TREND MICRO™

InterScan™ Messaging Security Suite 7

Comprehensive threat protection at the Internet messaging gateway

for LINUX™

Installation Guide

Messaging Security

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

http://www.trendmicro.com/download

Trend Micro, the Trend Micro t-ball logo, InterScan, and Trend Micro 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.

Copyright© 2009 Trend Micro, Incorporated. All rights reserved.

Document Part No. MSEM74062/90401

Release Date: June 2009

Patents Pending

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

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

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

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

Contents

Preface

Audience x
InterScan Messaging Security Suite Documentation x
Document Conventions xi

Chapter 1: Introducing InterScan Messaging Security Suite

About IMSS 1-2
What's New 1-2
IMSS Main Features and Benefits 1-5
About Spyware and Other Types of Grayware 1-13
About Web Reputation 1-14
About Trend Micro Control Manager 1-15
Integrating with Control Manager 1-16

Chapter 2: Component Descriptions

About IMSS Components 2-2
The IMSS Admin Database 2-2
Central Controller 2-2
Scanner Services 2-2
Policy Services 2-3
Policy Synchronization 2-3
End-User Quarantine Service 2-4
Primary and Secondary End-User Quarantine Services 2-4
End-User Quarantine Server Components 2-4
Apache and mod_jk 2-5
Tomcat 2-5

Struts Framework 2-6
End-User Quarantine Application 2-6
The End-User Quarantine Database 2-6
IP Filtering 2-7
Email Reputation Services 2-8
Types of Email Reputation Services 2-8
How IP Profiler Works 2-9
How Email Reputation Service Works 2-10
Using the ERS Management Console 2-11

About End-User Quarantine (EUQ) 2-15

About Centralized Reporting 2-15

Chapter 3: Planning for Deployment

Deployment Checklist 3-2

Component and Sub-module Installation 3-6

IMSS Ports 3-8

Network Topology Considerations 3-12
Installing without a Firewall 3-12
Installing in Front of a Firewall 3-13
Incoming Traffic 3-13
Outgoing Traffic 3-13
Installing Behind a Firewall 3-14
Incoming Traffic 3-14
Outgoing Traffic 3-14
Installing on a Former SMTP Gateway 3-15
Incoming Traffic 3-15
Outgoing Traffic 3-15
Installing in the De-Militarized Zone 3-16
Incoming Traffic 3-16
Outgoing Traffic 3-16

About Operating Models 3-17
The Standalone Model 3-17
The Sandwich Model 3-19
The Proxy Model 3-21

Understanding Installation Scenarios 3-22
Single-Server Installation 3-22
Multiple Scanner Service Installation 3-24
Multiple End-User Quarantine Service Installation 3-26
Other Considerations When Deploying End-User Quarantine .. 3-28
Communication Between Servers 3-29
Complex Distributed Installation 3-29
Wide-Area Network Installation 3-32
Trend Micro Control Manager 3-32
Fault Tolerance and Failover in a WAN Scenario 3-34

IP Filtering 3-35
Deploying IMSS with IP Filtering 3-35

About Failover 3-36

Chapter 4: Installing and Uninstalling IMSS 7.1

System Requirements 4-2

Preparing Message Transfer Agents 4-4
Preparing Postfix 4-4
Using Sendmail 4-5
Sendmail Daemons 4-6
Configuring Sendmail #1 4-6
Configuring Sendmail #2 4-8
Restarting Sendmail services 4-9
Using Qmail 4-9
Configuring Qmail 4-11

Installing IMSS Components and End-User Quarantine 4-11
Installation Steps 4-11

Installing IP Filtering Components 4-14
Installing Email Reputation Services and IP Profiler 4-15
Integrating IMSS with Sendmail and Qmail 4-17
Integrating FoxLib with Sendmail 4-18
Integrating FoxLib with Qmail 4-19

Verifying the Installation 4-20

Performing Uninstallation 4-21

Uninstalling IMSS Components 4-21
Uninstalling Email Reputation Services and IP Profiler 4-22
Performing Manual Uninstallation 4-22
Uninstalling IMSS Manually 4-22
Uninstalling the Database Manually 4-23
Uninstalling Postfix Manually 4-24
Uninstalling IP Profiler Manually 4-24

Chapter 5: Upgrading from Previous Versions

Upgrading from an Evaluation Version 5-2

Upgrading from Version 5.7 to Version 7.1 5-5
Upgrading IMSS 5.7: Policy Recommendations 5-6
Removing Unused Policy Objects 5-6
Merging Policy Objects 5-6
Modifying Policy Objects 5-7
Upgrading IMSS 5.7: Process Recommendations 5-7
Perform a Fresh Installation of IMSS 7.1 5-7
Become Familiar with IMSS 7.1 Before Upgrading 5-8
General IMSS 5.7 Migration Tasks 5-8
Verify IMSS 7.1 Operation after Migration 5-8
IMSS 5.7 Settings that Cannot be Migrated 5-9
IMSS 5.7 Settings that Change After Migration 5-12
Upgrade Options for Multiple Scanner Deployment 5-13
Single Admin Database 5-13
Multiple Admin Databases 5-14

Backing Up IMSS 5.7 Settings 5-15
Backing up InterScan Messaging Security Suite 5.7 Data for a Single-server Deployment 5-16
Backing up InterScan Messaging Security Suite 5.7 Data for a Distributed Deployment 5-17

Migrating from IMSS 5.7 to IMSS 7.1 5-19
Exporting IMSS 5.7 Settings 5-19
Importing IMSS 5.7 Settings to IMSS 7.1 5-20

Installing IMSS 7.1 Over IMSS 5.7 5-21

Upgrading from IMSS 7.0 to IMSS 7.1 5-25

IMSS 7.1 Settings That Cannot be Migrated 5-25
Backing Up IMSS 7.0 Settings 5-25
Upgrading an IMSS 7.0 Single Server Deployment 5-26
Upgrading an IMSS 7.0 Distributed Deployment 5-28

Migrating from IMSS 7.0 to IMSS 7.1 5-30
Exporting IMSS 7.0 Settings 5-30
Importing IMSS 7.0 Settings to IMSS 7.1 5-31

Activation of Supported Services 5-32

Rolling Back the Upgrade 5-32
Rolling Back to IMSS 5.7 5-32
Rolling Back to IMSS 7.0 5-34
Rolling Back After IMSS Components Upgrade 5-34
Rolling Back After IP Profiler Upgrades 5-36

Chapter 6: Troubleshooting, FAQ, and Support Information

Troubleshooting 6-2

Frequently Asked Questions 6-2
Postfix MTA Settings 6-2
Installation / Uninstallation 6-3
Upgrading 6-4

Using the Knowledge Base 6-7

Contacting Support 6-7

Index

Preface

Welcome to the *Trend Micro™ InterScan™ Messaging Security Suite 7.1 Installation Guide*. This manual contains information on InterScan Messaging Security Suite™ (IMSS) features, system requirements, as well as instructions on installation and upgrading.

Refer to the *IMSS 7.1 Administrator's Guide* for information on how to configure IMSS settings and the Online Help in the Web management console for detailed information on each field on the user interface.

Topics include:

- Audience on page x
- InterScan Messaging Security Suite Documentation on page x
- Document Conventions on page xi

Audience

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

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

The documentation does not assume the reader has any knowledge of antivirus or anti-spam technology.

InterScan Messaging Security Suite Documentation

The InterScan Messaging Security Suite (IMSS) documentation consists of the following:

- **Installation Guide:** Contains introductions to IMSS features, system requirements, and provides instructions on how to deploy and upgrade IMSS in various network environments.
- **Administrator's Guide:** Helps you get IMSS up and running with post-installation instructions on how to configure and administer IMSS.
- **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 Files:** 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 *Installation Guide, Administrator's Guide* and *readme files* are available at:

http://www.trendmicro.com/download

Document Conventions

To help you locate and interpret information easily, the IMSS documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and other user interface items
Italics	References to other documentation
Monospace	Examples, sample command lines, program code, Web URL, file name, and program output
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that must be avoided

Chapter 1

Introducing InterScan Messaging Security Suite

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

Topics include:

- About IMSS on page 1-2
- What's New on page 1-2
- IMSS Main Features and Benefits on page 1-5
- About Spyware and Other Types of Grayware on page 1-13
- About Web Reputation on page 1-14
- About Trend Micro Control Manager on page 1-15

About IMSS

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

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

What's New

Table 1-1 provides an overview of new features available in IMSS 7.1.

TABLE 1-1. 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 malicous URLs embedded in email messages with Web reputation.
NRS Terminology Change	Network Reputation Service (NRS) has been changed to **Email Reputation Service (ERS)**.

TABLE 1-1. IMSS 7.1 New Features

NEW FEATURE	DESCRIPTION
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.

IMSS 7.0 New Features

Table 1-2 provides an overview of new features available in IMSS 7.0.

TABLE 1-2. 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.

TABLE 1-2. IMSS 7.0 New Features

NEW FEATURE	DESCRIPTION
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 Services filters spam senders at the connection layer. • IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS). • Trend Micro Anti-spam engine detects and takes action on spam.
IntelliTrap	IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus in a compressed file will enter your network through email.
Delegated Administration	LDAP-integrated account management allows users to assign administrative rights for different configuration tasks.
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.

TABLE 1-2. IMSS 7.0 New Features

NEW FEATURE	DESCRIPTION
Integration with Trend Micro Control Manager™	Perform log queries on Email Reputation Services from Control Manager, in addition to other supported features.

IMSS Main Features and Benefits

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

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
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.	IMSS's enhanced virus/content scanner keeps your messaging system working at top efficiency.

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
IntelliTrap	Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files. Because there is the possibility that IntelliTrap may identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature. By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be classified as security risks.	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.

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
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.

TABLE 1-3. Main Features and Benefits

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.

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
Mass mailing virus containment	Email-borne viruses that may automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users. When IMSS detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses. For example, if IMSS detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if IMSS detects a mass-mailing virus, the program can automatically delete the entire message.	By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value. The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs℠ ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.
Spyware and other types of grayware		
Spyware and other types of grayware	Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see About Spyware and Other Types of Grayware on page 1-13	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.

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
Integrated spam		
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. **Note:** Activate SPS before you configure IP Profiler and ERS.	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 ERS	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. ERS blocks IP addresses of known spam senders that Trend Micro maintains in a central database.	With the integration of IP Filtering, which includes IP Profiler and Email Reputation Services (ERS), IMSS can block spammers at the IP level.

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
Others		
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. **Note:** You must have LDAP to use End-User Quarantine.	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 Web-based management console allows you to conveniently configure IMSS policies and settings.	The Web-based console is SSL-compatible. Being SSL-compatible means access to IMSS is more secure.
End-User Quarantine (EUQ)	IMSS provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Spam Prevention Solution (SPS) quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete, or approve for delivery.	With the Web-based EUQ console, end-users can manage messages that IMSS quarantines.
Delegated administration	IMSS offers the ability to create different access rights to the Web 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.

TABLE 1-3. Main Features and Benefits

FEATURE	DESCRIPTIONS	BENEFITS
Centralized reporting	Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports.	Helps you analyze how IMSS is performing. One time (on demand) reports allow you to specify the type of report content as and when required. Alternatively, you can configure IMSS to automatically generate reports daily, weekly, and monthly.
System availability monitor	A built-in agent monitors the health of your IMSS server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow.	Email and SNMP notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.
POP3 scanning	You can choose to enable or disable POP3 scanning from the Web 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.

TABLE 1-3. Main Features and Benefits

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. For details, see About Trend Micro Control Manager on page 1-15.	Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available.

About Spyware and Other Types of Grayware

Your clients are at risk from threats other than viruses. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization (see *Table 1-4*).

TABLE 1-4. Types of spyware/grayware

TYPES OF SPYWARE/GRAYWARE	DESCRIPTIONS
Spyware/Grayware	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, through a Web browser.
Dialers	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem.

TABLE 1-4. Types of spyware/grayware

TYPES OF SPYWARE/GRAYWARE	DESCRIPTIONS
Joke Program	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.
Hacking Tools	Helps hackers gain unauthorized access to computers.
Remote Access Tools	Helps hackers remotely access and control computers.
Password Cracking Applications	Helps hackers decipher account user names and passwords.
Others	Other types not covered above.

About Web Reputation

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

About Trend Micro Control Manager

Trend Micro Control Manager™ (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.

Control Manager consists of the following components:

- **Control Manager server**—The Control Manager server is the computer to which the Control Manager application installs. The Web-based Control Manager management console is hosted from this server.

  Note: You must install Patch 3 or later on the Control Manager 5.0 server for it to work with IMSS 7.1.

- **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 also collects logs from the product and sends them to Control Manager.

  Note: You do not need to install the agent separately. The agent automatically installs when you install IMSS.

- **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 on the Control Manager console displays all managed entities, and IMSS can be one of the entities.

  When you install an IMSS scanner, the Control Manager agent is also installed automatically. After the agent is enabled, each scanner will register to the Control Manager server and appear as separate entities.

Note: Use Control Manager server version 5.0 with patch 3 or later when using Control Manager to manage IMSS. For more information on the latest version and the most recent patches and updates, see the Trend Micro Update Center: http://www.trendmicro.com/download/product.asp?productid=7

Integrating with Control Manager

Table 1-5 shows a list of Control Manager features that IMSS supports.

TABLE 1-5. Supported Control Manager features

FEATURES	DESCRIPTIONS	SUPPORTED?
2-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
Log Upload for Query	Uploads IMSS virus logs, Content Security logs, and ERS logs to Control Manager for query purposes.	Yes
Single Sign-On	Manage IMSS from Control Manager directly without first logging on to the IMSS Web management console.	No. You need to first log on to the IMSS Web 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

TABLE 1-5. Supported Control Manager features

FEATURES	DESCRIPTIONS	SUPPORTED?
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.

TABLE 1-5. Supported Control Manager features

FEATURES	DESCRIPTIONS	SUPPORTED?
Configuration By User Interface Redirect	Configure IMSS through the IMSS Web management console accessible from Control Manager.	Yes
Renew Product Registration	Renew IMSS product license from Control Manager.	Yes
Mail-related Report on Control Manager	Generate the following IMSS mail-related reports from Control Manager: • Top 10 Virus Detection Points • All Entities Virus Infection List • Top 10 Infected Email Sender Report • Top 10 Security Violations Reports • Virus Infection Channel-Product Relationship Report • Filter Events by Frequency • Filter Events by Policy • Gateway Messaging Spam Summary Report • Gateway Messaging Spam Summary Report (for Domains)	Yes

TABLE 1-5. Supported Control Manager features

FEATURES	DESCRIPTIONS	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 Web management console: 1. Choose **Administration** > **Connections** from the menu. 2. Click the **TMCM Server** tab. 3. To enable/disable the agent, select/clear the check box next to **Enable TMCM 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

Chapter 2

Component Descriptions

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

Topics include:

- About IMSS Components on page 2-2
- IP Filtering on page 2-7
- Email Reputation Services on page 2-8
- About End-User Quarantine (EUQ) on page 2-15

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 section provides an overview of each component.

You can install IMSS components on a single computer or on multiple computers. For graphical representations of how these components work together, see Understanding Installation Scenarios on page 3-22.

The IMSS Admin Database

The IMSS admin database stores all global configuration information. The database contains server settings, policy information, log information, and other data that is shared between components. When installing IMSS, you must install the database server and run the appropriate queries to create the database tables before you install any other component. You can install a new database or use existing PostgreSQL databases.

Central Controller

The central controller contains a Web server component that serves Web console interface screens to browsers, allowing administrators to configure and control IMSS through the IMSS Web management console. The console provides an interface between the administrator and the IMSS database that the various components use to perform scanning, logging, and other message processing tasks.

Scanner Services

Servers configured as scanner services do the following:

- Accept SMTP and POP3 messaging traffic
- Request policy from a policy service
- Evaluate the message based on the applicable policies
- Take the appropriate action on the message based on the evaluation outcome
- Store quarantined and archived messages locally

- Log policy and system activity locally, and automatically update the log portion of the IMSS database at scheduled intervals, providing indexing to allow users to search through quarantined items and logs

As IMSS applies scanner service settings globally to all scanner services through the IMSS Web management console, choose servers that have the same hardware configuration to serve as scanner services. If your environment does not have computers with identical hardware configurations, set the scanner service limits so that they provide protection to the scanner service with the lowest resources. For instance, if you have two scanner services, one with a 10GB hard drive and another with an 80GB hard drive, set the maximum disk usage to 9GB to protect the computer with the least resources.

Alternatively, you can edit the scanner service's local configuration file to set the limit locally, as limits set in the configuration file override the global settings. Once you configure a scanner service locally, you can no longer configure it through the IMSS Web management console, and the interface may not reflect all the details of the local configuration.

Note: Use care when modifying an .ini file for customization. Contact your support provider if necessary.

Policy Services

To enhance performance and ensure that rule look-ups are efficient, IMSS uses a policy service to store the messaging rules using an in-memory cache. The policy service acts as a remote store of rules for the scanner services, caching rules that would otherwise require a database look-up (with associated network and disk I/O overhead). This mechanism also increases scanner service efficiency, allowing most message scanning tasks to occur in scanner service memory without the need for disk activity.

Policy Synchronization

The IMSS admin database schema includes a versioning mechanism. The policy service checks the database version periodically. If the version number in the database is different from the version cached on the policy service, the policy service performs a

database query and retrieves the latest version. This keeps the cached version of the database synchronized with the database, without the need to check the entire database for new or changed entries.

When you make changes through the IMSS Web management console, IMSS pushes the changes to the policy service within three minutes.

End-User Quarantine Service

The primary End-User Quarantine (EUQ) Service hosts a Web-based console similar to the IMSS Web management console so your users can view, delete, or resend spam that was addressed to them.

Primary and Secondary End-User Quarantine Services

To assist with load balancing, you can install additional EUQ services, referred to as *secondary services*. The first EUQ service you install, referred to as the *primary service*, runs Apache to work with the secondary services.

End-User Quarantine Server Components

The EUQ Server includes the following software components:

- **Apache HTTP Server**—Accepts the HTTP requests from end-users and distributes them across all installed EUQ Servers. Apache is only installed on the Primary EUQ Server.
- **Tomcat Application Server**—Accepts the HTTP requests from end-users and passes them to Struts.
- **Struts Framework**—Controls the page presentation flow for end-users.
- **End-User Quarantine Application**—Communicates with the other IMSS components to implement the EUQ Console logic.

The Tomcat and Apache servers are installed in the `{IMSS}/UI` directory. The other components are installed in the `{IMSS}/UI/euqUI` directory. Both Apache and Tomcat are controlled by the S99EUQ script in the `{IMSS}/script` directory accepting the stop, start and restart commands.

