TREND MICRO™

7.1 InterScan™ Messaging Security Suite

Installation Guide

Comprehensive threat protection at the Internet messaging gateway

for LINUX™ 7.1 SP1

Messaging Security

Document Part No.: MSEM76002_130725

Release Date: September 2013

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Chapter 3: Planning for Deployment

Chapter 4: Installing and Uninstalling IMSS 7.1 SP1

Chapter 5: Upgrading from Previous Versions

Chapter 6: Troubleshooting and Support Information

Index

Preface

About this Manual

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

Refer to the *IMSS 7.1 SP1 Administrator's Guide* for information about configuring IMSS settings and the Online Help in the management console for detailed information about each field on the user interface.

Topics include:

What's New

The following tables provide an overview of new features available in IMSS 7.1 SP1.

TABLE 1. IMSS 7.1 SP1 New Features

NEW FEATURE	DESCRIPTION
Marketing Email Management	Administrators can manage marketing messages separately from common spam. To allow end users to receive wanted marketings messages, email addresses and IP addresses specified in the marketing message exception list bypass scanning.
Smart Scan	Smart Scan facilitates a more efficient scanning process by offloading a large number of threat signatures previously stored on the IMSS server to the cloud.

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

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

Table 2. 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).

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.

Table 3. IMSS 7.0 New Features

New Feature	Description
Multiple Antivirus and Malware Policies	Multiple IMSS policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria.
Centralized Logging and Reporting	A consolidated, detailed report provides top usage statistics and key mail usage data. Centralized logging allows administrators to quickly audit message-related activities.
Centralized Archive and Quarantine Management	An easy way to search multiple IMSS quarantine and archive areas for messages.
Scalable Web End-User Quarantine (Web EUQ)	Multiple Web EUQ services offer end-users the ability to view quarantined email messages that IMSS detected as spam. Together with EUQ notification, IMSS will help lower the cost of helpdesk administrative tasks.

New Feature	Description
Multiple Spam Prevention Technologies	Three layers of spam protection: • Email Reputation Services filters connections from spam senders when establishing SMTP sessions. • IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS). • Trend Micro Anti-spam engine detects and takes action on spam.
IntelliTrap	IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus in a compressed file will enter your network through email.
Delegated Administration	LDAP-integrated account management allows users to assign administrative rights for different configuration tasks.
Easy Deployment with Configuration Wizard	An easy-to-use configuration wizard to get IMSS up and running.
Advance MTA Functions	Opportunistic TLS, domain based delivery, and other MTA functions help IMSS handle email efficiently and securely.
Migration	Easy upgrade process ensures that settings will be migrated with minimum effort during setup.
Mail Auditing and Tracking	Detailed logging for all messages tracks and identifies message flow related issues.
Integration with Trend Micro Control Manager	Perform log queries on Email Reputation Services from Control Manager, in addition to other supported features.

Audience

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

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

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

InterScan Messaging Security Suite Documentation

The IMSS documentation consists of the following:

Administrator's Guide

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

Installation Guide

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

Online Help

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

Readme File

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

The documentation is available at:

http://docs.trendmicro.com

Document Conventions

The documentation uses the following conventions:

TABLE 4. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions

CONVENTION	DESCRIPTION
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

Chapter 1

Introducing InterScan™ Messaging Security Suite

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

Topics include:

About InterScan Messaging Security Suite

InterScan Messaging Security Suite (IMSS) 7.1 SP1 integrates antivirus, anti-spam, anti-phishing, and content filtering technology for complete email protection. This flexible software solution features award-winning antivirus and zero-day protection to block known and potential viruses.

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

IMSS Main Features and Benefits

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

TABLE 1-1. Main Features and Benefits

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

FEATURE	DESCRIPTIONS	BENEFITS
Smart Scan	Smart Scan facilitates a more efficient scanning process by off-loading a large number of threat signatures previously stored on the IMSS server to the cloud.	Smart Scan leverages the Smart Protection Network to: • Enable fast, real-time security status lookup capabilities in the cloud • Reduce the time necessary to deliver protection against emerging threats • Lower memory consumption on the server
IntelliTrap	Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files. Because there is the possibility that IntelliTrap may identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature. By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be classified as security risks.	IntelliTrap helps reduce the risk that a virus compressed using different file compression schemes will enter your network through email.

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

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

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

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

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

FEATURE	DESCRIPTIONS	BENEFITS
Integration with Trend Micro Control Manager™	Trend Micro Control Manager™ (TMCM) is a software management solution that gives you the ability to control antivirus and content security programs from a central location regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus and content security policy.	Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available.

About Spyware/Grayware

Your clients are at risk from potential threats other than viruses/malware. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization.

TABLE 1-2. Types of Grayware

TYPE	DESCRIPTION
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties
Adware	Displays advertisements and gathers data, such as user web surfing preferences, to target advertisements at the user through a web browser
Dialers	Change computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Programs	Cause abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes

Type	Description
Hacking Tools	Help hackers enter computers
Remote Access Tools	Help hackers remotely access and control computers
Password Cracking Applications	Help hackers decipher account user names and passwords
Other	Other types not covered above

How Spyware/Grayware Gets into your Network

Spyware/grayware often gets into a corporate network when users download legitimate software that has grayware applications included in the installation package.

Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

Potential Risks and Threats

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

Table 1-3. Types of Risks

Type	Description
Reduced computer performance	To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
Increased web browser-related crashes	Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.

TYPE	DESCRIPTION
Reduced user efficiency	By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users can be unnecessarily distracted from their main tasks.
Degradation of network bandwidth	Spyware/grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network.
Loss of personal and corporate information	Not all data that spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network.
Higher risk of legal liability	If hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties.

About Web Reputation

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

About Trend Micro Control Manager

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

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

Control Manager Support

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

TABLE 1-4. Supported Control Manager Features

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

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

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

About Trend Micro Smart Protection

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

Smart protection services include:

File Reputation Services

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

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

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

Web Reputation Services

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

Web reputation technology prevents users from:

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

The Need for a New Solution

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

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

Trend Micro™ Smart Protection Network™

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

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

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

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

For more information on the Smart Protection Network, visit:

www.smartprotectionnetwork.com

About Marketing Email Message Scanning

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

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

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

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

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

Chapter 2

Component Descriptions

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

Topics include:

About IMSS Components

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

You can install IMSS components on a single computer or on multiple computers. For graphical representations of how these components work together, see *Understanding Installation Scenarios on page 3-25*.

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 console. The web 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 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 the Apache Web server 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. The Apache Web server 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 Web Server and mod_jk

The Apache HTTP Server (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.

The Apache Web server 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 the Apache Web server.

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

Email Reputation

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

How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email messages containing threats mentioned in the section *IP Filtering on page 2-7*. You can customize several criteria that determine when IMSS starts taking a specified action on an IP address. The criteria differ depending on the potential threat, but commonly include a duration during which IMSS monitors the IP address and a threshold.

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

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

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

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

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

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

Email Reputation

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

Types of Email Reputation

There are two types of Email reputation: *Standard on page 2-9* and *Advanced on page 2-10*.

Email Reputation: Standard

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

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

Email Reputation: Advanced

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

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

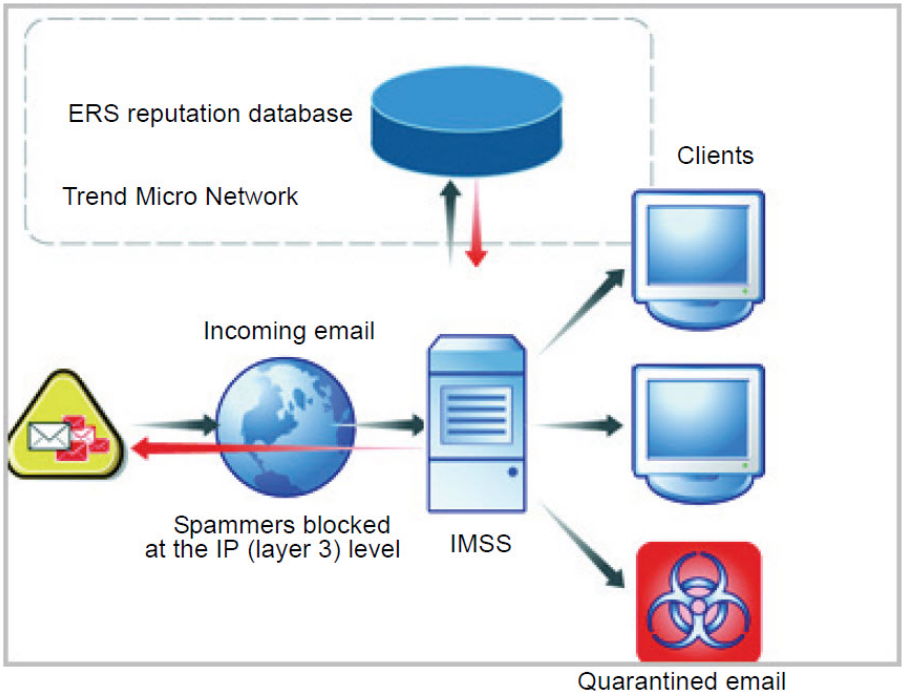
Like Email reputation: Standard, Email reputation: Advanced is a DNS query-based service, but two queries can be made to two different databases: the standard reputation database and the dynamic reputation database (a database updated dynamically in real time). These two databases have distinct entries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

How Email Reputation Technology Works

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

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

The figure below illustrates how Email reputation works.



