9.1

InterScan™ Messaging Security Suite

Patch 1

Installation Guide

Comprehensive threat protection at the Internet messaging gateway

for LINUX™

Messaging Security

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

http://docs.trendmicro.com/en-us/home.aspx

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

Document Part No.: MSEM98751/190801

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

Table of Contents

About this Manual

About this Manual v

What's New vi

Audience xiv

InterScan Messaging Security Suite Documentation xv

Document Conventions xv

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

How Spyware/Grayware Gets into Your Network 1-12

Potential Risks and Threats 1-12

About Web Reputation Services 1-13

About Email Reputation 1-13

Types of Email Reputation 1-14

How Email Reputation Technology Works 1-15

About Trend Micro Control Manager 1-16

Control Manager Support 1-17

About Trend Micro Smart Protection 1-19

The Need for a New Solution 1-20

Trend Micro Smart Protection Network 1-21

About Graymail Scanning 1-21

About Command & Control (C&C) Contact Alert Services 1-22

Chapter 2: Component Descriptions

About IMSS Components 2-2

Cloud Pre-Filter Service Overview 2-2
Sender Filtering 2-2
Reputation-Based Source Filtering 2-2
Virus and Spam Protection 2-3

About Spam Prevention Solution 2-3
Spam Prevention Solution Technology 2-3
Using Spam Prevention Solution 2-3

About Sender Filtering 2-3
How IP Profiler Works 2-4

About End-User Quarantine (EUQ) 2-5

About Centralized Reporting 2-5

Chapter 3: Planning for Deployment

Deployment Checklist 3-2

IMSS Ports 3-5

Network Topology Considerations 3-8
Installing without a Firewall 3-8
Installing in Front of a Firewall 3-9
Installing Behind a Firewall 3-10
Installing in the De-Militarized Zone 3-11

About Device Roles 3-12

About Device Services 3-13
Service Selection 3-13
Deployment with Sender Filtering 3-14

Understanding POP3 Scanning 3-14
Requirements for POP3 Scanning 3-14
Configuring a POP3 Client that Receives Email Through IMSS 3-15

Opening the IMSS Management Console 3-15

About Operating Models 3-16
The Standalone Model 3-18
The Sandwich Model 3-22
The Proxy Model 3-27

Chapter 4: Installation and Uninstallation

System Requirements 4-2
Preparing the Message Transfer Agents 4-5
Preparing Postfix 4-5
About Sendmail 4-6
Installing IMSS 4-13
Using Sender Filtering with Sendmail 4-15
Integrating FoxLib with Sendmail on Red Hat 6 4-15
Integrating FoxLib with Sendmail on Red Hat 7 or 8 4-18
Using Sender Filtering with Postfix 4-20
Verifying the Installation 4-21
About IPv6 Support 4-21
Configuring the Server for IPv6 4-22
Configuring IMSS for IPv6 Support 4-23
Uninstalling IMSS 4-27

Chapter 5: Upgrading from Previous Versions

Upgrading from an Evaluation Version 5-2
Upgrading to IMSS Linux 9.1 5-4
Data Transfer Considerations 5-4
Upgrading from IMSS Linux 7.1 SP2 Patch 1 to IMSS Linux 9.1 5-5
Upgrading to IMSS Linux 9.1 Patch 1 5-20
Migrating from Previous Versions to Linux 9.1 5-21
Migrating to IMSS Linux 9.1 5-22
Exporting Debugging Files 5-24

Chapter 6: Frequently Asked Questions

Postfix MTA Settings 6-2
If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally? 6-2
Installation / Uninstallation 6-3
Is there any problem if I install IMSS 9.1 on a computer with an external DNS server? 6-3
Is there any problem if I install IMSS 9.1 on a computer with an existing Apache Server? 6-3

Appendix A: Technical Support

Troubleshooting Resources A-2
Trend Community A-2
Using the Support Portal A-2
Security Intelligence Community A-3
Threat Encyclopedia A-3
Contacting Trend Micro A-4
Speeding Up the Support Call A-4
Sending Suspicious Content to Trend Micro A-5
File Reputation Services A-5
Email Reputation Services A-5
Web Reputation Services A-5
Other Resources A-6
TrendEdge A-6
Download Center A-6
TrendLabs A-7

Index

Index IN-1

Preface

About this Manual

Welcome to the Trend Micro™ InterScan™ Messaging Security Suite Installation Guide. This manual contains information about InterScan Messaging Security Suite (IMSS) features, system requirements, as well as instructions on installing and upgrading IMSS settings.

Refer to the *IMSS 9.1 Patch 1 Administrator's Guide* for information about configuring IMSS settings and the Online Help in the management console for detailed information about each field on the user interface.

Topics include:

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

What's New

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

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

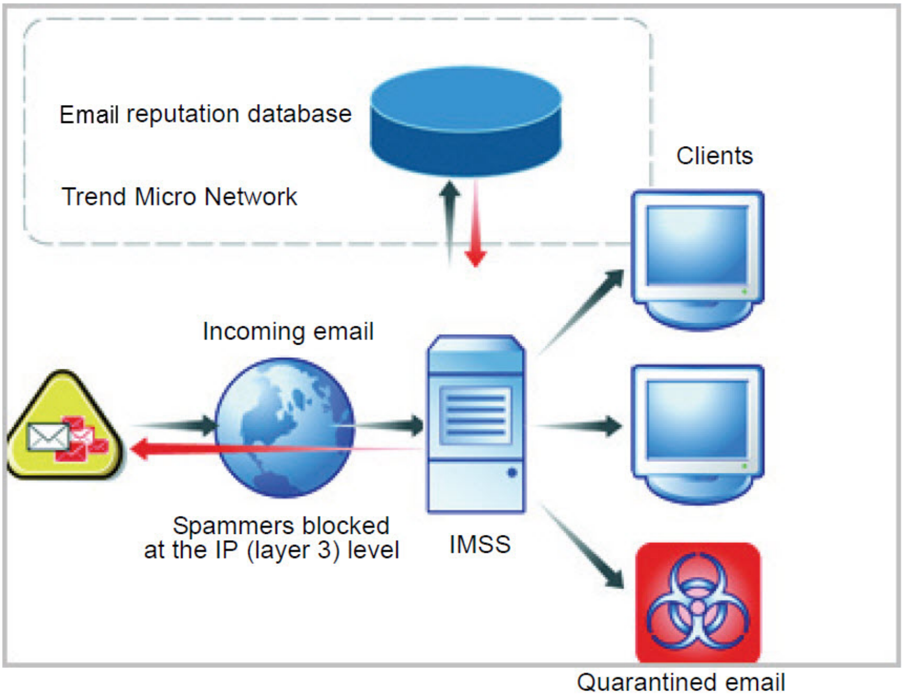
Trend Micro Email reputation technology is a Domain Name Service (DNS) query-based service. The following process takes place after IMSS receives a connection request from a sending mail server:

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.


Email reputation database
Trend Micro Network
Clients
Incoming email
Spammers blocked at the IP (layer 3) level
IMSS
Quarantined email

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

Component Descriptions

This chapter explains the requirements necessary to manage the product and the various software components it needs to function.

Topics include:

- *About IMSS Components on page 2-2*
- *Cloud Pre-Filter Service Overview on page 2-2*
- *About Spam Prevention Solution on page 2-3*
- *About Sender Filtering on page 2-3*
- *About End-User Quarantine (EUQ) on page 2-5*
- *About Centralized Reporting on page 2-5*

About IMSS Components

The new architecture of IMSS separates the product into distinct components that each perform a particular task in message processing. The following sections provide an overview of each component.

You can install IMSS components on a single computer or on multiple computers.

Cloud Pre-Filter Service Overview

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

Sender Filtering

By approving senders, Cloud Pre-Filter Service subscribers automatically allow messages from trusted mail servers or email addresses. Messages from approved senders are not checked for spam or source reputation. Messages from approved senders are scanned for viruses.

By blocking senders, subscribers automatically block messages from untrusted sources.

Reputation-Based Source Filtering

With Trend Micro Email Reputation, Cloud Pre-Filter service verifies email sources against dynamic and self-updating reputation databases to block messages from the latest botnets and other IP addresses controlled by spammers, phishers, and malware distributors.

Virus and Spam Protection

With Trend Micro antivirus technology, Cloud Pre-Filter Service protects against infectious messages from mass-mailing worms or manually crafted messages that contain Trojans, spyware, or other malicious code.

Cloud Pre-Filter Service checks messages for spam characteristics to effectively reduce the volume of unsolicited messages.

About Spam Prevention Solution

Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam-detection services to other Trend Micro products. The SPS license is included in the **Trend Micro Antivirus and Content Filter** license. For more information, contact to your sales representative.

Spam Prevention Solution Technology

SPS uses detection technology 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 spammers change their techniques.

Using Spam Prevention Solution

SPS works through a built-in spam filter that automatically becomes active when you register and activate the **Spam Prevention Solution** license.

About Sender Filtering

IMSS includes optional Sender Filtering, which consists of the following parts:

IP Profiler

Allows you to configure threshold settings used to analyze email traffic. When traffic from an IP address violates the settings, IP Profiler adds the IP address of the sender to its database and then blocks incoming connections from the IP address.

IP profiler detects any of these four potential Internet threats:

- **Spam**: Email messages with unwanted advertising content.
- **Viruses**: Various virus threats, including Trojan programs.
- **Directory Harvest Attack (DHA)**: A method used by spammers to collect valid email addresses by generating random email addresses using a combination of random email names with valid domain names. Emails are then sent to these generated email addresses. If an email message is delivered, the email address is determined to be genuine and thus added to the spam databases.
- **Bounced Mail**: An attack that uses your mail server to generate email messages that have the target's email domain in the "From" field. Fictitious addresses send email messages and when they return, they flood the target's mail server.

Email Reputation

Blocks email from known spam senders at the IP-level.

How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email messages containing threats mentioned in the section *About Sender Filtering on page 2-3*. You can customize several criteria that determine when IMSS starts taking a specified action on an IP address. The criteria differ depending on the potential threat, but commonly include a duration during which IMSS monitors the IP address and a threshold.

To accomplish this, IP Profiler makes use of several components, the most important of which is **Foxproxy**—a server that relays information about email traffic to IMSS.

The following process takes place after IMSS receives a connection request from a sending mail server:

1. FoxProxy queries the IP Profiler's DNS server to see if the IP address is on the blocked list.

2. If the IP address is on the blocked list, IMSS denies the connection request.

   If the IP address is not on the blocked list, IMSS analyzes the email traffic according to the threshold criteria you specify for IP Profiler.

3. If the email traffic violates the criteria, IMSS adds the sender IP address to the blocked list.

About End-User Quarantine (EUQ)

IMSS provides web-based EUQ to improve spam management. The Web-based EUQ service allows end users to manage their own spam quarantine. Messages that Spam Prevention Solution (licensed separately from IMSS), or administrator-created content filters, determine to be spam, are placed into quarantine. These messages are indexed into a database by the EUQ agent and are then available for end users to review and delete or approve for delivery.

About Centralized Reporting

To help you analyze how IMSS is performing, use the centralized reporting feature. You can configure one time (on demand) reports or automatically generate reports (daily, weekly, and monthly). IMSS allows you to send both one-time and scheduled reports through email.

Chapter 3

Planning for Deployment

This chapter explains how to plan for IMSS deployment.

Topics include:

- *Deployment Checklist on page 3-2*
- *IMSS Ports on page 3-5*
- *Network Topology Considerations on page 3-8*
- *About Device Roles on page 3-12*
- *About Device Services on page 3-13*
- *Understanding POP3 Scanning on page 3-14*
- *Opening the IMSS Management Console on page 3-15*
- *About Operating Models on page 3-16*

Deployment Checklist

The deployment checklist provides step-by-step instructions on the pre-installation and post-installation tasks for deploying IMSS.