Apache and mod_jk

The Apache HTTP Server v. 2.0.58 (see http://httpd.apache.org/) is installed on the Primary EUQ Server and uses the Apache Tomcat Connector `mod_jk` (see http://tomcat.apache.org/connectors-doc/) loadable module to forward all requests to the locally installed Tomcat Application Server.

Apache is installed in the `{IMSS}/UI/apache` directory that has a standard Apache ServerRoot structure. The Apache main configuration file, `EUQ.conf` in the `{IMSS}/UI/euqUI/conf` directory, contains configuration settings that define the TCP port where Apache accepts incoming connections (8447), the maximum number of serviced connections (150) and configuration settings for `mod_jk`, including the name of the Tomcat thread that will receive all requests forwarded by Apache.

Tomcat

The EUQ Server uses Tomcat Application server to handle the requests from end-users. The Tomcat Application Server installed in the Primary EUQ Server also accepts requests from the Apache HTTP Server and balances the load across all installed EUQ Servers using the Apache JServ Protocol version 1.3 protocol AJP13 (see http://tomcat.apache.org/tomcat-3.3-doc/AJPv13.html) and the round robin algorithm.

The Tomcat configuration file, `server.xml` in the `{IMSS}/UI/euqUI/conf` directory, defines various configuration settings, including TCP port (8446), protocol (HTTPS) and location of the SSL key ring (`{IMSS}/UI/tomcat/sslkey/.keystore`).

The `workers.properties` configuration file in the `{IMSS}/UI/euqUI/conf` directory (http://tomcat.apache.org/tomcat-3.3-doc/Tomcat-Workers-HowTo.html) keeps configuration settings for the Tomcat worker threads. It defines two thread types: loadbalancer and worker. The loadbalancer threads distribute the load across all installed EUQ Servers. The worker threads process the incoming requests and run the End-User Quarantine Application. This configuration file is maintained automatically - the Manager updates it during restart based on the information about all available EUQ Servers from the `tb_component_list` database table.

The AJP13 protocol keeps permanent connection between Apache and Tomcat that is used to forward requests to Tomcat and receive the results of processing this request, without additional overhead.

Struts Framework

Struts is a Model-View-Controller Java-based Framework used to simplify development and control of the complex Java-based applications that process HTTP requests (see http://struts.apache.org/).

Struts controls the relationship between the incoming HTTP request, the Java-program (Servlet) that is used to process this request, and the Java Server Page (JSP) that is used to display a result of this processing.

Struts itself is a set of Java classes packaged in the `struts.jar` archive file configured by the `struts-config-common.xml` and `struts-config-enduser.xml` configuration files.

End-User Quarantine Application

The End-User Quarantine Application is written in Java and takes care of presenting, releasing, or deleting the quarantined mail messages based on the end-user requests. It also allows end-users to maintain their Approved Senders Lists.

To implement this functionality, EUQ accesses the Admin and EUQ databases and communicates with Managers.

The EUQ Application is implemented as a set of Java classes in the `com.trendmicro.imss.ui` package stored in the `{IMSS}/UI/euqUI/ROOT/WEB-INF/classes` directory and set of Java Server Pages stored in the `{IMSS}/UI/euqUI/ROOT/jsp` directory.

The EUQ Application writes the log entries in the `{IMSS}/log/imssuieuq.<Date>.<Count>` log file. The `[general]/log_level` configuration setting in the `imss.ini` file controls the amount of information written by the EUQ Application. To increase the amount of information logged, set `log_level` to "`debug`" and restart Tomcat using the S99EUQ script: "`S99EUQ restart`".

The End-User Quarantine Database

The EUQ database stores quarantined spam email information, and the end-user approved sender list. If you install EUQ service, you must also install the EUQ database (or multiple databases for scalability). You can also use an existing PostgreSQL database server to install the EUQ database.

You can install the EUQ database called `imsseuq` using one of the following options:

- On the Database Server that hosts the Administration database
- On the other database server available in the network
- Together with the database server software

One IMSS instance can have up to 8 EUQ databases. The EUQ data is distributed across all EUQ databases. If a database is lost, the users whose data were stored in this database will not have access to their quarantined data.

IP Filtering

IMSS includes optional IP Filtering, which consists of two 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 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 Services (ERS)**—Blocks email from known spam senders at the IP-level.

Email Reputation Services

Trend Micro designed Email Reputation Services to identify and block spam before it enters a computer network by routing Internet Protocol (IP) addresses of incoming mail connections to Trend Micro Threat Protection Network for verification against an extensive Reputation Database.

Types of Email Reputation Services

ERS provides two types of service: Standard and Advanced.

Trend Micro Email Reputation Services Standard

This service helps block spam by validating requested IP addresses against the Trend Micro reputation database, powered by the Trend Micro Threat Prevention 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.

ERS Standard Service 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, ERS reports that email message as spam. You can set up your MTA to take the appropriate action on that message based on the spam identification from ERS.

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

Trend Micro Email Reputation Services Advanced

This service identifies and stops sources of spam while they are in the process of sending millions of messages.

This is a dynamic, real-time anti-spam 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 ERS Standard, ERS 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. ERS Advanced Service 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 IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email containing threats mentioned in the section IP Filtering on page 2-7. You can customize several criteria that determine when IMSS will start 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.

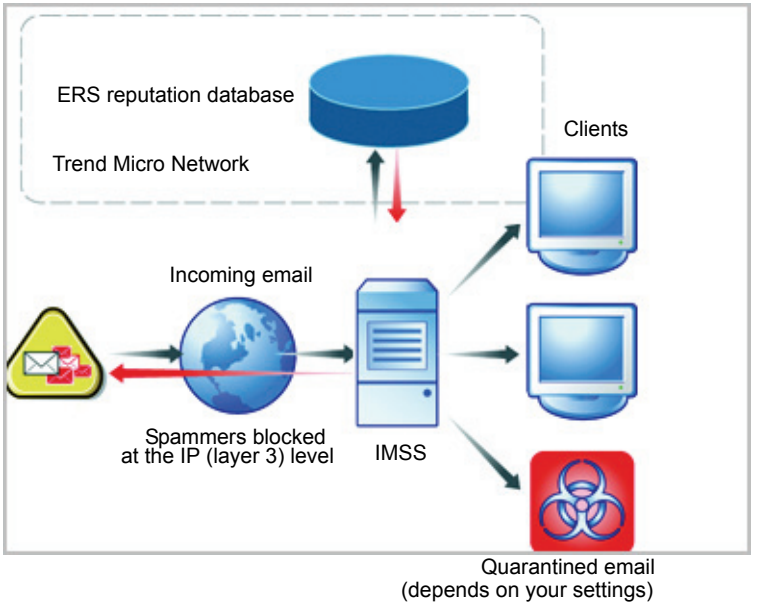
How Email Reputation Service Works

Trend Micro Email Reputation Services are Domain Name Service (DNS) query-based services. 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 ERS 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, ERS 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.

Figure 2-1 illustrates how ERS works.

FIGURE 2-1. How ERS works



For more information on the operation of Trend Micro Email Reputation Services, visit http://us.trendmicro.com/us/products/enterprise/network-reputation-services/index.html

Using the ERS Management Console

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

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

To open the ERS Management Console:

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

   https://tmspn.securecloud.com/

2. Log on using your Email Reputation Services user name and password. The Smart Protection Network portal opens with the **Email** tab selected and the **General** screen displaying.
3. Select **Global Spam Statistics** from the menu. The Global Spam Statistics screen appears.

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

TABLE 2-1. ISP Spam List

COLUMN	DESCRIPTION
Rank This Week	Displays the global rank for this week in terms of total spam volume.

TABLE 2-1. ISP Spam List

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

4. Click **News**. The News screen appears.

   The News screen displays breaking news about new spam and new features available for Email Reputation Services. Click the following tabs for information:

   - **Spam News:** Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.
   - **Release News:** Provides a brief overview of new features available in Email Reputation Services

5. To view reports that summarize the activity between the MTA and the Email Reputation Services database servers, do the following:
   a. Select **Report** from the menu. A sub-menu appears.
   b. Click one of the following:

TABLE 2-2. Report Types

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

6. To manage protection provided by ERS settings:
   a. Select **Policy** from the menu. A sub-menu appears.

b. Click one of the following:

TABLE 2-3. Policy Settings

POLICY	DESCRIPTION
Settings	Configure the Approved and Blocked senders lists. You can define your lists by individual IP address and CIDR by Country, or by ISP. • **Approved Sender:** Allows messages from the approved senders to bypass IP-level filtering. The Approved Sender lists are not applied to your MTA, but you can set up additional approved or blocked senders lists or do additional filtering at your MTA. • **Blocked Sender:** Instructs ERS to always block email messages from certain countries, ISPs, and IP addresses.
New ISP Request	Trend Micro welcomes suggestions from customers regarding other Internet Service Providers (ISPs) to be added to the service. Provide as much information about an ISP as you can. This helps Trend Micro to add the ISP to the service.
Reputation Settings	Configure ERS Standard and Advanced settings. Standard customers will see only the Enable Standard Settings section. Advanced customers will see both the Dynamic Settings and the Enable Standard Settings sections.

7. To change your password or Activation Code or to add your mail servers to ERS, choose **Administration** from the menu.

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).

Chapter 3

Planning for Deployment

This chapter explains how to plan for IMSS deployment.

Topics include:

- Deployment Checklist on page 3-2
- Component and Sub-module Installation on page 3-6
- IMSS Ports on page 3-8
- Network Topology Considerations on page 3-12
- About Operating Models on page 3-17
- Understanding Installation Scenarios on page 3-22
- IP Filtering on page 3-35
- About Failover on page 3-36

Deployment Checklist

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

TABLE 3-1. Deployment Checklist

TICK  WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Step 1 - Identify the location of IMSS		
	Choose one of the following locations on your network where you would like to install IMSS.		
	• Without a firewall		Installing without a Firewall on page 3-12
	• In front of a firewall		Installing in Front of a Firewall on page 3-13
	• Behind a firewall		Installing Behind a Firewall on page 3-14
	• On a former SMTP gateway		Installing on a Former SMTP Gateway on page 3-15
	• In the De-Militarized Zone		Installing in the De-Militarized Zone on page 3-16
	Step 2 - Plan the scope		
	Decide whether you would like to install one IMSS server or multiple servers.		

TABLE 3-1. Deployment Checklist

TICK ✓ WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	• Single-server installation		Single-Server Installation on page 3-22
	• Multiple scanner service		Multiple Scanner Service Installation on page 3-24
	• Multiple EUQ service		Multiple End-User Quarantine Service Installation on page 3-26
	• Complex distributed		Complex Distributed Installation on page 3-29
	• Wide area network		Wide-Area Network Installation on page 3-32
	• IP filtering **Tip:** Trend Micro recommends that you consider the failover plan before deciding on the scope.		IP Filtering on page 3-35
	Step 3 - Install or Upgrade		
	Perform a fresh installation of IMSS or upgrade from a previous version.		
	• Prepare MTA		Preparing Message Transfer Agents on page 4-4

TABLE 3-1. Deployment Checklist

TICK ✓ WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	• Install IMSS components		Installing IMSS Components and End-User Quarantine on page 4-11
	• Install IP Filtering	Yes	Installing IP Filtering Components on page 4-14
	• Upgrade from a previous version		Upgrading from Version 5.7 to Version 7.1 on page 5-5
	• Verify that installation is successful		Verifying the Installation on page 4-20
	Step 4 - Configure basic IMSS settings		
	Go through the 7 steps of configuring 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*.
	Step 5 - Start services		
	Activate IMSS services to start protecting your network against various threats.		
	• Scanner		IMSS Services section of the *Administrator's Guide*.
	• Policy		
	• EUQ	Yes	

TABLE 3-1. Deployment Checklist

TICK  WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Step 5 - Configure other IMSS settings		
	Configure various IMSS settings to get IMSS up and running.		
	• IP Filtering Rules	Yes	IP 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*.
	• 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*.
	Step 6 - Back up IMSS		
	Perform a full or minimal backup of IMSS as a precaution against system failure		

TABLE 3-1. Deployment Checklist

TICK ✓ WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Full backup		Backing Up IMSS section of the *Administrator's Guide*.
	Minimal backup		

Component and Sub-module Installation

When you install an IMSS component, additional sub-modules are also installed automatically. *Table 3-2* lists each component sub-module.

TABLE 3-2. Component and sub-module installation

MAIN COMPONENT	INSTALLED SUB-MODULE	SUB-MODULE DESCRIPTION
IMSS Admin Database	Administrator Database	The main IMSS admin database that stores all global settings.
	Database Server*	The server on which the IMSS admin database runs.
Central Controller	Apache® Tomcat®	The Web server for the IMSS Web management console, through which you configure settings.
	Named Server*	The DNS server for IP Profiler.
	FoxDNS	Contains the list of blocked and white IP addresses for IP Profiler and writes the list to the named server.
	IMSSMGR	A module that manages IMSS-related processes.

TABLE 3-2. Component and sub-module installation

MAIN COMPONENT	INSTALLED SUB-MODULE	SUB-MODULE DESCRIPTION
Scanner Service	Scanning Services	Performs all email-scanning actions.
	Policy Services	A remote store of rules for the scanner services, caching rules that would otherwise require a database look-up
	IMSSMGR	A module that manages scanner processes.
EUQ Service	Apache Tomcat	The Web server for the EUQ Web console, though which your users can access the email messages that IMSS quarantined as spam.
	Apache Service	Install this module with the primary EUQ services for load balancing purposes when you choose to install multiple EUQ services.
	IMSSMGR	A module that manages EUQ processes.
EUQ Database	EUQ Database	The database that contains all email messages that IMSS quarantined as spam.
	Database Server*	The server on which the EUQ database runs.
IP Profiler	FoxProxy	An IP Filtering module that checks the blocked list on FoxDNS to see if IMSS should reject or approve an email request.
	Foxlib	An IP filtering module that retrieves the IP address of the computer making a connection request and passes the IP address to Postfix.

TABLE 3-2. Component and sub-module installation

MAIN COMPONENT	INSTALLED SUB-MODULE	SUB-MODULE DESCRIPTION
ERS	Maillog Parser	A module to parse ERS-related mail logs.

Note: Sub-module(s) in the table marked with an asterisk (*) are the sub-components that you can choose to install when you install the main component.

IMSS Ports

See *Table 3-3* for the ports IMSS uses. Items with an asterisk (*****) are configurable from the IMSS Web management console.

TABLE 3-3. IMSS Ports

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
25	The Postfix mail 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.	master.cf
110	IMSS scanner generic POP3 port. The scanner uses this port to accept POP3 request and scan POP3 mails.	imss.ini / [Socket_2]/ proxy_port
5060	Policy Server listening port. The scanner will connect to this port to query matched rules for every message.	From the Web management console, click **Administration > IMSS Configuration > Connections > Components** on the menu.

TABLE 3-3. IMSS Ports

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
8005	Admin Web Server (Tomcat) management port that can handle Tomcat management commands.	{IMSS}/UI/adminUI/conf/server.xml: Server / port
8009	EUQ Console Tomcat AJP port. This port is used to perform load balancing between several Tomcat servers and the Apache HTTP server.	{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector (protocol=AJP/1.3) / port
8015	Tomcat management port that can handle Tomcat management commands.	{IMSS}/UI/euqUI/conf/server.xml: Server/port
8445	IMSS Web console listening port. Open this port to log on to the Web management console using a Web browser.	Tomcat listening port: {IMSS}/UI/adminUI/conf/server.xml: Server / Service / Connector / port
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 through this port for reprocessing.	imss.ini / [Socket_3]/ proxy_port

TABLE 3-3. IMSS Ports

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
10025	IMSS scanner scanning port. All messages that are sent through this port will be scanned by the scanner.	imss.ini / [Socket_1]/ proxy_port
10026	The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSS.) All messages sent through 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.	master.cf
15505	IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the Web management console. The manager also provides quarantine/archive query results to the Web management console and the EUQ Web console through this port.	From the Web management console, click **Administration > IMSS Configuration > Connections > Components** on the menu.

TABLE 3-3. IMSS Ports

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
IMSS uses the following ports when you enable related service:		
389	LDAP server listening port.	Not configurable on the IMSS server.
5432	PostgreSQL database listening port. Do not assign a different port number	You cannot change this port.
80	Microsoft IIS HTTP listening port. You need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu.
443	Microsoft IIS HTTPS listening port. You need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu
88	KDC port for Kerberos realm.	Not configurable on the IMSS server.
53	The Bind service listening port. Do not assign a different port number.	Not configurable on the IMSS server.

Note: Items with an asterisk are configurable from the IMSS Web management console.

Network Topology Considerations

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

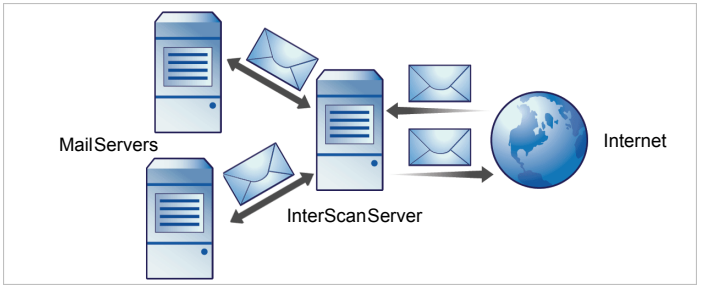
Deploy IMSS in an existing messaging environment at the SMTP gateway. This section provides a description of where IMSS fits in various network topologies, with illustrations of each scenario and general instructions for configuring other gateway services.

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

Figure 3-1 illustrates how to deploy IMSS and Postfix when your network does not have a firewall:

FIGURE 3-1. Installation topology: no firewall

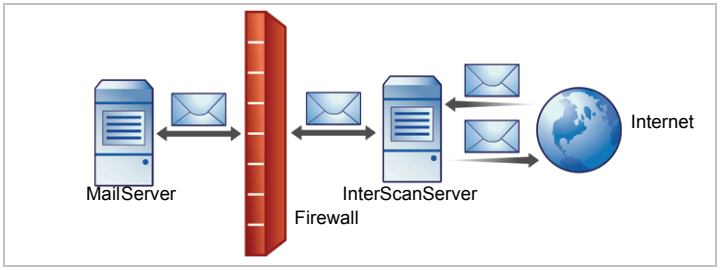


Note: Trend Micro does not recommend installing IMSS without a firewall. Placing the server hosting IMSS at the edge of the network may expose it to security threats.

