openldap.sh	start / stop / restart	Open LDAP local cache service
postfixctl.sh	start / stop / reload / restart	Postfix daemon
S99ADMINUI	start / stop / restart	Central Controller
S99CLEANEUQ		Removes expired quarantined data from the EUQ and admin databases as configured under the **Administration** > **User Quarantine Access** area of the management console.
S99CLEANEXPIRE		Removes expired quarantined and archived data from the EUQ and admin databases as configured under the **Quarantine & Archive** > **Settings** area of the management console.
S99CMAGENT	start / stop / restart / unregister / isregistered	CMAgent service
S99DIGEST		Sends the EUQ digest message
S99DTASAGENT	start / stop / restart	Virtual Analyzer agent service
S99EUQ	start / stop / restart	EUQ service
S99FOXDNS	start / stop / restart	Foxdns service
S99IMSS	start / stop / restart	IMSS scanner service
S99MANAGER	start / stop / restart	Manager service
S99MONITOR	start / stop / restart	Manager monitor service

SCRIPT	PARAMETERS	DESCRIPTION
S99POLICY	start / stop / restart	Policy service
S99REPORT	[option] start / stop / restart [option]: • `-s`: generates centralized reports (covers all one-time and scheduled reports configured on the management console) • `-h`: generates hourly individual traffic data • `-t`: generates hourly traffic data • `-d`: performs database log maintenance	Used by S99SCHEDULED to generate related reports. **Note** Do not run this script on its own.
S99SCHEDULED	start / stop	Starts the scheduled task.
S99UPDATE	start / stop / restart	Used by S99SCHEDULED to run the scheduled update. **Note** Do not run this script on its own.
S99WRSAGENT	start / stop / restart	WRS agent service

Appendix C

Default Directory Locations

This appendix provides information on the default directory locations that IMSS uses for email processing.

Topics include:

- *Default Mail Queues on page C-2*
- *eManager, Virus, and Program Logs on page C-3*
- *Temporary Folder on page C-3*
- *Notification Pickup Folder on page C-4*

Default Mail Queues

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

TABLE C-1. Default IMSS Mail Locations

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_malform= `/opt/trend/imss/queue/malform`	N/A	Stores malformed messages.
queue_archive= `/opt/trend/imss/queue/archive`	N/A	Stores archived messages.
queue_quarantine = `/opt/trend/imss/queue/quarantine`	N/A	Stores quarantined messages.
queue_notify= `/opt/trend/imss/queue/notify`	queue_notify_big= `/opt/trend/imss/queue/notifybig`	Stores notification messages.
queue_postpone= `/opt/trend/imss/queue/postpone`	queue_postpone_big= `/opt/trend/imss/queue/postponebig`	Stores postponed messages.
queue_deliver= `/opt/trend/imss/queue/deliver`	queue_deliver_big= `/opt/trend/imss/queue/deliverbig`	Stores messages for final delivery.
queue_reprocess= `/opt/trend/imss/queue/reprocess`	queue_reprocess_big= `/opt/trend/imss/queue/reprocessbig`	Stores messages pending reprocessing.

Queues for Regular Mails	Queues for Large Mails	Descriptions
queue_handoff= `/opt/trend/imss/queue/handoff`	queue_handoff_big= `/opt/trend/imss/queue/handoffbig`	Stores messages pending handoff.
queue_undeliverable= `/opt/trend/imss/queue/undeliverable`	N/A	Stores undeliverable messages.
queue_unnotify= `/opt/trend/imss/queue/unnotify`	N/A	Stores undeliverable notification messages.
`/opt/trend/imss/queue/dtas_upload`	N/A	Stores messages pending analysis or being analyzed by Virtual Analyzer.

eManager, Virus, and Program Logs

Many modules in IMSS write log information for troubleshooting purposes to the following folder:

- `/opt/trend/imss/log`
- `/var/log`

Temporary Folder

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

- `/opt/trend/imss/temp/`
- `/tmp`

Note

This directory is not configurable.

Notification Pickup Folder

IMSS stores all notification messages, picks them up from the following folders, and then delivers them to a specified SMTP notification server:

`/opt/trend/imss/queue/notify/`

and

`/opt/trend/imss/queue/notifybig`

Configuring the SMTP Notification Server

For details, see *Configuring SMTP Settings on page 10-3*.