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

About 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

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

1. **Identify the location of IMSS**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Select one of the following locations on your network where you would like to install IMSS.		
	Without a firewall		*Installing without a Firewall on page 3-12*
	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*

2. **Plan the scope**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Decide whether you would like to install one IMSS server or multiple servers.		
	Single-server installation		*Single-Server Installation on page 3-26*
	Multiple scanner service		*Multiple Scanner Service Installation on page 3-27*
	Multiple EUQ service		*Multiple End-User Quarantine Service Installation on page 3-30*
	Complex distributed		*Complex Distributed Installation on page 3-33*
	Wide area network		*Wide-Area Network Installation on page 3-35*
	IP filtering **Tip** Trend Micro recommends that you consider the failover plan before deciding on the scope.		*IP Filtering on page 3-38*

3. **Install or Upgrade**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Perform a fresh installation of IMSS or upgrade from a previous version.		
	Prepare MTA		*Preparing the Message Transfer Agents on page 4-5*
	Install IMSS components		*Installing IMSS Components and End-User Quarantine on page 4-12*
	Install IP Filtering	Yes	*Installing Email Reputation Services and IP Profiler on page 4-17*
	Upgrade from a previous version		*Upgrading from Previous Versions on page 5-1*
	Verify that installation is successful		*Verifying the Installation on page 4-24*

4. **Configure basic IMSS settings**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Configure the Central Controller through the Configuration Wizard.		
	Configure settings using the Configuration Wizard		Performing Basic Configuration with the Configuration Wizard section of the *Administrator's Guide*

5. **Start services**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Activate IMSS services to start protecting your network against various threats.		
	Scanner		IMSS Services section of the Administrator's Guide
	Policy		
	EUQ	Yes	

6. **Configure other IMSS settings**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	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

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Policy and scanning exceptions		Managing Policies section of the *Administrator's Guide* **Note** If scanning for marketing messages, make sure that the DNS configuration and DNS query are correct.
	Perform a manual update of components and configure scheduled updates		Updating Scan Engine and Pattern Files section of the Administrator's Guide
	Log settings		Configuring Log Settings section of the Administrator's Guide

7. **Back up IMSS**

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Perform a full or minimal backup of IMSS as a precaution against system failure.		
	Full backup		Backing Up IMSS section of the *Administrator's Guide*.
	Minimal backup		

Component and Sub-module Installation

When you install an IMSS component, additional sub-modules are also installed . The following table lists each component sub-module.

TABLE 3-1. 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 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 processes.
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.

Main Component	Installed Sub-module	Sub-module Description
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.
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 the following table for the ports IMSS uses.

TABLE 3-2. 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
953	The IP Filtering service port.	Not configurable on the IMSS server.
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 console, go to **Administration** > **IMSS Configuration** > **Connections** > **Components** on the menu.
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`

Port Number	Component and Role	Configuration Location
8446	EUQ service listening port.	`{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector / port`
8447	EUQ service listening port with load balance.	`{IMSS}/UI/euqUI/conf/EUQ.conf: Listen / VirtualHost / ServerName`
10024	IMSS scanner reprocessing port. Messages released from the central quarantine area in the Admin database and from the EUQ database will be sent through this port for reprocessing.	`imss.ini / [Socket_3]/ proxy_port`
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

Port Number	Component and Role	Configuration Location
15505	IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the web console. The manager also provides quarantine/archive query results to the web console and the EUQ Web console through this port.	From the web console, go to **Administration** > **IMSS Configuration** > **Connections** > **Components** on the menu.
IMSS uses the following ports when you enable related services:		
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 console, go to **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 console, go to **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.

Network Topology Considerations

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

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

Note

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

Installing without a Firewall

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

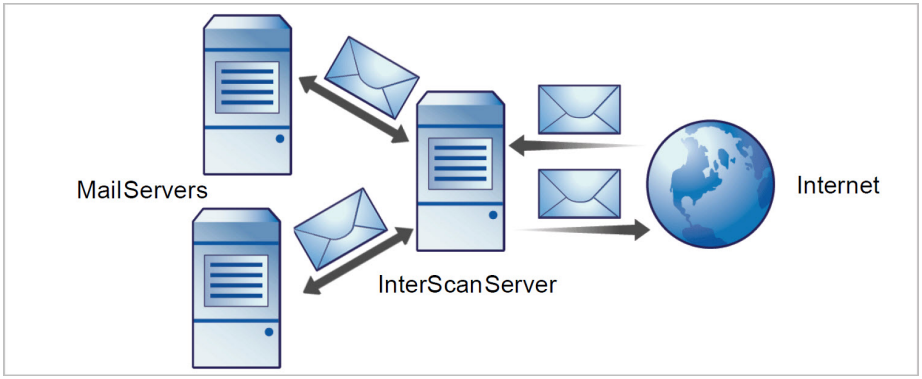


FIGURE 3-1. Installation topology: no firewall

Note

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

Installing in Front of a Firewall

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

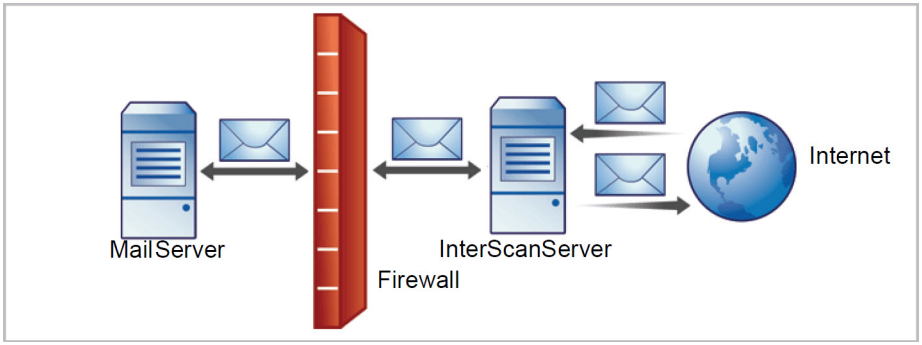


FIGURE 3-2. Installation topology: in front of the firewall

Incoming Traffic

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

Outgoing Traffic

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

- Outgoing SMTP messages can only go to Postfix first and then go to IMSS servers.
- Incoming SMTP messages only come from IMSS servers.

- Configure IMSS to allow internal SMTP gateways to relay, through Postfix, to any domain through IMSS.

Tip

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

Installing Behind a Firewall

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

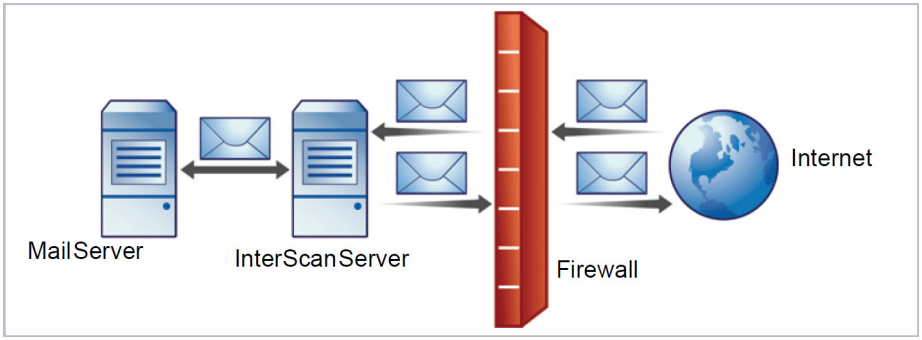


FIGURE 3-3. Installation scenario: behind a firewall

Incoming Traffic

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

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

Outgoing Traffic

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

Tip

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

Installing 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 messages to the SMTP gateway and the newly allocated port.

Outgoing Traffic

- Configure the SMTP gateway to route outgoing email messages to the IMSS port 25.
- Configure Postfix and IMSS to route all outgoing email messages (destined for 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 messages can only go from the DMZ to the internal email servers.
- Configure your packet-based firewall.
- Configure Postfix and IMSS to route email messages destined for your local domain(s) to the SMTP gateway or your internal mail server.

Outgoing Traffic

- Configure Postfix to route all outgoing messages (destined for domains other than the local domains) to the firewall or deliver them using IMSS .

- Configure all internal SMTP gateways to forward outgoing mail to Postfix and then to IMSS.
- Configure IMSS to allow internal SMTP gateways to relay to any domain, through Postfix and IMSS.

Tip

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

About 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:

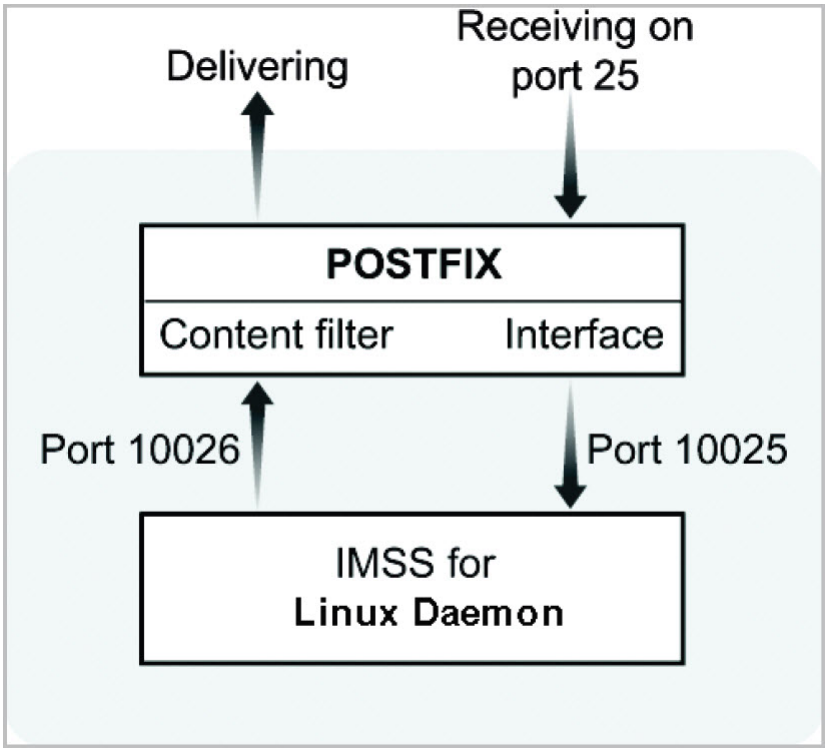


FIGURE 3-4. Standalone model

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 Standalone Model in IPv6 Environments

For IPv6 support, make the following changes to 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:[::1]:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=200
```

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