Installing in Front of a Firewall

Figure 3-2 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 transfers them to IMSS. Configure IMSS to reference your SMTP server(s) or 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

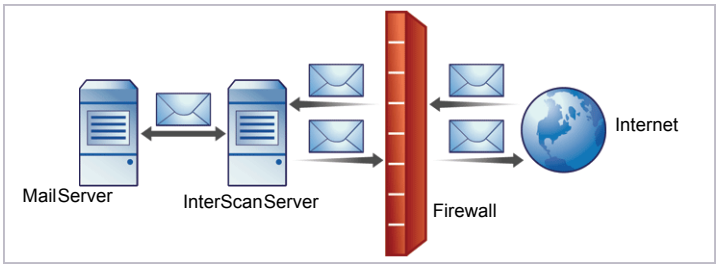
- Configure the firewall (proxy-based) to route all outbound messages to IMSS, so that:
  - Outgoing SMTP email goes to Postfix first and then to IMSS servers.
  - Incoming SMTP email can only come from Postfix to IMSS servers.
- Configure IMSS to allow internal SMTP gateways to relay, through Postfix, to any domain through IMSS.

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

Installing Behind a Firewall

Figure 3-3 illustrates how to deploy IMSS and Postfix behind your firewall:

FIGURE 3-3. Installation scenario: behind a firewall



Incoming Traffic

- Configure your proxy-based firewall, as follows:
  - Outgoing SMTP email goes to Postfix first and then to the IMSS server or the switch performing load balancing between scanners.
  - Incoming SMTP email goes 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 email destined to 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 mail to Postfix and then to IMSS servers.
- If you are replacing your SMTP gateway with IMSS, configure your internal mail server to send outgoing email through Postfix and then to IMSS servers.

- Configure Postfix and IMSS to route all outgoing email (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 Configuring SMTP Routing section of the *Administrator's Guide*.

Installing on a Former SMTP Gateway

You can also install IMSS and Postfix on the same server that formerly hosted your SMTP gateway.

On the SMTP gateway:

- Allocate a new TCP/IP port to route SMTP mail to IMSS. Ensure the port is not used by any other services.
- Configure IMSS to bind to the newly allocated port, which frees port 25.

Note: The existing SMTP gateway binds to port 25.

Incoming Traffic

- Configure IMSS to route incoming email to the SMTP gateway and the newly allocated port.

Outgoing Traffic

- Configure the SMTP gateway to route outgoing email to the IMSS port 25.
- Configure Postfix and IMSS to route all outgoing email (those messages destined to domains that are not local) to the firewall or deliver them.

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

Outgoing Traffic

- Configure Postfix to route all outgoing email (destined to 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 Configuring SMTP Routing section of the *Administrator's Guide*.

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:

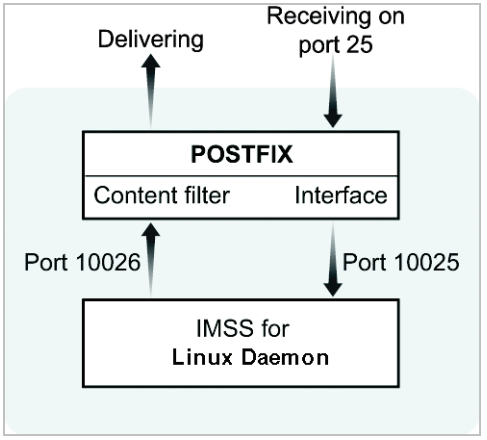
- **Standalone model**—Deploys IMSS on the same computer as an MTA, such as Postfix.
- **Sandwich model**—Deploys IMSS between an upstream MTA and a downstream MTA.
- **Proxy model**—Deploys IMSS between an upstream mail server and a downstream mail server.

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



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:

```
mydomain = your.domain.name
myhostname = your.hostname.domainname
mydestination = $myhostname, localhost.$mydomain,
$mydomain
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
```

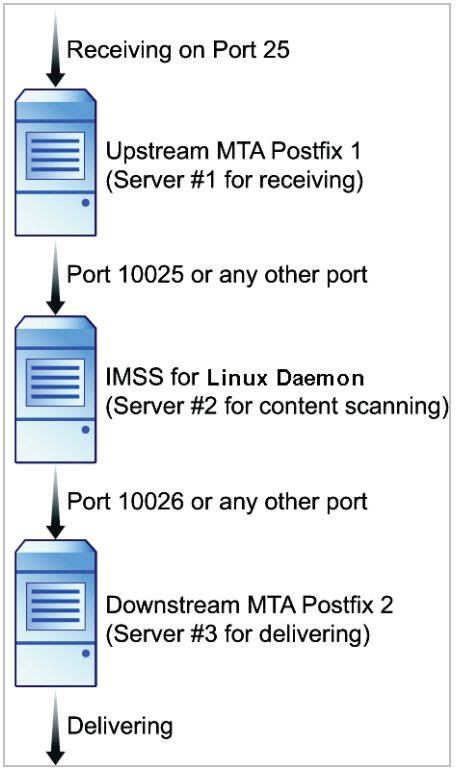
In /etc/postfix/master.cf:

```
#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
#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
```

The Sandwich Model

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

FIGURE 3-5. Sandwich model



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=smtp:[ip_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:

```
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
```

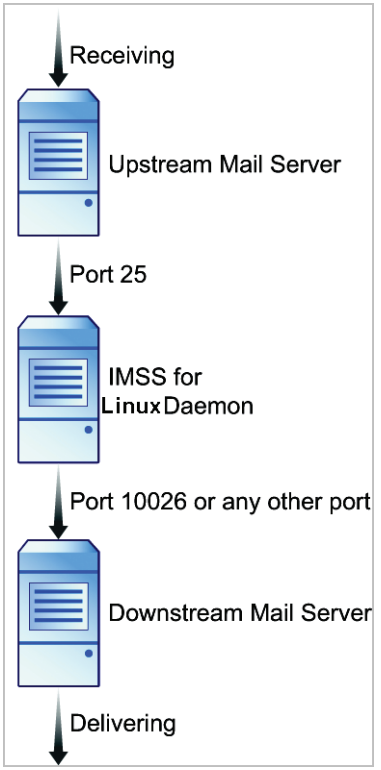
- In /etc/postfix/master.cf on server #3, modify smtpd settings to receive mail on port 10026:

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

The 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 3-6. 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.

Understanding Installation Scenarios

IMSS provides tools for installing either a single instance of each component on a single server (single-server installation) or installing the IMSS components on multiple servers (distributed deployment installation). Use the following information as a guide to choose a scenario.

Single-Server Installation

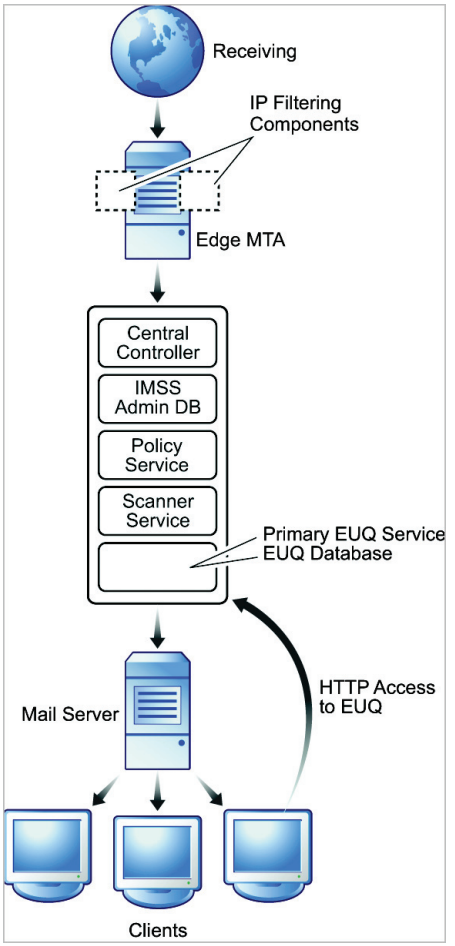
For a single-server installation, you need a server that meets the single-server installation requirements. The single-server installation of IMSS can handle average messaging traffic for approximately 1,000 users. If you install IMSS as a single-server installation and need to add capacity later, you can easily add additional scanner services by appending components to the existing IMSS server from the installation program.

You can install all the IMSS components on a single server, including:

- Central Controller
- IMSS Admin Database
- Policy Service
- Scanner Service
- Primary EUQ Service and EUQ Database

Figure 3-7 shows how a single-server installation of IMSS fits into a standard messaging network topology.

FIGURE 3-7. Single server deployment



To perform a single-server installation:

1. Install IMSS and End-User Quarantine (see Installing IMSS Components and End-User Quarantine on page 4-11).
2. On the edge MTA server, install all IP Filtering components (see Installing IP Filtering Components on page 4-14).

Multiple Scanner Service Installation

For some larger organizations, a single server cannot provide sufficient message throughput. In these cases, you can install all the IMSS components on one server, and then install the scanner service component on additional servers. The scanner services share access to the IMSS Admin database. You can also choose to install the end-user console to enable end-user quarantine (EUQ) management of spam quarantined items.

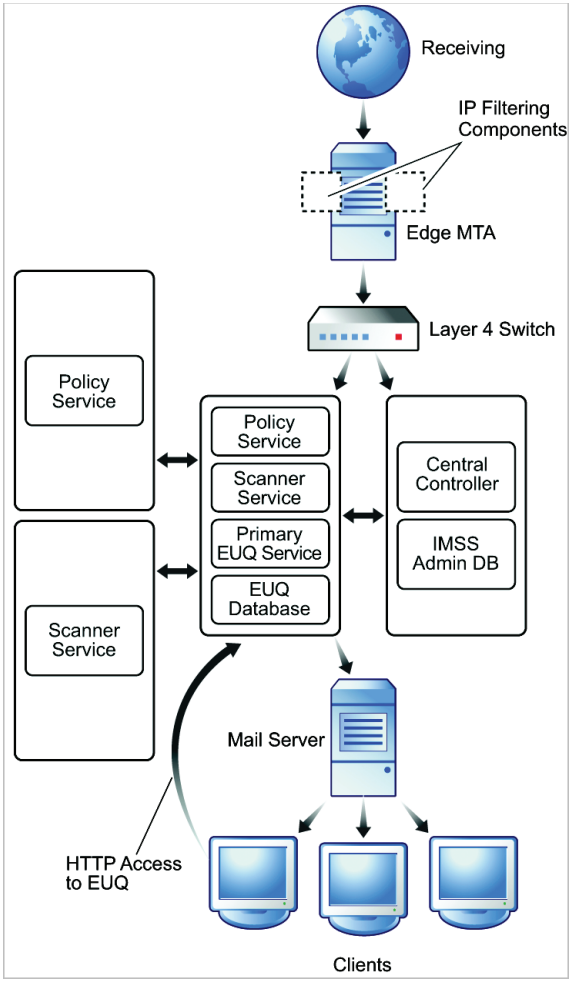
To handle a large amount of messaging traffic, you can install multiple IMSS scanner services as follows:

- Install one scanner service on your first server.
- Append the installation to install another scanner on a second server. To increase performance, add additional scanner services or policy service/scanner service pairs to your installation later.

Figure 3-8 shows how a single-server installation of IMSS with two additional scanner services fits into standard messaging network topology.

You must deploy a layer 4 switch between the MTA and the scanner services.

FIGURE 3-8. Multiple scanner service and policy service deployment



To perform a multiple scanner service installation:

1. On one computer, install IMSS and End-User Quarantine (see Installing IMSS Components and End-User Quarantine on page 4-11).
2. On other computers, install the necessary scanner service and policy services. On the edge MTA server, install all IP Filtering components (see Installing IP Filtering Components on page 4-14).

   Note: The policy service is always installed together with the scanner service. You can choose to start-up any policy service as needed.

3. After you open the IMSS Web management console and perform initial configuration (see *Performing Basic Configuration with the Configuration Wizard* section of the *Administrator's Guide*), go to the System Summary screen.
4. Click **Start** for the scanner or policy services you want to enable.

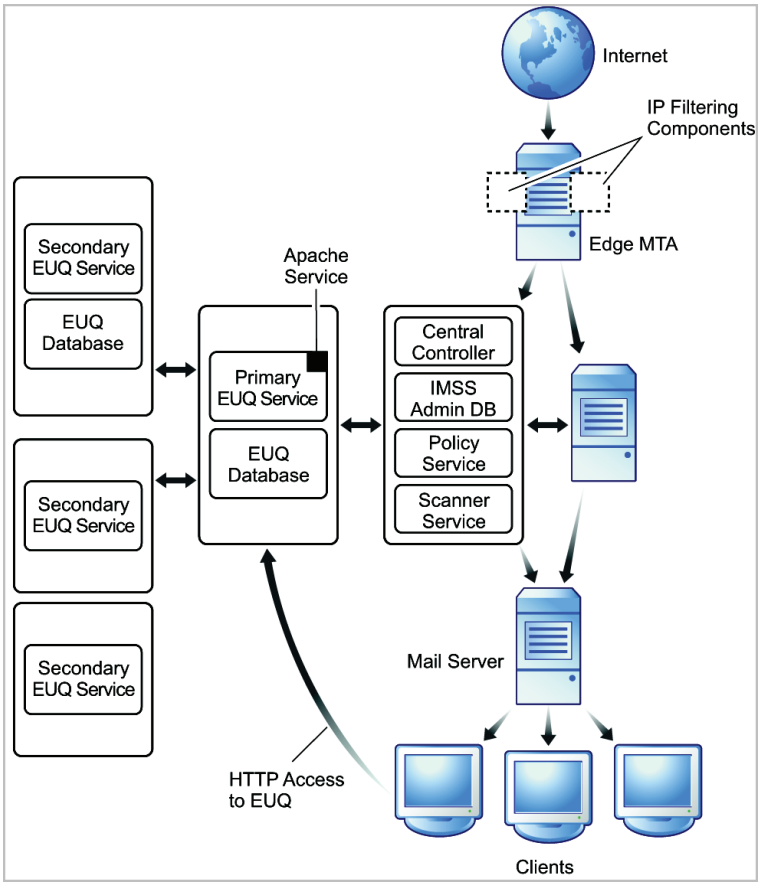
Multiple End-User Quarantine Service Installation

You can improve access to quarantined spam by installing several EUQ services.

If your organization is receiving large amounts of spam and you want to give your users access to the spam, install multiple secondary EUQ services.

Figure 3-9 shows how a single-server installation of IMSS with a separate primary EUQ service and additional secondary EUQ services (with Apache services for load balancing) and distributed EUQ databases fit into a standard messaging network topology.

FIGURE 3-9. Multiple EUQ service deployment



To perform a multiple EUQ service installation:

1. On one computer, install IMSS (see Installing IMSS Components and End-User Quarantine on page 4-11).

   Note: You can choose whether to install an EUQ service on the same computer. To install the first EUQ service on another computer, do not choose EUQ-related components on the first computer. The first EUQ service will be the primary EUQ service. For load balancing, the Apache service is installed with the primary EUQ service.

2. On other computers that can communicate with the primary EUQ service, install additional EUQ services. You must install at least one EUQ database for EUQ services. You can also install additional EUQ databases for better performance.

   Note: The EUQ database can be installed on the same computer where EUQ services will run, or on different computers. However, for performance reasons, IMSS does not allow installing multiple EUQ databases on the same database server.

3. On the edge MTA server, install all IP Filtering components (see Installing IP Filtering Components on page 4-14).
4. After you open the IMSS Web management console and perform initial configuration (see Performing Basic Configuration with the Configuration Wizard and Configuring IMSS Settings sections of the Administrator's Guide), go to the System Summary screen.
5. Click **Start** for the EUQ services you want to enable.

   Note: A single IMSS central controller and database can manage up to eight (8) EUQ services/databases.

Other Considerations When Deploying End-User Quarantine

For the end-users in your organization to be able to access the Web-based quarantine, they must have HTTPS access to the server. In addition, server hosting the EUQ components must be able to connect to the EUQ database that IMSS uses to store information about quarantined items.

This means that any firewall between EUQ and end-user computers on your network must not prevent HTTPS connections from internal addresses, or must be configured to allow such traffic.

You can also install Web-based quarantine and the database on a separate server from IMSS. In this case, you must configure any firewall between IMSS and the other server to allow database connections between them.

For more information, see Installing IMSS Components and End-User Quarantine on page 4-11.

Communication Between Servers

If you have an internal firewall, configure it to allow communication between IMSS, the EUQ service, and the database. For instance, if you install the EUQ service on one system, and the database on another, you must configure any firewall between the two systems to allow communication on port 5432. The systems use this port for database connectivity.

Complex Distributed Installation

For very large organizations, a distributed deployment installation is the best solution. You will need to have servers that meet the component installation requirements. In this scenario, you will be installing IMSS and EUQ components on different servers. You can install the database on one server, the central controller on another, and then install both a policy service and scanner service on additional servers.

You can also choose to install multiple instances of the end-user console to enable EUQ management of spam quarantined items. Likewise, you can install multiple EUQ databases to enhance EUQ performance.

If your environment requires high-throughput, you can install each IMSS component on a separate computer and deploy multiple scanner services, EUQ services, and databases.

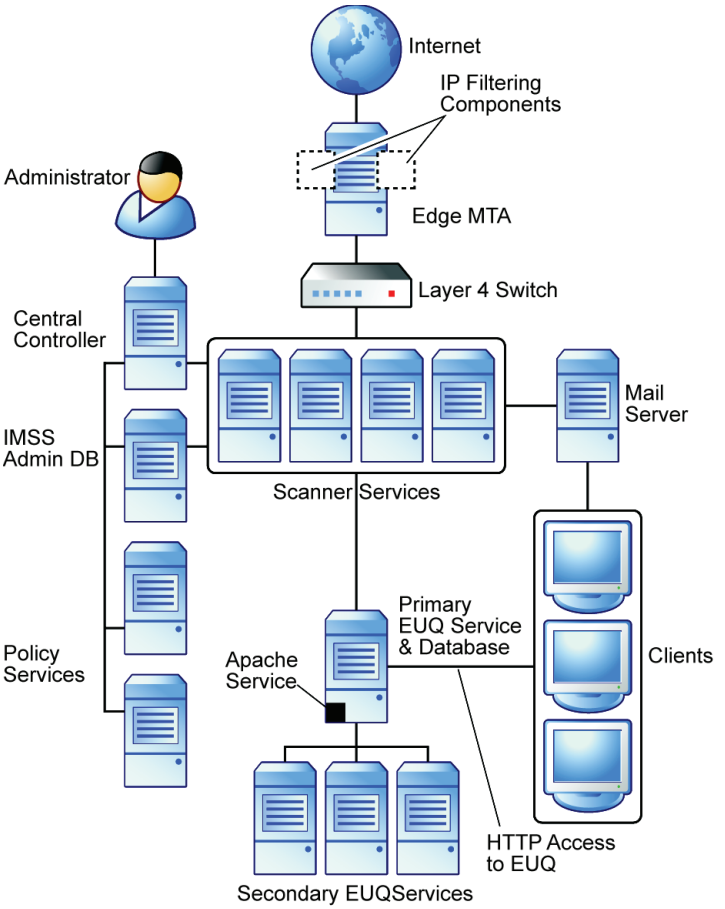
Note: Do not confuse EUQ databases with the IMSS admin database. You can install multiple EUQ databases, but only one IMSS admin database for a centralized IMSS deployment.