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, 29-23
    product, 29-24
add
    administrator accounts, 29-2
address group
    add, 14-6
    delete, 14-9
    edit, 14-9
address groups
    examples of, 14-2
    understand, 14-2
administrator accounts
    add, 29-2
    delete, 29-5
    edit, 29-5
    manage, 29-2
Advanced Threat Scan Engine, 6-2
adware, 1-11
antivirus rule, 17-10
APOP, 12-4
approved list
    add hosts, 9-5
approved senders list
    configure, 17-19
archive
    configure settings, 25-2
archive areas
    manage, 25-6
archived messages
    view, 25-17
asterisk wildcard
    use, 20-15
attachment size
    scanning conditions, 17-35
audience, xx

B

back up
    IMSS, 27-4
blocked list
    add records, 9-6
blocked senders list
    configure, 17-19
bounced mail settings
    configure, 9-13

C

change
    management console password, 2-3
Cloud Pre-Filter
    configure DNS MX records, 8-14
    create account, 5-5
    create policy, 8-3
    policies, 8-2
    suggested settings, 8-15
    troubleshoot, 31-36
    understand, 5-2
    verify it works, 8-14
Cloud Pre-Filter tab, 22-5
Command & Control (C&C) Contact Alert Services, 1-22
commands, B-2
community, A-2
component update, 4-6
condition statements, 14-44

Configuration Wizard
accessing, 3-2
configure
approved senders list, 17-19
archive settings, 25-2
blocked senders list, 17-19
connection settings, 10-4, 29-6
Control Manager server settings, 3-11
database maintenance schedule, 29-19
delivery settings, 26-2
Direct Harvest Attack (DHA) settings, 9-11
DNS MX records, 8-14
Email reputation, 9-14
encrypted message scan actions, 19-8
expressions, 14-14
internal addresses, 3-9, 15-2
LDAP settings, 29-7
log settings, 24-2
Messaged Delivery settings, 10-12
Message Rule settings, 10-8
notification messages, 26-5
notification settings, 3-2
other scanning exceptions scan actions, 19-5, 19-9
POP3 settings, 12-4, 29-12
product settings, 3-12
quarantine settings, 25-2
route, 17-7
scan exceptions, 19-2
scheduled reports, 23-8
security setting violation exceptions, 19-3, 19-7
security setting violation scan actions, 19-4
Sender Filtering, 9-4
Sender Filtering bounced mail settings, 9-13
Sender Filtering spam settings, 9-7
Sender Filtering virus settings, 9-9
SMTP routing, 10-2
SMTP settings, 10-3
spam text exemption rules, 17-20
TMCM settings, 29-15
update source, 3-4
Web EUQ Digest settings, 26-8
configure event criteria, 26-5
configuring
Encryption settings, 18-2
connection settings
configure, 10-4, 29-6
Control Manager
enable agent, 27-7
replicate settings, 27-9
see Trend Micro Control Manager, 1-16
Control Manager server settings
configure, 3-11
Conventional scan, 16-8
criteria
customized expressions, 14-31
keywords, 14-40, 14-41
customized expressions, 14-30, 14-31, 14-35
criteria, 14-31
importing, 14-35
customized keywords, 14-40
criteria, 14-40, 14-41
importing, 14-42

customized templates, 14-44
creating, 14-45
importing, 14-47

D

dashboard
using, 22-2
database
configure maintenance schedule, 29-19
data identifiers, 14-28
expressions, 14-28
file attributes, 14-28
keywords, 14-28
Data Loss Prevention, 14-28
data identifiers, 14-28
expressions, 14-29–14-31, 14-35
file attributes, 14-35, 14-37
keywords, 14-38–14-42
templates, 14-43–14-45, 14-47
Data Loss Prevention (DLP), 14-28
default tabs, 22-3
delete
address group, 14-9
administrator accounts, 29-5
delivery settings
configure, 26-2
dialers, 1-11
Direct Harvest Attack (DHA) settings
configure, 9-11
display
domains, 9-17
suspicious IP addresses, 9-17
DLP, 14-28
documentation, xxi
domains
display, 9-17
Email Encryption, 7-4, 7-5