1. Identify the location of IMSS

Tick when completed	Tasks	Optional	Reference
	Select one of the following locations on your network where you would like to install IMSS.		
	Without a firewall		*Installing without a Firewall on page 3-8*
	In front of a firewall		*Installing in Front of a Firewall on page 3-9*
	Behind a firewall		*Installing Behind a Firewall on page 3-10*
	In the De-Militarized Zone		*Installing in the De-Militarized Zone on page 3-11*

2. Install or Upgrade

Tick when complete d	Tasks	Optional	Reference
	Perform a fresh installation of IMSS or upgrade from a previous version.		
	Prepare MTA		*Preparing the Message Transfer Agents on page 4-5*
	Install IMSS components		*Installing IMSS on page 4-13*

Tick when completed	Tasks	Optional	Reference
	Upgrade from a previous version		*Upgrading from Previous Versions on page 5-1*
	Verify that installation is successful		*Verifying the Installation on page 4-21*

3. Configure basic IMSS settings

Tick when completed	Tasks	Optional	Reference
	Configure the Central Controller through the Configuration Wizard.		
	Configure settings using the Configuration Wizard		Performing Basic Configuration with the Configuration Wizard section of the *Administrator's Guide*

4. Start services

Tick when completed	Tasks	Optional	Reference
	Activate IMSS services to start protecting your network against various threats.		
	Scanner		IMSS Services section of the *Administrator's Guide*
	Policy		
	EUQ	Yes	

5. Configure other IMSS settings

Tick when complete d	Tasks	Option al	Reference
	Configure various IMSS settings to get IMSS up and running.		
	Sender Filtering Rules	Yes	Sender Filtering Service section of the *Administrator's Guide*
	SMTP Routing		Scanning SMTP Messages section of the *Administrator's Guide*
	POP3 Settings	Yes	Scanning POP3 Messages section of the *Administrator's Guide*
	Policy and scanning exceptions		Managing Policies section of the *Administrator's Guide* **Note** If scanning for graymail messages, make sure that the DNS configuration and DNS query are correct.
	Perform a manual update of components and configure scheduled updates		Updating Scan Engine and Pattern Files section of the *Administrator's Guide*
	Log settings		Configuring Log Settings section of the *Administrator's Guide*

6. Back up IMSS

Tick when completed	Tasks	Optional	Reference
	Perform a full or minimal backup of IMSS as a precaution against system failure.		
	Full backup		Backing Up IMSS section of the *Administrator's Guide*.
	Minimal backup		

IMSS Ports

The following tables outline all ports used by IMSS in their default configuration.

Table 3-1. IMSS Ports

Port Number	Component and Role	Configuration Location
25	The MTA service port. The mail server will listen at this port to accept messages. This port must be opened at the firewall, or the server is not able to accept mails.	Go to **Administration** > **IMSS Configuration** > **SMTP Routing** > **Connections**.
110	IMSS scanner generic POP3 port. The scanner uses this port to accept POP3 request and scan POP3 mails for all POP3 servers.	Go to **Administration** > **IMSS Configuration** > **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**.

Port Number	Component and Role	Configuration Location
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.

Network Topology Considerations

This section illustrates different ways to deploy IMSS based on the location of firewalls on your network.

Deploy IMSS in an existing messaging environment at the SMTP gateway. This section provides a description of where IMSS fits in various network topologies, with illustrations of each scenario and general instructions for configuring other gateway services.

Note

The illustrations below assume a single-server installation of IMSS. Since any IMSS installation functions as a logical unit, the same topologies would apply to a distributed deployment installation. However, as IMSS does not handle the distribution of messages between scanners, you need to use third-party software or a switch to balance the traffic between multiple instances of the IMSS scanner component.

Installing without a Firewall

The following figure illustrates how to deploy IMSS and Postfix when your network does not have a firewall.

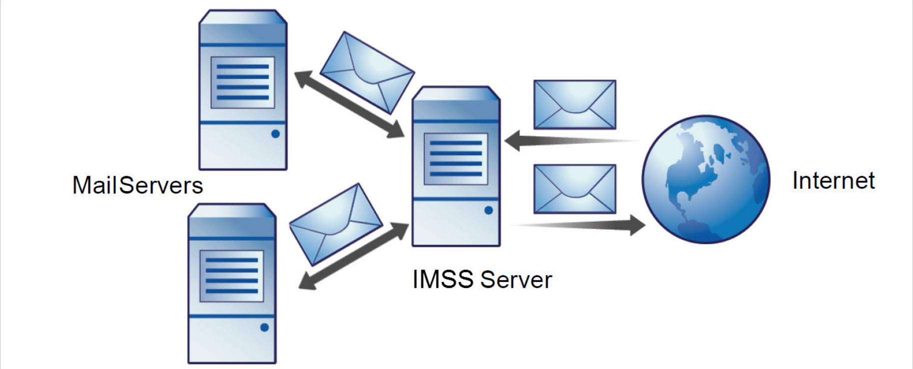


FIGURE 3-1. Installation topology: no firewall

Note

Trend Micro does not recommend installing IMSS without a firewall. Placing the server hosting IMSS at the edge of the network may expose it to security threats.

Installing in Front of a Firewall

The following figure illustrates the installation topology when you install IMSS in front of your firewall.

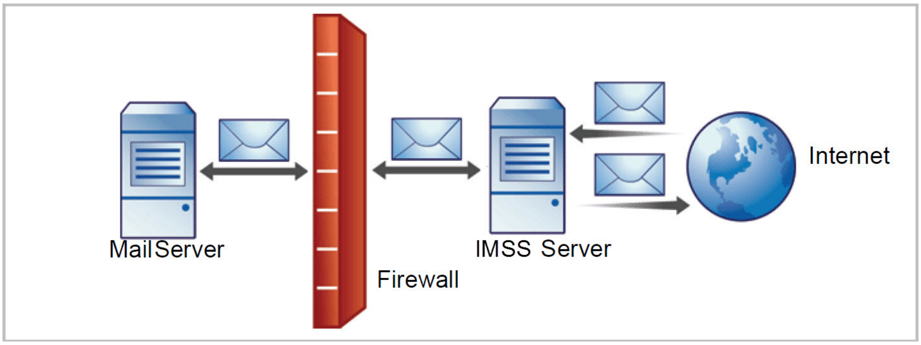


FIGURE 3-2. Installation topology: in front of the firewall

Incoming Traffic

- Postfix should receive incoming messages first, then transfer them to IMSS. Configure IMSS to reference your SMTP server(s) and configure the firewall to permit incoming traffic from the IMSS server.
- Configure the Relay Control settings to only allow relay for local domains.

Outgoing Traffic

- Configure the firewall (proxy-based) to route all outbound messages to IMSS, so that:

  - Outgoing SMTP messages can only go to Postfix first and then go to IMSS servers.
  - Incoming SMTP messages only come from IMSS servers.
- Configure IMSS to allow internal SMTP gateways to relay, through Postfix, to any domain through IMSS.

Tip

For more information, see the *Configuring SMTP Routing* section of the *IMSS Administrator's Guide*.

Installing Behind a Firewall

The following figure illustrates how to deploy IMSS behind your firewall.

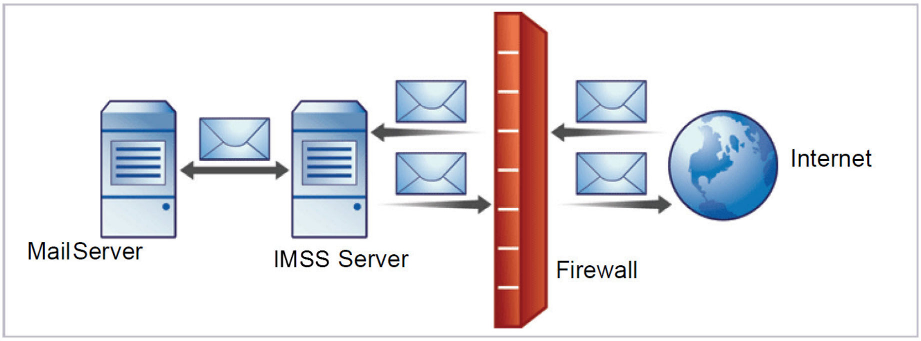


FIGURE 3-3. Installation scenario: behind a firewall

Incoming Traffic

- Configure your proxy-based firewall, as follows:
  - Outgoing SMTP messages go to Postfix first and then to the IMSS server or the switch performing load balancing between scanners.
  - Incoming SMTP messages go first to Postfix, then to IMSS, and then to the SMTP servers in the domain.

- Configure your packet-based firewall, as follows:
    - Change the MX records on the DNS server that currently reference your SMTP gateway to reference the address of the server hosting IMSS.
    - Point your MX records to IMSS or the firewall, if you configured it to manage a secure subnet.
- Configure IMSS to route messages destined for your local domain(s) to the SMTP gateway or your internal mail server.
- Configure relay restriction to only allow relay for local domain(s).

Outgoing Traffic

- Configure all internal SMTP gateways to send outgoing messages to Postfix and then to IMSS servers.
- If you are replacing your SMTP gateway with IMSS, configure your internal mail server to send outgoing messages through Postfix and then to IMSS servers.
- Configure Postfix and IMSS to route all outgoing messages (to domains other than local), to the firewall, or deliver the messages.
- Configure IMSS to allow internal SMTP gateways to relay to any domain using IMSS.

Tip

For more information, see the **Configuring SMTP Routing** section of the *IMSS Administrator's Guide*.

Installing in the De-Militarized Zone

You can also install IMSS and Postfix in the De-Militarized Zone (DMZ).

Incoming Traffic

- Configure your proxy-based firewall, so that incoming and outgoing SMTP messages can only go from the DMZ to the internal email servers.
- Configure your packet-based firewall.
- Configure Postfix and IMSS to route email messages destined for your local domain(s) to the SMTP gateway or your internal mail server.

Outgoing Traffic

- Configure Postfix to route all outgoing messages (destined for domains other than the local domains) to the firewall or deliver them using IMSS .
- Configure all internal SMTP gateways to forward outgoing mail to Postfix and then to IMSS.
- Configure IMSS to allow internal SMTP gateways to relay to any domain, through Postfix and IMSS.

Tip

For more information, see the **Configuring SMTP Routing** section of the *IMSS Administrator's Guide*.

About Device Roles

IMSS can act as a parent or child device. Parent and child devices compose a group, where the parent provides central management services to the child devices registered to it.

- **Parent**: Manages child devices. If you are deploying a single IMSS device, select **parent mode** during setup so that all IMSS components are deployed.
- **Child**: Managed by a single parent device and uses all global settings that you configure through the parent device’s management console.

A **group** refers to a parent device with at least one child device registered to it.

About Device Services

You can enable different kinds of services on IMSS devices.

Parent-only services:

- **Admin user interface service (management console)**: Manages global settings.

Parent and child services:

- **Policy service**: Manages the rules that you configure.
- **Scanner service**: Scans email traffic.
- **EUQ service**: Manages End-User Quarantine, which allows your users to view their messages that IMSS determined were spam.

A child device is functional only when it is registered to a parent.

Service Selection

You can enable different types of services on parent and child devices. For example, to increase throughput, add more child devices, enable all their services and allow the child devices to scan traffic and provide EUQ services.

You can deploy IMSS devices in a parent/child group in either deployment scenario. However, if you enable the scanner service on parent and child devices, you must use the same type of deployment for all devices in a single group. You cannot deploy some child devices at the gateway and others behind the gateway.

In addition to the above SMTP-scanning scenarios, you might want IMSS to scan POP3 traffic. See *Understanding POP3 Scanning on page 3-14* for more information.

Deployment with Sender Filtering

The Trend Micro Sender Filtering, which includes IP Profiler, Email Reputation and SMTP Traffic Throttling, blocks connections at the IP level.

To use Sender Filtering, any firewall between IMSS and the edge of your network must not modify the connecting IP address as Sender Filtering is not compatible with networks using network address translation (NAT). If IMSS accepts SMTP connections from the same source IP address, for instance, Sender Filtering will not work, as this address would be the same for every received message and the sender filtering software would be unable to determine whether the original initiator of the SMTP session was a known sender of spam.

Understanding POP3 Scanning

In addition to SMTP traffic, IMSS can scan POP3 messages at the gateway as your clients retrieve them. Even if your company does not use POP3 email, your employees might access personal, web-based POP3 email accounts, which can create points of vulnerability on your network if the messages from those accounts are not scanned.

The most common email scanning deployments will use IMSS to scan SMTP traffic, which it does by default. However, to scan POP3 traffic that your organization might receive from a POP3 server over the Internet, enable POP3 scanning.

With POP3 scanning enabled, IMSS acts as a proxy, positioned between mail clients and POP3 servers, to scan messages as the clients retrieve them.

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.

Requirements for POP3 Scanning

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

Note

If you disable POP3 scanning, your clients cannot receive POP3 mail.

Configuring a POP3 Client that Receives Email Through IMSS

To configure a POP3 client using a generic POP3 connection, configure the following:

- **IP address/Domain name**: The IMSS IP address or domain name
- **Port**: IMSS Generic POP3 port
- **Account**: account_name#POP3_Server_Domain-name

  For example: user#10.18.125.168

To configure a POP3 client using dedicated POP3 connections, configure the following:

- **IP address**: The IMSS IP address
- **Port**: The IMSS dedicated POP3 port
- **Account**: account_name

  For example: user

Opening the IMSS Management Console

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

To view the console in a browser, go to the following URL:

https://{IMSS}:8445

where {IMSS} refers to the IP address or Fully Qualified Domain Name.

For example: `https://196.168.10.1:8445` or `https://IMSS1:8445`

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN). To view the management console using SSL, type "https://" before the domain name and append the port number after it.

The default logon credentials are as follows:

- Administrator user name: **admin**
- Password: **imss9.1**

Type the logon credentials the first time you open the console and click **Log on**.

WARNING!

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.

Note

If you are using Internet Explorer (IE) to access the management console, IE will block the access and display a popup dialog box indicating that the certificate was issued from a different web address. Simply ignore this message and click **Continue to this website** to proceed.