A centralized IMSS deployment can manage up to eight (8) EUQ services/databases.

Figure 3-10 shows how a centralized installation of IMSS with multiple scanner services, policy services, and EUQ services (with Apache services for load balancing) fits in a standard messaging network topology.

Note: The policy service is always installed together with the scanner service. You can choose to start up any policy service as needed.

FIGURE 3-10. Complex architecture deployment



Wide-Area Network Installation

If you have multiple sites over a wide area network (WAN), you can install components in a distributed scenario and deploy the IMSS components in a variety of ways.

Tip: To ensure proper communication between components, Trend Micro recommends that each site has at least one Central Controller component and one IMSS admin database component. To do this, perform a fresh IMSS installation at each site and append components on subsequent installation if you are installing multiple scanner or EUQ services.

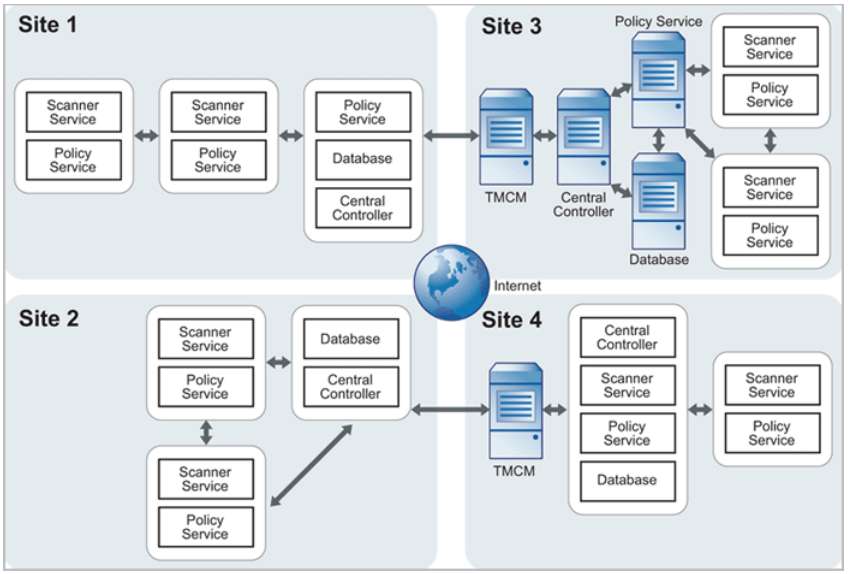
Trend Micro Control Manager

This scenario includes two Control Manager servers that manage all sites. Each Control Manager server can replicate database information between IMSS scanners registered to Control Manager.

Tip: To easily manage all IMSS servers (with Central Controllers installed), Trend Micro recommends installing a Trend Micro Control Manager™ (TMCM) server.

Figure 3-11 shows a multi-site WAN deployment.

FIGURE 3-11. WAN deployment



The following describes how each site differs in this scenario:

- **Site 1**—An IMSS server with a Central Controller, IMSS admin database, and policy service + two IMSS scanner services with policy services enabled.
- **Site 2**—An IMSS server with a Central Controller, IMSS admin database, and policy service + two IMSS scanner services with policy services enabled (for fault tolerance).
- **Site 3**—An IMSS Central Controller + IMSS admin database + a single policy service only + two IMSS scanner services with policy services enabled (for fault tolerance).
- **Site 4**—An IMSS server with a Central Controller and IMSS admin database + one IMSS scanner services with policy services enabled.

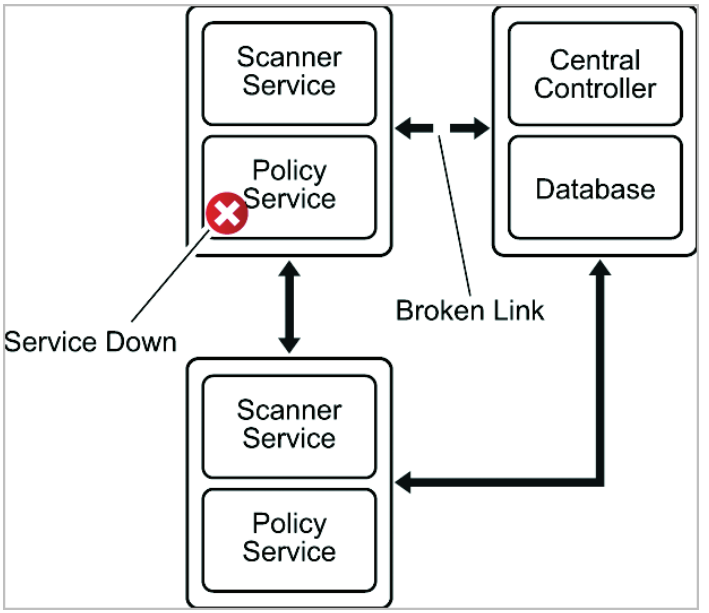
Fault Tolerance and Failover in a WAN Scenario

Three out of the four sites in this scenario use multiple scanner services with policy services installed. Policy services can access cached IMSS settings from the IMSS admin database. Any scanner service that goes down can use another active policy service. Therefore, if one policy service stops or if communication between the central database is interrupted, both scanner services will remain operational and continue processing mail by using the active policy service that has a connection to the IMSS server. See *Figure 3-12*.

Each site has its own Central Controller and database server, all of which are reporting back to two Control Manager servers. A Control Manager server can replicate IMSS admin databases that directly report to it. If one of the IMSS admin databases becomes corrupted or unoperational, you can restore the replicated databases.

Note: Control Manager servers cannot replicate IMSS admin database information if the server does not report to Control Manager.

FIGURE 3-12. Failover



IP Filtering

If you will be deploying IP Filtering (IP Profiler or ERS), there are some additional network topology considerations you must address.

Deploying IMSS with IP Filtering

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

Note: No address modification can occur between the edge of your network and the connection to IMSS. This means that any firewall between IMSS and the edge of your network must be of a type that does not modify the connecting IP address, or must be configured not to do so.

If IMSS always accepts SMTP connections from a router, for instance, the IP filter will not work, as this address would be the same for every received message and the IP filtering software would be unable to determine if the original initiator of the SMTP session was a known sender of spam.

For more information on deploying IMSS with IP Filtering, see Installing IP Filtering Components section of this document and IP Filtering Service section of the *Administrator's Guide*.

About Failover

Table 3-4 shows what happens when certain IMSS components malfunction, and how you can plan for failover to keep your IMSS protection up and running. For more information about failover in a WAN deployment scenario, see Fault Tolerance and Failover in a WAN Scenario on page 3-34.

TABLE 3-4. Failover Scenarios

COMPONENT THAT MALFUNCTIONS	EXPECTED RESULT	RECOMMENDED FAILOVER PLAN
Scanner service is not running or becomes disconnected	1. IMSS tries to restart the scanner service 2. IMSS sends an event notification if the service cannot be started within the time you specify for notifications.	Install multiple scanners for load balancing and failover. For details, see Multiple Scanner Service Installation on page 3-24.

TABLE 3-4. Failover Scenarios

COMPONENT THAT MALFUNCTIONS	EXPECTED RESULT	RECOMMENDED FAILOVER PLAN
Policy service is not running or a communication problem with the IMSS server occurs	1. Scanner services using the stopped policy service switch to an active policy service (if available). 2. IMSS tries to restart the policy service. 3. IMSS sends an event notification if the service cannot be started or reconnected within the time you specify for notifications.	Install multiple scanners for load balancing and failover. For details, see Multiple Scanner Service Installation on page 3-24.
IMSS admin database is not running	1. The IMSS server will continue to operate.	Back up the admin database periodically. For more information on backup and restore, visit www.postgresql.org.
EUQ service database is not running	1. An error message appears on the EUQ Web console.	Back up the EUQ Database periodically. For more information on backup and restore, visit www.postgresql.org.

TABLE 3-4. Failover Scenarios

COMPONENT THAT MALFUNCTIONS	EXPECTED RESULT	RECOMMENDED FAILOVER PLAN
LDAP server is not running	1. An error message appears on the EUQ Web console during EUQ log on. 2. Foxhunter will not use the LDAP settings. 3. If LDAP is disconnected and you have specified LDAP groups in the policy route, IMSS will continue to run normally using the cached LDAP entities (if available) when performing a policy match. IMSS will also automatically send an event notification regarding the disconnection to the addressees specified in **Administration** > **Notifications** > **Delivery Settings**. **Note:** IMSS automatically sends the LDAP disconnection notification in the backend and you cannot configure the notification settings from the Web management console.	Enable a secondary LDAP server as follows: 1. Choose **Administration** > **Connections**. 2. Click the **LDAP** tab. 3. Select the check box next to **Enable LDAP2** and provide the required information. **Tip:** Trend Micro recommends that you enable the fault tolerance feature on the LDAP server.

Chapter 4

Installing and Uninstalling IMSS 7.1

This chapter explains how to install IMSS under different scenarios.

Topics include:

- System Requirements on page 4-2
- Preparing Message Transfer Agents on page 4-4
- Installing IMSS Components and End-User Quarantine on page 4-11
- Installing IP Filtering Components on page 4-14
- Verifying the Installation on page 4-20
- Performing Uninstallation on page 4-21

System Requirements

Table 4-1 provides the recommended and minimum system requirements for running IMSS.

TABLE 4-1. System Requirements

HARDWARE/SOFTWARE	DESCRIPTION
Operating System	• Red Hat™ Enterprise Linux™ AS 4 Update 3 or above • Red Hat Enterprise Linux ES 4 Update 3 or above • Red Hat Enterprise Linux 5 servers **Note:** Only 32-bit operating systems for Red Hat are supported.
Recommended CPU	Intel™ Quad Core 1.6GHz or above
Minimum CPU	Intel™ Dual Pentium™ IV 3GHz or above
Recommended Memory	4GB RAM
Minimum Memory	2GB RAM
Recommended Disk Space	250GB total • 10GB for mail storage • 50GB or more for the Admin database • 20GB or more for the EUQ database • 40GB or more for the working quarantine folder **Note:** These recommendations are based on 500,000 email messages/day, a 50% quarantine rate, and logs preserved for a month.

TABLE 4-1. System Requirements

HARDWARE/SOFTWARE	DESCRIPTION
Minimum Disk Space	80GB total • 10GB for mail storage • 20GB for the Admin database • 10GB for the EUQ database • 10GB for the working quarantine folder **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/`.
Recommended Swap Space	• 2GB swap space if memory is greater than or equal to 4GB • 4GB swap space if memory is less than 4GB
Minimum Swap Space	2GB swap space
Browser	• Internet Explorer 6 SP1, 7 or 8 • Firefox 3.0
Monitor	Monitor that supports 800 x 600 resolution with 256 colors or higher
PostgreSQL	• Version 7.4 series: 7.4.8 or above • Version 8.1 series: 8.1.3 or above **Note:** IMSS for Linux is bundled with PostgreSQL 8.1.3.

TABLE 4-1. System Requirements

HARDWARE/SOFTWARE	DESCRIPTION
LDAP server	• Microsoft™ Active Directory 2000 or 2003 • IBM Lotus™ Domino™ 6.0 or above • Sun™ One LDAP 5.2 or above
MTA	• Postfix™: Version 2.1 or above • Sendmail™ 8.2 or above • Qmail™ 1.0.3 or above
Linux Libraries (for all platforms)	• glibc-2.3.4 • libstdc++-libc6.2-2.so.3 (Required for PostgreSQL)

Preparing Message Transfer Agents

IMSS supports three (3) types of Message Transfer Agents (MTA), namely, Postfix, Sendmail and Qmail. 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 www.postfix.org for details.

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

```
mydomain = your.domain.name
myhostname = your.hostname.domainname
```

```
mydestination = $myhostname, localhost.$mydomain, $mydomain
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
#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
```

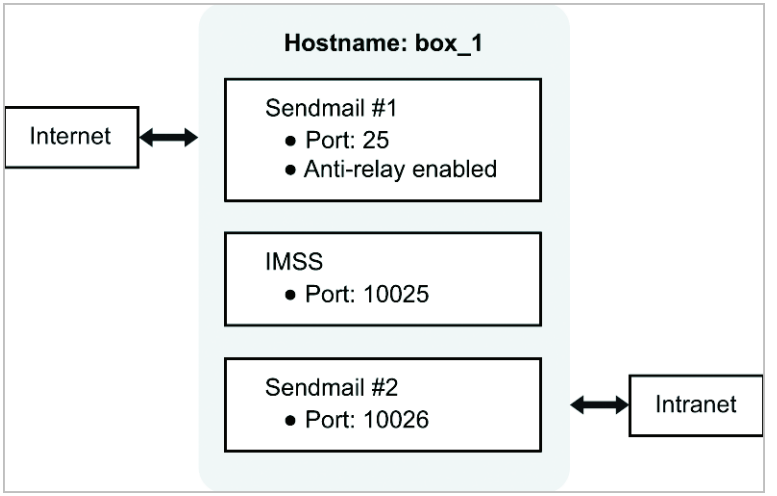
Using Sendmail

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

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

To configure Sendmail #1:

1. Copy the `Sendmail.cf` file called `Sendmail.cf.delivery`.
2. Change the "A" option in `sendmail.cf` for **Msmtp**, **Mesmtp**, **Msmtp8**, and **Mrelay** from "`TCP $h`" to "`TCP localhost.your_domain_name 10025`", where 10025 is an arbitrary free port on box_1.

3. Add the "k" flag to the "F" option for **Msmtp**, **Mesmtp**, **Msmtp8**, and **Mrelay** in `sendmail.cf`.

   The changes for **Msmtp** (as an example) should appear as follows:

   Msmtp Before:

   P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,

   T=DNS/RFC822/SMTP,

   A=TCP $h

   Msmtp After:

   P=[IPC], F=kmDFMuX, S=11/31, R=21, E=\r\n, L=990,

   T=DNS/RFC822/SMTP,

   A=TCP localhost.your_domain_name 10025

   To make these changes through the macro file, use the following:

   ```
   define('SMTP_MAILER_FLAGS','k')dnl
   define('SMTP_MAILER_ARGS','TCP [127.0.0.1] 10025')dnl
   ```

4. Replace the local mailer with [IPC] for **Mlocal** in `sendmail.cf`.
5. Change the "A" option to "`TCP localhost.your_domain_name 10025`" for **Mlocal** in `sendmail.cf`.
6. Add the "k" flag to the "F" option for **Mlocal** in `sendmail.cf`.

   The changes for **Mlocal** appear as follows:

   Mlocal Before:

   P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9, S=10/30, R=20/40,

   T=DNS/RFC822/X-Unix,

   A=mail.local -d $u

   Mlocal After:

   P=[IPC], F=klsDFMAw5:/|@qSmn9, S=10/30, R=20/40,

   T=DNS/RFC822/X-Unix,

   A=TCP localhost.your_domain_name 10025

   The corresponding (steps 4 - 6) changes to the macro file are:

   ```
   define('LOCAL_MAILER_PATH','[IPC]')dnl
   define('LOCAL_MAILER_FLAGS','k')dnl
   ```

define('LOCAL_MAILER_ARGS','TCP [127.0.0.1] 10025')dnl

Note: Make sure the "F" option of **Mlocal** does not include the "f"" and "z" flags.

Configuring Sendmail #2

To configure Sendmail #2:

1. Change the listening port to 10026 in `sendmail.cf.delivery` file.

   Before:

   O DaemonPortOptions=Name=MTA-v4, Family=inet

   O DaemonPortOptions=Name=MTA-v6, Family=inet6

   O DaemonPortOptions=Port=587, Name=MSA, M=E

   After:

   #O DaemonPortOptions=Name=MTA-v4, Family=inet

   #O DaemonPortOptions=Name=MTA-v6, Family=inet6

   #O DaemonPortOptions=Port=587, Name=MSA, M=E

   O DaemonPortOptions=Port=10026

   Corresponding macro file change:

   DAEMON_OPTIONS('Port=10026')dnl

2. Change the mail queue to a different directory in `sendmail.cf.delivery`.

   Before:

   O QueueDirectory=/var/spool/mqueue

   After:

   O QueueDirectory=/var/spool/mqueue1

   Corresponding macro file change:

   define('QUEUE_DIR','/var/spool/mqueue1')dnl

3. Create the directory `/var/spool/mqueue1` and make sure it has the same ownership and permissions as the original in `/var/spool/mqueue`.

4. Add the "k" flag to the "F" option for **Mlocal, Msmtp, Mesmtp, Msmtp8**, and **Mrelay** in `sendmail.cf.delivery`.

   The macro file changes are:

define('LOCAL_MAILER_FLAGS','k')dnl
define('SMTP_MAILER_FLAGS','k')dnl
define('ESMTP_MAILER_FLAGS','k')dnl
define('SMTP8_MAILER_FLAGS','k')dnl
define('RELAY_MAILER_FLAGS','k')dnl

Restarting Sendmail services

To finish Sendmail setup, restart Sendmail services:

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

   ```
   /usr/lib/sendmail -bd -q1h
   ```

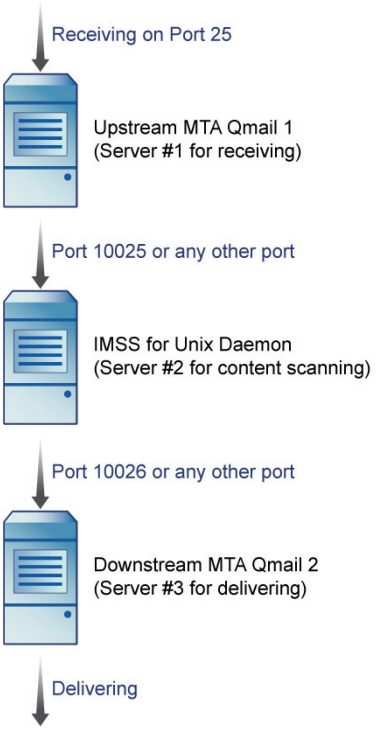
2. Restart the second Sendmail daemon to receive SMTP traffic from IMSS using the following command:

   ```
   /usr/lib/sendmail -bd -q1h -C/etc/mail/sendmail.cf.delivery
   ```

Using Qmail

The following illustration depicts deploying Qmail with IMSS based on the sandwich model.

FIGURE 4-2. Deploying Qmail with IMSS



For detailed information on installing and configuring Qmail, visit

http://www.lifewithqmail.org/lwq.html.

Note: You can only deploy IMSS using the sandwich or proxy model if you use Qmail as the MTA.

Configuring Qmail

To configure Qmail:

On the computer where Qmail is installed, add the name or IP address of the server that hosts IMSS to the `smtproutes` file using the command:

echo ":[server name/IP:port]" > /var/qmail/control/smtproutes

Installing IMSS Components and End-User Quarantine

This section shows you how to install IMSS components and End-User Quarantine.