```
#IMSS: content filter smtp transport imss for IMSS
imss unix - - n - - smtp
-o disable_dns_lookups=yes
-o smtp_connect_timeout=$imss_connect_timeout
-o smtp_data_done_timeout=$imss_timeout
#IMSS: content filter loop back smtpd
[::1]:10026 inet n - n - 200 smtpd
-o content_filter=
-o smtpd_timeout=$imss_timeout
-o local_recipient_maps=
-o myhostname=postfix.imss71
-o smtpd_client_restrictions=
-o smtpd_enforce_tls=no
```

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

```
[socket]
proxy_smtp_server_ip=all
[smtp]
smtp_allow_client_ip=127.0.0.1, ::1
downstream_smtp_server_addr=::1
```

The Sandwich Model

In this configuration, one server hosts a Postfix instance as an upstream MTA for receiving (Server #1) and a second server hosts a Postfix instance as the downstream

MTA for delivering (Server #3). A third server hosts the IMSS daemon , which sits between the two Postfix servers as a scanning proxy (Server #2).

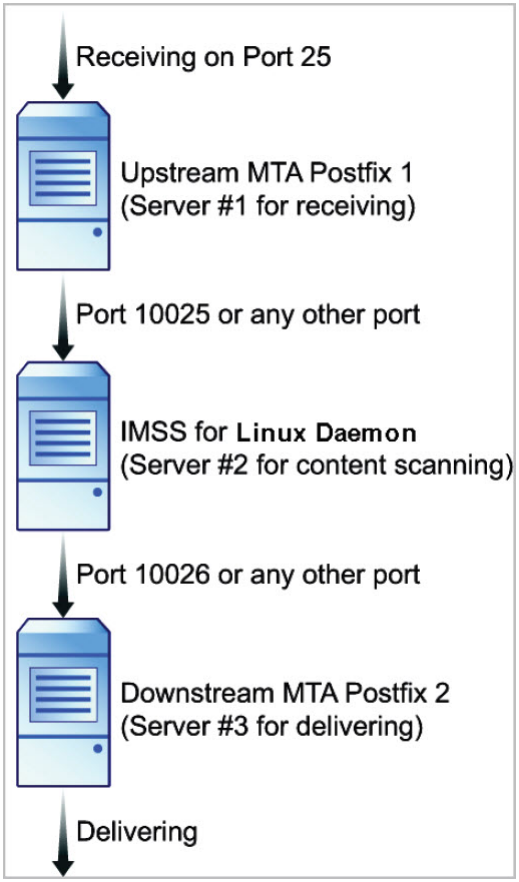


FIGURE 3-5. Sandwich model

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=[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 Sandwich Model in IPv6 Environments

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

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

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

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

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

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

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

The Proxy Model

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

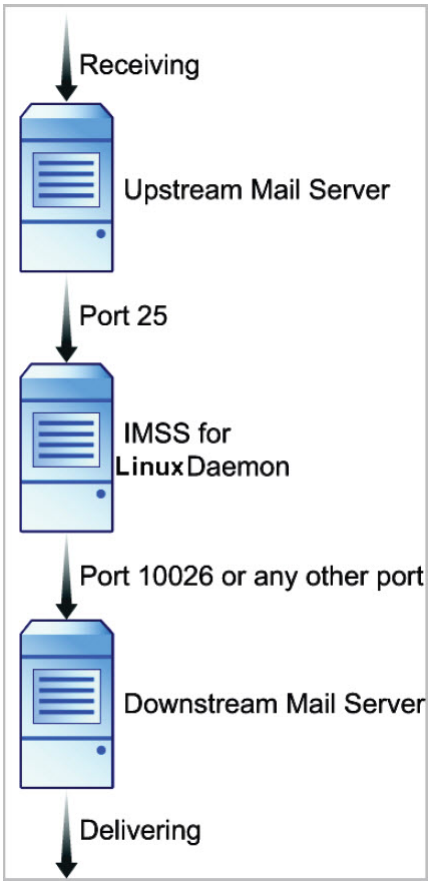


FIGURE 3-6. Proxy model

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.

The Proxy Model in IPv6 Environments

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

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

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

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

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

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

Tip

IMSS 7.1 SP1 can connect to TMCM servers residing in IPv6 networks. Make sure to configure the TMCM to support IPv6.

Understanding Installation Scenarios

IMSS allows you to install either a single instance of each component on a single server (single-server installation) or several 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 Setup 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

The following figure shows how a single-server installation of IMSS fits into a standard messaging network topology.

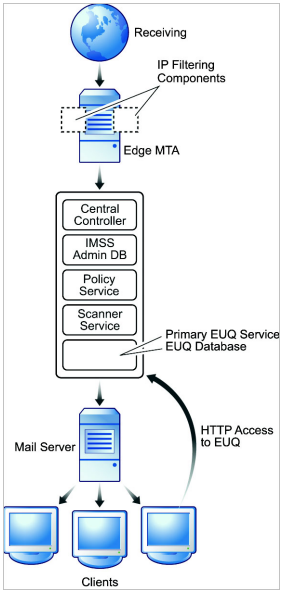


FIGURE 3-7. Single server deployment

Performing Single-Server Installation

Procedure

1. Install IMSS and End-User Quarantine.
2. On the edge MTA server, install all IP Filtering components.

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.

The following figure 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.

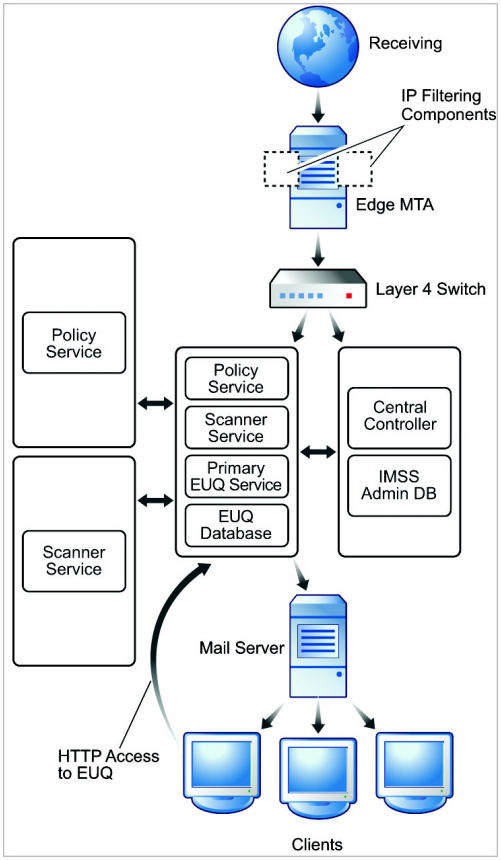


FIGURE 3-8. Multiple scanner service and policy service deployment

Performing Multiple Scanner Service Installation

Procedure

1. On one computer, install IMSS and End-User Quarantine.

See *Installing IMSS Components and End-User Quarantine on page 4-12*

See *Complex Distributed Installation on page 3-33*.

2. On other computers, install the necessary scanner service and policy services.

   On the edge MTA server, install all IP Filtering components. See *Deployment with IP Filtering on page 3-38*.

   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 console and perform the initial configuration (see *Using the Configuration Wizard* chapter 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.

The following figure 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.

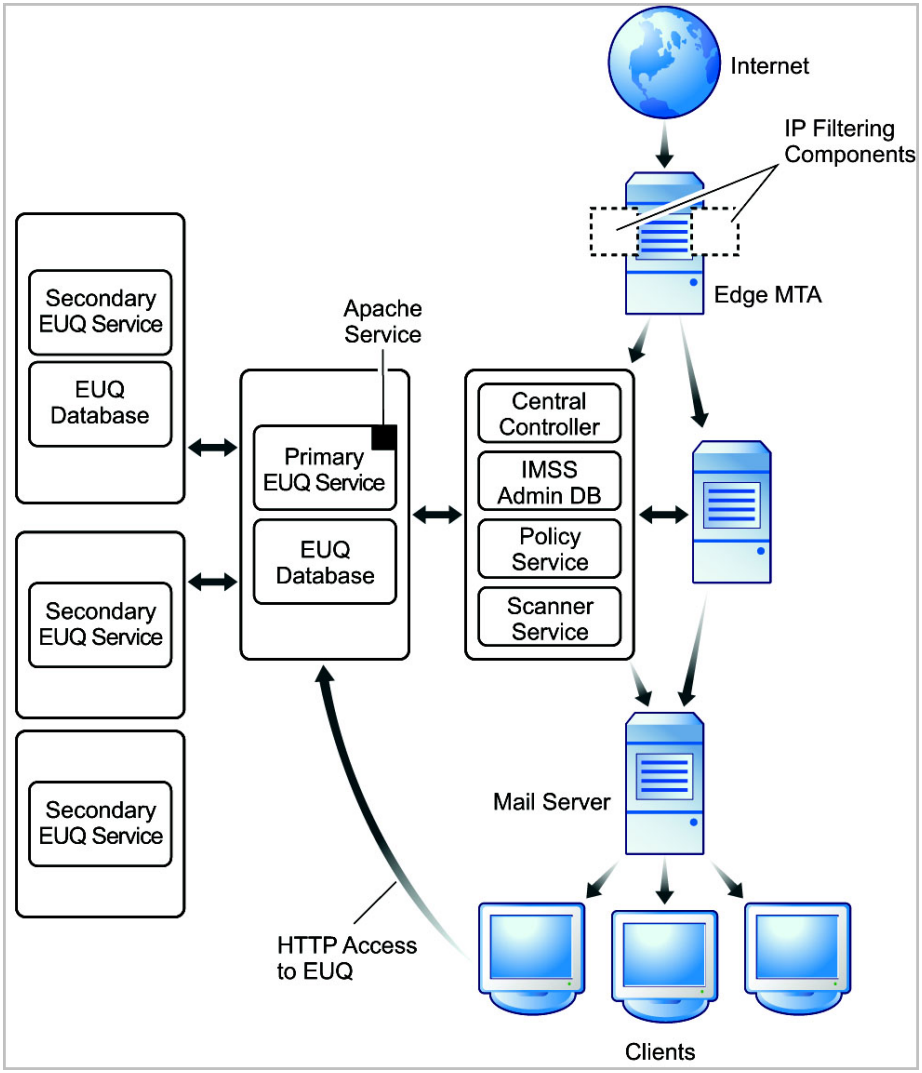


FIGURE 3-9. Multiple EUQ service deployment

Performing Multiple EUQ Service Installation

Procedure

1. On one computer, install IMSS.

   See *Installing IMSS Components and End-User Quarantine on page 4-12*

   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

   You can install the EUQ database 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 Email Reputation Services and IP Profiler on page 4-17*.

4. After you open the IMSS web 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 4-12*.

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 server, and the database on another, configure any firewall between the two servers to allow communication on port 5432 for database connections.

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 EUQ 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.

The following figure 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.

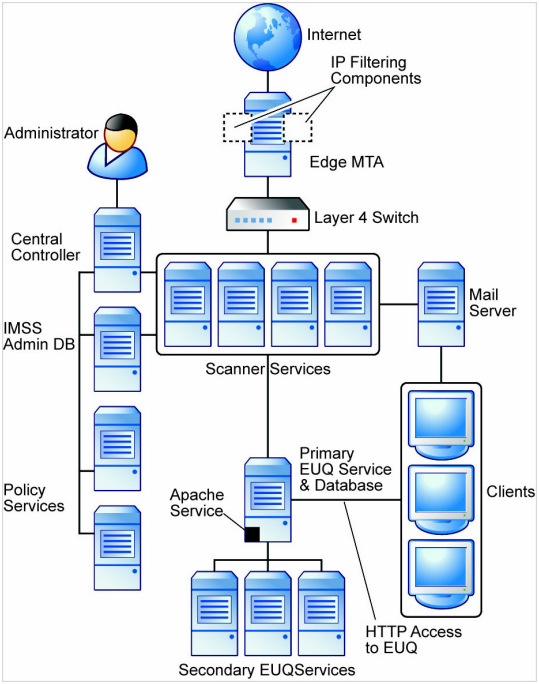


FIGURE 3-10. Complex architecture deployment

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 Trend Micro Control Manager (TMCM) 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 Control Manager server.

The following figure describes how each site differs in this scenario:

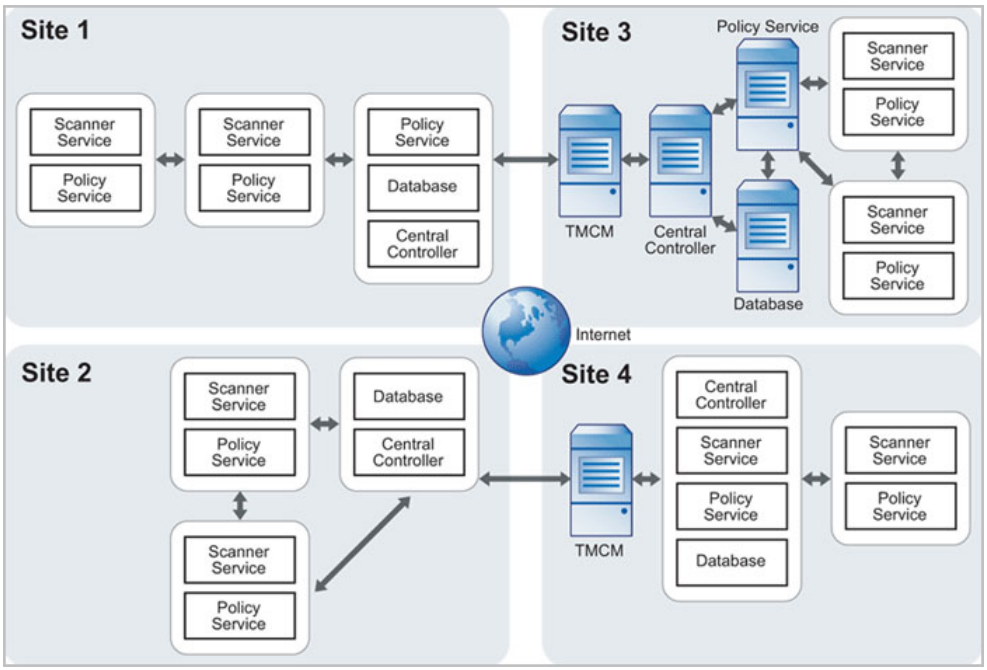


FIGURE 3-11. WAN deployment

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.

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 replicateIMSS Admin databases that directly report to it. If one of the IMSS Admin databases becomes corrupted or nonoperational, 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.

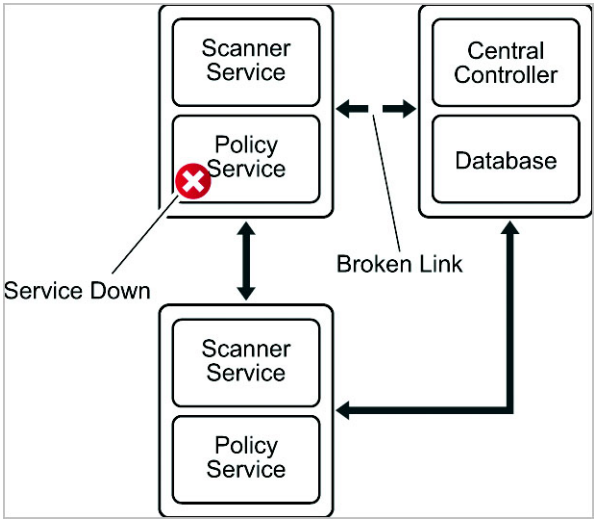


FIGURE 3-12. Failover

IP Filtering

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

Deployment with IP Filtering

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

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 the *IP Filtering Service* section of the *Administrator's Guide*.

About Failover

The following table 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 3-37*.

TABLE 3-3. 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 3-27*.

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 3-27*.
IMSS Admin database is not running	1. The IMSS server will continue to operate. 2. The IMSS web console is unavailable.	Back up the Admin database periodically. For more information on backup and restore, visit www.postgresql.org.
EUQ service database is not running	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.

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 logon. 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. Go to **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 SP1

This chapter explains how to install IMSS under different scenarios.

Topics include:

System Requirements

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

TABLE 4-1. System Requirements

SPECIFICATION	DESCRIPTION
Operating System	• Red Hat™ Enterprise Linux™ AS 4 Update 3 or above • Red Hat Enterprise Linux ES 4 Update 3 or above • Red Hat Enterprise Linux 5 (32/64-bit) • Red Hat Enterprise Linux 6.0, 6.1, 6.2, 6.3, 6.4 (32/64-bit)
CPU	• Recommended: Intel™ Quad Core 2.0GHz or above • Minimum: Intel™ Dual Pentium™ IV 3GHz or above
Memory	• Recommended: 4GB RAM • Minimum: 2GB RAM

SPECIFICATION	DESCRIPTION

Disk Space	• Recommended:
	250GB total
	The following recommendations are based on 500,000 messages/day, a 50% quarantine rate, and logs preserved for a month.
	  • 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
	• Minimum:
	80GB total
	Note
	The default location for the Admin database and EUQ database is `/var/imss`. The Default location for the working quarantine folders is `/opt/trend/imss/queue/`.

Swap Space	• Recommended:
	  • 2GB swap space if memory is greater than or equal to 4GB
	  • 4GB swap space if memory is less than 4GB
	• Minimum:
	2GB swap space

Browser	• Microsoft™ Internet Explorer™ 7, 8, 9, 10 • Mozilla™ Firefox™ 3.5, 3.6, 21
Monitor	Monitor that supports 800 x 600 resolution with 256 colors or higher

SPECIFICATION	DESCRIPTION
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.
LDAP server	• IBM™ Lotus Domino 6.0 • Microsoft Active Directory 2000, 2003, 2008 R2 • Sun iPlanet Directory 5.2
MTA	• Postfix™: Version 2.1, 2.2, 2.3, 2.6 • Sendmail™ 8.2, 8.13, 8.14 • Qmail™ 1.0.3
Linux Libraries (for all platforms)	• glibc-2.3.4 • libstdc++-libc6.2-2.so.3 (Required for PostgreSQL)
Server Platform Compatibility	IMSS should install and operate without issues on many brands of "off-the-shelf " server platforms. However, Trend Micro cannot guarantee 100% compatibility with all brands and models of server platforms. To obtain a list of Trend Micro certified servers that are guaranteed compatible with IMSS, access the following URL: http://www.trendmicro.com/go/certified To obtain a general list of available platforms that should operate with IMSS, access the following URL: http://wiki.centos.org/HardwareList Trend Micro cannot guarantee full compatibility with the hardware components from this general list.

Preparing the 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 http://www.postfix.org for details.

Procedure

- 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
```