About Operating Models

You can deploy IMSS in different ways depending on how the IMSS server interacts with your existing MTAs and mail servers. There are three operating models:

Standalone model

Deploys IMSS on the same computer as an MTA, such as Postfix.

Sandwich model

Deploys IMSS between an upstream MTA and a downstream MTA.

Proxy model

Deploys IMSS between an upstream mail server and a downstream mail server.

Note

In the proxy model, IMSS is placed at the edge of your intranet without any co-work MTA. This model does not support the use of IP Filtering features (IP Profiler and ERS).

The Standalone Model

In the standalone model, a computer hosts one Postfix instance acting as the MTA and one IMSS daemon:

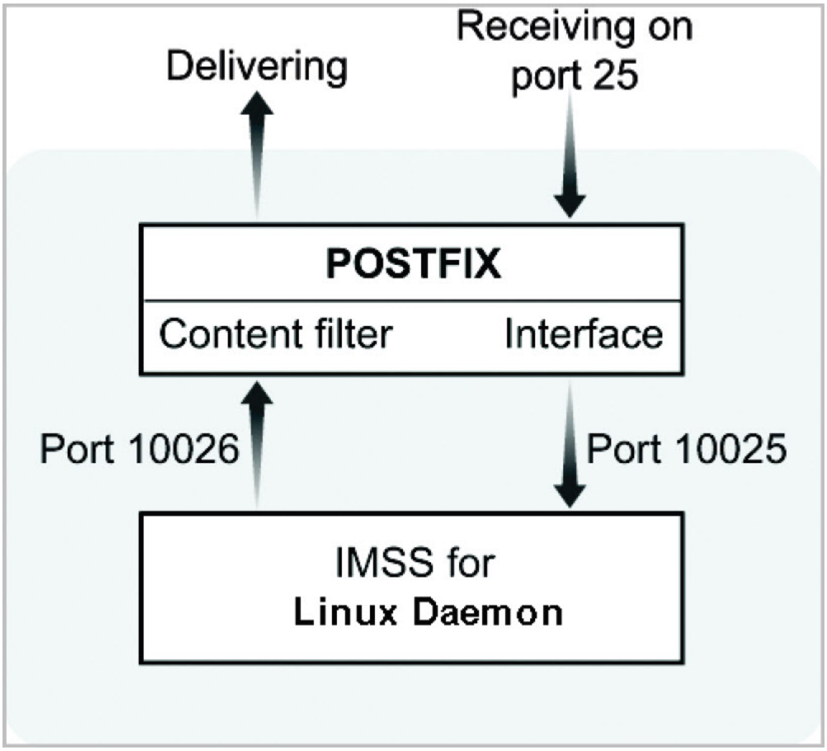


FIGURE 3-4. Standalone model

Trend Micro recommends deploying Sender Filtering as the first line of defense in your messaging infrastructure. If you choose to enable the Sender Filtering service, the preceding standalone model will change.

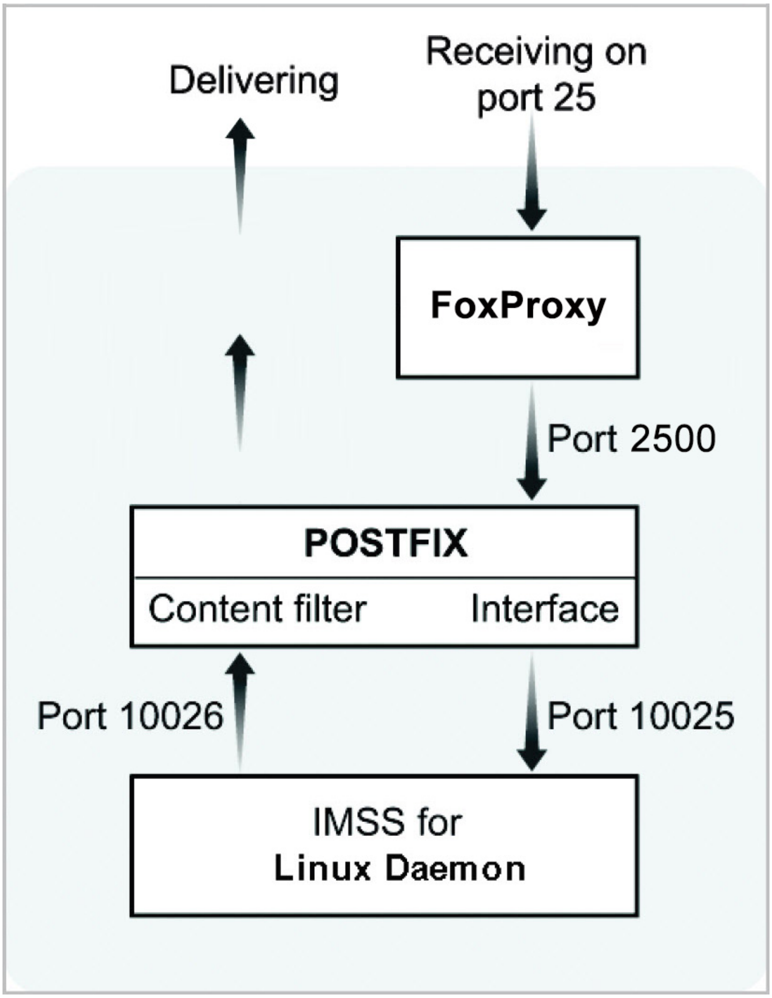


FIGURE 3-5. Standalone model with Sender Filtering enabled

This setup meets most of the needs of a small to medium-sized company and has low impact on the network since all the processes are running on the same server. Since they are sharing the same resources, however, this configuration requires a powerful server to host Postfix and the IMSS daemon.

The default configuration parameters for both sides are:

In `/etc/postfix/main.cf`:

```
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

In `/etc/postfix/master.cf`:

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=$imss_connect_timeout
  -o smtp_data_done_timeout=$imss_timeout
  -o smtpd_tls_security_level=none
#IMSS: content filter loop back smtpd
localhost:10026 inet n - n - 200 smtpd
  -o content_filter=
  -o smtpd_timeout=$imss_timeout
  -o local_recipient_maps=
  -o myhostname=postfix.imss71
  -o smtpd_client_restrictions=
  -o smtpd_enforce_tls=no
  -o smtpd_tls_security_level=none
```

Note

If you copy and paste the preceding configurations, make sure you correct the indentation of all lines accordingly.

The Standalone Model in IPv6 Environments

For IPv6 support, make the following changes to in `/etc/postfix/main.cf`:

```
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:[::1]:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

For IPv6 support, make the following changes to in `/etc/postfix/master.cf`:

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=$imss_connect_timeout
  -o smtp_data_done_timeout=$imss_timeout
  -o smtpd_tls_security_level=none
#IMSS: content filter loop back smtpd
[::1]:10026 inet n - n - 200 smtpd
  -o content_filter=
  -o smtpd_timeout=$imss_timeout
  -o local_recipient_maps=
  -o myhostname=postfix.imss71
  -o smtpd_client_restrictions=
  -o smtpd_enforce_tls=no
  -o smtpd_tls_security_level=none
```

Note

If you copy and paste the preceding configurations, make sure you correct the indentation of all lines accordingly.

In `/opt/trend/imss/config/imss.ini`, open connection restrictions and point the downstream server IP to IPv6 localhost:

```
[socket]
proxy_smtp_server_ip=all
```

```
[smtp]
smtp_allow_client_ip=127.0.0.1, ::1
downstream_smtp_server_addr=::1
```

The Sandwich Model

In this configuration, one server hosts a Postfix instance as an upstream MTA for receiving (Server #1) and a second server hosts a Postfix instance as the downstream MTA for delivering (Server #3). A third server hosts the IMSS daemon , which sits between the two Postfix servers as a scanning proxy (Server #2).

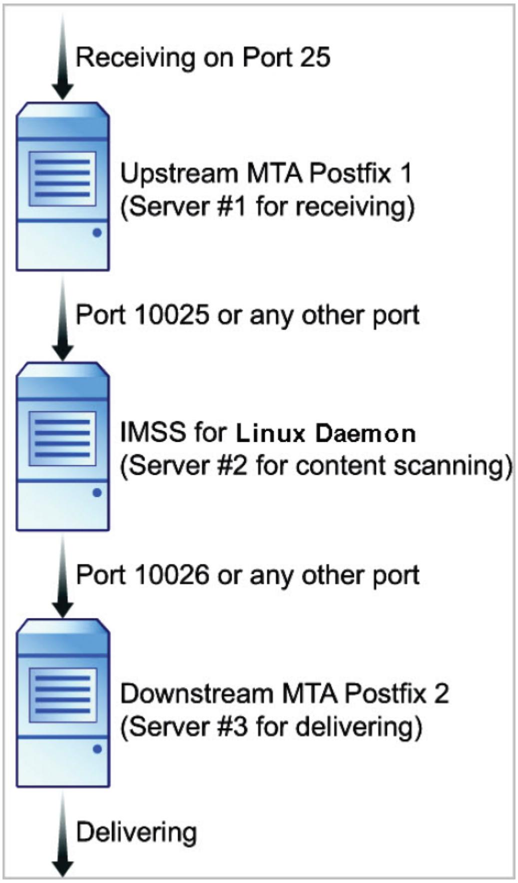

Receiving on Port 25
Upstream MTA Postfix 1
(Server #1 for receiving)
Port 10025 or any other port
IMSS for Linux Daemon
(Server #2 for content scanning)
Port 10026 or any other port
Downstream MTA Postfix 2
(Server #3 for delivering)
Delivering

FIGURE 3-6. Sandwich model

Trend Micro recommends deploying Sender Filtering as the first line of defense in your messaging infrastructure. If you choose to enable the Sender Filtering service, the preceding sandwich model will change.

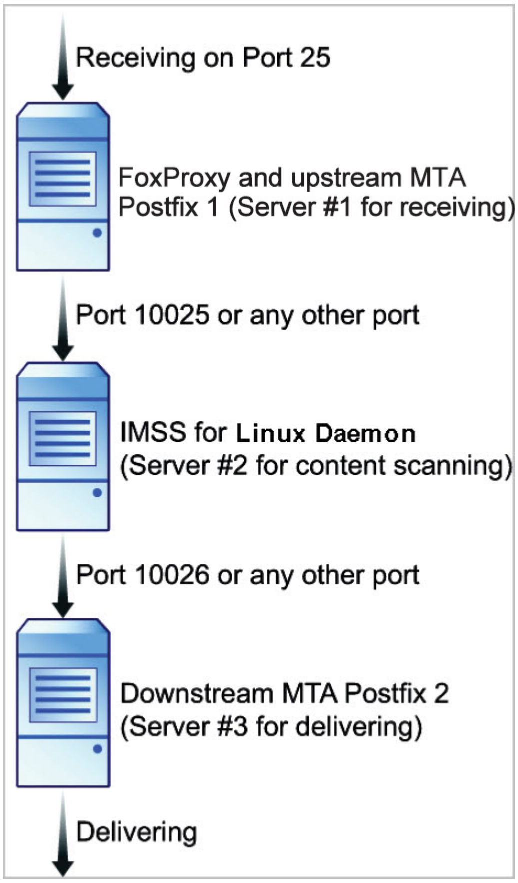

Receiving on Port 25
FoxProxy and upstream MTA
Postfix 1 (Server #1 for receiving)
Port 10025 or any other port
IMSS for Linux Daemon
(Server #2 for content scanning)
Port 10026 or any other port
Downstream MTA Postfix 2
(Server #3 for delivering)
Delivering

FIGURE 3-7. Sandwich model with Sender Filtering enabled

This configuration is suitable for large corporations with heavy SMTP traffic. Each server has its own specific purpose and task and will not affect other servers. Using this type of setup increases your network load.

This configuration is highly flexible; you can replace Postfix with any SMTP MTA. But you are responsible for setting up connection control and domain relaying.

Here are the configuration settings if you use Postfix as the MTA:

- In `/etc/postfix/main.cf` on server#1, add the following to relay mail to server #2:

  ```
  relayhost=[ip_of_server2]:10025
  default_destination_recipient_limit=100
  default_destination_concurrency_limit=50
  ```

  (Sender Filtering only) FoxProxy is a key FoxHunter component that collects the client behavior statistics and blocks or rejects SMTP client connections depending in the reputation data available from the local BIND server or Trend Micro Email Reputation Services (ERS). FoxLib is a component used by Postfix to provide the IP address of the SMTP client that contacts FoxProxy instead of the FoxProxy IP address (127.0.0.1). FoxLib is implemented by a shared library `libTmFoxSocketLib.so`. Postfix loads this library during startup based on the `import_environment` configuration setting in the `Postfix main.cf` configuration file:

  ```
  import_environment = MAIL_CONFIG MAIL_DEBUG MAIL_LOGTAG
  TZ XAUTHORITY DISPLAY LANG=C
  LD_PRELOAD=/opt/trend/imss/lib/libTmFoxSocketLib.so
  TM_FOX_PROXY_LIST=/opt/trend/imss/config/foxproxy.list
  TM_FOX_PROXY_CONNECT_PORT=2500
  ```

- In `/opt/trend/imss/config/imss.ini`, open connection restrictions and point the downstream server IP to server #3:

  ```
  imss socket binding address
  [socket]
  proxy_smtp_server_ip=all
  [smtp]
  smtp_allow_client_ip=127.0.0.1, ip_of_server1
  downstream_smtp_server_addr=ip_of_server3
  ```

- In /etc/postfix/master.cf on server #3, modify smtpd settings to receive mail on port 10026:

  ```
  10026 inet n - n - - smtpd
  ```

The Sandwich Model in IPv6 Environments

Here are the configuration settings if you use Postfix as the MTA.