When installing IMSS components, both the Admin and EUQ database must be in the same IP segment as IMSS. If the components are not in the same IP segment, the components cannot connect to the databases.

To resolve the issue:

1. Change the file "/var/imss/pgdata/pg_hba.conf" in both the Admin and EUQ databases by adding the following line:

   ```
   host all all <IMSS component IP address> <IMSS component
   netmask> password
   ```

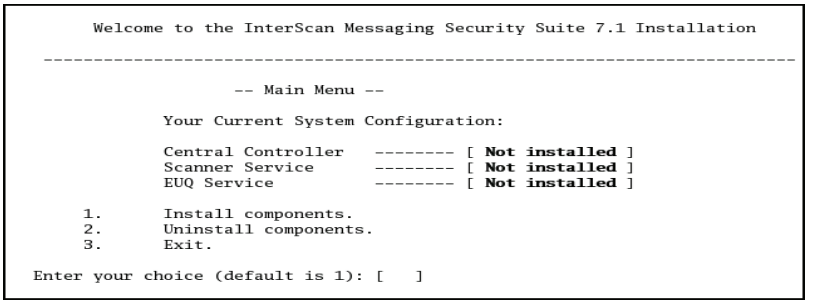
2. Reload the databases using the command:

   ```
   /opt/trend/imss/script/dbctl.sh reload
   ```

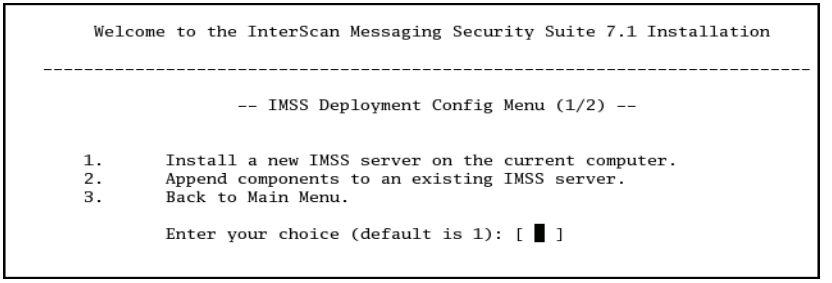
Installation Steps

The following is a list of the key steps you need to perform to install IMSS and End-User Quarantine.

1. Log on as a superuser and go to the installation package directory.
2. Type **`./isinst.sh`**. The Main Menu appears showing the status of each component. If you are installing IMSS for the first time, **[Not Installed]** appears.



3. Type **1** to begin installation.
4. Read and accept the license agreement.
5. On the IMSS Deployment Config Menu, decide whether to install a new IMSS server or append to an existing installation. To append a scanner service or EUQ service to an existing IMSS server, you will need the database information for those components.



6. Do one of the following:
   - If you chose to install a new IMSS server, decide whether to install a new database server or use an existing database server, and then type that database server's information.
   - If you chose to append the installation, type the database information.

```
      Welcome to the InterScan Messaging Security Suite 7.1 Installation

------------------------------------------------------------------------------

                    -- IMSS Deployment Config Menu (2/2) --

    Specify how to install the database.

    1.      Install a new database server on the current computer.
    2.      Use an existing database server.
    3.      Back to previous menu.

            Enter your choice (default is 1): [ ]
```

The Install Components Menu screen appears showing the status of the IMSS components. **[YES]** appears next to the component that the installer will install. By default, the installer will install **Central Controller** and a **Scanner Service**. These two components are necessary to use IMSS.

```
      Welcome to the InterScan Messaging Security Suite 7.1 Installation

------------------------------------------------------------------------------

                    -- Install Components Menu --

    InterScan Messaging Security Suite 7.1 Installation List

    Install Central Controller       -------- [ YES ]
    Install Scanner Service          -------- [ YES ]
    Install EUQ Service              -------- [ NO ]
    Install EUQ Database             -------- [ NO ]

    1.      Modify option for Central Controller.
    2.      Modify option for Scanner Service.
    3.      Modify option for EUQ Service.
    4.      Modify option for EUQ Database.
    5.      Modify option for Install path (current: /opt/trend).
    6.      Start installation.
    7.      Back to Main Menu.

Enter a choice (default is 6): [   ]
```

7. To modify the selection of the components to install, type the corresponding number for the component and enter yes **(Y/y)** or no **(N/n)** to the install question.

   You can also modify the install directory. The default is `/opt/trend`.

   The installer will install a primary service if no EUQ service exists. The installer will not install an EUQ service if an EUQ service exists.

If you want to install the EUQ database, you can install a new database server or use an existing database server, and then type that database server's information.

8. Type **6** to continue.

   The installer checks the available free disk space, memory, swap space, and BIND server on the computer and gives you an opportunity to cancel the installation if your computer does not meet the minimum requirements.

   If you continue the installation, required settings for your Postfix server appear. For a summary of these settings, see Preparing Postfix on page 4-4.

   Note: IP Profiler requires BIND server 9.x or above. Please make sure your existing DNS server meets this requirement. Otherwise, please uninstall the lower version of BIND, and then install BIND 9.5.0 (provided with the IMSS install package).

9. Press `Enter` to continue. The installer provides a note on whether the DNS server on your computer is active. To use IP Profiler, which you can install later, the DNS server must be active and running properly. For instructions on how to install IP Profiler, see Installing IP Filtering Components on page 4-14.

   Note: To verify DNS settings, use the command:
   nslookup www.antivirus.com

   A valid IP address should return.

10. Press `Enter` to begin installing the components you selected.

Installing IP Filtering Components

Trend Micro IP Filtering consists of two components:

- **IP Profiler**—Takes action on email messages when IMSS detects spam, virus threats, DHA, or bounced mail attacks.
- **Email Reputation Services (ERS)**—Blocks known spammers at the network (IP) level.

Installing Email Reputation Services and IP Profiler

The Trend Micro Email Reputation Service runs on a modified Postfix installation. The ERS installation script modifies the Postfix configuration files and installs a log parser to allow IP filter reporting. During installation, you will also be asked for an ERS Activation Code and for information about your IMSS Admin Database. Install the database before installing Email Reputation Services and IP Profiler.

The server on which you install ERS must already have an instance of Postfix installed. It must also be able to connect to the IMSS Admin Database and the server that is processing your messaging (most likely the IMSS server). Trend Micro recommends running ERS and IP Profiler on a gateway/edge server.

Note: You must activate ERS during installation, you cannot activate it later from the Web console.

If you are issued an Activation Code for Trend Micro Spam Prevention Solution (SPS), you can activate Email Reputation Service using the same SPS Activation Code.

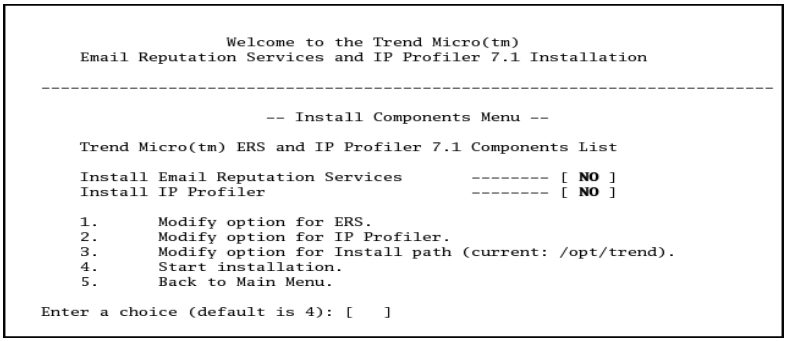
To install IP Profiler and ERS:

1. Log on as a superuser and go to the installation package directory.
2. Type **`./ipfilterinst.sh`**. The Main Menu displays showing the status of IP Profiler and ERS. If you are installing these products for the first time, **[Not Installed]** appears.

```
                    Welcome to the Trend Micro(tm)
     Email Reputation Services and IP Profiler 7.1 Installation

 ------------------------------------------------------------------------------

                          -- Main Menu --

              Your Current System Configuration:

              Email Reputation Services        -------- [ Not installed ]
              IP Profiler                      -------- [ Not installed ]

      1.      Install Components.
      2.      Uninstall Components.
      3.      Exit.

 Enter your choice (default is 1): [    ]
```

3. Type **1** to begin installation.
4. Read and accept the license agreement.

The Installation List screen appears showing the status of the two IMSS components. **[YES]** appears next to the component that the installer will install. By default, the installer will **not** install **IP Profiler** or **ERS**.



5. Choose to install IP Profiler or ERS:

   To install ERS:

   a. Type **1**. The ERS Configuration screen appears.

   b. Decide whether to install ERS on the current computer.

   c. Type the ERS Activation Code. The installer prompts you with a note about how it will change the Postfix server.

   d. Accept the change.

   e. The installer then prompts you to enter the following IMSS details to register ERS settings with the Admin database:

      i. IP address

      ii. Database name

      iii. Database user name

      iv. Database user password

   f. Type the path for the mail log.

      The install menu reappears showing **[YES]** next to **Install ERS**.

   To install IP Profiler:

   a. Type **2**. The IP Profiler Configuration screen appears.

b. Decide whether to install IP Profiler on the current computer.

c. Type a port for the IP Profiler (default is 25).

The installer prompts you with a note about ports if port 25 is already in use. Change the port number if necessary or change your Postfix listening port to 2500 after installation is complete.

d. Press `Enter` to continue.

e. Type the IP address where you installed the Central Controller that contains the IMSS foxdns. IP Profiler requires communication with foxdns.

f. Type the domain name of your mail server.

g. Press `Enter`.

h. The installer then prompts you to enter the following IMSS Postgres database details to register IP Profiler settings with the Admin database:

i. IP address

ii. Database name

iii. Database user name

iv. Database user password

Type the requested information. The install menu reappears showing **[YES]** next to **Install IP Profiler**.

6. To modify the install directory, type **3**, and then type the new directory path. The default is `opt/trend`.
7. Type **4** to begin the installation.
8. Press Enter to begin installing the components you selected.

Integrating IMSS with Sendmail and Qmail

IMSS allows you to replace Postfix with other MTAs. This section describes the procedures for configuring Sendmail and Qmail to support FoxProxy and ERS.

Integrating FoxLib with Sendmail

If IP Profiler is used together with the Sendmail MTA, the following steps must be done to ensure that Sendmail uses FoxLib and therefore gets the real IP address of the SMTP client contacting FoxProxy:

1. Change the listening port to 2500 in the `sendmail.cf` file and restart sendmail.

   Before:

   O DaemonPortOptions=Name=MTA-v4, Family=inet

   O DaemonPortOptions=Name=MTA-v6, Family=inet6

   O DaemonPortOptions=Port=587, Name=MSA, M=E

   After:

   #O DaemonPortOptions=Name=MTA-v4, Family=inet

   #O DaemonPortOptions=Name=MTA-v6, Family=inet6

   #O DaemonPortOptions=Port=587, Name=MSA, M=E

   `O DaemonPortOptions=Port=2500`

2. Collect information about Sendmail:

   a. Use the `which` command to find the Sendmail program file:

      # which sendmail

      /usr/sbin/sendmail

   b. Use the `ls` command to identify the user and group used by Sendmail:

      # ls –al /usr/sbin/sendmail

      -rwxr-sr-x 1 root root 732356 Sep 1 2004 /usr/sbin/sendmail

      (User is root and group is root)

   c. Find the user ID and the group ID for the user and group used by Sendmail:

      `# fgrep root /etc/passwd`

      root:x:0:0:root:/root:/bin/bash

      `# fgrep root /etc/group`

      root:x:0:root

      (User ID is 0, group ID is 0)

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

   a. Set the `TM_FOX_UID` parameter to the user ID:

TM_FOX_UID=0

b. Set the `TM_FOX_GID` parameter to the group ID:

TM_FOX_GID=0

c. 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/ipprofiler/config` directory:

- Change the value of the `has_foxlib_installed` parameter from "0" to "1"

5. Use the `foxlibd` script instead of `sendmail` to start Sendmail:

/opt/trend/ipprofiler/script/foxlibd start/stop

6. Restart FoxProxy:

/opt/trend/ipprofiler/script/foxproxyd start/stop

Integrating FoxLib with Qmail

If IP Profiler is used together with the Qmail MTA, the following steps must be done to ensure that Qmail uses FoxLib and therefore gets the real IP address of the SMTP client contacting FoxProxy:

1. Modify the Qmail start script.

a. If you have installed the daemon tool to start Qmail, the smtpd start script should be located at `/service/qmail-smtpd/run`.

b. Modify the run file and add the following lines at the head of the file after the line that contains `#!/bin/sh`

TM_FOX_PROXY_LIST=/opt/trend/ipprofiler/config/foxproxy.list

LD_PRELOAD=/lib/libTmFoxSocketLib.so

TM_FOX_PROXY_CONNECT_PORT=2500

export TM_FOX_PROXY_CONNECT_PORT

export TM_FOX_PROXY_LIST

export LD_PRELOAD

2. Get the qmail user and group, then copy the correct `.so` file.
   a. Run the following commands to check user and group:

      #id qmaild

      uid=101(qmaild) gid=100(nofiles)

      The smtp user is qmaild, and the group is nofiles.

   b. Copy the `.so` file to the correct path, change its attributes, then run the following commands:

      #cp /opt/trend/ipprofiler/lib/libTmFoxSocketLib.so /lib/libTmFoxSocketLib.so

      #chown qmaild /lib/libTmFoxSocketLib.so

      #chgrp nofiles /lib/libTmFoxSocketLib.so

      #chmod 550 /lib/libTmFoxSocketLib.so
3. Modify the `foxproxy.ini` configuration file in the `/opt/trend/ipprofiler/config` directory as follows:

   Change the value of the `has_foxlib_installed` parameter from "0" to "1"
4. Run the following script to restart foxproxyd:

   #/opt/trend/ipprofiler/script/foxproxyd restart
5. Type the following command to start Qmail:

   #/command/svscanboot </dev/null >/var/log/svscan 2>&1 &

   Alternatively, restart the system if Qmail has been started previously and has been added into the system start-up script.

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.

Performing Uninstallation

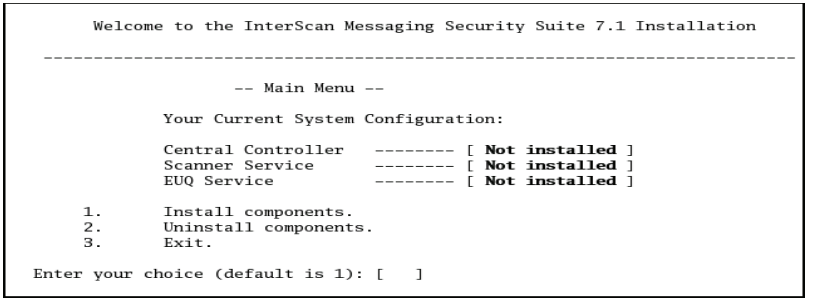
This section describes how to remove IMSS components.

After uninstalling IMSS 7.1, report data that was generated is backed up to `/opt/trend/installlog/data`. This occurs only if IMSS was installed at `/opt/trend`.

Uninstalling IMSS Components

You can uninstall the Central Controller, Scanner services, and EUQ components separately or concurrently.

1. Log on as a superuser and go the installation package directory.
2. Type **`./isinst.sh`**. The Main Menu shows the status of the components. If you already installed these products, **[Installed]** appears.



3. Type **2**.

   The uninstallation menu appears showing the components that you can remove. By default, the uninstallation status for each component is set to **[NO]**, signifying that they will not be removed. If a component was not installed, **[Not installed]** appears.
4. To remove the components, type the number that corresponds to the component, and then type **Y/y** to change the uninstall status to **[YES]** on the uninstallation menu.
5. After you have changed the uninstallation status to **[YES]** for the components that you want to uninstall, type **4**.

The components uninstall.

Note: During the uninstallation, a message will display prompting if you would like to stop the PostgreSQL process. You can choose not to stop the process if some other applications are still using it.

Uninstalling Email Reputation Services and IP Profiler

To uninstall ERS and IP Profiler:

1. Log on as a superuser and go the installation package directory.
2. Type **`./ipfilterinst.sh`**. The Main Menu displays showing the status of IP Profiler and ERS. If you already installed these products, **[Installed]** appears.
3. Type **2**.

   The uninstallation menu appears showing the components that you can remove. By default, the uninstallation status for each component is set to **[NO]**, signifying that they will not be removed. If a component was not installed, **[Not installed]** appears.
4. To remove the components, type the number that corresponds to the component, and then type **Y/y** to change the uninstall status to **[YES]** on the uninstallation menu.
5. After you have changed the uninstallation status to **[YES]** for the components that you want to uninstall, type **3**.

   The components uninstall.

Performing Manual Uninstallation

Uninstalling IMSS Manually

Uninstall IMSS manually only if automated uninstallation encounters issues.

To uninstall IMSS manually:

1. Stop all IMSS related processes using the command:

   $Home_IMSS/script/imssstop.sh
2. Remove the IMSS package as follows:

rpm -e imsscctrl-7.1-1

rpm -e imss-7.1-1

rpm -e imsseuq-7.1-1

If some components have not been installed, the uninstall command may not work.

3. Remove `$Home_IMSS`, such as `/opt/trend/imss`.
4. Remove daemon start/stop scripts.
   - Start scripts run automatically upon system restart. Remove these scripts from `/etc/rc2.d/ /etc/rc3.d /etc/rc5.d`.

     S99IMSS, S98dbctl, S99CMAGENT, S99POLICY, S99bindctl, S99IMSSUI, S99FOXDNS, S99SCHEDULED, S99MONITOR, S99MANAGER
   - Stop scripts kill the processes automatically upon system shutdown. Remove these scripts from `/etc/rc0.d and /etc/rc6.d`.

     K98dbctl, K97CMAGENT, K97IMSS, K97POLICY, K97EUQ, K97bindctl, K97IMSSUI, K97FOXDNS, K97SCHEDULED, K96MONITOR, K96MANAGER, K99IMSSSTOP

Uninstalling the Database Manually

Uninstall the database manually only if automated uninstallation encounters issues.

To uninstall database manually:

1. Stop postmaster processes using the command:

   $Home_IMSS/script/dbctl.sh stop

   OR

   Stop the processes forcefully using the command:

   kill -9 pid
2. Remove `$Home_IMSS/PostgreSQL`.
3. Remove `/var/imss`.
4. Remove `/tmp/.sPGSQL.5432`, and `/tmp/.s.PGSQL.5432.lock`, if you choose to kill the processes forcefully in step 1.

Uninstalling Postfix Manually

To uninstall Postfix manually:

1. Stop Postfix related processes using the command `postfix stop`
2. Remove `/etc/postfix`.
3. Remove `/usr/libexec/postfix`.
4. Remove Postfix related files from the directory `/usr/sbin/post*`, such as:
   - postalias
   - postcat
   - postconf
   - postdrop
   - postfix
   - postkick
   - postlock
   - postlog
   - postmap
   - postqueue
   - postsuper
5. Remove `/var/spool/postfix` (optional).