Enabling Postfix IPv6 Support

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

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

Procedure

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

About Sendmail

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

Note

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

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

Sendmail Daemons

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

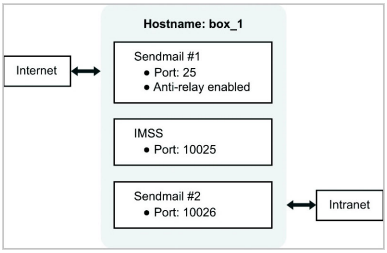


FIGURE 4-1. Sendmail daemons on one server

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

Configuring Sendmail #1

Procedure

1. Copy the `Sendmail.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 =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.

7. To enable IPv6 support, use:

```
DaemonPortOptions=Port=25,Addr=<IPv6_address>,
Name=MTA, Family=inet6
```

Configuring Sendmail #2

Procedure

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
```

Finishing Setup and Restarting Sendmail services

Procedure

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
```

About Qmail

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

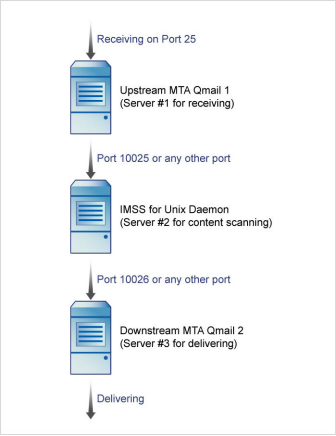


FIGURE 4-2. Deploying Qmail with IMSS

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

Procedure

- 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
```

Preparing to Install 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.

Procedure

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
   ```

Installing IMSS Components and End-User Quarantine

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

Procedure

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.