In /etc/postfix/main.cf on server#1, add the following to relay mail to server #2:

```
relayhost=[ipv6_address_of_server2]:10025
default_destination_recipient_limit=100
default_destination_concurrency_limit=50
```

In /opt/trend/imss/config/imss.ini, open connection restrictions and point the downstream server IP to server #3:

```
[socket]
proxy_smtp_server_ip=all
[smtp]
smtp_allow_client_ip=127.0.0.1, ipv6_address_of_server1
downstream_smtp_server_addr=ipv6_address_of_server3
```

In /etc/postfix/master.cf on server #3, modify smtpd settings to receive mail on port 10026:

```
10026 inet n - n - - smtpd
```

The Proxy Model

In this model, IMSS is located between an upstream and downstream mail server, with MTAs located in other places on the network.

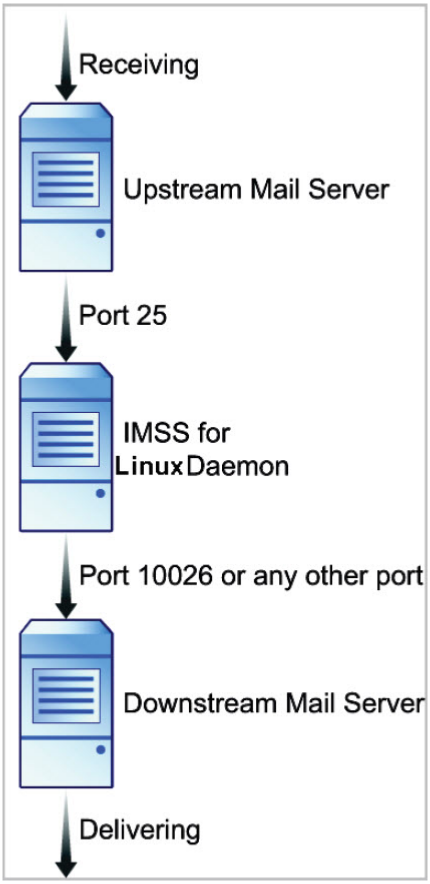


FIGURE 3-8. Proxy model

The greatest advantage of this model is better performance and faster throughput. However, with this model, you cannot use IP Profiler or ERS, which requires that there are no modifications to incoming IP addresses before they reach IMSS.

The Proxy Model in IPv6 Environments

In `/etc/postfix/main.cf` on server#1, add the following to relay mail to server #2:

```
relayhost=[ipv6_address_of_server2]:10025
default_destination_recipient_limit=100
default_destination_concurrency_limit=50
```

In `/opt/trend/imss/config/imss.ini`, open connection restrictions and point the downstream server IP to server #3:

```
[socket]
proxy_smtp_server_ip=all
[smtp]
smtp_allow_client_ip=127.0.0.1, ipv6_address_of_server1
downstream_smtp_server_addr=ipv6_address_of_server3
```

In `/etc/postfix/master.cf` on server #3, modify smtpd settings to receive mail on port 10026:

```
10026 inet n - n - - smtpd
```

Tip

IMSS 9.1 Patch 1 can connect to TMCM servers residing in IPv6 networks. Make sure to configure the TMCM to support IPv6.

Chapter 4

Installation and Uninstallation

This chapter explains how to install IMSS under different scenarios.

Topics include:

- *System Requirements on page 4-2*
- *Preparing the Message Transfer Agents on page 4-5*
- *Installing IMSS on page 4-13*
- *Using Sender Filtering with Sendmail on page 4-15*
- *Verifying the Installation on page 4-21*
- *About IPv6 Support on page 4-21*
- *Uninstalling IMSS on page 4-27*

System Requirements

The following table provides the recommended and minimum system requirements for running IMSS.

TABLE 4-1. System Requirements

SPECIFICATION	DESCRIPTION
Operating System	• Red Hat™ Enterprise Linux™ 6 Servers (6.0, 6.1, 6.2, 6.3, 6.4, 6.6, 6.7, 6.8, 6.9, 6.10) • Red Hat Enterprise Linux 7 Servers (7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7) • Red Hat Enterprise Linux 8 Servers (8.0, 8.1, 8.2, 8.3)
CPU	• Recommended: 8-core Intel(TM) Xeon(TM) processor or equivalent • Minimum: Dual-core Intel(TM) Xeon(TM) processor or equivalent
Memory	• Recommended: 8 GB RAM • Minimum: 4 GB RAM

Specification	Description
Disk Space	- Recommended: 250 GB total The following recommendations are based on 500,000 messages/day, a 50% quarantine rate, and logs preserved for a month. - 10 GB for mail storage - 50 GB or more for the Admin database - 20 GB or more for the EUQ database - 40 GB or more for the working quarantine folder - Minimum: 80 GB total **Note** The default location for the Admin database and EUQ database is `/var/imss`. The Default location for the working quarantine folders is `/opt/trend/imss/queue/`.
Swap Space	Recommended: 2 GB swap space
Browser	- Microsoft Internet Explorer(TM) 10, 11 or Edge 15063 - Firefox 53
PostgreSQL	Version 9.6.3
LDAP server	- Microsoft Active Directory 2012 R2, 2016 - IBM™ Lotus Domino 8.5, 9.0 - Sun One LDAP 5.2 or above - OpenLDAP 2.4.44

Specification	Description
MTA	• Postfix™ 2.6 or above • Sendmail™ 8.14 or above
Linux Libraries (for all platforms)	• Red Hat 6 (32-bit/64-bit): net-tools; bind-utils; lsof; wget; perl; fontconfig.i686; cyrus-sasl-gssapi.i686; cyrus-sasl-md5.i686; glibc.i686 • Red Hat 7.0-7.2: nss-softokn; net-tools; bind-utils; lsof; wget;perl; fontconfig.i686; cyrus-sasl-gssapi.i686; cyrus-sasl-md5.i686; glibc.i686 • Red Hat 7.3: nss-softokn; lsof; wget; perl; fontconfig.i686;cyrus-sasl-gssapi.i686; cyrus-sasl-md5.i686; glibc.i686 • Red Hat 7.4: glibc.i686; bind-utils;lsof; wget;perl; fontconfigi686; cyrus-sasl-gssapii686; cyrus-sasl-md5.i686; • Red Hat 7.5: glibc.i686; net-tools; bind-utils; lsof; wget; perl; fontconfig.i686; cyrus-sasl-gssapi.i686; cyrus-sasl-md5.i686; • Red Hat 7.6: glibc.i686; net-tools; bind-utils; lsof; wget; perl; fontconfig.i686; cyrus-sasl-gssapi.i686; cyrus-sasl-md5.i686; • Red Hat 7.7: glibc.i686; net-tools; bind-utils; lsof; wget; perl; fontconfig.i686; cyrus-sasl-gssapi.i686; cyrus-sasl-md5.i686;

Note

To enable support for Red Hat Enterprise Linux 7.5, 7.6 or 7.7 servers, you must install IMSS 9.1 hot fix 1211 or any later hot fixes.

Preparing the Message Transfer Agents

IMSS supports two types of Message Transfer Agents (MTAs), namely, Postfix and Sendmail. This section explains how to prepare these MTAs for use with IMSS before installing IMSS components.

Preparing Postfix

If you will install IMSS on the same computer that has a Postfix installation, configure Postfix as listed in this section.

Note

The installer does not install an MTA during IMSS server installation. You should already have your MTAs installed and operational. If you install Postfix on the same computer on which you will install IMSS, verify that the Postfix settings are correct. Trend Micro strongly recommends that you install and use the Postfix distributed with your version of Linux. See http://www.postfix.org for details.

Procedure

- Insert or modify the following settings to `/etc/postfix/main.cf`:

```
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

- Insert the following settings to `/etc/postfix/master.cf`:

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
  -o disable_dns_lookups=yes
  -o smtp_connect_timeout=$imss_connect_timeout
  -o smtp_data_done_timeout=$imss_timeout
  -o smtpd_tls_security_level=none

#IMSS: content filter loop back smtpd
localhost:10026 inet n - n - 200 smtpd
  -o content_filter=
  -o smtpd_timeout=$imss_timeout
  -o smtpd_tls_security_level=none
  -o local_recipient_maps=
  -o myhostname=postfix.imss91
  -o smtpd_client_restrictions=
  -o smtpd_enforce_tls=no
```

Note

If you copy and paste the preceding configurations, make sure you correct the indentation of all lines accordingly.

Enabling Postfix IPv6 Support

The following procedure explains how configure Postfix for IPv6 support. For details about Postfix 2.2 support for IPv6 protocol, visit:

http://www.postfix.org/IPV6_README.html

Procedure

1. Open `/etc/postfix/main.cf`.
2. Set `inet_protocols` = `all`.
3. Restart the Postfix service.

About Sendmail

This section explains how to configure and use Sendmail with IMSS.

Note

Sendmail supports IPv6 from v8.10. For details, see the supporting documentation available at:

http://www.sendmail.org/~gshapiro/8.10.Training/IPv6.html

Sendmail Daemons

The following illustration depicts running two Sendmail daemons and IMSS on the same server.

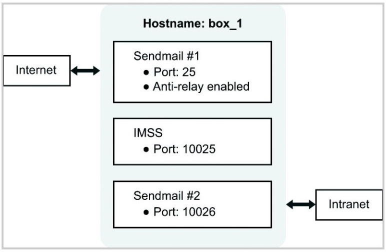


FIGURE 4-1. Sendmail daemons on one server

Port 10025 and 10026 are arbitrary port numbers, so replace 10025 and 10026 with free ports when completing the configuration below (port 25 is the standard SMTP port.)

Configuring Sendmail #1

Procedure

1. Copy the `sendmail.mc` file and rename it `sendmail.d.mc` for later use.

```
# cp -p /etc/mail/sendmail.mc /etc/mail/sendmail.d.mc
```

2. In the `sendmail.mc` file, add the following statements before `MAILER(smtp)dnl` to relay all email messages to IMSS:

```
define(`SMTP_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`SMTP', `+k') dnl
define(`ESMTP_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`ESMTP', `+k') dnl
define(`SMTP8_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`SMTP8', `+k') dnl
define(`RELAY_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
MODIFY_MAILER_FLAGS(`RELAY', `+k') dnl
MODIFY_MAILER_FLAGS(`LOCAL', `+k') dnl
define(`LOCAL_MAILER_PATH',`[IPC]')dnl
define(`LOCAL_MAILER_ARGS',`TCP [127.0.0.1] 10025')dnl
```

3. Change the existing **DAEMON_OPTIONS** setting in the `sendmail.mc` file into the following to receive SMTP requests from all hosts:

   ```
   DAEMON_OPTIONS(`Port=smtp, Addr=0.0.0.0, Name=MTA')dnl
   ```

   If necessary, add the following **DAEMON_OPTIONS** setting to enable IPv6 support:

   ```
   DAEMON_OPTIONS(`Port=smtp, Addr=<IPv6_address>,
   Name=MTA_IPv6, Family=inet6')dnl
   ```

4. Run the following command for the `sendmail.cf` file to take effect:

   ```
   # m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
   ```

Configuring Sendmail #2

Procedure

1. Copy the `/var/spool/mqueue` queue directory and rename it `/var/spool/mqueue1` for Sendmail #2.

   ```
   # cp -pr /var/spool/mqueue /var/spool/mqueue1
   ```

2. In the `sendmail.d.mc` file, add the following statements before `MAILER(smtp)dnl`:

```
define(`QUEUE_DIR', `/var/spool/mqueue1')dnl
define(`confPID_FILE', `/var/run/sendmail_delivery.pid')dnl
```

3. Change the existing **DAEMON_OPTIONS** setting in the `sendmail.d.mc` file into the following to receive SMTP requests from IMSS:

   ```
   DAEMON_OPTIONS(`Port=10026, Addr=127.0.0.1,
   Name=MTA_DELIVERY')dnl
   ```

4. Run the following command for the `sendmail.cf.delivery` file to take effect:

   ```
   # m4 /etc/mail/sendmail.d.mc > /etc/mail/
   sendmail.cf.delivery
   ```

Finishing Setup and Restarting Sendmail services

Procedure

1. Restart the first Sendmail daemon to receive SMTP traffic on port 25 using the following command:

   - RedHat Enterprise Linux 6

     ```
     # /etc/init.d/sendmail restart
     ```

   - RedHat Enterprise Linux 7 or 8

     ```
     #systemctl restart sendmail
     ```

2. Create the following new file for the second Sendmail daemon.

   Note

   Make sure there are no extra trailing spaces in each line of the new file.

