TREND MICRO™

InterScan™ Messaging Security Suite 7

Comprehensive threat protection at the Internet messaging gateway

for LINUX™ & Solaris™

Installation Guide

Messaging Security

Document Part Number: MSEM73220/70515

Release Date: September 2007

The Installation Guide for Trend Micro InterScan Messaging Security Suite 7.0 is intended to introduce the main features of the product and provide deployment instructions for various network environment. You should read through this document prior to deploying the product. For post-installation instructions on configuring and administering IMSS, please refer to the IMSS Administrator's Guide.

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

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

Contents

Chapter 4: Installing and Upgrading

Preface

Welcome to the *Trend Micro™ InterScan™ Messaging Security Suite 7.0 Installation Guide*. This manual contains information on InterScan Messaging Security Suite (IMSS) features, system requirements, as well as instructions on installation and upgrade.

Please refer to the IMSS 7.0 Administrator's Guide for information on how to configure IMSS settings and the Online Help in the Web management console for detailed information on each field on the user interface.

This preface discusses the following topics:

InterScan Messaging Security Suite 7.0 Documentation

The InterScan Messaging Security Suite 7.0 (IMSS) documentation consists of the following:

- **Installation Guide**—Contains introductions to IMSS features, system requirements, and provides instructions on how to deploy and upgrade IMSS in various network environments.
- **Administrator's Guide**—Helps you get IMSS up and running with post-installation instructions on how to configure and administer IMSS.
- **Online Help**—Provides detailed instructions on each field and how to configure all features through the user interface. To access the online help, open the Web management console, then click the help icon ( ).
- **Readme Files**—Contain late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

The *Installation Guide*, *Administrator's Guide* and *readme files* are available at http://www.trendmicro.com/download.

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
- LDAP
- Database management

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

Document Conventions

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

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

Chapter 1

Introducing InterScan™ Messaging Security Suite

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

Topics include:

About IMSS 7.0

InterScan Messaging Security Suite (IMSS) 7.0 integrates antivirus, anti-spam, anti-phishing, and content filtering for complete email protection. This flexible software solution features award-winning anti-virus and zero-day protection to block known and unknown viruses.

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

What's New

Table 1-1 provides an overview of what's new in version 7.0.

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 your 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.

TABLE 1-1. New Features

New Feature	Description
Multiple spam prevention technologies	Three layers of spam protection: • Network Reputation Services filters spam senders at the connection layer. • IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS). • Trend Micro Anti-spam engine accurately detects and takes action on spam.
IntelliTrap	IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods will enter your network through email.
Delegated administration	LDAP-integrated account management which 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 right out of the box.
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 transferred with minimum effort during setup.
Mail auditing and tracking	Detailed logging for all messages to track and identify message flow related issues.
Integration with Trend Micro Control Manager™	Perform log queries on Network Reputation Services from Control Manager, in addition to other supported features.

TABLE 1-1. New Features

IMSS Main Features and Benefits

Feature	Descriptions	Benefits
Antivirus protection	IMSS performs virus detection using Trend Micro scan engine and a technology called pattern matching. The scan engine compares code in files traveling through your gateway with binary patterns of known viruses that reside in the pattern file. If the scan engine detects a match, it attempts to clean the file by removing the virus code, quarantining the message or taking other actions as configured in the policy rules.	IMSS's enhanced virus/content scanner keeps your messaging system working at top efficiency.
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 incorrectly identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when the 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 incorrectly classified as security risks.	Helps reduce the risk that a virus compressed using different file compression schemes will enter your network via email.
Content management	IMSS analyzes email messages and their attachments, traveling to and from your network, for appropriate content.	Content that you deem inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using IMSS.

TABLE 1-2. Main features and benefits

Feature	Descriptions	Benefits
Protection against other email threats		
DoS attacks	By flooding a mail server with large attachments, or sending messages that contain multiple viruses or recursively compressed files, individuals with malicious intent can disrupt mail processing.	IMSS allows you to configure the characteristics of messages that you want to stop at the SMTP gateway, thus reducing the chances of a DoS attack.
Malicious email content	Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions.	IMSS allows you to configure the types of messages that are allowed to pass through the SMTP gateway.
Degradation of services	Non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours.	Most companies have acceptable usage policies for their messaging system—IMSS provides tools to enforce and ensure compliance with existing policies.
Legal liability and business integrity	Improper use of email can also put a company at risk of legal liability. Employees may engage in sexual or racial harassment, or other illegal activity. Dishonest employees can use a company messaging system to leak confidential information. Inappropriate messages that originate from a company's mail server damage the company's reputation, even if the opinions expressed in the message are not those of the company.	IMSS provides tools for monitoring and blocking content to help reduce the risk that messages containing inappropriate or confidential material will be allowed through your gateway.