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

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

                    -- Main Menu --

             Your Current System Configuration:

             Central Controller   -------- [ Not installed ]
             Scanner Service      -------- [ Not installed ]
             EUQ Service          -------- [ Not installed ]

     1.      Install components.
     2.      Uninstall components.
     3.      Exit.

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

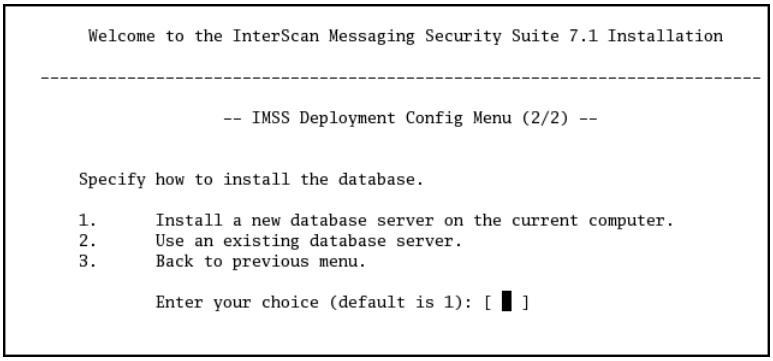
3. Type `1` to begin installation.
4. Read and accept the license agreement.
5. On the IMSS **Deployment Config Menu**, decide whether to install a new IMSS server or append to an existing installation.

   To append a scanner service or EUQ service to an existing IMSS server, you will need the database information for those components.

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

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

                  -- IMSS Deployment Config Menu (1/2) --


    1.      Install a new IMSS server on the current computer.
    2.      Append components to an existing IMSS server.
    3.      Back to Main Menu.

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

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.



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 type 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 4-5*.

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 *About IP Filtering Components on page 4-16*.

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.

About 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.

IPv6 Support and IP Filtering

Due to the large address pool of IPv6 addresses, IP Filtering only supports IPv4 networks. If you enable Email Reputation and IP Profiler, rules do not apply to

incoming email messages from IPv6 networks. Email Reputation or IP Profiler will not not block incoming email messages from IPv6 networks.

Enabling Port 25 on IPv6 Networks

If you enable IP Profiler and IPv6 at the same time, the IP Profiler listens to IPv4 only using port 25 while Postfix listens on both IPv4 and IPv6 using port 2500. To enable port 25 on IPv6 networks when IP Profiler is enabled, add an additional Postfix instances on the IPv6 network, using port 25.

Procedure

1. Add the following configuration in the Postfix `master.cf` file:

   ```
   :::25 inet n - n - - smtpd
   ```

2. Restart Postfix.

   A new Postfix instance listening on the IPv6 network using port 25 is added.

Installing Email Reputation Services and IP Profiler

Trend Micro Email Reputation Service (ERS) 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.

Procedure

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.

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

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

                        -- Install Components Menu --

    Trend Micro(tm) ERS and IP Profiler 7.1 Components List

    Install Email Reputation Services       -------- [ NO ]
    Install IP Profiler                     -------- [ NO ]

    1.      Modify option for ERS.
    2.      Modify option for IP Profiler.
    3.      Modify option for Install path (current: /opt/trend).
    4.      Start installation.
    5.      Back to Main Menu.

Enter a choice (default is 4): [   ]
```

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 specify 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:

Procedure

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
   ```

6. Restart FoxProxy:

   ```
   /opt/trend/ipprofiler/script/foxproxyd restart
   ```

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:

Procedure

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.

About IPv6 Support

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

SMTP routing

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

POP3 connections

IMSS supports connections to IPv6 POP3 servers.

Trend Micro services

IMSS supports communication with the following services using IPv6:

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

Email protection

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

Notifications

IMSS supports sending notifications to IPv6 Notification servers.

Network proxy

IMSS supports proxies in IPv6 networks. For configuration details, see *The Proxy Model in IPv6 Environments on page 3-25*.

Trend Micro Control Manager

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

IP address imports and exports

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

Configuring the Server for IPv6

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

Procedure

1. Enable the IPv6 network.
   a. Log on shell and edit `/etc/sysconfig/network` using the following command:

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

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

      ```
      NETWORKING_IPV6=yes
      ```

2. Configure the IPv6 address.
   a. Edit the configuration file for interfaces.

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

   b. Add the following lines:

      ```
      IPV6INIT=yes

      IPV6_AUTOCONF=no

      IPV6ADDR= 2001:db8:10ff::ae:44f2/64
      ```

   c. Restart the network service.

      ```
      # service network restart
      ```

Verifying the IPv6 Configuration

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

Procedure

1. Use the server to ping other endpoints.

   ```
   # ping6 ::1

   # ping6 <IPv6_address_of_another_endpoint>
   ```

2. Use another endpoint to ping the server.

   ```
   # ping6 <IPv6_address_of_this_endpoint>
   ```

Configuring IMSS for IPv6 Support

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

Proxy Settings for IPv6 Support

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

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

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

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

Settings to Allow IPv6 Clients

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

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

  127.0.0.1

  ::1

  123.123.123.123

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

  123.123.123.123/24

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

  123.123.123.123-223

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

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

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

Settings for Downstream IPv6 Servers

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

Note

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

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

  127.0.0.1

  ::1

  123.123.123.123

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

  Domain.com

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

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

Verifying the IPv6 Configuration

Before you begin

Configure the following parameters:

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

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

Procedure

1. Restart the IMSS daemon using the following command:

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

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

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

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

   The email message should successfully send.

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

   The email message should be rejected.

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

   The email message should be recieved.

IMSS 7.1 SP1 IPv6 support is correctly configured.

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.

Procedure

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.

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

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

                    -- Main Menu --

             Your Current System Configuration:

             Central Controller   -------- [ Not installed ]
             Scanner Service      -------- [ Not installed ]
             EUQ Service          -------- [ Not installed ]

     1.      Install components.
     2.      Uninstall components.
     3.      Exit.

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

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

Procedure

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.