Uninstalling IP Profiler Manually

To uninstall IP Profiler manually:

1. Stop IP Profiler related processes using the command:
   /opt/trend/ipprofiler/script/foxproxyd stop
2. Remove IP Profiler and ERS packages using the command:
   rpm -e ipprofiler-7.1-1
   rpm -e nrs-7.1-1
3. Remove `/etc/postfix/ imss_rbl_reply`.
4. Recover the configuration in `main.cf`.
5. Recover the configuration for mail debug in `/etc/syslog.conf`.

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 from Version 5.7 to Version 7.1 on page 5-5
- Backing Up IMSS 5.7 Settings on page 5-15
- Migrating from IMSS 5.7 to IMSS 7.1 on page 5-19
- Installing IMSS 7.1 Over IMSS 5.7 on page 5-21
- Upgrading from IMSS 7.0 to IMSS 7.1 on page 5-25
- Migrating from IMSS 7.0 to IMSS 7.1 on page 5-30
- Activation of Supported Services on page 5-32
- Rolling Back the Upgrade on page 5-32

Upgrading from an Evaluation Version

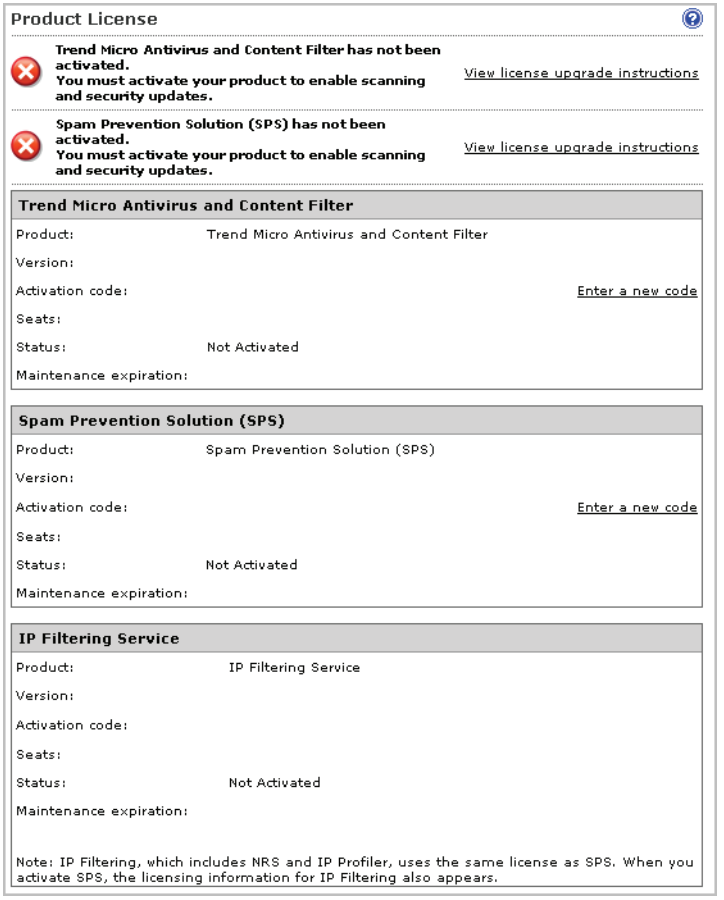
If you provided an evaluation Activation Code to activate IMSS previously, you have started an evaluation period that allows you to try the full functionality of the product. The evaluation period varies depending on the type of Activation Code used.

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

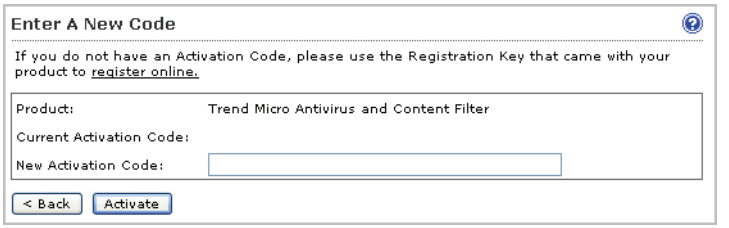
To continue using IMSS, please purchase the full licensed product. You will then be provided a new licensed Activation Code.

To upgrade from the evaluation period:

1. Choose **Administration** > **Product Licenses** from the menu.



2. Click the **Enter a new code** hyperlink under the Trend Micro Antivirus and Content Filter or Spam Prevention Solution (SPS) sections accordingly.



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**.

Upgrading from Version 5.7 to Version 7.1

Upgrading from IMSS 5.7 to IMSS 7.1 can be done in one of the following ways:

- Installing a fresh version of IMSS 7.1 on a server and then migrating all settings from IMSS 5.7
- Installing IMSS 7.1 over an installation of IMSS 5.7

Tip: 1. Trend Micro recommends migration, using the Migration Tool, to perform an upgrade instead of installing over the previous version.

2. Although the installation program will back up your old IMSS settings, Trend Micro recommends that you back up your version 5.7 settings manually before performing the migration (see Backing Up IMSS 5.7 Settings on page 5-15). If problems occur during migration, you can roll back to version 5.7 (see Rolling Back the Upgrade on page 5-32).

3. If you choose not to migrate your old IMSS settings, Trend Micro recommends that you completely uninstall IMSS 5.7 and then do a fresh install, rather than installing IMSS 7.1 over an existing installation.

The IMSS installation program can automatically upgrade from InterScan Messaging Security Suite version **5.7** on the supported platforms. If the installation program detects this version, it can do the following:

WARNING! **1. The installation program does not support automatic rollback from IMSS 5.7. If the installation encounters issues, a manual rollback is the only option.**

2. After upgrading, IMSS 5.7 queue data will be lost.

---

1. Back up your old IMSS settings
2. Install IMSS 7.1
3. Migrate the existing settings

Upgrading IMSS 5.7: Policy Recommendations

To streamline migration and to avoid issues during migration, Trend Micro recommends the following actions before exporting configuration settings:

- Remove unused policy objects
- Merge policy objects
- Modify existing policy objects

Removing Unused Policy Objects

Removing unused policy objects before exporting configuration settings can improve performance and simplify policy management for the new IMSS server.

TABLE 5-1. Unused Policy Objects to Remove

UNUSED POLICY OBJECT	BENEFIT
Policy routes	Reduces policy management
Policies	Reduces the number of migrated filters
Sub-policies	Reduces complexity of inheritance relationships
Spam block/approved list entries	Improves performance
Keywords and expressions	Improves performance
Address groups	Improves performance
Filter actions	Improves performance
Quarantine areas	Improves performance

Merging Policy Objects

Merging policy objects results in improved performance and simplified policy management.

- Merge similar filters whenever possible. For example, attachment filters enabling "attachment extension and name", "MIME type", and "attachment type" separately could be merged into single policy.
- Merge SPS filter's "Blocked senders", "Phishing emails" and "Spam" action names. For example, if SPS filters were configured with different action names and those filters take the same actions, rename them using the same name.
- Merge policies of the same priority level.
- Merge quarantine areas because IMSS 7.1 does not support quarantining email messages to different physical folders.

Modifying Policy Objects

For policy objects that do not migrate, described in *Table 5-2. IMSS 5.7 Settings that cannot migrate* on page 5-9, modify the objects to other similar functions to avoid unexpected behavior.

For policy objects that migrate, described in *Table 5-3. IMSS 5.7 settings that change after migrating* on page 5-12, modify them to other similar functions if you do not want migration to change them.

Upgrading IMSS 5.7: Process Recommendations

The following topics outline Trend Micro recommended tasks when upgrading from IMSS 5.7 to IMSS 7.1.

Perform a Fresh Installation of IMSS 7.1

Perform a fresh installation of IMSS 7.1, and then migrate to IMSS 7.1, instead of installing over an existing IMSS 5.7 installation.

Tip: 1. Prepare the system environment according to Trend Micro recommended system requirements.

2. Carefully plan your deployment strategy for IMSS 7.1.

Become Familiar with IMSS 7.1 Before Upgrading

To ease implementing IMSS 7.1 into the network, administrators need to familiarize themselves with IMSS 7.1 before upgrading from IMSS 5.7. This also gives administrators the opportunity to learn about new features.

Tip: 1. Study the Administrator's Guide.

2. Create a test environment for IMSS 7.1 to test functions and policies.

General IMSS 5.7 Migration Tasks

Perform the following tasks to simplify migration:

- Delete all mail messages under the quarantine and archive areas.
- Clean up IMSS 5.7 policies. See Upgrading IMSS 5.7: Policy Recommendations on page 5-6 for detailed information.
- Export settings using the Export Tool.
- If you want to continue testing the delivery route, do not migrate MTA settings. This will mean manually configuring MTA settings after migration.

Tip: If no complex address groups, detailed approved lists, or rules exist in IMSS 5.7, Trend Micro recommends manually configuring IMSS 7.1.

Verify IMSS 7.1 Operation after Migration

After migration is complete, perform the following tasks to verify that migration completed successfully:

- Open the Summary screen to verify all services can start successfully.
- Navigate to the Policy section of the IMSS 7.1 Web console to verify that policies have the same settings as those in IMSS 5.7.
- Send sample email messages to verify that IMSS 7.1 has the same message delivery behavior as IMSS 5.7.

IMSS 5.7 Settings that Cannot be Migrated

Certain IMSS 5.7 settings cannot migrate to IMSS 7.1:

TABLE 5-2. IMSS 5.7 Settings that cannot migrate

SETTING	SETTINGS NOT MIGRATED
EUQ Settings	EUQ approved senders
	EUQ spam mail
	LDAP server settings
	LDAP group settings
MTA Settings	Postfix settings manually configured (Web console was not used to configure the settings)
	IP address of SMTP Interface
NRS Settings	All settings
Policy Settings	Security limits: • "Number of cleaning attempts" • "Number of viruses reported" • "Message size"
	Virus actions: • "No virus detected" • "Joke program attachment detected"

TABLE 5-2. IMSS 5.7 Settings that cannot migrate

SETTING	SETTINGS NOT MIGRATED
Policy Settings	Spam Filter settings: • "Global spam scanning mode" • "Baseline detection rate" • "Additional sensitivity" • Approved and blocked lists for POP3 • Actions for Graymail • Advanced action settings
	Advanced Content Filter settings: • Expression list for Mail attachments
	Expression settings: • Synonym settings • Disabled expressions
	Processing actions: • Quarantine original message • Forward original message
	Archive actions: • Archive to specific folder • Archive original message
	Notify actions: • Notifications with original mail attachments
	All Outbreak Prevention Filters
	PASE related settings

TABLE 5-2. IMSS 5.7 Settings that cannot migrate

SETTING	SETTINGS NOT MIGRATED
Configuration Settings	Log paths
	Postpone paths
	Limit on notifications for process per hour
	Web console password
	Database settings
	TMCM settings
Quarantine/Archive folder path and email	Path of quarantine area and archive folder paths
	Email messages in queue folder
Report Settings	Perl reports
	SPS reports

IMSS 5.7 Settings that Change After Migration

Certain IMSS 5.7 settings change after migrating to IMSS 7.1:

TABLE 5-3. IMSS 5.7 settings that change after migrating

SETTING	SETTINGS THAT CHANGE
Policy Settings	Message size filter: • If an attachment/message size exceeds 99999MB, migration truncates the attachment/message size to 99999MB. • If the number of attachments in an email message exceeds 99999, migration truncates the number to 99999.
	Scanning limits: Any policies that exceed the maximum value for IMSS 7.1 will be reset to the maximum value for IMSS 7.1.
	Forward actions: Migration changes the filter's forward action to "Change Recipient", and scan exception's forward action to "Delete and Notify"
	Archive actions: Migration changes "archive to mail" to "BCC"
	Message tokens: Migration changes: • "%GLOBALACTION%" to "%ACTION%" • "%ACTION%" to "%VIRUSACTION%" for the antivirus filter and "TACTION" for other types of filters

TABLE 5-3. IMSS 5.7 settings that change after migrating

SETTING	SETTINGS THAT CHANGE
Configuration Settings	Maximum log file size: If the minimum log size is less than 100MB, migration changes this setting to 100MB. If the maximum log size exceeds 99999MB, migration changes this setting to 99999MB. Specifying "0" (meaning there is no limit to the log file size) is no longer supported.
	Number of days to keep log: If IMSS 5.7 settings specify keeping logs less than 150 days, migration changes the setting 150 days. Specifying "0" (meaning there is no limit to the length of time to keep files) is no longer supported.
	Notifications: If the SMTP server setting specifies "default", migration changes the value to "127.0.0.1".

Upgrade Options for Multiple Scanner Deployment

If you have installed multiple scanner services in IMSS 5.7, you may need to perform the upgrade differently depending on whether you want to install a single admin database shared by all the scanners or one admin database for each scanner in IMSS 7.1.

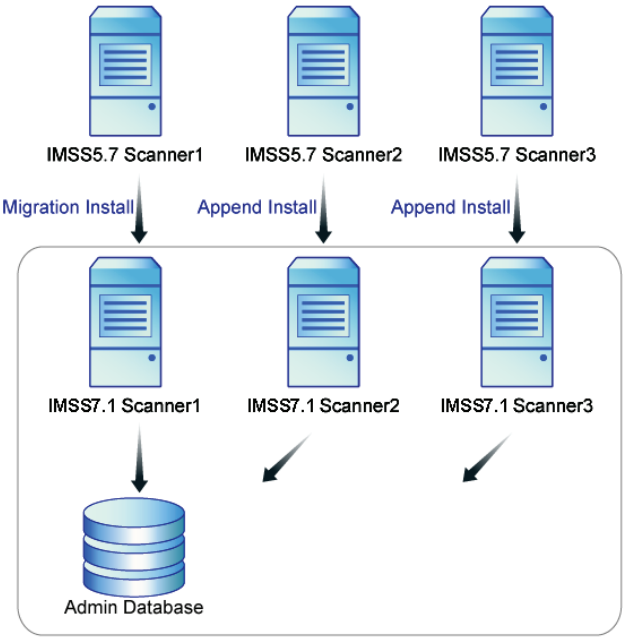
Single Admin Database

If you want all the IMSS scanners to access the same admin database in IMSS 7.1, do the following to upgrade from IMSS 5.7:

1. For the first scanner, run the IMSS 7.1 installer and perform a migration.
2. For subsequent scanners, run the IMSS 5.7 installer to uninstall the existing IMSS, then run IMSS 7.1 installer and choose append install.

Note: The single admin database upgrade option has the following characteristics:
1. There is only one IMSS suite.
2. You can control all scanners centrally.
3. Choose this upgrade option only if all the scanners share the same settings.
4. If you configured different settings for each scanner, but choose this upgrade option, IMSS will only retain the settings for the first scanner.

FIGURE 5-1. Single admin database

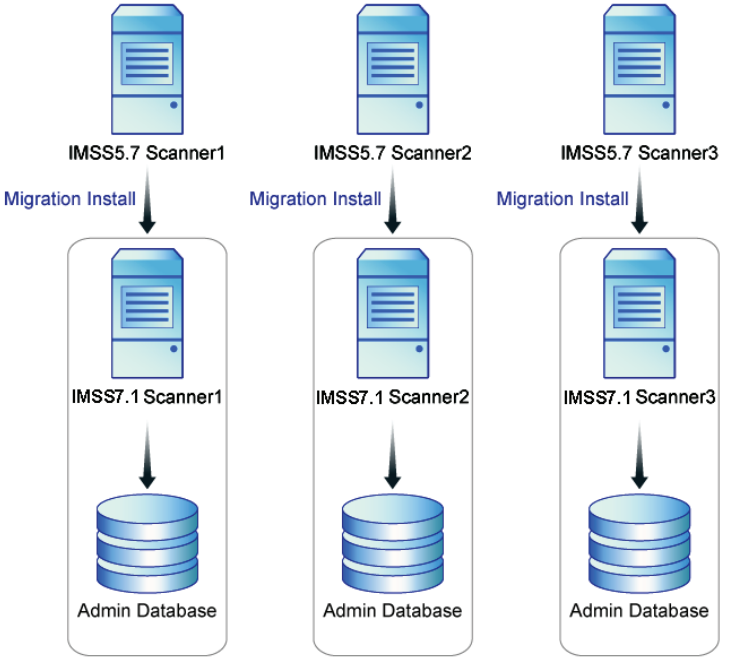


Multiple Admin Databases

If you want each IMSS scanner to access a different admin database in version 7.1, perform migration for each scanner as illustrated below.

Note: The multiple admin databases upgrade option has the following characteristics:
1. Multiple IMSS suites are installed on multiple sites.
2. Choose this option if you want to configure different settings for the scanners.
3. You can control the scanners centrally using Control Manager.

FIGURE 5-2. Multiple admin databases



Backing Up IMSS 5.7 Settings

See the following sections:

- Backing up InterScan Messaging Security Suite 5.7 Data for a Single-server Deployment on page 5-16

- Backing up InterScan Messaging Security Suite 5.7 Data for a Distributed Deployment on page 5-17

Tip: Although the IMSS installation program will back up your old IMSS settings, Trend Micro recommends that you perform the backup manually before migrating.

Backing up InterScan Messaging Security Suite 5.7 Data for a Single-server Deployment

Back up IMSS 5.7 data before migration or a direct upgrade.

Note: The IMSS 7.1 installer will help you make a full binary backup. However, users are responsible for making a full backup of the IMSS 5.7 package information and the IMSS 5.7 EUQ database (optional).

To back up InterScan Messaging Security Suite 5.7 data:

1. Stop IMSS 5.7 message traffic for approximately one minute.
2. Stop all IMSS 5.7 processes using the commands:

   ```
   $IMSS_HOME/imss/script/S99ISIMSS stop
   $IMSS_HOME/imss/script/S99ADMINUI stop
   $IMSS_HOME/imss/script/S99EUQ stop
   $IMSS_HOME/imss/script/dbctl.sh stop
   ```

3. Stop postfix using the command:

   ```
   postfix stop
   ```

4. Back up the home folder of IMSS 5.7 using the command:

   ```
   tar cvf imss57.tar /$IMSS_HOME/imss
   ```

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

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

6. Back up the IMSS 5.7 EUQ database:
   a. If you use the IMSS 5.7 bundled PostgreSQL to manage the IMSS 5.7 EUQ database, complete the following:
      i. Stop the PostgreSQL server with the command
      $IMSS_HOME/imss/script/dbctl.sh
      ii. Back up the PostgreSQL data with the command:
      tar cvf imssdb.tar /var/imss
   b. If you use your own PostgreSQL server to manage the IMSS 5.7 EUQ database, perform either a cold physical backup or a hot logical backup. For detailed instructions, refer to your DBMS documentation.
7. Back up the Postfix configuration files using the command:

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

Backing up InterScan Messaging Security Suite 5.7 Data for a Distributed Deployment

First, back up your IMSS 5.7 data before migration. This scenario assumes the following distributed deployment:

- Server 1—running scanners
- Server 2—running the database
- Server 3—running EUQ and central reporting
- Server 4—running NRS

In the commands below, "**s1**" refers to server 1, "**s2**" refers to server 2, and so on.