TABLE 1-2. Main features and benefits

Feature	Descriptions	Benefits
Mass mailing virus containment	Email-borne viruses that may automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users. When IMSS detects a mass-mailing virus, the action taken 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^{SM} ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.
Spyware and other types of grayware		
Spyware and other types of grayware	Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see *About Spyware and Other Types of Grayware* on page 1-9	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.

TABLE 1-2. Main features and benefits

Feature	Descriptions	Benefits
Integrated spam		
Spam Prevention Solution (SPS)	Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam-detection services to other Trend Micro products. To use SPS, you must pay for and obtain an SPS Activation Code. For more information, refer to your sales representative. SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license. **Note:** Please activate SPS before you configure IP Profiler and NRS.	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 originators change their techniques.
Spam Filtering with IP Profiler and NRS	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. NRS blocks IP addresses of known spam senders that Trend Micro maintains in a central database For details, see the following: • *IP Filtering* on page 2-10 • *Network Reputation Services* on page 2-11 • *How IP Profiler Works* on page 2-11 • *How Network Reputation Service Works* on page 2-12	With the integration of IP Filtering, which includes IP Profiler and Network Reputation Services (NRS), IMSS can block spammers at the IP level.
Others		
LDAP & domain-based policies	You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™ or Microsoft™ Active Directory™ for user-group definition and administrator privileges. Note that you have to enable LDAP in order to use web quarantine tool.	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	Web-based management console allows you to conveniently configure IMSS policies and settings on the Web.	The Web-based console also provides greater security as it is SSL-compatible.

TABLE 1-2. Main features and benefits

Feature	Descriptions	Benefits
End-User Quarantine (EUQ)	IMSS provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Spam Prevention Solution (SPS) quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete or approve for delivery.	With the Web-based EUQ console, end-users can manage messages that IMSS quarantines.
Delegated administration	IMSS offers the ability to create different access rights to the Web management console. You can choose which sections of the console are accessible for different administrator logon account.	By delegating administrative roles to different employees, you can create backups of human resources and promote the sharing of administrative duties.
Centralized reporting	Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports.	Helps you analyze how IMSS is performing. One time (on demand) reports allow you to specify the type of report content as and when required. Alternatively, you can configure IMSS to automatically generate reports daily, weekly, and monthly.
System availability monitor	A built-in agent monitors the health of your IMSS server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow.	Email notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.
POP3 scanning	You can choose to enable or disable POP3 scanning from the Web management console.	In addition to SMTP traffic, IMSS can also scan POP3 messages at the gateway as messaging clients in your network retrieve them.
Clustered architecture	The current version of IMSS has been designed to make distributed deployment possible.	You can install the various IMSS components on different computers, and some components can exist in multiples. For example, if your messaging volume demands, you can install additional IMSS scanner components on additional servers, all using the same policy services.

TABLE 1-2. Main features and benefits

Feature	Descriptions	Benefits
Integration with Trend Micro Control Manager™	Trend Micro Control Manager™ (TMCM) is a software management solution that gives you the ability to control antivirus and content security programs from a central location regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus and content security policy. For details, see *About Trend Micro Control Manager* on page 1-11.	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.

TABLE 1-2. Main features and benefits

About Spyware and Other Types of Grayware

Your clients are at risk from threats other than viruses. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization (see Table 1-3).

Types of Spyware/Grayware	Descriptions
Spyware/Grayware	Gathers data, such as account user names and passwords, and transmits them to third parties.
Adware	Displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser.
Dialers	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem.

TABLE 1-3. Types of spyware/grayware

Types of Spyware/Grayware	Descriptions
Joke Program	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.
Hacking Tools	Helps hackers enter computers.
Remote Access Tools	Helps hackers remotely access and control computers.
Password Cracking Applications	Helps hackers decipher account user names and passwords.
Others	Other types not covered above.