Procedure

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
   ```

   Note

   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`, and `/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.

Procedure

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

Procedure

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

Procedure

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

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

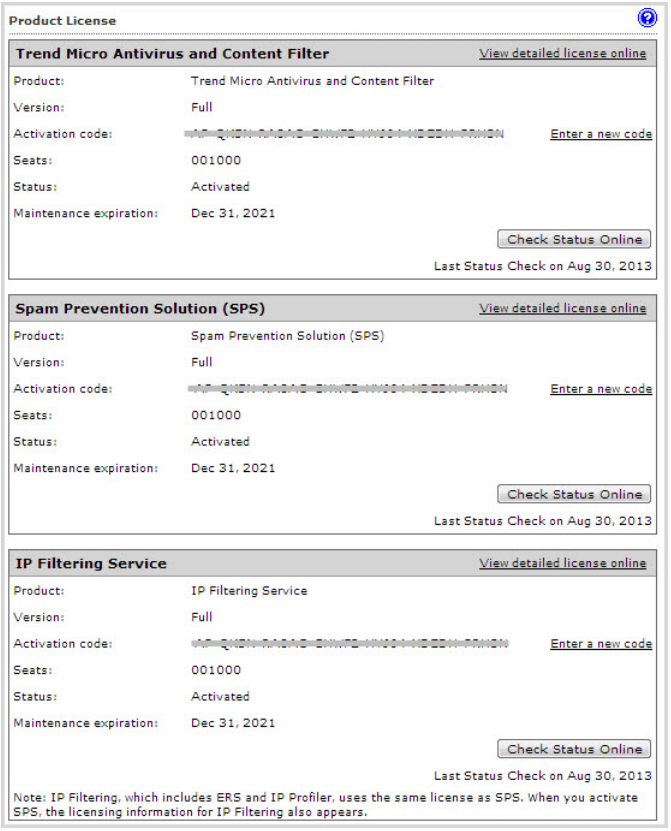
Fourteen (14) days prior to the expiry of the evaluation period, IMSS will display a warning message on the management console alerting you of the impending expiration.

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

Procedure

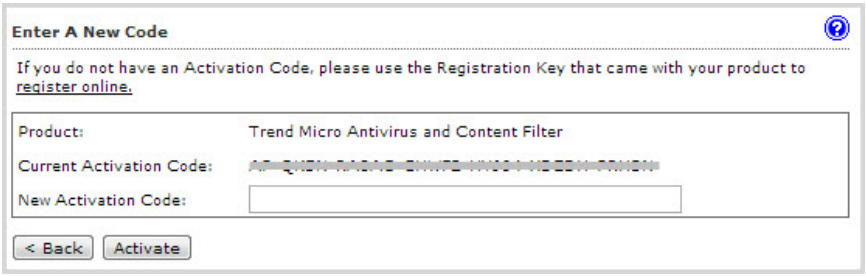
1. Go to **Administration** > **Product Licenses**.

The **Product License** screen appears.



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

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



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

Note

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

4. Click **Activate**.

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

Upgrading to IMSS 7.1 Linux

Upgrading from IMSS Linux 5.7 to IMSS 7.1

Upgrade from IMSS Linux 5.7 to IMSS Linux 7.1 in one of the following ways:

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

WARNING!

- The Setup program does not support automatic rollback to IMSS Linux 5.7. If the installation encounters issues, a manual rollback is the only option.

  For more information, see *Rolling Back the Upgrade on page 5-45*.

- After upgrading, IMSS Linux 5.7 queue data will be lost.

IMSS Linux 5.7 Upgrade Considerations

Consider the following before migrating or installing over IMSS Linux 5.7:

- Installing over IMSS Linux 5.7 , IMSS Linux 7.1 retains IMSS Linux 5.7 logs and email messages (in the local quarantine and archive areas). However, you will not be able to query the logs from the IMSSLinux 7.1 web console.
- Installing over IMSS 5.7 Linux requires stopping message traffic to the server where IMSS Linux 5.7 resides. Migration to an IMSS Linux 7.1 server does not impact message traffic on your network.

Tip

- Trend Micro recommends migration, using the Migration Tool, to perform an upgrade instead of installing over the previous version.
- 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 5-16*). If problems occur during migration, you can roll back to version 5.7 (see *Rolling Back the Upgrade on page 5-45*.
- 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 Setup program can automatically upgrade from InterScan Messaging Security Suite version 5.7 on the supported platforms. If the Setup program detects this version, it can do the following:

1. Back up your old IMSS settings.

2. Install IMSS Linux 7.1.

3. Migrate the existing settings.

The Setup program does not unregister the current IMSS server from Control Manager. That means that all logs from the old server can still be queried by Control Manager.

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 a single policy.
- Merge SPS filter's "Blocked senders", "Phishing email" 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 Linux 7.1 does not support quarantining email messages to different physical folders.

Modifying Policy Objects

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

For policy objects that migrate, described in *IMSS Linux 5.7 Settings that Change After Migration 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 Linux 5.7 to IMSS Linux 7.1.

Perform a Fresh Installation of IMSS 7.1 Linux

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

Tip

1. Prepare the system environment according to Trend Micro recommended system requirements. See the system requirements for more information.
2. Carefully plan your deployment strategy for IMSS Linux 7.1.

Become Familiar with IMSS Linux 7.1 Before Upgrading

To ease implementing IMSS Linux 7.1 into the network, administrators need to familiarize themselves with IMSS Linux 7.1 before upgrading from IMSS Linux 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 Linux 7.1 to test functions and policies.

General IMSS Linux 5.7 Migration Tasks

Perform the following tasks to simplify migration:

- Back up and then delete all mail messages under the quarantine and archive areas.
- Clean up IMSS Linux 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 Linux 5.7 Linux, Trend Micro recommends manually configuring IMSS Linux 7.1 Linux.

Verify IMSS 7.1 Linux 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.
- Go to the **Policy** section of the IMSS Linux 7.1 web console to verify that policies have the same settings as those in IMSS Linux 5.7.
- Send sample email messages to verify that IMSS Linux 7.1 has the same message delivery behavior as IMSS Linux 5.7 .

IMSS Linux 5.7 Settings that Cannot be Migrated

Certain IMSS Linux 5.7 settings cannot migrate to IMSS Linux 7.1:

TABLE 5-2. IMSS 5.7 Linux 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 not configured from the Web console
	IP address of SMTP Interface

SETTING	SETTINGS NOT MIGRATED
Policy Settings	Security limits: • "Number of cleaning attempts" • "Number of viruses reported" • "Message size"
	Virus actions: • "No virus detected" • "Joke program attachment detected"
	Spam Filter settings: • "Global spam scanning mode" • "Baseline detection rate" • "Additional sensitivity" • Approved and blocked lists for POP3 • Actions for Graymail • Advanced action settings

Setting	Settings not Migrated
Policy 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
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

Setting	Settings not Migrated
Report Settings	Perl reports
	SPS reports

IMSS Linux 5.7 Settings that Change After Migration

Certain IMSS Linux 5.7 settings change after migrating to IMSS Linux 7.1:

Table 5-3. IMSS 5.7 Linux Settings that Change After Migration

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 Linux 7.1 will be reset to the maximum value for IMSS Linux 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

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. The maximum value is specified.
	Number of days to keep log: If IMSS 5.7 settings specify keeping logs less than 150 days, migration changes the setting to 150 days. Specifying "0" (meaning there is no limit to the length of time to keep files) is no longer supported. The maximum value is specified.
	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 Linux 5.7 Linux, 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 Linux 7.1.

Single Admin Database

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

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

Note

The single Admin database upgrade option has the following characteristics:

1. There is only one IMSS server.
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.

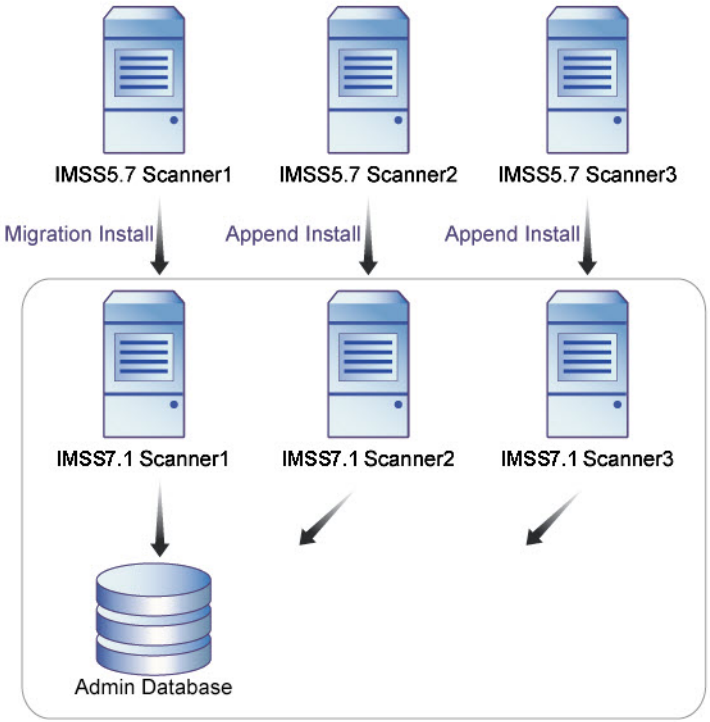


FIGURE 5-1. Single Admin database

Multiple Admin Databases

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

Note

The multiple Admin databases upgrade option has the following characteristics:

1. Multiple IMSS servers 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.

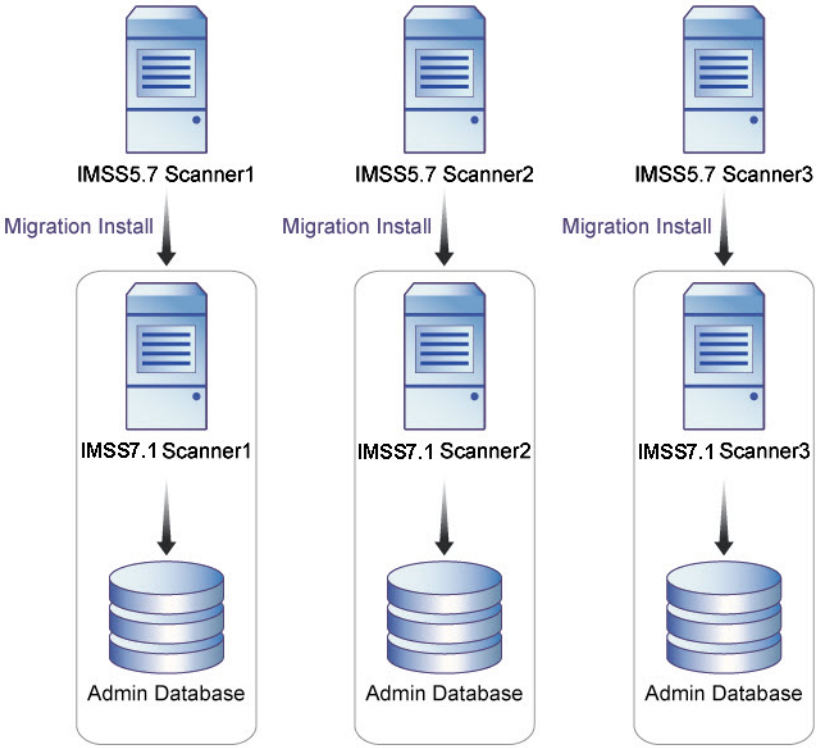


FIGURE 5-2. Multiple Admin databases

Backing Up IMSS 5.7 Settings

Although the IMSS Setup program backs up your old IMSS settings, Trend Micro recommends that you perform the backup manually before migrating.

Backing up IMSS 5.7 Linux Data for a Single-server Deployment

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

Note

The IMSS 7.1 Linux installer creates a full binary backup. However, users are responsible for creating a full backup of the IMSS 5.7 Linux package information and the IMSS 5.7 EUQ database (optional).

Procedure

1. Stop IMSS 5.7 Linux 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 IMSS 5.7 Linux Data for a Distributed Deployment

Back up your IMSS 5.7 Linux 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

Note

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

Procedure

- 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
```

Installing IMSS Linux 7.1 Over IMSS Linux 5.7

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

Tip

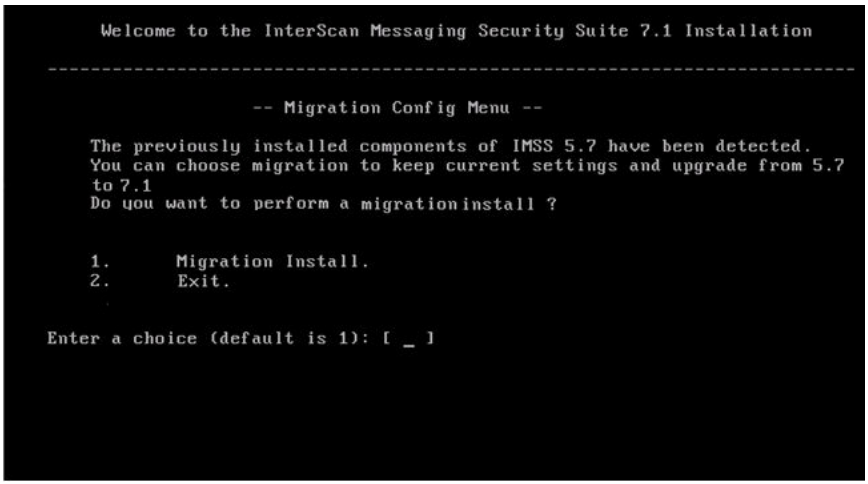
Trend Micro recommends migration to perform an upgrade, instead of installing over the previous version. See *Migrating from IMSS Linux 5.7 to IMSS Linux 7.1 on page 5-33* for more information.

The Setup program does not unregister the current IMSS server from Control Manager. That means that all logs from the old server can still be queried by Control Manager.