E

edit
address group, 14-9
administrator accounts, 29-5
Email Encryption
managing domains, 7-4
registering domains, 7-5
understand, 7-2
email relay, 10-8
Email reputation, xix
about, 1-13
Administration Console, 9-4
configure, 9-14
enable, 9-4
types, 1-14
email threats
spam, 1-5
unproductive messages, 1-5
enable
Control Manager agent, 27-7
Email reputation, 9-4
End-User Access, 28-8
EUQ, 28-3
IP Profiler, 9-4
POP3 scanning, 12-3
sender filtering rules, 9-7
encrypting messages, 18-3
Encryption settings
configuring, 18-2
End-User Access
enable, 28-8
ERS
MTA settings, 9-3
using, 9-2
EUQ, 28-2

authentication, 28-2
disable, 28-16
enable, 28-3
open the console, 28-13
start, 28-7
web console, 28-13
Web console, 2-7
event criteria
configure, 26-5
event notifications, 26-2
export notes, 27-2
expression lists
manage, 14-13
expressions, 14-28, 14-29
configure, 14-14
customized, 14-30, 14-35
criteria, 14-31
predefined, 14-29
regular, 14-21

F

FAQ
ERS, 31-20
EUQ, 31-24
IMSS components, 31-19
IP Profiler, 31-20
mail areas, 31-22
postfix, 31-18
queues, 31-22
file attributes, 14-28, 14-35, 14-37
creating, 14-37
importing, 14-37
wildcards, 14-37
File Reputation Services, 1-19, 16-2
filtering, how it works, 1-7
filters
examples of, 14-2

G

generate
reports, 23-2
graymail, 1-21

H

hacking tools, 1-11

I

import notes, 27-2
IMSA
scripts, B-2
IMSS
about, 1-2
backing up, 27-4
restore, 27-6
scripts, B-2
internal addresses
configure, 3-9, 15-2
IP Profiler, xix
enable, 9-4

J

joke program, 1-11

K

keywords, 14-28, 14-38
customized, 14-40–14-42
predefined, 14-39
known hosts, 11-2
add, 11-3
export, 11-4
import, 11-4

L

LDAP settings
configure, 3-6, 29-7
LDAP User or Group

search for, 15-6
license
activate, 29-23
renew, 29-23
logical operators, 14-44
logs, 24-2
configure settings, 24-2
query, 24-6
query message tracking, 24-10
query MTA event, 24-20
query policy event, 24-14
query quarantine event, 24-17
query sender filtering, 24-20
query system event, 24-12
query URL click tracking, 24-18

M

manage
administrator accounts, 29-2
expression lists, 14-13
notifications list, 14-47
one-time reports, 23-5
product licenses, 29-20
manage domains for Email Encryption, 7-4
management console password
change, 2-3
manual update, 4-4
mass mailing viruses
pattern, 1-6
message delivery, 10-12
Message Delivery settings
configure, 10-12
Message Rule settings
configure, 10-8
messages in the Virtual Analyzer queue
view, 25-19
message size
scanning conditions, 17-36
message traffic tab, 22-4
MIME content type
scanning conditions, 17-34
MTA
with ERS, 9-3

N

new features, xii
notes
export, 27-2
import, 27-2
notification messages
configure, 26-5
notifications
event, 26-2
notification settings
configure, 3-2
notifications list
manage, 14-47

O

one-time reports
manage, 23-5
online
community, A-2
online help, xxi
other rule, 17-11

P

password
management console, 2-3
password cracking applications, 1-11
pattern files
update, 4-2

PCRE, 14-30
Perle Compatible Regular Expressions, 14-30
permitted senders, 10-10
policies
    add, 17-2
    example 1, 20-5
    finalize, 17-48
policy management
    DLP, 14-28
policy notification
    add, 14-49
    edit, 14-49
POP3 messages
    scan, 12-2
POP3 scanning
    enable, 12-3
POP3 settings
    configure, 12-4, 29-12
postponed messages
    view, 25-18
predefined expressions, 14-29
    viewing, 14-29
predefined keywords
    distance, 14-39
    number of keywords, 14-39
predefined templates, 14-44
product licenses
    manage, 29-20
    view, 29-21
product services, 2-6
product settings
    configure, 3-12