TABLE 1-3. Types of spyware/grayware

About Trend Micro Control Manager

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

Control Manager consists of the following components:

- **Control Manager server**—The Control Manager server is the computer upon which the Control Manager application installs. The Web-based Control Manager management console generates on this server.

  Note: You **must** install hot fix 1430 or later on the Control Manager Server for it to work with IMSS 7.0 Solaris.

- **Agent**—The agent is an application installed on a product-server that allows Control Manager to manage the product. It receives commands from the Control Manager server, and then applies them to the managed product. It also collects logs from the product, and sends them to Control Manager.

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

- **Entity**—An entity is a representation of a managed product on the Product Directory link. You see these icons in the directory tree of the Entity section. The directory tree is a composition of all managed entities, residing on the Control Manager console. IMSS can be an entity on the Control Manager management console.

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

Note: Use Control Manager server version 3.5 or later when using Control Manager to manage IMSS. For more information on the latest version and the most recent patches and updates, see the Trend Micro Update Center: `http://www.trendmicro.com/download/product.asp?productid=7`

Integrating with Control Manager

Table 1-4 shows a list of Control Manager features that IMSS supports.

Features	Descriptions	Supported?
2-way communication	In a 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 take in order to reduce the likelihood of the IMSS server or its clients from becoming infected. Trend Micro ActiveUpdate Server then deploys this policy to IMSS via Control Manager.	Yes
Log Upload for Query	Uploads IMSS virus logs, Content Security logs, and NRS logs to Control Manager for query purposes.	Yes
Single Sign On	Manage IMSS from Control Manager directly without first logging on to the IMSS Web management console.	No. You need to first log on to the IMSS Web management console before you can manage IMSS from Control Manager.
Configuration Replication	Replicate configuration settings from an existing IMSS server to a new IMSS server from Control Manager.	Yes
Pattern Update	Update virus/malware pattern files from Control Manager	Yes

TABLE 1-4. Supported Control Manager features

Features	Descriptions	Supported?
Engine Update	Update Scan Engine 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 via the IMSS Web management console accessible from Control Manager.	Yes
Renew Product Registration	Renew IMSS product license from Control Manager.	Yes
Mail-related Report on Control Manager	Generate the following IMSS mail-related reports from Control Manager: • Top 10 Virus Detection Points • All Entities Virus Infection List • Top 10 Infected Email Sender Report • Top 10 Security Violations Reports • Virus Infection Channel-Product Relationship Report • Filter Events by Frequency • Filter Events by Policy • Gateway Messaging Spam Summary Report • Gateway Messaging Spam Summary Report (for Domains)	Yes
Control Manager Agent Installation /Un-installation	Install / uninstall IMSS Control Manager Agent from Control Manager.	No. IMSS Control Manager agent is automatically installed when you install IMSS. To enable/disable the agent, do the following from the IMSS Web management console: 1. Choose **Administration** > **Connections** from the menu. 2. Click the **TMCM Server** tab. 3. To enable/disable the agent, select/deselect the check box next to **Enable TMCM Agent** respectively.
Event Notification	Send IMSS event notification from Control Manager.	Yes

TABLE 1-4. Supported Control Manager features

Features	Descriptions	Supported?
Command Tracking for All Commands	Track the status of commands that the Control Manager issues to IMSS.	Yes

TABLE 1-4. Supported Control Manager features

Chapter 2

System Requirements and Component Descriptions

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

Topics include:

System Requirements

Table 2-1 provides the recommended and minimum system requirements for running IMSS.

Operating System	**Linux**: • Red Hat™ Enterprise Linux™ AS 3 Update 3 or above • Red Hat Enterprise Linux AS 4 Update 3 or above • Red Hat Enterprise Linux ES 3 Update 3 or above • Red Hat Enterprise Linux ES 4 Update 3 or above • SUSE Linux Enterprise Server 9 SP3 • SUSE Linux Enterprise Server 10 SP1 **Solaris**: Solaris™ SPARC 8, 9, 10
Recommended CPU	**Linux**: Intel™ Dual Pentium™ IV 3GHz or above **Solaris**: UltraSPARC IIIi 1.0 GHz or above
Minimum CPU	**Linux**: Intel Pentium IV 2.4GHz **Solaris**: Ultra SPARC II 650Hz
Recommended Memory	2GB RAM
Minimum Memory	1GB RAM
Recommended Disk Space	• 10GB for mail storage • 50GB or more for the Admin database • 20GB or more for the EUQ database • 40GB or more for the working quarantine folder **Note:** These recommendations are based on 500,000 email messages/day, a 50% quarantine rate, and logs preserved for a month.