Procedure

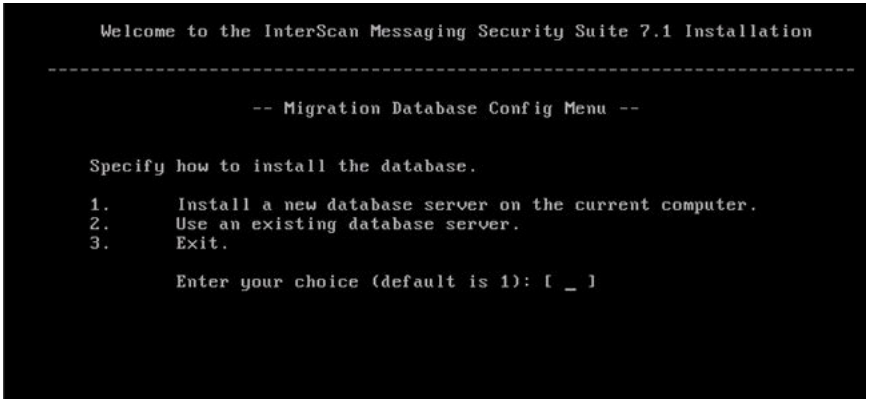
1. Log on as a superuser on the computer where you installed version 5.7 and go to the installation package directory.
2. Type `./isinst.sh`.

   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.

Note

If you want to use the existing IMSS 5.7 database server to install the IMSS 7.1 admin database or EUQ database, you need to modify the access control of PostgreSQL as follows:

i. `vi /var/imss/pgdata/pg_hba.conf`

ii. Modify "`255.255.255.255`" on line 60 to "`255.255.255.0`"

iii. Modify "`ffffff00`" on line 63 to "`255.255.255.0`"

iv. Save the changes

v. `/opt/trend/imss/script/dbctl.sh stop`

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

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

Note

By default, the installer uses the install path of the old version. You cannot modify the install path if you choose migration install.

- If you want to install the EUQ service, please note that the first EUQ service you installed is a primary service. Secondary services provide load-balance assistance to the primary service.
- If you want to install the EUQ database, you can install a new database server or use an existing database server, and then enter that database server's information.

8. 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.

9. 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.

10. Check Postfix configuration of IMSS 7.1 and press ENTER to continue.

The configuration sample is saved to:

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

a. 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.

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

Note

a. 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.

b. 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**

c. 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 Linux 7.0 to IMSS Linux 7.1

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

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

The Setup program does not unregister the current IMSS server from Control Manager. That means that all logs from the old server can still be queried by Control Manager.

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

Migrating or Installing Over IMSS 7.0 Linux

Consider the following before migrating or installing over IMSS 7.0:

- IMSS 7.1 retains all IMSS 7.0 data.
- IMSS 7.1 retains IMSS 7.0 hidden key configuration settings in the file.
- IMSS 7.1 retains all IMSS 7.0 reports.
- IMSS 7.1 retains all IMSS 7.0 Control Manager settings.
- While in a distributed deployment, IMSS 7.1 maintains the deployment. This means you do not need to make any changes to your deployment or make any configuration modifications to maintain the deployment.
- Administrators must stop message traffic to the server where IMSS 7.0 resides. Migration to an IMSS 7.1 server does not impact message traffic on your network.

SELinux enabled servers also require special preparation before upgrading to IMSS 7.1 . See *Preparing an SELinux Server for Upgrade on page 5-25* for detailed information.

IMSS 7.1 Linux Settings That Cannot be Migrated

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

Preparing an SELinux Server for Upgrade

SELinux impacts IMSS 7.1 Linux upgrading in two ways:

- Dynamic library context setup
- Port bind policy

During installation, IMSS 7.1 Linux sets up the context of all dynamic libraries used by IMSS automatically. However, users must configure the SELinux port bind policy manually.

WARNING!

Many IMSS services will not function properly without setting up the port bind policy.

Configure the port bind policy before launching the IMSS 7.1 Linux installer. After installation, each time users change the port assignment from the web console, manually configure the port bind policy.

TABLE 5-4. Default IMSS Ports

PORT	DESCRIPTION
Internal Ports	
25	SMTP port
2500	SMTP port when FoxHunter has been installed
53	Bind port
8005	IMSS web console management port
8015	EUQ web console management port
8445	IMSS web console port (HTTPS)
8446	EUQ web console port (HTTPS)
8447	EUQ Load balance port
10024	Mail re-process port
10025	IMSS scanner port
10026	Postfix delivery port
5432	PostgreSQL port
Occupied Ports	
15505	IMSS manager port
5060	Policy server port

PORT	DESCRIPTION
110	Incoming POP3 port

Users can use both the command line SELinux configuration tool (semanage) and the GUI configuration tool (system-config-securitylevel) to open these ports.

Note

The above table only lists the default port numbers. If port numbers were modified from the default values, change the corresponding port number in SELinux policy rules.

Backing Settings Up

To back up a product means to copy the product data and log files to a backup folder. If an error occurs during an upgrade, the new database can be dropped. Then attaching the backup data and log files to the original product database fully recovers the original database.

Configuration Settings Backup

The IMSS 7.1 Linux Setup program automatically backs up IMSS 7.0 Linux configuration files when IMSS 7.1 Linux installs over an IMSS 7.0 Linux installation. Back up of configuration files occurs just prior to the Admin database upgrade, during the course of installation.

Backing up IMSS 7.0 Linux Settings

Procedure

1. Stop IMSS 7.0 Linux mail traffic for approximately one minute.
2. Stop all IMSS 7.0 Linux 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 7.0 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

If upgrading an SELinux server refer to *Preparing an SELinux Server for Upgrade on page 5-25* for instructions on preparing the SELinux server.

Note

IMSS 7.0 SP1 with patch 2 or above is required when upgrading or migrating.

Procedure

1. Back up IMSS 7.0 data before installation. See *Backing Settings Up on page 5-27* 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

If upgrading SELinux servers refer to *Preparing an SELinux Server for Upgrade on page 5-25* for instructions on preparing the SELinux server.

Note

IMSS 7.0 SP1 with patch 2 or above is required when upgrading or migrating.

Procedure

1. Back up IMSS 7.0 data before installation. See *Backing Settings Up on page 5-27* 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. 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.

8. 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.

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

```
imss/ipfilterinst.sh
```

Note

IP Profiler upgrades automatically once started.

10. Upgrade all other scanners following steps 4 to 9. No special sequence is required when upgrading subsequent scanners.

11. After upgrading all scanners, start the IMSS service on all scanners using the command:

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

Migrating to IMSS 7.1 Linux

The following migration paths are supported:

Migrating from IMSS Linux 5.7 to IMSS Linux 7.1

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

Exporting IMSS Linux 5.7 Settings

Use the IMSS Linux 5.7 Export Tool to export settings from IMSS Linux 5.7. The IMSS Linux 5.7 Export Tool is located in the IMSS Linux 7.1 installation folder.

You can obtain the latest migration tool at:

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

Procedure

1. Clean up IMSS Linux 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 `migration_tool_57to71.tar.gz` to a directory on the IMSS Linux 5.7 server.

3. Use the following command to extract the Export Tool:

   ```
   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 Linux 5.7 Settings to IMSS Linux 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.

Procedure

1. Install IMSS Linux7.1 on a server.
2. Use the IMSS Linux 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.

   - `C:\Imss7InstLog\migrationfrom57\MigrationReport`
   - `C:\Imss7InstLog\migrationfrom57`

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 Linux 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.

Migrating from IMSS Linux 7.0 to IMSS Linux 7.1

The migration process requires the following tasks:

- **Step 1**: Exporting IMSS 7.0 Linux settings
- **Step 2**: Importing IMSS 7.0 Linux settings to IMSS 7.1

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

Note

IMSS Linux 7.0 SP1 with patch 2 or above is required when upgrading or migrating.

Exporting IMSS Linux 7.0 Settings

Use the IMSS Linux 7.0 Export Tool to export settings from IMSS Linux 7.0. The IMSS Linux 7.0 Export Tool is located in the IMSS Linux 7.1 installation folder.

You can obtain the latest migration tool at:

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

Procedure

1. Copy to following file to the IMSS 7.0 server.

   ```
   migration_tool_70to71.tar.gz
   ```

2. Use the following command to extract the Export Tool:

   ```
   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 Linux 7.0 Settings to IMSS Linux 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 Linux 7.1.

Procedure

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 Linux configuration package onto IMSS 7.1. See *Exporting IMSS Linux 7.0 Settings on page 5-36* for detailed information.
4. Start the migration tool using the following command:

   ```
   ./migration_tool_70.sh
   ```

   Note

   Read the Migration Tool 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:

a. Check the results for migrated items.

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

c. Verify that all policies can be accessed on the web console.

Migrating to IMSS 7.1 SP1 Linux

The following migration paths are supported:

- IMSS 7.0 SP1 Linux to IMSS 7.1 SP1 Linux
- IMSS 7.0 SP1 Patch 4 Solaris to IMSS 7.1 SP1 Linux
- IMSS 7.1 Patch 3 Linux to IMSS 7.1 SP1 Linux

Migrating from IMSS 7.0 SP1 Linux to IMSS 7.1 SP1 Linux

The migration process requires the following tasks:

- **Step 1**: Exporting IMSS 7.0 settings
- **Step 2**: Importing IMSS 7.0 settings to IMSS 7.1 SP1

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

Exporting IMSS 7.0 Linux Settings

Use the IMSS 7.0 Linux Export Tool to export settings from IMSS 7.0 Linux. The IMSS 7.0 Linux Export Tool is located in the IMSS 7.1 SP1 installation folder.

You can obtain the latest migration tool at:

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

Note

There are no command line tools for the IMSS 7.1 SP1 Linux migration. Use the IMSS web console to export or import settings.