To back up IMSS 5.7 data for a distributed deployment:

1. Do the following on the relevant server (depending on your IMSS deployment):

   On computers with scanner services:

   a. Stop all IMSS 5.7 related processes using the command:

```
# /$IMSS_HOME/imss/script/S99ISIMSS stop
```

   b. Back up the IMSS 5.7 home folder using the command:

```
# tar cvf imss57_s1_scanner.tar /$IMSS_HOME/imss
```

On computers with only an IMSS 5.7 database:

a. Back up the database using the command:

```
# $IMSS_HOME/imss/PostgreSQL/bin//pg_dump –d imss –U
sa > /home/sam/imss57_db
```

b. Stop all database-related processes using the command:

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

c. Back up the IMSS 5.7 home folder using the command:

```
# tar cvf imss57_s2_db.tar /$IMSS_HOME/imss
```

d. Back up the database-related data folder using the command:

```
# tar cvf imss57_s2_db_data.tar /var/imss
```

On computers with EUQ and central reporting:

a. Stop all IMSS related processes with scripts using the command:

```
# /$IMSS_HOME/imss/script/S99ADMINUI stop
# /$IMSS_HOME/imss/script/S99EUQ stop
```

b. Back up the IMSS 5.7 home folder using the command:

```
# tar cvf imss57_s3_euq.tar /$IMSS_HOME/imss
```

On computers with NRS:

a. Stop all IMSS related processes and stop the maillog parser process if it is still running.

b. Back up the IMSS 5.7 home folder using the command:

```
# tar cvf imss57_s4_nrs.tar /$IMSS_HOME/imss
```

c. Stop Postfix using the command:

```
# postfix stop
```

d. Back up the Postfix configuration files using the command:

```
# tar cvf s4_postfix_config.tar /etc/postfix
```

Migrating from IMSS 5.7 to IMSS 7.1

Using the IMSS 5.7 Migration Tool is the Trend Micro recommended process to upgrade from IMSS 5.7 to IMSS 7.1.

Tip: Before migrating refer to the best practices: Upgrading IMSS 5.7: Policy Recommendations on page 5-6 and Upgrading IMSS 5.7: Process Recommendations on page 5-7.

The migration process requires the following steps:

Step 1. Exporting IMSS 5.7 settings

Step 2. Importing IMSS 5.7 settings to IMSS 7.1

Exporting IMSS 5.7 Settings

Use the IMSS 5.7 Export Tool to export settings from IMSS 5.7.

To export IMSS 5.7 settings with the IMSS 5.7 Export Tool:

1. Clean up IMSS 5.7 configuration settings. See Upgrading IMSS 5.7: Policy Recommendations on page 5-6 and Upgrading IMSS 5.7: Process Recommendations on page 5-7 for detailed information.
2. Copy the migration_tool_57to71.tar.gz on to the IMSS 5.7 server.
3. Extract the Export Tool using the following command:

   ```
   tar xzvf migration_tool_57to71.tar.gz
   ```

4. Run the Export Tool using the following command:

   ```
   ./export_tool_57.sh -e <filename>
   ```

   Note: Use -h to display the Export Tool help notes.

   The Export Tool exports configuration settings to imss_config_57.tar.gz under the current folder if no parameters are specified.

Note: The Export Tool creates a detailed export log export_57.yyyymmdd.log under the current folder.

Importing IMSS 5.7 Settings to IMSS 7.1

After migration, IMSS settings are overwritten and all services are restarted.

WARNING! During migration do not perform any database operations.

During migration do not start/stop any services in the group.

To migrate settings from IMSS 5.7 to IMSS 7.1:

1. Install IMSS 7.1on a server.
2. Use the IMSS 5.7 Export Tool to obtain the IMSS 5.7 migration package.
3. Put the migration package migration_tool_57to71.tar.gz on to IMSS 7.1.
4. Before migration, ensure port 5069 is not used by other applications.
5. Extract the migration tool using the following command:

   ```
   tar xzvf migration_tool_57to71.tar.gz
   ```

6. Start the migration tool using the following command:

   ```
   ./migration_tool_57.sh
   ```

   Note: Read the Migration Tool's scope and limitations carefully before continuing.

7. Follow the instructions that display to use the Migration Tool.

   IMSS 7.1 creates a detailed migration report and logs at the following location:

   ```
   {IMSS_INSTALLPATH}/installlog/migration/MigrationReport and
   migration_57.yyyymmdd.log
   ```

8. Perform the following post-migration tasks to verify the results of the migration:
   a. Check for items that did not migrate. Add missing items manually to IMSS 7.1.

b. Check the results for migrated items. This helps to gain a basic understanding about the mapping relationship between IMSS 5.7 filters and IMSS 7.1 rules.

c. Verify that all services can be started, especially the policy server.

d. Verify that all policies can be accessed on the Web console.

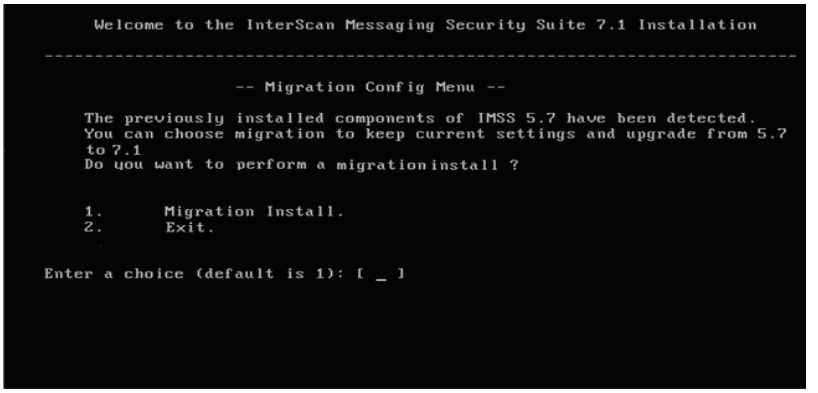
Installing IMSS 7.1 Over IMSS 5.7

Installing IMSS 7.1 over an installation of IMSS 5.7, requires IMSS 5.7 with patch 4 installed.

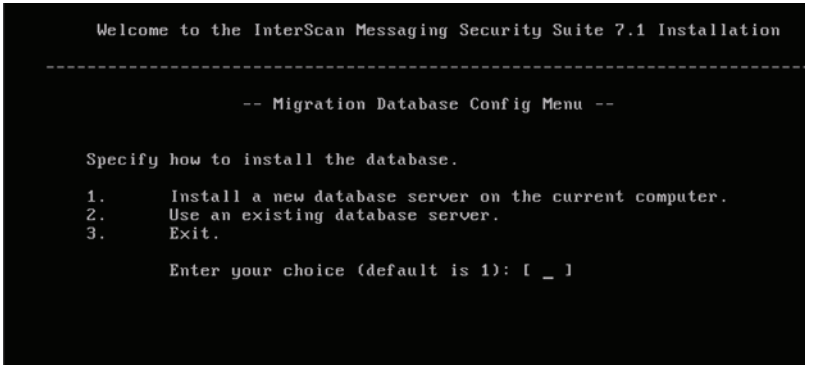
Tip: Trend Micro recommends migration to perform an upgrade, instead of installing over the previous version. See Migrating from IMSS 5.7 to IMSS 7.1 on page 5-19 for more information.

To upgrade to IMSS 7.1:

1. Log on as a superuser on the computer where you installed version 5.7 and go to the installation package directory.
2. Type `./isinst.sh`. The Migration Config Menu appears indicating that previous IMSS 5.7 components have been detected.



3. Type **1** to install IMSS 7.1 over IMSS 5.7. The Migration Database Config Menu appears. The installer will back up the old IMSS settings before uninstalling IMSS 5.7 and installing IMSS 7.1.

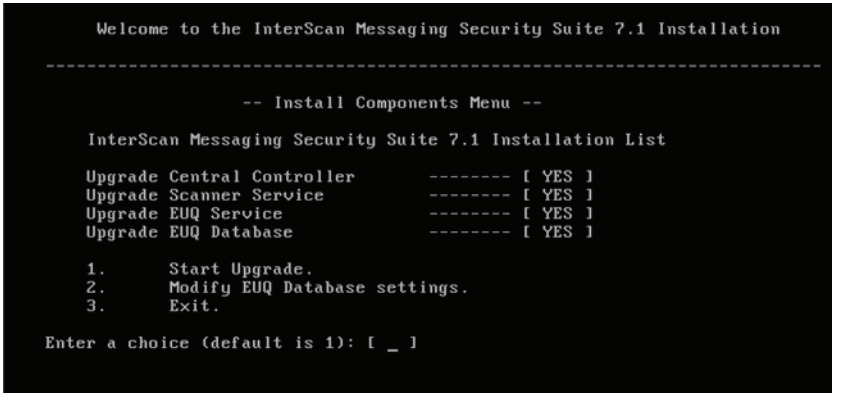


4. Select whether to install a new IMSS admin database server or use an existing server.
5. Supply database connection information if you choose to use an existing database server:
   a. Database server address (required when using an external database server)
   b. Database name (required when using external database server). Default is **imss**.

c. Database account. Default is **sa**.

Note: You must specify a superuser account.

d. Database password.



The Install Components Menu screen appears showing the status of the IMSS components. **[YES]** appears next to the component that the installer will install. By default, IMSS will install the **Central Controller** and a **Scanner**. These two components are necessary to use IMSS.

6. If EUQ is installed with IMSS 5.7, type **2** if you want to modify EUQ database settings (by default IMSS 7.1 installer uses the same database server as administrative database).
7. Type **1** to start installation. The installer checks the available free disk space, memory, and swap space on the computer and gives you an opportunity to cancel the installation if your computer does not meet the minimum requirements. The Migration Report appears.
8. Check the migration report and press Enter to continue.

   This report is saved to:

   `/opt/trend/installlog/migration/MigrationReport/GeneralReport.txt`

WARNING! **This is the last chance to stop the upgrade process without harming the current IMSS 5.7 installation. If you are not ready to upgrade, press Ctrl-C to stop the installation, otherwise press Enter to continue.**

9. Check Postfix configuration of IMSS 7.1 and press Enter to continue.

   The configuration sample is saved to:

   `/opt/trend/installlog/ImssInstall.log`

   e. If you choose to proceed with the installation, the installer then checks for an existing domain name server (DNS) on your computer and prompts you to install BIND if you intend to install Trend Micro IP Profiler later.

Note: IMSS 7.1 Linux is bundled with BIND 9.5.0.

Next, a list of the settings that cannot be migrated appears.

f. The installer backs up the old settings, uninstalls IMSS 5.7 and then installs IMSS 7.1.

Note: 1. Filters under your version 5.7 policies and sub-policies will appear as rules in version 7.1. The installer will automatically detect and migrate your policies to rules. For more information on IMSS 7.1 rules, see the Online Help from the Web console.

2. The installer might not be able to migrate old IMSS 5.7 policies with special routes. For these cases, the Policy Migration Menu appears and you need to select one of the following policy directions:
[1]—incoming
[2]—outgoing

3. Uninstall the old version of ERS in IMSS 5.7 manually if you want to install ERS of IMSS 7.1 after migration.

Upgrading from IMSS 7.0 to IMSS 7.1

The IMSS installation program can automatically upgrade from IMSS version **7.0** on the supported platforms. If the installation program detects this version, it can do the following:

- Back up your old IMSS settings
- Install IMSS 7.1
- Migrate the existing settings

Upgrading to IMSS 7.1 from IMSS 7.0 varies depending on your deployment of IMSS. Single server and distributed deployments require different procedures to upgrade.

IMSS 7.1 Settings That Cannot be Migrated

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

Backing Up IMSS 7.0 Settings

The IMSS 7.1 installer creates a full binary backup during installation. However, users must make a full backup of IMSS 7.0 administrative database and IMSS 7.0 package information manually.

To back up IMSS 7.0 settings:

1. Stop IMSS 7.0 mail traffic for approximately one minute.
2. Stop all IMSS 7.0 processes using the command:

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

3. Stop postfix using the command:

   ```
   postfix stop
   ```

4. Back up the IMSS 7.0 administrative database (required if the current scanner has an IMSS Central Controller installed) and EUQ database (required if the current scanner has an IMSS EUQ database installed):
   a. If you use the IMSS 5.7 bundled PostgreSQL to manage the IMSS 7.1 administrative database or the EUQ database, complete the following:
      i. Stop the PostgreSQL server with the command
      ```
      $IMSS_HOME/imss/script/dbctl.sh
      ```
      ii. Back up the PostgreSQL data with the command:
      ```
      tar cvf imssdb.tar /var/imss
      ```
   b. If you use your own PostgreSQL server to manage the IMSS 5.7 EUQ database, perform either a cold physical backup or a hot logical backup. For detailed instructions, refer to your DBMS documentation.
5. Back up the RPM database-related data using the command:
   ```
   tar cvf rpm.tar /var/lib/rpm
   ```
6. Back up the Postfix configuration files using the command:
   ```
   tar cvf postfix_config.tar/etc/postfix
   ```

Upgrading an IMSS 7.0 Single Server Deployment

Note: IMSS 7.0 SP1 is required when upgrading or migrating.

To upgrade a single server deployment of IMSS 7.0:

1. Back up IMSS 7.0 data before installation. See Backing Up IMSS 7.0 Settings on page 5-25 for detailed information.
2. Extract the IMSS 7.1 package, IMSS_v7.1_Linux_1144.tar.gz, using the command:
   ```
   tar xzvf IMSS_v7.1_Linux_1144.tar.gz
   ```

   Note: On each scanner, first upgrade IMSS components, and then upgrade IP Profiler. This sequence cannot be changed.

3. Start the installation using the command:

```
imss/isinst.sh
```

The Main Menu appears and the IMSS installer reports that IMSS 7.0 has been detected.

4. Type **1** to migrate your settings and upgrade to version 7.1. This upgrades the current IMSS 7.0 server to 7.1 and retains existing configuration settings.

   The Install Components Menu screen appears showing the status of the IMSS components. **[YES]** appears next to the component that the installer will install.

5. Type **1** to start installation. The installer checks the available free disk space, memory, and swap space on the computer and gives you an opportunity to cancel the installation if your computer does not meet the minimum requirements.

WARNING! **This is the last chance to stop the upgrade process without harming the current IMSS 7.0 installation. If you are not ready to upgrade, press Ctrl-C to stop the installation, otherwise press Enter to continue.**

The installer then performs constraint verification of the following:

- IMSS 7.0 administrative database connectivity check
- IMSS 7.0 component status check. The installer checks the status of the process imssmgr on all scanners and ensures all of them have been shut down.
- IMSS 7.0 distribution upgrade sequence check (performed only when upgrading a distributed installation)

After constraint verification, the installer performs the following:

- Backs up the administrative database (only on the Central Controller)
- Creates an IMSS binary package
- Installs IMSS 7.1 component packages
- Migrates all configuration settings to IMSS 7.1

Note: Depending on your hardware and deployment, this process may take up to 1 hour.

---

6. After the upgrade of components completes, upgrade IPProfiler using the command:

```
imss/ipfilterinst.sh
```

Note: IP Profiler upgrades automatically once started.

Upgrading an IMSS 7.0 Distributed Deployment

Note: IMSS 7.0 SP1 is required when upgrading or migrating.

To upgrade a distributed deployment of IMSS 7.0:

1. Back up IMSS 7.0 data before installation. See Backing Up IMSS 7.0 Settings on page 5-25 for detailed information.
2. Stop all mail traffic in the group and wait for approximately one minute.
3. Stop all components on all scanners in the group:
   a. On each scanner, type following command:

      ```
      /etc/rc.d/init.d/S99IMSSSTOP stop
      ```

   b. If you use the IMSS 7.0 bundled PostgreSQL database, restart the PostgreSQL (the S99IMSSSTOP command stops it) using the command:

      ```
      /etc/rc.d/init.d/S98dbctl start
      ```

4. Upgrade the Central Controller by extracting the IMSS 7.1 package, IMSS_v7.1_Linux_1144.tar.gz, using the command:

   ```
   tar xzvf IMSS_v7.1_Linux_1144.tar.gz
   ```

   Note: On each scanner, first upgrade IMSS components, and then upgrade IP Profiler. This sequence cannot be changed.

5. Start the installation using the command:

   ```
   imss/isinst.sh
   ```

   The Main Menu appears and the IMSS installer reports that IMSS 7.0 has been detected.

6. Type **1** to migrate your settings and upgrade to version 7.1. This upgrades the current IMSS 7.0 server to 7.1 and retains existing configuration settings.

   The Install Components Menu screen appears showing the status of the IMSS components. **[YES]** appears next to the component that the installer will install.

7. Type **1** to start installation. The installer checks the available free disk space, memory, and swap space on the computer and gives you an opportunity to cancel the installation if your computer does not meet the minimum requirements.

   WARNING! **This is the last chance to stop the upgrade process without harming the current IMSS 7.0 installation. If you are not ready to upgrade, press Ctrl-C to stop the installation, otherwise press Enter to continue.**

   The installer then performs constraint verification of the following:

   - IMSS 7.0 administrative database connectivity check
   - IMSS 7.0 component status check. The installer checks the status of the process imssmgr on all scanners and ensures all of them have been shut down.
   - IMSS 7.0 distribution upgrade sequence check (performed only when upgrading a distributed installation)

   After constraint verification, the installer performs the following:

   - Backs up the administrative database (only on the Central Controller)
   - Creates an IMSS binary package
   - Installs IMSS 7.1 component packages
   - Migrates all configuration settings to IMSS 7.1

   Note: Depending on your hardware and deployment, this process may take up to 1 hour.

8. After the upgrade of components completes, upgrade IPProfiler using the command:

   ```
   imss/ipfilterinst.sh
   ```

   Note: IP Profiler upgrades automatically once started.

9. Upgrade all other scanners following steps 4 to 9. No special sequence is required when upgrading subsequent scanners.
10. After upgrading all scanners, start the IMSS service on all scanners using the command:

    ```
    $IMSS_HOME/imss/script/imssstart.sh
    ```

Migrating from IMSS 7.0 to IMSS 7.1

The migration process requires the following steps:

Step 1. Exporting IMSS 7.0 settings

Step 2. Importing IMSS 7.0 settings to IMSS 7.1

Before migrating verify the status and operation of the IMSS 7.0 database.

Note: IMSS 7.0 SP1 is required when upgrading or migrating.

Exporting IMSS 7.0 Settings

Use the IMSS 7.0 Export Tool to export settings from IMSS 7.0.