TABLE 2-1. System Requirements

Minimum Disk Space	• 1GB for mail storage • 20GB for the Admin database • 10GB for the EUQ database • 10GB for the working quarantine folder **Note:** The default location for the Admin database and EUQ database is `/var/imss`. The Default location for the working quarantine folders is `/opt/trend/imss/queue/`.
Recommended Swap Space	Trend Micro recommends a swap space 4 times the physical memory size. **Note:** Each IMSS child process consumes 120MB of memory. Therefore, for better performance, enough physical and virtual memory should be allocated to handle peak traffic. For example, a computer with 2GB of physical memory and 8GB of swap space might be able to allow 75 child processes to be created. The required swap space also depends on the other application's memory usage. IMSS can then simultaneously handle 75 incoming connections from upstream MTA.
Minimum Swap Space	**Linux**: 2GB swap space **Solaris:** 4GB swap space
Browser	• Internet Explorer 6 SP1 or Internet Explorer 7 • Firefox 1.5
PostgreSQL	Version 7.4.8 or above **Note:** IMSS 7.0 Linux is bundled with PostgreSQL 8.1.3. IMSS 7.0 Solaris is bundled with PostgreSQL 8.1.5.
LDAP server	• Microsoft™ Active Directory 2000 or 2003 • IBM Lotus™ Domino™ 6.0 or above • Sun™ One LDAP 5.2 or above

TABLE 2-1. System Requirements

MTA	• Postfix™ (for IMSS only): Version 2.0 or above • Postfix (with IP Profiler): Version 2.1 or above • Sendmail™ 8.2 or above • Qmail™ 1.0.3 or above **Note:** IMSS 7.0 Solaris is bundled with Postfix 2.3.8.
Linux Libraries (for all platforms)	• glibc-2.2.5 • libstdc++-libc6.2-2.so.3 (Required for PostgreSQL) • libreadline.so.4
Solaris Patches	Patch 118833-36 is required if you have installed patch 119689 on Solaris 10. Patch 118833-36 also requires the following patches: • 118918-13 • 119042-09 • 119254-36 • 119578-30 • 120900-04 • 121133-02
Solaris Packages	Install the following before installing IMSS: SUNWlibC for Solaris 8 and Solaris 9 Install the following if you intend to install IP Profiler: • Bash Shell • BIND version 9.x or above **Note:** IMSS 7.0 Linux is bundled with BIND 9.3.2. IMSS 7.0 Solaris is bundled with BIND 9.4.0 Install the following if you intend to install NRS: • SUNWcsu on Solaris 8 and Solaris 9 • SUNWbind on Solaris 10 Install the following if you intend to install PostgreSQL: • SUNWzlib on Solaris 8 and Solaris 9 • SUNWcstu on Solaris 10 Install the following if you intend to use Control Manager agent: • SUNWcsl or SUNWcslx on Solaris 8 and Solaris 9 • SUNWcsl or SUNWcslr on Solaris 10 • Patch 2 and Hot fix 1430 or later for Control Manager server

TABLE 2-1. System Requirements

About IMSS Components

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

You can install IMSS components on a single computer or over multiple computers. For graphical representations of how these components work together, see *Understanding Installation Scenarios* on page 3-23.

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

Scanner Services

Servers configured as scanner services do the following:

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

- Logs policy and system activity locally, and automatically updates 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, you will need to 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, you will need to set the maximum disk usage to 9GB to protect the computer with the least resources.

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

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

Policy Services

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

Policy Synchronization

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

version of the database synchronized with the database, without the need to check the entire database for new or changed entries.

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

End-User Quarantine Service

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

Primary and Secondary End-User Quarantine Services

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

End-User Quarantine Server Components

The EUQ Server includes the following software components:

- **Apache HTTP Server**—Accepts the HTTPS-requests from end-users and distributes them across all installed EUQ Servers. Apache is only installed on the Primary EUQ Server.
- **Tomcat Application Server**—Accepts the HTTPS-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 software are installed in the `{IMSS}/UI` directory. The other components are installed in the `{IMSS}/UI/euqUI` directory. Both Apache and Tomcat are controlled by the S99EUQ script in the `{IMSS}/script` directory accepting the stop, start and restart commands.