   - RedHat Enterprise Linux 6

     Create the `sendmail_delivery` file.

```
vi /etc/init.d/sendmail_delivery
```

```
#!/bin/bash
#
# sendmail_delivery  This shell script takes care of
#                    starting and stopping
#                    sendmail_delivery
#
# chkconfig: 2345 80 30
#

PROG=sendmail_delivery
CONFFILE=/etc/mail/sendmail.cf.delivery
PIDFILE=/var/run/sendmail_delivery.pid

# Source function library.
. /etc/rc.d/init.d/functions

# Source networking configuration.
[ -f /etc/sysconfig/network ] && \
. /etc/sysconfig/network

# Source sendmail configureation.
if [ -f /etc/sysconfig/sendmail ]; then
    . /etc/sysconfig/sendmail
else
    DAEMON=no
    QUEUE=1h
fi

# Check that we're a privileged user
[ `id -u` = 0 ] || exit 4

# Check that networking is up.
[ "${NETWORKING}" = "no" ] && exit 1

[ -x /usr/sbin/sendmail ] || exit 5


start() {
    ret=0
    echo -n $"Starting $PROG: "
    daemon --pidfile $PIDFILE /usr/sbin/sendmail \
        $([ "x$DAEMON" = xyes ] && echo -bd) \
    $([ -n "$QUEUE" ] && echo -q$QUEUE) \
        $SENDMAIL_OPTARG -C $CONFFILE
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/$PROG
    let ret+=$RETVAL

    [ $ret -eq 0 ] && return 0 || return 1
}

stop() {
    echo -n $"Shutting down $PROG: "
    killproc $PROG
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/$PROG
    return $RETVAL
}

status -p $PIDFILE >/dev/null
running=$?

case "$1" in
    start)
    [ $running -eq 0 ] && exit 0
    start
    RETVAL=$?
    ;;
    stop)
    [ $running -eq 0 ] || exit 0
    stop
    RETVAL=$?
    ;;
    restart)
    stop
    start
    RETVAL=$?
    ;;
    status)
    echo -n $PROG ; status -p $PIDFILE -l $PROG
    RETVAL=$?
    ;;
    *)
    echo $"Usage: $0 {start|stop|restart|status}"
    RETVAL=2
esac

exit $RETVAL
```

- RedHat Enterprise Linux 7 or 8

   a. Create the `sendmail_delivery.service` file.

   `vi /usr/lib/systemd/system/sendmail_delivery.service`

```
[Unit]
 Description=Sendmail Mail Transport Agent
 for Delivery
 After=syslog.target network.target
 Conflicts=postfix.service exim.service

 [Service]
 Type=forking
 StartLimitInterval=0
 PIDFile=/var/run/sendmail_delivery.pid
 Environment=SENDMAIL_OPTS="-q1h"
 EnvironmentFile=-/etc/sysconfig/sendmail
 ExecStartPre=-/etc/mail/make
 ExecStartPre=-/etc/mail/make aliases
 ExecStart=/usr/sbin/sendmail -bd $SENDMAIL_OPTS
 $SENDMAIL_OPTARG -C /etc/mail/sendmail.cf.delivery

 [Install]
 WantedBy=multi-user.target
```

   b. Create a soft link to the `sendmail_delivery.service` file.

```
ln -s /usr/lib/systemd/system/
sendmail_delivery.service /etc/systemd/system/multi-
user.target.wants/sendmail_delivery
```

3. Restart the second Sendmail daemon to receive SMTP traffic from IMSS using the following command:

- RedHat Enterprise Linux 6

  ```
  #chmod 755 /etc/init.d/sendmail_delivery
  ```

  ```
  # /etc/init.d/sendmail_delivery restart
  ```

- RedHat Enterprise Linux 7 or 8

  ```
  #systemctl restart sendmail_delivery
  ```

Installing IMSS

The following is a list of the key steps you need to perform to install IMSS.

Note

Before installation, make sure the font size on your screen is less than 24; otherwise, the installation may fail.

Procedure

1. Run the `/IMSSPackagePath/imss/install.sh` file to start the IMSS installation wizard.
2. Press F12 to continue installation.
3. Press F12 to agree with the license agreement.
4. Select the installation type.
   - **Fresh install**
   - **Append install**

     If you select this option, select **Child Device** and specify the IP address, logon user name and password for the management console of the parent device.

Note

Pay attention to the following:

- The logon user account that you specified must have full administration rights.
- If the child and parent devices are not in the same subnet, **Append install** will fail. In this case, modify the parent configuration file `pg_hba.conf` in `/var/imss/pgdata` to allow the child device to connect to the parent device's database.

5. Choose to install a local or remote database.

- Internal PostgreSQL database: This is the default database used.
- External PostgreSQL database: If you select this option, provide external database information as required.

Note

To use the external database, do the following:

a. Make sure the account used to install the IMSS admin database has the superuser role.

b. Manually change the maximum number of database connections to 600:

```
vi /var/lib/pgsql/9.6/data/postgresql.conf

max_connection = 600 (default 100)

restart DB service (service postgresql-9.6 restart OR
systemctl restart postgresql)
```

c. Make sure that IMSS and the external database server use the same timezone and time settings; otherwise, some unexpected issues may happen.

d. Make sure that **max_locks_per_transaction** in `postgresql.conf` is set to 256, and then restart the database service.

6. Specify the destination folder to install IMSS.

7. Choose to enable the components of the Sender Filtering Service.

    - Enable Email Reputation

    - Enable IP Profiler

8. Verify that your environment meets all minimum system requirements.

9. Wait until the progress bar shows 100%.

    If a message saying "Installation Complete" appears, the installation is successful.

Using Sender Filtering with Sendmail

Sender Filtering (IP Profiler and Email reputation) blocks connections at the IP level. IP Profiler uses your customized settings for email messages that signify different types of attacks. Email reputation uses information from the Trend Micro Threat Reputation Network to determine if the computer initiating an SMTP connection is a known sender of spam.

If Sender Filtering (IP Profiler or Email reputation) is used together with the Sendmail MTA, additional configurations must be done to ensure that Sendmail uses FoxLib and therefore gets the real IP address of the SMTP client contacting FoxProxy.

This section describes the procedures for configuring FoxLib on Red Hat 6 and 7 to support Sendmail and Sender Filtering.

Integrating FoxLib with Sendmail on Red Hat 6

Procedure

1. Modify the first Sendmail to receive SMTP traffic only from FoxProxy.

    a. Change the **DAEMON_OPTIONS** settings in the `sendmail.mc` file into the following:

```
DAEMON_OPTIONS(`Port=2500, Addr=127.0.0.1, Name=MTA')dnl
```

b. Run the following command for the `sendmail.cf` file to take effect:

```
# m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

2. Modify the properties of Sendmail.

a. List the properties.

```
ll /usr/sbin/sendmail.sendmail
```

```
-rwxr-sr-x 1 root smmsp 746328 Jan 22 2007 /usr/sbin/
sendmail.sendmail
```

b. Delete the SGID bit.

```
chmod g-s /usr/sbin/sendmail.sendmail
```

c. Change the group used by Sendmail.

```
chgrp root /usr/sbin/sendmail.sendmail
```

d. Verify the properties.

```
ll /usr/sbin/sendmail.sendmail
```

```
-rwxr-xr-x 1 root root 746328 Jan 22 2007 /usr/sbin/
sendmail.sendmail
```

3. Modify the `foxlibd` script in the `/opt/trend/imss/script` directory.

a. Set the **TM_FOX_UID** parameter to the ID of the user used by Sendmail.

```
TM_FOX_UID=0
```

b. Set the **TM_FOX_GID** parameter to the ID of the group used by Sendmail.

```
TM_FOX_GID=0
```

c. (Optional) If you are using Red Hat (64-bit), set the **LD_PRELOAD** parameter as follows:

```
LD_PRELOAD=/opt/trend/imss/lib64/libTmFoxSocketLib.so
```

d. Add the following two lines after the line containing **export LD_LIBRARY_PATH**:

```
TM_FOX_PROXY_CONNECT_PORT=2500

export TM_FOX_PROXY_CONNECT_PORT
```

4. Modify the `foxproxy.ini` configuration file in the `/opt/trend/imss/config` directory.

   a. Change the value of the **has_foxlib_installed** parameter from `0` to `1`.

   ```
   has_foxlib_installed=1
   ```

5. Restart Sendmail and FoxProxy using the `foxlibd` script.

   a. Stop the upstream MTA.

   ```
   /opt/trend/imss/script/foxlibd stop
   ```

   If the following error message appears, ignore it:

   ```
   "ERROR: ld.so: object '/opt/trend/imss/lib
   /libTmFoxSocketLib.so' from LD_PRELOAD cannot be
         preloaded: ignored."
   ```

   b. Restart the upstream MTA.

   ```
   /opt/trend/imss/script/foxlibd start
   ```

   If the error message mentioned in the preceding step appears, ignore it.

   c. Restart FoxProxy.

   ```
   /opt/trend/imss/script/foxproxyd stop

   /opt/trend/imss/script/foxproxyd start
   ```

   d. Restart the sendmail.

   ```
   #/etc/init.d/sendmail restart

   #/etc/init.d/sendmail_delivery restart
   ```

6. Verify the installation using a test server.

    a. Test the connection to the IMSS server.

    ```
    telnet <IMSS server address> 25
    ```

    ```
    ehlo imss
    ```

    > **Note**
    >
    > The IMSS server and test server addresses must be in the same subnet.

    b. Check if the response contains the test server address.

    The installation is unsuccessful if the response contains the string “127.0.0.1”.

Integrating FoxLib with Sendmail on Red Hat 7 or 8

Procedure

1. Modify the first Sendmail to receive SMTP traffic only from FoxProxy.

    a. Change the **DAEMON_OPTIONS** settings in the `sendmail.mc` file into the following:

    ```
    DAEMON_OPTIONS(`Port=2500, Addr=127.0.0.1, Name=MTA')dnl
    ```

    b. Run the following command for the `sendmail.cf` file to take effect:

    ```
    # m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
    ```

2. Modify the properties of Sendmail.

    a. List the properties.

    ```
    ll /usr/sbin/sendmail.sendmail
    ```

    ```
    -rwxr-sr-x 1 root smmsp 746328 Jan 22 2007 /usr/sbin/
    sendmail.sendmail
    ```

b. Delete the SGID bit.

```
chmod g-s /usr/sbin/sendmail.sendmail
```

c. Change the group used by Sendmail.

```
chgrp root /usr/sbin/sendmail.sendmail
```

d. Verify the properties.

```
ll /usr/sbin/sendmail.sendmail
```

```
-rwxr-xr-x 1 root root 746328 Jan 22 2007 /usr/sbin/
sendmail.sendmail
```

3. Modify the Sendmail environment.

a. Run the following command:

```
# systemctl edit sendmail
```

b. Add the following lines and save the change:

```
[Service]
Environment="LD_PRELOAD=/opt/trend/imss/lib64
/libTmFoxSocketLib.so"
Environment="TM_FOX_PROXY_CONNECT_PORT=2500"
Environment="TM_FOX_PROXY_LIST=
/opt/trend/imss/config/foxproxy.list"
```

Note

If IMSS is not installed in the default path (`/opt/trend`), change the paths in the preceding lines accordingly.

Make sure there are no extra trailing spaces in each line.

4. Modify the `foxproxy.ini` configuration file in the `/opt/trend/imss/config` directory.

a. Change the value of the **has_foxlib_installed** parameter from `0` to `1`.