Procedure

1. Export the settings by running the following migration tool on the IMSS 7.0 Linux server:

   ```
   migration_tool_70to71.tar.gz
   ```

2. Use the following command to extract the Export Tool:

   ```
   tar zvf migration_tool_70to71.tar.gz
   ```

3. Use the following command to run the Export Tool:

   ```
   ./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`.

4. Copy the exported settings file to any computer with access to the IMSS web management console.

Importing IMSS Settings to IMSS 7.1 SP1 Linux

The following procedure explains how to import configuration files from the following IMSS versions:

- IMSS 7.0 Linux SP1
- IMSS 7.1 Linux Patch 3
- IMSS 7.1 Linux SP1
- IMSS 7.0 Solaris SP1 Patch 4

Note

IMSS 7.1 SP1 Linux will not import configuration files exported from other product versions.

Procedure

1. From the IMSS 7.1 SP1 Linux web console, go to **Administration** > **Import/Export**.

   The **Import/Export** screen appears.

2. Under **Import Configuration Files**, click **Choose File**.

   Note

   Only the following configurations are accepted:

   IMSS 7.0 Linux SP1, IMSS 7.1 Linux Patch 3, IMSS 7.1 Linux SP1 or IMSS 7.0 Solaris SP1 Patch 4.

3. Select the previously exported settings file, then click **Open**.
4. Click **Import**.
5. Click **OK** to confirm.
6. Wait a moment for the configuration import to complete.
7. Click **Return** to go back to the **Import/Export** screen.

Migrating from IMSS 7.0 SP1 Patch 4 Solaris to IMSS 7.1 SP1 Linux

The migration process requires the following tasks:

- **Step 1**: Exporting IMSS 7.0 settings
- **Step 2**: Importing IMSS 7.0 settings to IMSS 7.1 SP1

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

Exporting IMSS 7.0 Solaris Settings

Use the IMSS 7.0 Solaris Export Tool to export settings from IMSS 7.0 Solaris. The IMSS 7.0 Solaris Export Tool is located in the IMSS 7.1 SP1 installation folder.

You can obtain the latest migration tool at:

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

Note

There are no command line tools for the IMSS 7.1 SP1 Linux migration. Use the IMSS web console to export or import settings.

Procedure

1. Export the settings by running the following migration tool on the IMSS 7.0 Solaris server:

   ```
   export_tool_sol_70.tar.gz
   ```

2. Use the following command to extract the Export Tool:

   ```
   tar zvf export_tool_sol_70.tar.gz
   ```

3. Use the following command to run the Export Tool:

   ```
   ./export_tool_70.sh
   ```

   Note

   Solaris ignores all option switches.

   The Export Tool exports the configuration settings package, `imss_config_70.tar.gz`, to the current directory.

4. Copy the exported settings file to any computer with access to the IMSS web management console.

Importing IMSS Settings to IMSS 7.1 SP1 Linux

The following procedure explains how to import configuration files from the following IMSS versions:

- IMSS 7.0 Linux SP1
- IMSS 7.1 Linux Patch 3
- IMSS 7.1 Linux SP1
- IMSS 7.0 Solaris SP1 Patch 4

Note

IMSS 7.1 SP1 Linux will not import configuration files exported from other product versions.

Procedure

1. From the IMSS 7.1 SP1 Linux web console, go to **Administration** > **Import/Export**.

   The **Import/Export** screen appears.

2. Under **Import Configuration Files**, click **Choose File**.

   Note

   Only the following configurations are accepted:

   IMSS 7.0 Linux SP1, IMSS 7.1 Linux Patch 3, IMSS 7.1 Linux SP1 or IMSS 7.0 Solaris SP1 Patch 4.

3. Select the previously exported settings file, then click **Open**.
4. Click **Import**.

5. Click **OK** to confirm.
6. Wait a moment for the configuration import to complete.
7. Click **Return** to go back to the **Import/Export** screen.

Migrating from IMSS 7.1 Linux Patch 3 to IMSS 7.1 SP1 Linux

The migration process requires the following tasks:

- **Step 1**: Exporting IMSS 7.1 settings
- **Step 2**: Importing IMSS 7.1 settings to IMSS 7.1 SP1

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

Exporting IMSS 7.1 Patch 3 Linux Settings

Procedure

1. From the IMSS 7.1 Patch 3 Linux web console, go to **Administration** > **Import/Export**

   The **Import/Export** screen appears.
2. Under **Export Configuration Files**, click **Export** to export the settings
3. Wait a moment for the configuration files to generate.
4. Save the exported configuration file to local storage on the server.

Importing IMSS Settings to IMSS 7.1 SP1 Linux

The following procedure explains how to import configuration files from the following IMSS versions:

- IMSS 7.0 Linux SP1

- IMSS 7.1 Linux Patch 3
- IMSS 7.1 Linux SP1
- IMSS 7.0 Solaris SP1 Patch 4

Note

IMSS 7.1 SP1 Linux will not import configuration files exported from other product versions.

Procedure

1. From the IMSS 7.1 SP1 Linux web console, go to **Administration** > **Import/Export**.

   The **Import/Export** screen appears.

2. Under **Import Configuration Files**, click **Choose File**.

   Note

   Only the following configurations are accepted:

   IMSS 7.0 Linux SP1, IMSS 7.1 Linux Patch 3, IMSS 7.1 Linux SP1 or IMSS 7.0 Solaris SP1 Patch 4.

3. Select the previously exported settings file, then click **Open**.
4. Click **Import**.
5. Click **OK** to confirm.
6. Wait a moment for the configuration import to complete.
7. Click **Return** to go back to the **Import/Export** screen.

Activating Supported Services

After upgrading, IMSS 7.1 SP1 retains the Activation Code from the previous product version. 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 Email reputation, you can specify the Activation Code during installation or from the web console after installation completes.

Rolling Back the Upgrade

If any problems occur with the upgrade to version 7.1 SP1, 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 Linux 7.1 Over IMSS Linux 5.7 on page 5-20* process) where rolling back must be performed manually.

The rollback process requires the following steps:

Related information

➥ *Removing IMSS 7.1 Components*
➥ *Rolling Back to IMSS 7.0*

Removing IMSS 7.1 Components

Procedure

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 SP1 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
```

Completing the Rollback to IMSS 5.7

Procedure

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 5-28* process or Step 8 in the *Upgrading an IMSS 7.0 Distributed Deployment on page 5-30*.

- 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

Removing IMSS 7.1 Components

Procedure

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
```

Completing the Rollback to IMSS 7.0

Procedure

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 may encounter 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

Removing IMSS 7.1 Components

Procedure

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
```

Completing the Rollback to IMSS 7.0

Procedure

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 and Support Information

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

Topics include:

Troubleshooting

For common issues that you might encounter when installing, or configuring and administering IMSS, see *Installation Troubleshooting Issues on page 6-2*. If you have additional problems, check the Trend Micro Knowledge Base.

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 About Installation

Postfix MTA Settings

If I deploy multiple scanners with Postfix, how can I manage these Postfix instances centrally?

To control all the Postfix computers from the web management console, enable the **Apply settings to all scanners** option. Choose **Administrator** > **SMTP Routing** > **SMTP** from the menu.

Can I make an exception on the settings for some Postfix instances separately?

To make an exception for some Postfix settings, search for the key "detach_key_postfix" in `imss.ini`, and add the keys that you do not want to apply from the web management console. For example:

```
detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_direct
ory
```

The parameters above will not be overwritten by any settings that you configure through the web console. You can modify `main.cf` manually.

Note

"`{Parameter1:{Parameter2}:…::{Parameter n}`" means you can use one or more parameters by separating them using colons.

You can find the parameter names in the table `tb_postfixconfig` from the database, under the column fieldname.

WARNING!

Use extreme caution when modifying the configuration file.

Installation / Uninstallation

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. IMSSApache takes the port 8447.

Upgrading

Are all IMSS 7.1 settings retained during an upgrade or migration?

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. The settings can be found in the general migration report:

`$IMSS_HOME/installlog/migration/MigrationReport/GeneralReport.txt`.

How do I upgrade IMSS 7.1 scanners?

To upgrade from multiple IMSS 7.1 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 7.1 database server?

Yes. IMSS 7.1 database settings (such as LDAP settings and EUQ settings) are kept.

Is rollback to IMSS 7.1 possible after upgrading?

Yes. For details instructions, see *Rolling Back the Upgrade on page 5-45*.

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

No. Upgrade from a computer with an IMSS 7.1 scanner installed.

How do I simplify SPS rules after an upgrade?

To keep all SPS filter settings for all policies of IMSS 7.1, IMSS 7.5 migrates each SPS filter to one or multiple SPS rule(s) in IMSS 7.5. 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 7.1 filters and policies mapped during an upgrade?

The architectures of IMSS 7.0 and IMSS7.1 are very similar. All policies and filters map without issues.

The architectures of IMSS 5.7 and IMSS7.1 are very different. Therefore, the upgrade module maps all IMSS 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 IMSS5.7 for both SMTP and POP3 traffic.
  - There will be only one rule for one virus filter after migration if it is "inactive" in IMSS 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 email"

    - "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 IMSS 5.7 for both SMTP and POP3 traffic.
    - There will be one rule for one eManager filter after migration if it is "inactive" in IMSS 5.7 for both SMTP and POP3 traffic. The rule direction is for "Both incoming and outgoing directions". You can add the related rule for the POP3 rule direction in IMSS 7.0 if necessary.

For the detailed mapping relationship of each policy, check:

```
$IMSS_HOME/installlog/migration/MigrationReport/
DetailReport.txt
```

Support Information

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

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

   The **Technical Support** product page appears.

3. Use the **Search Support** box to search for available solutions.

4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

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

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

Contacting Technical Support

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

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

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

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

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Security Intelligence

Comprehensive security information is available at the Trend Micro website.

http://www.trendmicro.com/vinfo

Security information includes:

- List of malware and malicious mobile code currently active or "in the wild"
- Computer malware hoaxes
- Internet threat advisories
- Malware weekly report
- Threat Encyclopedia, which includes a comprehensive list of names and symptoms for known malware, spam, malicious URLs, and known vulnerabilities, plus write-ups on web attacks and online trends.

Download Center

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

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

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

Sending Suspicious Content to Trend Micro

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

Email Reputation Services

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

https://ers.trendmicro.com/

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

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Web Reputation Services

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

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

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

Index

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com
www.trendmicro.com
Item Code: MSEM76002/130725