Q

quarantine
    configure settings, 25-2
quarantine and archive, 25-2
quarantine areas
    manage, 25-4
quarantined messages
    view, 25-15
query
    archive areas, 25-11
    logs, 24-6
    messages, 25-9
    messages in the Virtual Analyzer queue, 25-14
    MTA event logs, 24-20
    policy event logs, 24-14
    postponed messages, 25-13
    quarantine areas, 25-9
    quarantine event logs, 24-17
    sender filtering logs, 24-20
    system event logs, 24-12
    URL click tracking logs, 24-18

R

readme file, xxi
register domains for Email Encryption, 7-5
remote access tools, 1-11
renew
    license, 29-23
replicating settings, 27-7
reports
    content, 23-2
    generate, 23-2
    manage one-time, 23-5
    scheduled reports, 23-8, 23-11
restore
    IMSS, 27-6
roll back
    components, 4-5

route
configure, 17-7
specify, 17-2

S

scan
POP3 messages, 12-2
SMTP messages, 10-2
scan actions
configure encrypted message settings, 19-8
configure other scanning exceptions settings, 19-5, 19-9
scan engine
update, 4-2
scan exceptions
configure, 19-2
Scan methods, 16-7
scanning conditions, 17-34
attachment names, 17-33
attachment number, 17-35
attachments, 17-32
attachment size, 17-35
extensions, 17-33
message size, 17-36
MIME content type, 17-34
spam, 17-17
specify, 17-10
true file type, 17-34
scheduled reports
access, 23-8
configure, 23-8
use, 23-11
scheduled updates, 4-7
security risks
spyware/grayware, 1-11
security setting violations
configure exceptions, 19-3, 19-7
configure scan actions, 19-4
Sender Filtering
configure, 9-4
configure bounced mail settings, 9-13
configure Direct Harvest Attack (DHA) settings, 9-11
configure spam settings, 9-7
configure virus settings, 9-9
Sender Filtering Service
about, 9-2
Sender Filtering tab, 22-4
services, 2-6
Sender Filtering Service, 9-2
smart protection, 16-6
source, 16-6
sources
comparison, 16-6
protocols, 16-6
Smart Protection, 1-19, 16-2
Smart Protection Network, 1-21, 16-3
Smart Scan, 16-8
SMTP
notification server, C-4
SMTP messages
scan, 10-2
SMTP routing, 10-3
configure, 10-2
SMTP settings
configure, 10-3
spam settings
configure, 9-7
spam text exemption rules
configure, 17-20
specify

actions, 17-41
route, 17-2
scanning conditions, 17-10
update source, 4-3
spyware/grayware, 1-11
adware, 1-11
dialers, 1-11
entering the network, 1-12
hacking tools, 1-11
joke program, 1-11
password cracking applications, 1-11
remote access tools, 1-11
risks and threats, 1-12
start
EUQ, 28-7
support
knowledge base, A-2
resolve issues faster, A-4
TrendLabs, A-7
suspicious IP addresses
display, 9-17
system overview tab, 22-3
System Status screen, 21-2

T

tabs
add a tab, 22-5
Cloud Pre-Filter, 22-5
configure a tab, 22-6
default tabs, 22-3
message traffic, 22-4
Sender Filtering, 22-4
system overview, 22-3
understand, 22-2
tag subject
add, 17-47
templates, 14-43–14-45, 14-47
condition statements, 14-44
customized, 14-44, 14-45, 14-47
logical operators, 14-44
predefined, 14-44
TMCM settings
configure, 29-15
transport layer, 10-7
TrendLabs, A-7
Trend Micro Control Manager, 1-16
agent, 1-16
server, 1-16
troubleshooting, 31-2
imssps daemon, 31-2
true file type, 17-34

U

understand
Email Encryption, 7-2
widgets, 22-6
update
automatically, 4-7
manually, 4-4
pattern files, 4-2
scan engine, 4-2
system and application, 30-2
update source
configure, 3-4
specify, 4-3

V

view
archived messages, 25-17
messages in the Virtual Analyzer queue, 25-19
postponed messages, 25-18
product licenses, 29-21

quarantined messages, 25-15
Virtual Analyzer, 6-4
virus settings
configure, 9-9

W

Web EUQ Digest
configure settings, 26-8
Web Reputation Services, 1-20, 16-2
what's new, xii
widgets
add a widget, 22-9
configure a widget, 22-8
edit a widget, 22-8
understanding, 22-6
using a widget, 22-7
wildcards, 14-37
file attributes, 14-37

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: MSEM98750/190801