```
has_foxlib_installed=1
```

5. Restart Sendmail and FoxProxy.

   a. Restart the upstream MTA.

      ```
      systemctl restart sendmail
      ```

   b. Restart FoxProxy.

      ```
      /opt/trend/imss/script/foxproxyd stop
      ```

      ```
      /opt/trend/imss/script/foxproxyd start
      ```

6. Verify the installation using a test server.

   a. Test the connection to the IMSS server.

      ```
      telnet <IMSS server address> 25
      ```

      ```
      ehlo imss
      ```

      Note

      The IMSS server and test server addresses must be in the same subnet.

   b. Check if the response contains the test server address.

      The installation is unsuccessful if the response contains the string "127.0.0.1".

Using Sender Filtering with Postfix

After installation, go to **Administration** > **IMSS Configuration** > **SMTP Routing** > **Connections** and change the listening port of Postfix into 2500.

The following settings are added to the `main.cf` file during installation:

```
import_environment = MAIL_CONFIG MAIL_DEBUG
MAIL_LOGTAG TZ XAUTHORITY DISPLAY LANG=C
LD_PRELOAD=/opt/trend/imss/lib64/libTmFoxSocketLib.so
TM_FOX_PROXY_LIST=/opt/trend/imss/config/foxproxy.list
```

```
LD_LIBRARY_PATH=/opt/trend/imss/lib
TM_FOX_PROXY_CONNECT_PORT=2500
```

Do not remove those settings because they are necessary for the Sender Filtering service to communicate with Postfix.

Verifying the Installation

After the installation is complete, to see a list of the daemons, type the following at the command prompt:

```
# ps -ef | grep imss
```

Telnet to port 25 to ensure that IMSS/Postfix answers.

About IPv6 Support

Configure IPv6 support after installing IMSS. IMSS supports the following IPv6 features in IPv6 networks and proxies in IPv6 networks:

SMTP routing

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

POP3 connections

IMSS supports connections to IPv6 POP3 servers.

Trend Micro services

IMSS supports communication with the following services using IPv6:

- Web Reputation Services
- Product Registration
- ActiveUpdate
- Smart Feedback

Email protection

IMSS supports incoming message scanning from IPv6 networks, including marketing messages.

Notifications

IMSS supports sending notifications to IPv6 Notification servers.

Network proxy

IMSS supports proxies in IPv6 networks. For configuration details, see *The Proxy Model in IPv6 Environments on page 3-28*.

Trend Micro Control Manager

IMSS can connect to TMCM servers residing in IPv6 networks. Make sure to configure the TMCM to support IPv6.

IP address imports and exports

IMSS recognizes addresses imported in IPv6 format, and can export addresses to IPv6 format.

Configuring the Server for IPv6

To configure IPv6 support, enable the IPv6 network, then configure the IPv6 address on the server.

Procedure

1. Enable the IPv6 network.

    a. Log on shell and edit `/etc/sysconfig/network` using the following command:

    ```
    # vi /etc/sysconfig/network
    ```

    b. Add the following line, if it does not exist:

    ```
    NETWORKING_IPV6=yes
    ```

2. Configure the IPv6 address.

    a. Edit the configuration file for interfaces.

Example: `# vi /etc/sysconfig/network-scripts/ifcfg-eth0`

b. Add the following lines:

```
IPV6INIT=yes

IPV6_AUTOCONF=no

IPV6ADDR=<endpoint_IPv6_address> (Example:
2001:db8:10ff::ae:44f2/64)
```

c. Restart the network service.

```
# service network restart
```

Verifying the IPv6 Configuration

The following procedure explains how to verify that IPv6 support is working.

Procedure

1. Use the server to ping other endpoints.

```
# ping6 ::1

# ping6 <IPv6_address_of_another_endpoint>
```

2. Use another endpoint to ping the server.

```
# ping6 <IPv6_address_of_this_endpoint>
```

Configuring IMSS for IPv6 Support

Once you configure the server operating system to support IPv6, configure IMSS IPv6 support. The settings are configured in `<imss_install_path>/imss/config/imss.ini`.

Proxy Settings for IPv6 Support

Modify proxy_smtp_server_ip and proxy_pop3_server_ip to configure the IP address that the IMSS daemon binds to.

- If proxy_smtp_server_ip is not specified, the SMTP proxy service sets the IP address to 127.0.0.1.
- If proxy_pop3_server_ip is not specified, the proxy service sets the IP address to 0.0.0.0.
- If proxy_smtp_server_ip and proxy_pop3_server_ip specified as all, the proxy service receives packets from all interfaces, including IPv4 or IPv6 clients.
- If proxy_smtp_server_ip and proxy_pop3_server_ip specified as 0.0.0.0, the proxy service receives packets from all interfaces, but is limited to IPv4 clients only.

The following changes configure the daemon to listen to both IPv4 and IPv6 networks:

```
proxy_smtp_server_ip=all
proxy_pop3_server_ip=all
```

Settings to Allow IPv6 Clients

Modify smtp_allow_client_ip to specify the client IP addresses (separated by a comma or space) that can connect to the IMSS daemon SMTP stream port.

- If smtp_allow_client_ip is not specified, the default value is 127.0.0.1.
- smtp_allow_client_ip supports IPv4 and IPv6 addresses in the following IP formats:

  127.0.0.1

  ::1

  123.123.123.123

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

123.123.123.123/24

2001:db8:10ff::ae:44f2/64

123.123.123.123-223

2001:db8:10ff::ae:44f2-45ff

For example, if you only want to allow a localhost (either IPv4 and IPv6) and the IPv6 address `2001:db8:10ff::ae:44f3` to connect to the daemon service, use the following configuration:

```
smtp_allow_client_ip=127.0.0.1, ::1, 2001:db8:10ff::ae:44f3
```

Settings for Downstream IPv6 Servers

Modify `downstream_smtp_server_addr` and `downstream_smtp_server_port` to specify the downstream or backend MTA server IP address or hostname and port.

Note

To avoid security issues that arise from resolving the host, Trend Micro recommends using the IP address.

- If `downstream_smtp_server_addr` and `downstream_smtp_server_port` are not specified, the default values are `127.0.0.1` and 10026, respectively.
- `downstream_smtp_server_addr` supports IPv4 and IPv6 addresses in the following IP formats:

  127.0.0.1

  ::1

  123.123.123.123

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

Domain.com

For example, if the downstream IP address is `2001:db8:10ff::ae:44f2` and the port is 25, use the following configuration:

```
downstream_smtp_server_addr=2001:db8:10ff::ae:44f2
downstream_smtp_server_port=25
```

Verifying the IPv6 Configuration

Before you begin

Configure the following parameters:

- `proxy_smtp_server_ip`
- `proxy_pop3_server_ip`
- `smtp_allow_client_ip`
- `downstream_smtp_server_addr`
- `downstream_smtp_server_port`

After configuring the parameters , do the following to verify the configuration:

Procedure

1. Restart the IMSS daemon using the following command:

   `<IMSS install path>/imss/script/S99IMSS restart`

2. Use the following commands to check the daemon service listening port.

   ```
   # netstat -ltpn|grep 10025
   #netstat -ltpn|grep 110
   ```

3. Send an email message from an IP address in the `smtp_allow_client_ip` list to the daemon IPv4/IPv6 SMTP port.

The email message should successfully send.

4. Send an email message from an IP address **not** in the `smtp_allow_client_ip` to the daemon IPv4/IPv6 SMTP port.

   The email message should be rejected.

5. Receive the email message from the daemon IPv4/IPv6 POP3 port.

   The email message should be recieved.

IMSS 9.1 Patch 1 IPv6 support is correctly configured.

Uninstalling IMSS

The following is a list of the key steps you need to perform to uninstall IMSS.

Procedure

1. Run the `/$IMSS_HOME/imss/backup/uninstall.sh` script file to start the IMSS uninstallation wizard.

   Note

   In a parent-child deployment, uninstall the child devices before the parent device.

2. Press F12 to continue uninstallation.

3. Confirm to remove configurations, logs, queues, and database data.

4. Wait until the progress bar shows 100%.

   If a message saying "Uninstallation Complete" appears, the uninstallation is successful.

Chapter 5

Upgrading from Previous Versions

This chapter provides instructions on upgrading from previous versions of IMSS.

Topics include:

- *Upgrading from an Evaluation Version on page 5-2*
- *Upgrading to IMSS Linux 9.1 on page 5-4*
- *Upgrading to IMSS Linux 9.1 Patch 1 on page 5-20*
- *Migrating from Previous Versions to Linux 9.1 on page 5-21*

Upgrading from an Evaluation Version

If you provided an evaluation Activation Code to activate IMSS previously, you have started an evaluation period that allows you to try the full functionality of the product. The evaluation period varies depending on the type of Activation Code used.

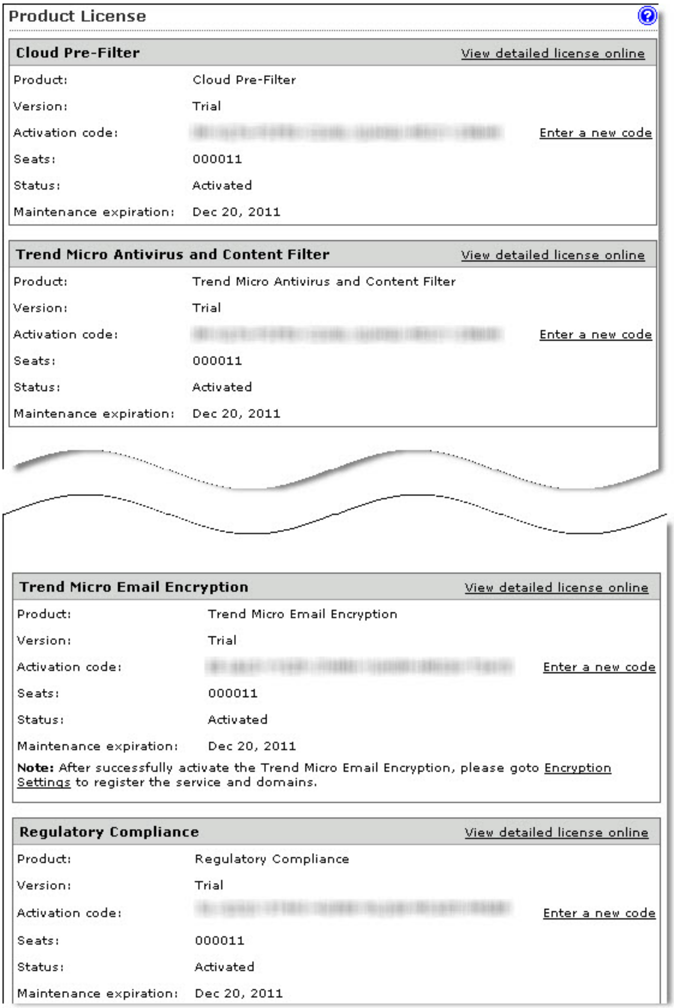
Fourteen (14) days prior to the expiry of the evaluation period, IMSS will display a warning message on the management console alerting you of the impending expiration.

To continue using IMSS, purchase the full version license for the product. You will then be provided a new Activation Code.

Procedure

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

The **Product License** screen appears.



Product License

Cloud Pre-Filter View detailed license online

Product: Cloud Pre-Filter
Version: Trial
Activation code: [redacted] Enter a new code
Seats: 000011
Status: Activated
Maintenance expiration: Dec 20, 2011

Trend Micro Antivirus and Content Filter View detailed license online

Product: Trend Micro Antivirus and Content Filter
Version: Trial
Activation code: [redacted] Enter a new code
Seats: 000011
Status: Activated
Maintenance expiration: Dec 20, 2011

Trend Micro Email Encryption View detailed license online

Product: Trend Micro Email Encryption
Version: Trial
Activation code: [redacted] Enter a new code
Seats: 000011
Status: Activated
Maintenance expiration: Dec 20, 2011

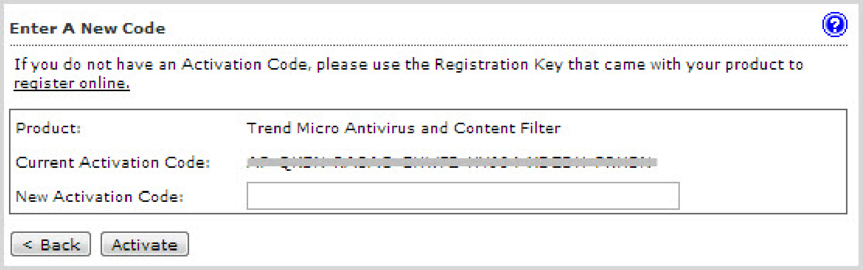
Note: After successfully activate the Trend Micro Email Encryption, please goto Encryption Settings to register the service and domains.

Regulatory Compliance View detailed license online

Product: Regulatory Compliance
Version: Trial
Activation code: [redacted] Enter a new code
Seats: 000011
Status: Activated
Maintenance expiration: Dec 20, 2011

2. Click the **Enter a new code** hyperlink in section for the product or service you want to activate.

The **Enter A New Code** screen appears.



Enter A New Code

If you do not have an Activation Code, please use the Registration Key that came with your product to register online.

Product: Trend Micro Antivirus and Content Filter

Current Activation Code: [redacted]

New Activation Code:

3. Type the new Activation Code in the box provided.

> **Note**
>
> When you purchase the full licensed version of IMSS, Trend Micro will send the new Activation Code to you by email. To prevent mistakes when typing the Activation Code (in the format xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx), you can copy the Activation Code from the email and paste it in the box provided.

4. Click **Activate**.

5. Repeat steps 2 to 5 for all the products or services you want to activate.

Upgrading to IMSS Linux 9.1

Data Transfer Considerations

Compared with IMSS 7.1, IMSS 9.1 uses a different database schema for policy event logs, quarantined messages and archived messages. Therefore, data transfer is done both during and after upgrade. IMSS 9.1 transfers data generated within 24 hours during the upgrade, but transfers data older than 24 hours after the upgrade. That is, data generated within 24 hours before upgrade will be shown immediately after the upgrade, while data older than 24 hours will not be shown immediately.

The data transfer status can be found in the notification area of the **Dashboard** screen. Generally, the data transfer time is determined by the database size of IMSS 7.1. For example, sometimes it takes 2.5 hours to finish data transfer.

Note

Before upgrading, stop your email traffic and make sure the policy event logs have been imported to the database. Otherwise, logs that are not imported will be lost during upgrade. If the log import is completed, the size of the `polevt.imss.latesttime` file recorded in `/INSTALLPATH/imss/bin/policy_event_bookmark` will be the same as the actual size of the file under `/INSTLLPATH/imss/log`.

Upgrading from IMSS Linux 7.1 SP2 Patch 1 to IMSS Linux 9.1

The IMSS Setup program can automatically upgrade from IMSS version 7.1 SP2 Patch 1 on supported platforms. If the Setup program detects this version, it can do the following:

- Back up your old IMSS settings
- Install IMSS IMSS
- Migrate the existing settings

There is no need to unregister the current IMSS server from Control Manager before the upgrade. The Setup program still maintains the registration settings, which means that all logs from the old server can still be queried by Control Manager after the upgrade.

Migrating or Installing Over IMSS

Consider the following before migrating or installing over IMSS 7.1 SP2 Patch 1:

- IMSS 9.1 retains all IMSS 7.1 SP2 Patch 1 data.
- IMSS 9.1 retains IMSS 7.1 SP2 Patch 1 hidden key configuration settings in the file.
- IMSS 9.1 retains all IMSS 7.1 SP2 Patch 1 reports.
- IMSS 9.1 retains all IMSS 7.1 SP2 Patch 1 Control Manager settings.
- Administrators must stop message traffic to the server where IMSS 7.1 SP2 Patch 1 resides.

Note

The End-User Quarantine feature is disabled after upgrade or migration. Manually enable this feature if you want to use it. For details, see "Enabling EUQ" in the IMSS Administrator Guide.

IMSS Linux 9.1 Settings That Cannot be Migrated

All data and configuration on all scanners remain after upgrading or migrating.

Backing Up IMSS Settings

Do not perform any operation on RPM packages during manual backup and rollback; otherwise, the RPM packages will be lost.

Procedure

1. Check the IMSS 7.1 SP2 Patch 1 components installed on your server.

   The following table lists the detailed mapping relationships between component names and home folders.

COMPONENT NAME	HOME FOLDER
imss-7.1	`$IMSS_HOME`

Component Name	Home Folder
imssctrl	`$IMSS_HOME` **Note** This home folder exists only on the parent server.
imsseuq	`$IMSS_HOME`
nrs	`$NRS_HOME`
ipprofiler	`$IPP_HOME`

Note

If you do not know the home folder, run the following command:

```
rpm -ql Components Name|tee 2|head -1
```

2. Stop the cron service and back up IMSS 7.1 settings.

    - If your operating system is Red Hat 7 or higher, run the following commands:

        ```
        systemctl stop crond.service
        ```

        ```
        crontab -l >cronlist.bak
        ```

    - If your operating system is lower than Red Hat 7, run the following commands:

        ```
        service crond stop
        ```

        ```
        crontab -l >cronlist.bak
        ```

3. Stop IMSS 7.1 message traffic for approximately 5 minutes.

4. Stop all IMSS 7.1 processes using the following commands:

    ```
    $IMSS_HOME/imss/script/imssstop.sh stop
    ```

    ```
    $NRS_HOME/nrs/imssstop.sh
    ```

```
$IPP_HOME/ipprofiler/script/imssstop.sh
```

5. Back up the Postfix configuration files using the following command:

   ```
   tar cvf postfix_config.tar /etc/postfix
   ```

6. Back up the home folder for all IMSS 7.1 components installed.

   ```
   tar cvf imss71.tar /$IMSS_HOME/imss
   ```

   ```
   tar cvf nrs.tar /$NRS_HOME/nrs
   ```

   ```
   tar cvf ipprofiler.tar /$IPP_HOME/ipprofiler
   ```

7. If IMSS 7.1 is not installed in the default path and uses the internal database, back up the database using the following command:

   ```
   tar cvf default_path_folder.tar /opt/trend/imss
   ```

8. Back up the RPM database-related data using the following command:

   ```
   tar cvf rpm.tar /var/lib/rpm
   ```

9. Back up the IMSS 7.1 database.

   - If you use the IMSS 7.1 bundled PostgreSQL to manage the database, complete the following:

     a. Stop the PostgreSQL server using the following command:

        ```
        $IMSS_HOME/imss/script/dbctl.sh stop
        ```

     b. Back up the PostgreSQL data using the following command:

        ```
        tar cvf imssdb.tar /var/imss
        ```

   - If you use your own PostgreSQL server to manage the IMSS 7.1 database, perform either a cold physical backup or a hot logical backup.

Upgrading an IMSS Single Server Deployment

Note

IMSS 7.1 SP2 Patch 1 or above is required during the upgrade or migration.

Procedure

1. Make sure that all IMSS services are working properly on the management console.

   On the **Summary** screen, all the services under **Managed Server Settings** are active.

2. Start the IMSS upgrade wizard in the installation package path (`/imss/upgrade.sh`).

   Note

   Locate and decompress the installation package in the working directory that general users can access (for example, `/var/tmp`). Run the upgrade wizard as the **root** user.

   Otherwise, the upgrade may fail due to the following error in the installation log:

   ```
   Fail to migrate the adminDB. tool exited with code 16.
   ```

3. Press F12 to continue upgrade.

4. Press F12 to agree with the license agreement.

5. Verify the installed components and database and press F12 to continue.

6. Verify that your environment meets all minimum system requirements and press F12 to continue.

7. Verify the admin database configurations and press F12 to continue.

   - If you are using an internal database, the wizard will migrate your data to the PostgreSQL 9.6 internal database.

- If you are using an external database, dump your data and transfer data to the PostgreSQL 9.6 database server. Complete the remote database configurations.

  For details, see *Upgrading the External Admin Database on page 5-12*.

8. Wait until the progress bar shows 100%.

If a message saying "Upgrade Complete" appears, the upgrade is successful.

Note

To use Sender Filtering together with the Sendmail MTA, additional configurations must be done to ensure that Sendmail uses FoxLib and therefore gets the real IP address of the SMTP client contacting FoxProxy. For details, see *Using Sender Filtering with Sendmail on page 4-15*.

Upgrading an IMSS Distributed Deployment

IMSS now supports upgrading an entire distributed deployment, for example, in a network where IMSS is being used in a parent-child deployment.

Note

IMSS 7.1 SP2 Patch 1 or above is required when upgrading or migrating.

If IP Profiler is deployed on an edge server while the scanner service runs on another downstream server, perform the following recommended tasks:

1. Uninstall the IMSS 7.1 server where IP Profiler is installed.
2. Upgrade the remaining IMSS 7.1 servers to 9.1.
3. Enable the known host setting and IP Profiler.

Procedure

1. Prepare for the upgrade.

   a. Back up IMSS settings.

   > **Note**
   >
   > For details, see *Backing Up IMSS Settings on page 5-6*.

   b. Use the following command to verify there are no messages in the Postfix queue:

   ```
   postqueue -p
   ```

   c. Make sure that all IMSS services are working properly on the management console.

   On the **Summary** screen, all the services under **Managed Server Settings** are active.

   d. Stop all services on child devices using the following command:

   ```
   # /opt/trend/imss/script/imssstop.sh stop
   ```

   > **Note**
   >
   > In a distributed deployment, the parent device must be upgraded before child devices.

   e. Start the database service on child devices using the following command:

   ```
   # /opt/trend/imss/script/dbctl.sh start
   ```

2. Upgrade the parent and child devices.

   a. Upgrade the parent device.

   For details, see *Upgrading an IMSS Single Server Deployment on page 5-9*.

b. Use the following command to verify that the database is working properly on the parent device:

```
# ps -ef |grep imss
```

Information similar to the following appears:

```
imss 5602 0.0 0.2 63412 3376 ? S Oct14 1:09 /opt/trend/
imss/PostgreSQL/bin/postgres -D /var/imss/pgdata -i
```

c. Upgrade all the child devices one at a time, a few at a time, or all at once.

WARNING!

Do not restart IMSS services until all devices have been upgraded.

3. Check information under **Old Components That Need Upgrade** and make sure all servers have been upgraded.

Note

To use Sender Filtering together with the Sendmail MTA, additional configurations must be done to ensure that Sendmail uses FoxLib and therefore gets the real IP address of the SMTP client contacting FoxProxy. For details, see *Using Sender Filtering with Sendmail on page 4-15*.

Make sure you complete the configurations on each device.

Upgrading the External Admin Database

If IMSS 7.1 is installed with the external admin database, upgrade the PostgreSQL server first before IMSS upgrade. In addition, provide the new PostgreSQL information in *Upgrading an IMSS Single Server Deployment on page 5-9*.

To upgrade the PostgreSQL server, perform the following steps:

Procedure

1. Dump the database from the original PostgreSQL server.

   a. Copy the IMSS installation package to the original PostgreSQL server and decompress the package.

   b. Set the environmental variable.

   ```
   export LD_LIBRARY_PATH=IMSSPackagePath/imss/imssbase/lib
   ```

   c. Run the following commands to dump the database:

   ```
   IMSSPackagePath/imss/database/pg_dump -U DBUSERNAME -v -
   Fc IMSSDBNAME > backupfile.tar
   ```

   ```
   ex: pg_dump -U sa -v -Fc imss > backup_admin.tar
   ```

2. Upgrade the PostgreSQL server to version 9.6, or prepare a new PostgreSQL 9.6 server.

   a. Create a database account same as the IMSS 7.1 admin database account (that is, “DBUSERNAME” mentioned in Step 1). Make sure it has the superuser role.

   b. Manually change the maximum number of database connections to 600.

   ```
   vi /var/lib/pgsql/9.6/data/postgresql.conf
   ```

   ```
   max_connection = 600 (default 100)
   ```

   c. Restart PostgreSQL service.

   d. Make sure that IMSS and the external database server use the same time zone and time settings.

3. Restore the database to the PostgreSQL 9.6 server.

   a. Copy `backupfile.tar` from the original PostgreSQL server to the destination PostgreSQL server.

   b. Copy IMSS installation package to the new PostgreSQL server and decompress the package.

c. Change the local authentication method to the password in `pg_hba.conf`.

```
change "local all all peer"
```

```
TO "local all all password"
```

d. Restart the PostgreSQL service.

e. Install the glibc.i686 library.

f. Set environmental variables.

```
export LD_LIBRARY_PATH=IMSSPackagePath/imss/imssbase/lib
```

g. Run the following commands to restore the database:

```
IMSSPackagePath/imss/database/pg_restore -U DBUSERNAME -
d postgres -C -v -e < backupfile.tar
```

```
ex: pg_restore -U sa -d postgres -C -v -e <
backup_admin.tar
```

Note

You may encounter the following error message when you run the **pgrestore** command:

```
pg_restore: connecting to database for restorePassword:
pg_restore: creating DATABASE xxxx
pg_restore: connecting to new database "xxxx"
pg_restore: connecting to database "xxxx" as user "xx"
pg_restore: creating SCHEMA public
pg_restore: creating COMMENT SCHEMA public
pg_restore: creating PROCEDURAL LANGUAGE plpgsql
pg_restore: [archiver (db)] Error while PROCESSING TOC:
pg_restore: [archiver (db)] Error from TOC entry 10536;
2612 94235 PROCEDURAL LANGUAGE plpgsql imss
pg_restore: [archiver (db)] could not execute query:
ERROR:  role "XXXX" does not exist
Command was: ALTER PROCEDURAL LANGUAGE plpgsql OWNER TO imss;
```

If this occurs, add the database role as required in the error message. The database will still be restored despite of this error. After creating the role in the database, delete the database that has been restored and run the **pgrestore** command again.

4. Restore the local authentication method in `pg_hba.conf`.

5. Restart the PostgreSQL service.

Upgrading the External EUQ Database

If an IMSS 7.1 server is installed only with the EUQ database, it will be considered as the external EUQ database server. The upgrade to IMSS 9.1 cannot run on this server, and a manual upgrade of the EUQ database is required.

Procedure

1. Dump the EUQ database from the original PostgreSQL server.

   For details, see Step 1 in *Upgrading the External Admin Database on page 5-12*.

2. **2.** Upgrade the PostgreSQL server to version 9.6, or prepare a new PostgreSQL 9.6 server.

   For details, see Step 2 in *Upgrading the External Admin Database on page 5-12*.

3. Restore the EUQ database to the PostgreSQL 9.6 server.

   For details, see Step 3 in *Upgrading the External Admin Database on page 5-12*.

4. Update the EUQ database schema.