To export IMSS 7.0 configuration settings:

1. Copy the migration_tool_70to71.tar.gz on to the IMSS 7.0 server.
2. Extract the Export Tool using the following command:

   ```
   tar zxf migration_tool_70to71.tar.gz
   ```

3. Run the Export Tool using the following command:

   ```
   ./export_tool_70.sh -e <filename>
   ```

   Note: Use -h to display the Export Tool help notes.

   The Export Tool exports the configuration settings package, imss_config_70.tar.gz, to $PWD.

Note: The Export Tool creates a detailed export log export_70.xxxxxxxx.log under the current folder.

Importing IMSS 7.0 Settings to IMSS 7.1

After migration, IMSS settings are overwritten and all services are restarted.

WARNING! **During migration do not perform any database operations.**

During migration do not start/stop any services in the group.

Tip: Trend Micro recommends performing migration on a fresh installation of IMSS 7.1.

To migrate settings from IMSS 7.0 to IMSS 7.1:

1. Copy the migration package migration_tool_70to71.tar.gz on to IMSS 7.1.
2. Extract the migration tool using the following command:

   ```
   tar zxf migration_tool_70to71.tar.gz
   ```

3. Copy the IMSS 7.0 configuration package onto IMSS 7.1. See Exporting IMSS 7.0 Settings on page 5-30 for detailed information.
4. Start the migration tool using the following command:

   ```
   ./migration_tool_70.sh
   ```

   Note: Read the Migration Tool's scope and limitations carefully before continuing.

5. Follow the instructions that display to use the Migration Tool.

   IMSS 7.1 creates a detailed migration report and logs at the following location:

   ```
   {IMSS_INSTALLPATH}/installlog/migration/MigrationReport and
   migration_70.yyyymmdd.log
   ```

6. Perform the following post-migration tasks to verify the results of the migration:

c. Check the results for migrated items.

d. Verify that all services can be started, especially the policy server.

e. Verify that all policies can be accessed on the Web console.

Activation of Supported Services

After upgrading, IMSS 7.1 retains the Activation Code from IMSS 5.7/7.0. If the Activation Code has expired, provide a new Activation Code to use the following:

- Antivirus and Content Filter
- SPS (includes IP Profiler)

To use ERS you must type the Activation Code during installation.

Rolling Back the Upgrade

If any problems occur with the upgrade to version 7.1, you can roll back to the previous version. For more information about IMSS 5.7/7.0 installation, see your IMSS 5.7/7.0 documentation.

Rolling Back to IMSS 5.7

To a certain stage the upgrade process automatically rolls back upgrading. However, there is a point of no return (step 10 in the Installing IMSS 7.1 Over IMSS 5.7 on page 5-21 process) where rolling back must be performed manually.

The rollback process requires the following steps:

Step 1. Removing IMSS 7.1 components

Step 2. Rolling Back to IMSS 5.7

To remove IMSS 7.1 components:

1. Remove the IMSS 7.1 package using the command:

```
rpm –e imss imsscctrl imsseuq
```

Note: Ignore any error messages that appear concerning missing packages.

2. Remove PostgreSQL if a new PostgreSQL was installed during the upgrade using the commands:

```
su - imss -c "/opt/trend/imss/PostgreSQL/bin/pg_ctl -D
'/var/imss/pgdata' -w -m fast stop"

rm -rf /var/imss
```

3. Remove all existing IMSS 7.1 autostart scripts, using the commands:

```
rm -rf /etc/rc.d/*/*dbctl

rm -rf /etc/rc.d/*/*bindctl

rm -rf /etc/rc.d/*/*CMAGENT

rm -rf /etc/rc.d/*/*FOXDNS

rm -rf /etc/rc.d/*/*IMSS

rm -rf /etc/rc.d/*/*IMSSSTOP

rm -rf /etc/rc.d/*/*IMSSUI

rm -rf /etc/rc.d/*/*MANAGER

rm -rf /etc/rc.d/*/*MONITOR

rm -rf /etc/rc.d/*/*POLICY

rm -rf /etc/rc.d/*/*SCHEDULED
```

To complete the rollback to IMSS 5.7:

1. Roll back to the IMSS 5.7 package information using the commands:

```
tar xvf rpm.tar -C /

rpm -rebuilddb
```

Note: After doing this, information of all RPM packages installed after the backup has been created will be lost. Do not install other RPM packages during the IMSS 5.7 upgrade.

2. Roll back to the IMSS 5.7 binary using the command:

   ```
   tar xvf imss57.tar -C /
   ```

3. Roll back to the IMSS 5.7 EUQ database using the command:

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

4. Roll back to the Postfix configuration using the command:

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

5. Re-create the IMSS 5.7 auto start script using the command:

   ```
   imss/recreate_rclink_57.sh
   ```

   The IMSS 5.7 environment should now be the same as before the upgrade.

Rolling Back to IMSS 7.0

To a certain stage the upgrade process automatically rolls back upgrading. However, there is a point of no return:

- Upgrading IMSS components: After Step 6 in the Upgrading an IMSS 7.0 Single Server Deployment on page 5-26 process or Step 8 in the Upgrading an IMSS 7.0 Distributed Deployment on page 5-28
- Upgrading IP Profiler

During the above processes rolling back must be performed manually.

Rolling Back After IMSS Components Upgrade

At this stage during the upgrade process, the installer removes the IMSS 7.0 package, the IMSS 7.1 package administrative database installs, and data migrates to the new administrative database.

When the installer encounters issues at this stage, the rollback process requires the following steps:

Step 1. Removing IMSS 7.1 components

Step 2. Rolling back to IMSS 7.0

To remove IMSS 7.1 components:

1. Remove the IMSS 7.1 package using the command:

   ```
   rpm –e imss imsscctrl imsseuq
   ```

   Note: Ignore any error messages that appear concerning missing packages.

2. Remove PostgreSQL if a new PostgreSQL was installed during the upgrade using the commands:

   ```
   su - imss -c "/opt/trend/imss/PostgreSQL/bin/pg_ctl -D
   '/var/imss/pgdata' -w -m fast stop"
   ```

   ```
   rm –rf /var/imss
   ```

To complete the rollback to IMSS 7.0:

1. Roll back to the IMSS 7.0 package information using the commands:

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

   ```
   rpm –rebuilddb
   ```

   Note: After doing this, information of all RPM packages installed after the backup has been created will be lost. Do not install other RPM packages during the IMSS 7.0 upgrade.

2. Roll back to the IMSS 7.0 binary using the command:

   ```
   mv $IMSS_HOME/imss/queue $IMSS_HOME/installlog/binary
   ```

   ```
   rm –rf $IMSS_HOME/imss
   ```

   ```
   mv $IMSS_HOME/installlog/binary $IMSS_HOME/imss
   ```

3. Roll back to the IMSS 7.0 EUQ database using the command:

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

4. Roll back to the Postfix configuration using the command:

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

5. Re-create the IMSS 7.0 auto start script using the command:

   ```
   imss/recreate_rclink_70.sh
   ```

   The IMSS 7.0 environment should now be the same as before the upgrade.

Rolling Back After IP Profiler Upgrades

At this stage during the upgrade process, the installer removed the IMSS 7.0 package, the IMSS 7.1 package administrative database was installed, and data migrated to the new administrative database. IP Profiler attempts to install but encounters issues.

When the installer encounters issues at this stage, the rollback process requires the following steps:

Step 1. Removing IMSS 7.1 components

Step 2. Rolling back to IMSS 7.0

To remove IMSS 7.1 components:

1. Remove the IMSS 7.1 package using the command:

   ```
   rpm –e imss imsscctrl imsseuq
   ```

   Note: Ignore any error messages that appear concerning missing packages.

2. Remove PostgreSQL if a new PostgreSQL was installed during the upgrade using the commands:

   ```
   su - imss -c "/opt/trend/imss/PostgreSQL/bin/pg_ctl -D
   '/var/imss/pgdata' -w -m fast stop"
   ```

   ```
   rm –rf /var/imss
   ```

To complete the rollback to IMSS 7.0:

1. Roll back to the IMSS 7.0 package information using the commands:

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

   Note: After doing this, information of all RPM packages installed after the backup has been created will be lost. Do not install other RPM packages during the IMSS 7.0 upgrade.

2. Roll back to the IMSS 7.0 binary using the command:

   ```
   mv $IMSS_HOME/imss/queue $IMSS_HOME/installlog/binary
   rm –rf $IMSS_HOME/imss
   mv $IMSS_HOME/installlog/binary $IMSS_HOME/imss
   ```

3. Roll back to the IMSS 7.0 EUQ database using the command:

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

4. Roll back to the Postfix configuration using the command:

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

5. Re-create the IMSS 7.0 auto start script using the command:

   ```
   imss/recreate_rclink_70.sh
   ```

   The IMSS 7.0 environment should now be the same as before the upgrade.

6. Remove IP Profiler packages using the command:

   ```
   imss/remove_ipp.sh
   ```

7. Complete the rollback to IMSS 7.0 with the command:

   ```
   imss/ipfilterinsh.sh #IMSS 7.0
   ```

Note: Provide the ERS/IP Profiler Activation Code when you re-install the IP Profiler.

Chapter 6

Troubleshooting, FAQ, and Support Information

This chapter explains how to troubleshoot common IMSS issues, search the Trend Micro Knowledge Base, and contact support.

Topics include:

- Troubleshooting on page 6-2
- Frequently Asked Questions on page 6-2
- Using the Knowledge Base on page 6-7
- Contacting Support on page 6-7

Troubleshooting

Table 6-1 shows common troubleshooting issues that you might encounter when installing IMSS. Read the solutions below. If you have additional problems, check the Trend Micro Knowledge Base.

For troubleshooting and FAQ information pertaining to the administration or maintenance of IMSS, refer to the *IMSS Administrator's Guide*.

TABLE 6-1. Installation Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
The ERS installation does not validate the ERS Activation Code	To validate the Activation Code, the ERS installation script accesses Trend Micro through the Internet. Verify that your DNS server is functioning properly and that the computer on which you are installing ERS has access to the Internet.

Frequently Asked Questions

Postfix MTA Settings

If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally? Can I make an exception on the settings for some Postfix instances separately?

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.

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:queue_directory:{Parameter1
:{Parameter2}:…::{Parameter n}
```

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

Can the IMSS admin database be installed separately?

Yes. You can install IMSS admin database separately. Run the installation program and configure the IMSS database only without selecting any other IMSS components.

How many EUQ services and EUQ databases can be installed?

Up to eight (8) EUQ services and EUQ databases can be installed.

Should I install an EUQ database for each EUQ service?

No. Multiple EUQ services can share an EUQ database, but the EUQ service requires at least one EUQ database.

Is the IMSS EUQ database deleted during uninstallation?

No. The IMSS EUQ database is not removed during IMSS uninstallation.

Why am I not able to remove the old IMSS database during installation?

Some applications may be connected to the old IMSS database when the installation program tries to remove it. Disconnect all connections to the old database, and retry.

Is there any problem if I install IMSS 7.1 on a computer with an external DNS server?

There should be no functional problem integrating IMSS 7.1 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 7.1 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. IMSS Apache takes the port 8447.

Upgrading

Will all InterScan Messaging Security Suite 5.7 settings be retained during an upgrade?

No. Due to architectural changes in IMSS 7.1, some settings cannot be retained. The IMSS 7.1 installer will ask for the new values of these settings during an upgrade and the settings can also be found in the general migration report:

$IMSS_HOME/installlog/migration/MigrationReport/

GeneralReport.txt

How do I upgrade IMSS 5.7 scanners?

To upgrade from multiple IMSS 5.7 scanners:

- Upgrade from the scanner with the most desired settings for the migration.
- Uninstall the remaining scanners.
- Append the multiple scanners.

For more information, see Upgrade Options for Multiple Scanner Deployment on page 5-13.

Can I upgrade the administrator database and EUQ database from the same IMSS 5.7 database server?

Yes. IMSS 5.7 database settings (such as LDAP settings and EUQ settings) are kept.

Is a smooth rollback to IMSS 5.7 possible after upgrading?

Yes. See Rolling Back the Upgrade on page 5-32 for detailed rollback instructions.

Is it possible to upgrade on a computer that only has the EUQ component?

No. Upgrade from a computer with an installed IMSS 5.7 scanner.

How do I simplify SPS rules after an upgrade?

To keep all SPS filter settings for all policies of IMSS 5.7/7.0, IMSS 7.1 migrates each SPS filter to one or multiple SPS rule(s) in IMSS 7.1. To reduce the number of SPS rules after upgrading, perform the following:

- Create a new SPS rule after migration.
- Delete all migrated SPS rules.

How are IMSS 5.7/7.0 filters and policies mapped during an upgrade?

The architectures of InterScan Messaging Security Suite 7.0 and IMSS 7.1 are very similar. All policies and filters map without issues.

The architectures of InterScan Messaging Security Suite 5.7 and IMSS 7.1 are very different. Therefore, the upgrade module maps all InterScan Messaging Security Suite 5.7 filters to related rules in IMSS 7.1 in the following ways:

- **Virus filter(s) —** The number of virus rules vary according to the following:
  - There will be several rules for one virus filter after migration if there are multiple routes with different "To" or "From" addresses.

    For example: A virus filter with the routes (a->b; c->d; e->b) will be migrated to two virus rules with the routes (a,e->b; c->d)
  - There will be two rules for one virus filter after migration if it was "active" in InterScan Messaging Security Suite 5.7 for both SMTP and POP3 traffic.
  - There will be only one rule for one virus rule after migration if it is "inactive" in InterScan Messaging Security Suite 5.7 for both SMTP and POP3 traffic. The rule direction is for "all routes".
- **SPS filter(s) —** The migration module maps each SPS filter to one SPS rule after migration or several SPS rules depending on the Routes and Filter Actions. There will normally be one SPS rule after migration. The following are exceptions when there will be several SPS rules:
  - **If there are multiple routes with different "To" or "From" addresses**.

    For example: SPS filter with the routes (a->b; c->d; e->b) will be migrated to two SPS rules with the routes (a,e->b; c->d)

- **If three filter actions are different**.

  For example, SPS filter with the following filter actions will be migrated to two SPS rules named "Spam Filter (SPS) BlackWhiteList And Phish->Global Policy" and "Spam Filter (SPS) Spam->Global Policy"

  - "Tag and Deliver" for "Blocked senders"
  - "Delete" for "Phishing emails"
  - "Quarantine" for "Spam"

- eManager filter
  - There will be several rules for one eManager filter after migration if there are multiple routes with different "To" or "From" addresses.

    For example: eManager filter with the routes (a->b; c->d; e->b) will be migrated to two eManager rules with the routes (a,e->b; c->d)
  - There will be one rule for one eManager filter after migration if it was "active" in InterScan Messaging Security Suite 5.7 for both SMTP and POP3 traffic.
  - There will be one rule for one eManager filter after migration if it is "inactive" in InterScan Messaging Security Suite 5.7 for both SMTP and POP3 traffic. The rule direction is for "Both incoming and outgoing directions".

For the detailed mapping relationship of each policy, check `$IMSS_HOME/installlog/migration/MigrationReport/DetailReport.txt`

Using the Knowledge Base

The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

http://esupport.trendmicro.com

The contents of Knowledge Base are being continuously updated, and new solutions are added daily. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

Contacting Support

Trend Micro provides technical support, virus pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, feel free to contact us. We also welcome your comments.

Trend Micro Incorporated provides worldwide support to all of our registered users. Get a list of the worldwide support offices:

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

In the United States, you can reach the Trend Micro representatives by phone, fax, or email:

Trend Micro, Inc.
10101 North De Anza Blvd.
Cupertino, CA 95014

Toll free: +1 (800) 228-5651 (sales)

Voice: +1 (408) 257-1500 (main)

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email address: support@trendmicro.com

Index

A

about IMSS 1-2
admin database 3-6
Apache 3-7
  Tomcat 3-6
archive 1-3
audience X

B

backing up settings 5-15
browser requirements 4-3

C

central controller 2-3
centralized archive and quarantine 1-3
centralized logging 1-3
centralized policy 1-3
component and sub-module installation 3-6
configuration wizard 1-4
contact
  support 6-7
Control Manager
  about 1-15
Control Manager MCP agent, agent
  Control Manager MCP 1-15
CPU requirements 4-2

D

database
  on central controller 2-2
database server 3-6
disk space requirements 4-2
documentation
  IMSS related X

E

email threats
  spam 1-7
  unproductive messages 1-7
ERS 1-4
  about 2-8
  Administration Console 2-11
  how it works 2-10
  services 2-8
EUQ 1-4

F

failover 3-36
FAQ
  postfix 6-2
filtering, how it works 1-10
Firefox 4-3

I

IMSS
  about 1-2
IMSS 5.7 5-5
IMSS components
  admin database 2-2
  central controller 2-2
  EUQ database 2-6
  EUQ primary and secondary services 2-4
  installation 3-6
  policy services 2-3
  policy services synchronization 2-3
  scanner services 2-2
IMSSMGR 3-6
installation
  clustered 3-29
  IP Filtering 4-14
  IP Filtering, installation
    EUQ 3-35
  preparing Postfix 4-4

procedures 4-11
removing IMSS 4-21
scenarios 3-22
using Control Manager 3-32
verifying 4-20
installing
before a firewall 3-13
behind a firewall 3-14
in the DMZ 3-16
no firewall 3-12
on SMTP gateway 3-15
Internet Explorer 4-3
IP Filtering
about 2-7
installation 4-14
removing 4-22
IP Profiler 1-4
about 2-7
detects 2-7
how it works 2-9

K

Knowledge Base 6-7

L

LDAP server requirements 4-4
logs 1-3

M

maillog parser 3-8
mass mailing viruses
pattern 1-9
memory requirements 4-2
migrating
from IMSS 5.7 5-19
from IMSS 7.0 5-30
migration
rollback 5-32
minimum requirements 4-2
MTA
Postfix preparation 4-4
MTA features, opportunistic TLS 1-4
MTA requirements 4-4

N

named server 3-6
new features 1-2

O

online help X

P

pattern matching 1-5
policy 1-3
policy service 2-3
Postfix preparation 4-4
Postgre requirements 4-3

Q

quarantine 1-3—1-4

R

readme file X
reports 1-3
requirements 4-2
rolling back
to IMSS 5.7 5-32
to IMSS 7.0 5-34
rolling back the migration 5-32

S

scanners 2-4
settings
backup 5-15
spam prevention 1-4
spyware and grayware 1-13
support 6-7
swap space requirements 4-3
system requirements 4-2

T

TMCM

about 1-15
Tomcat 3-6—3-7
Trend Micro Knowledge Base 6-7
troubleshooting 6-2
ERS 6-2

U

uninstallation 4-21
IP Filtering components 4-22
upgrading
IMSS 5.7 5-5
policy recommendations 5-6
process recommendations 5-7
IMSS 7.0 5-25
install over IMSS 5.7 5-21

V

verifying the installation 4-20
version 5.7 5-5

W

Web EUQ 1-4
what's new 1-2