```
 CREATE TABLE
    tb_dl_entry_keys(  id serial NOT
    NULL ,
    distribution_list varchar(256),  submitter
    varchar(256),
    authentication_code varchar(8),  created_time
    timestamptz,  expired_time
    timestamptz,  heartbeat_time
    timestamptz,  is_logined int4
    DEFAULT 0
);
```

5. Detach the original EUQ database.

   a. Log on to the IMSS management console.

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

   c. Click the **Database** tab.

   d. Disable the database, select the check box next to the database, and then click **Detach**.

6. Attach the new EUQ database.

   To attach an EUQ database, click **Attach**. Type the new EUQ database server IP address, port number, administrator user name, password and database name.

Rolling Back an Upgrade

IMSS rolls back automatically if there are problems during the upgrade process. However, if the automatic rollback encounters issues, you need to perform a manual rollback.

Procedure

1. Stop the cronjob service and roll back cronjob to the status when IMSS 7.1 is installed.

   - If your operating system is Red Hat 7 or higher, run the following commands:

     ```
     systemctl stop crond.service
     
     crontab ./cronlist.bak
     ```

   - If your operating system is lower than Red Hat 7, run the following commands:

     ```
     service crond stop
     
     crontab ./cronlist.bak
     ```

2. Uninstall IMSS 9.1 and remove the `$IMSS_HOME` folder using the following commands:

   ```
   $IMSS_HOME/imss/backup/uninstall.sh
   
   rm -rf $IMSS_HOME
   ```

3. Remove the data folder using the following command:

   ```
   rm -rf /var/imss/pgdata
   ```

4. Roll back package information to the status when IMSS 7.1 is installed:

   ```
   tar xvf rpm.tar -C /
   
   rpm --rebuilddb
   ```

5. Roll back IMSS components using the following commands:

```
tar xvf imss71.tar -C /

tar xvf nrs.tar -C /

tar xvf ipprofiler.tar -C /
```

6. If you use the internal database and IMSS components are not installed in the default path, run the following command:

   ```
   tar xvf default_path_folder.tar -C /
   ```

7. Roll back to the IMSS 7.1 database using the following command:

   ```
   tar xvf imssdb.tar -C /
   ```

8. Roll back the Postfix configuration files using the following command:

   ```
   tar xvf postfix_config.tar -C /
   ```

9. Re-create the IMSS auto start script.

   - If your operating system is lower than Red Hat 7, do the following:

     a. Save the following script information as a file, replace `$IMSS_HOME` with your actual folder name, and run the file:

     ```
     work_directory=$IMSS_HOME/imss
     RC_D="/etc/rc.d"
     RCDIR0="/etc/rc.d/rc0.d"
     RCDIR1="/etc/rc.d/rc1.d"
     RCDIR2="/etc/rc.d/rc2.d"
     RCDIR3="/etc/rc.d/rc3.d"
     RCDIR4="/etc/rc.d/rc4.d"
     RCDIR5="/etc/rc.d/rc5.d"
     RCDIR6="/etc/rc.d/rc6.d"
     RCDIR=$RCDIR3
     RCINITDIR="$RC_D/init.d"

     CreateLink()
     {
         test -f $1 && (rm -rf $2 ; ln -s $1 $2)
     }

     CreateRCLinkLinux()
     {
         if test -f $1 ; then
             if test ! -f $RCINITDIR/$2 ; then
                 cp $1 $RCINITDIR/$2
                 chmod +x $RCINITDIR/$2
             fi
             CreateLink $RCINITDIR/$2 $RCDIR2/$2
             CreateLink $RCINITDIR/$2 $RCDIR3/$2
             CreateLink $RCINITDIR/$2 $RCDIR5/$2
     ```

```
    fi
}

CreateRCKLinkLinux()
{
    if test -f $1 ; then
        if test ! -f $RCINITDIR/$2 ; then
            cp $1 $RCINITDIR/$2
            chmod +x $RCINITDIR/$2
        fi

        CreateLink $RCINITDIR/$2  $RCDIR0/$3
        CreateLink $RCINITDIR/$2  $RCDIR6/$3
    fi
}


CreateRCLinkLinux $work_directory/script/S99MONITOR S99MONITOR
CreateRCKLinkLinux $work_directory/script/S99MONITOR S99MONITOR K01MONITOR

CreateLink $work_directory/script/imssstop.sh $RCINITDIR/imssstop
CreateLink $RCINITDIR/imssstop  $RCDIR0/K00IMSSSTOP
CreateLink $RCINITDIR/imssstop  $RCDIR6/K00IMSSSTOP
CreateRCLinkLinux $work_directory/script/S99CMAGENT S99CMAGENT
CreateRCKLinkLinux $work_directory/script/S99CMAGENT S99CMAGENT K97CMAGENT
CreateRCLinkLinux $work_directory/bind/bindctl.sh S99bindctl
CreateRCKLinkLinux $work_directory/bind/bindctl.sh S99bindctl K03bindctl
CreateRCLinkLinux $work_directory/UI/adminUI/bin/Tomcat.sh S99IMSSUI
CreateRCKLinkLinux $work_directory/UI/adminUI/bin/Tomcat.sh S99IMSSUI K97IMSSUI
CreateRCLinkLinux $work_directory/script/S99FOXDNS S99FOXDNS
CreateRCKLinkLinux $work_directory/script/S99FOXDNS S99FOXDNS K02FOXDNS
CreateRCLinkLinux $work_directory/script/S99SCHEDULED S99SCHEDULED
CreateRCKLinkLinux $work_directory/script/S99SCHEDULED S99SCHEDULED K02SCHEDULED
CreateRCLinkLinux $work_directory/script/dbctl.sh S98dbctl
CreateRCKLinkLinux $work_directory/script/dbctl.sh S98dbctl K98dbctl
if [ -f $RCINITDIR/S99dbctl ];then
    DeleteRCLinkLinux S99dbctl K99dbctl
    DeleteRCLinkLinux S99dbctl K03dbctl
    CreateRCLinkLinux $work_directory/script/dbctl.sh S98dbctl
    CreateRCKLinkLinux $work_directory/script/dbctl.sh S98dbctl K03dbctl
fi
```

b. Run the following command to automatically start the IMSS service:

```
chkconfig --add S98dbctl
```

- If your operating system is Red Hat 7 or higher, do the following:

  a. Create the `imss.service` file in `/usr/lib/systemd/system`.

  b. Save the following script information to the `imss.service` file and replace `$IMSS_HOME` with your actual folder name:

```
[Unit]
Description=InterScan Messaging Security Suite
After=network.target remote-fs.target nss-lookup.target
```

```
[Service]
Type=simple
RemainAfterExit=yes
ExecStart=$IMSS_HOME/imss/script/imssstart.sh start
ExecStop=$IMSS_HOME/imss/script/imssstop.sh stop
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

c. Start the IMSS service using the following command:

```
systemctl enable imss.service
```

Upgrading to IMSS Linux 9.1 Patch 1

IMSS supports upgrade to 9.1 Patch 1 from version 9.1 or any later hot fixes. For versions earlier than 9.1, make sure you upgrade them to IMSS 9.1 before installing 9.1 Patch 1.

Procedure

1. Obtain the IMSS 9.1 Patch 1 package from the Download Center.
2. Upload the 9.1 Patch 1 package file.
    a. Log on to the IMSS management console.
    b. Go to **Administration** > **Updates** > **System & Applications**.
    c. Under **Upload**, click **Browse** and locate the package file.
    d. Click **Upload**.

    After the file finishes uploading, the package type, build number, and title appear under **Latest uploaded package**.
3. Deploy the 9.1 Patch 1 package file.
    a. Select the check boxes next to the devices to which you want to deploy the update.

b. Click **Update**.

c. Accept the license agreement.

   After an operating system update or upgrade, IMSS reboots. An application upgrade might force IMSS to automatically reboot.

d. If IMSS rebooted, wait for it to start up and log on again.

e. Go to **Administration** > **Updates** > **System & Applications** to view the summary screen.

Note

i. 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.

ii. 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.

Migrating from Previous Versions to Linux 9.1

IMSS 9.1 supports migration from previous versions of IMSS.

The following table lists the minimum version that supports migration to IMSS 9.1.

TABLE 5-1. Supported Migration Platform and Versions

PLATFORM	VERSION
IMSS for Linux	7.1 SP2 Patch 1

Migrating to IMSS Linux 9.1

The migration process requires the following tasks:

- **Step 1**: Exporting the settings from previous versions of IMSS
- **Step 2**: Importing the settings to IMSS 9.1

Exporting Settings from IMSS 7.1 SP2 Patch 1

The following settings do not migrate:

TABLE 5-2. Settings that Cannot Migrate

MTA SETTINGS	SETTINGS NOT MIGRATED
MTA Settings	IP address and port of the SMTP interface
Configuration Settings	Database settings (example: Internal file path)
	Management console password
	Control Manager settings

Important

When exporting configuration settings, ensure that the IMSS server is:

- Not performing database-related tasks.
- Not stopped or started.

Certificate usage for child devices cannot be exported.

Procedure

1. Go to **Administration** > **Import/Export** from the IMSS servers to migrate from.

   The **Import/Export** screen appears.

2. Click **Export**.

   The configuration settings export to a package that IMSS can import.

Importing Settings to IMSS 9.1

Procedure

1. Perform a fresh installation of IMSS 9.1.

   Tip

   Trend Micro recommends importing configuration packages to a fresh installation of IMSS 9.1, because the imported configuration settings overwrite all existing settings.

2. Retrieve the package that contains the configuration settings that you wish to migrate.

3. Go to **Administration** > **Import/Export** on the IMSS 9.1 management console.

   The **Import/Export** screen appears.

4. Import the configuration package.

   Note

   By default, all child devices use the certificates of the parent device after migration. If you do not want to use those certificates, assign other certificates to child devices.

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** > **Export Debugging Files**.
2. Next to **Scanner**, select a device.
3. Select the number of days to export.
4. Click **Export**.

   The process might take 10 minutes to 1 hour or more depending on the total log file size.

Chapter 6

Frequently Asked Questions

This chapter lists the frequently asked questions about IMSS installation.

Topics include:

- *Postfix MTA Settings on page 6-2*
- *Installation / Uninstallation on page 6-3*

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_direct
ory
```

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.

Installation / Uninstallation

Is there any problem if I install IMSS 9.1 on a computer with an external DNS server?

There should be no functional problem integrating IMSS 9.1 with DNS server. Functionally, you can integrate IMSS with an external DNS server on the same computer, but this is not recommended for performance reasons.

Is there any problem if I install IMSS 9.1 on a computer with an existing Apache Server?

IMSS installs Apache server in `$IMSS_HOME/imss/UI/apache` directory for the purpose of EUQ Server load balancing. It will not conflict with the existing Apache server if there is no port conflict. IMSSApache takes the port 8447.

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 http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cyber security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to http://www.trendmicro.com/us/security-intelligence/index.html to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

Address	Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014
Phone	Toll free: +1 (800) 228-5651 (sales) Voice: +1 (408) 257-1500 (main)
Fax	+1 (408) 257-2003
Website	http://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version

- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Sending Suspicious Content to Trend Micro

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

Index

A

about IMSS, 1-2
adware, 1-11
audience, xiv

B

browser requirements, 4-3

C

Centralized Reporting, 2-5
Command & Control (C&C) Contact Alert Services, 1-22
community, A-2
Control Manager
- see Trend Micro Control Manager, 1-16

CPU requirements, 4-2

D

dialers, 1-11
disk space requirements, 4-3
documentation, xv

E

Email reputation, xiii
- about, 1-13
- types, 1-14

email threats
- spam, 1-5
- unproductive messages, 1-5

End-User Quarantine, 2-5

F

FAQ
- postfix, 6-2

File Reputation Services, 1-19
filtering, how it works, 1-7
Firefox, 4-3

G

graymail, 1-21

H

hacking tools, 1-11

I

IMSS
- about, 1-2

imss.ini, 4-26
installation
- procedures, 4-13
- verifying, 4-21

installing
- before a firewall, 3-9
- behind a firewall, 3-10
- in the DMZ, 3-11
- no firewall, 3-8

Internet Explorer, 4-3
IP Profiler, xiii
- about, 2-4
- detects, 2-4
- how it works, 2-4

IPv6, 4-21, 4-23
- allowing clients, 4-24
- downstream, 4-25
- verify, 4-26

J

joke program, 1-11

L

LDAP server requirements, 4-3

Linux Libraries requirements, 4-4

M

mass mailing viruses
 pattern, 1-6
memory requirements, 4-2
minimum requirements, 4-2
MTA requirements, 4-4

N

network topology, 3-8
new features, vi

O

online
 community, A-2
online help, xv

P

password cracking applications, 1-11
POP3
 deployment planning, 3-14
Postgre requirements, 4-3
Pre-Filter Service, 2-2
preparation
 configuring IPv6, 4-22
 verifying IPv6, 4-23

R

readme file, xv
remote access tools, 1-11
requirements, 4-2

S

security risks
 spyware/grayware, 1-11
Sender Filtering
 about, 2-3
Smart Protection, 1-19
Smart Protection Network, 1-21
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
support
 knowledge base, A-2
 resolve issues faster, A-4
 TrendLabs, A-7
swap space requirements, 4-3
system requirements, 4-2

T

TrendLabs, A-7
Trend Micro Control Manager, 1-16
 agent, 1-16
 server, 1-16

U

upgrading
 IMSS 7.1 SP2 Patch 1, 5-5

V

verifying the installation, 4-21

W

Web Reputation Services, 1-20
what's new, vi

TREND MICRO

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: MSEM98751/190801