Apache and mod_jk

The Apache HTTP Server v. 2.0.58 (see http://httpd.apache.org/) is installed on the Primary EUQ Server and uses the Apache Tomcat Connector `mod_jk` (see

http://tomcat.apache.org/connectors-doc/) loadable module to forward all requests to the locally installed Tomcat Application Server.

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

Tomcat

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

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

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

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

Struts Framework

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

Simply speaking, 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, it accesses the databases and communicates with Managers.

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

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

The End-User Quarantine Database

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

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

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

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

IP Filtering

IMSS includes optional IP Filtering, which consists of two parts:

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

  IP profiler detects any of these four potential Internet threats:

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

Network Reputation Services

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

Types of Network Reputation Services

NRS provides two types of services:

- **Real-time Blackhole List (RBL+)™ Service**—Blocks spam at its source by validating IP addresses against the industry's most comprehensive and reliable reputation database. Your designated mail server makes a DNS query to the RBL+ database server whenever an incoming mail message is received from an unknown host. If the host is listed in the RBL+ database, IMSS can reject the connection and block spam from the sender.
- **Network Anti-Spam™ Service**—A dynamic real-time solution that identifies and stops sources of spam while they are in the process of sending messages in bulk. Network Anti-Spam Service is a DNS query-based service like RBL+ Service. At the core of this service is the RBL+ database, along with the QIL database, a dynamic real-time database. These two databases have distinct entries and there is no overlap of the IP addresses, allowing us to maintain a highly efficient and effective database that can quickly respond to zombies, BGP attacks and other highly dynamic sources of spam.

How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email containing threats mentioned in the section *IP Filtering* on page 2-10. You can customize several criteria that determine when IMSS will start taking a specified action on an IP address. The criteria differ depending on the potential threat, but commonly include a duration during which IMSS monitors the IP address and a threshold.

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

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

1. FoxProxy queries the IP Profiler's DNS server to see if the IP address is on the blocked list.
2. If the IP address is on the blocked list, IMSS denies the connection request.

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

How Network Reputation Service Works

Trend Micro Network Reputation Services are Domain Name Service (DNS) query-based services. The following process takes place after IMSS receives a connection request from a sending mail server:

1. IMSS records the IP address of the computer requesting the connection.
2. IMSS forwards the IP address to the Trend Micro NRS 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, NRS instructs IMSS to permanently or temporarily block the connection request. The decision to block the request depends on the type of spam source, its history, current activity level, and other observed parameters.

Figure 2-1. illustrates how NRS works.

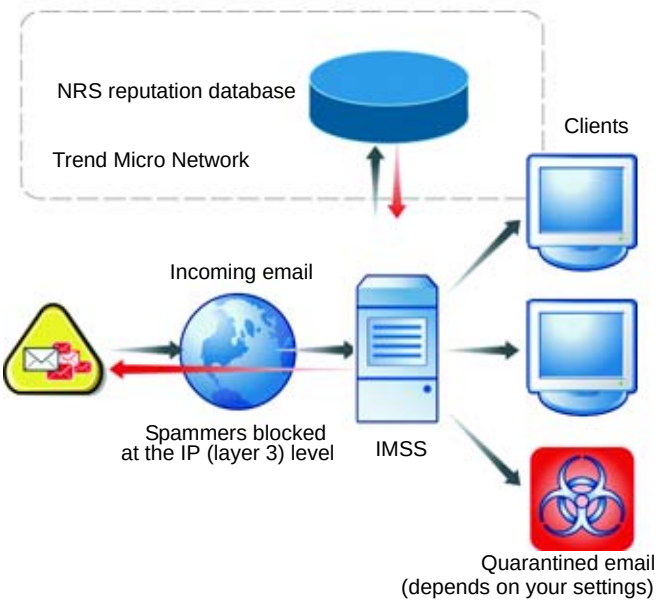


FIGURE 2-1. How NRS works

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

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 and post-installation tasks for deploying IMSS.

Tick ☑ when completed	Tasks	Optional	Reference
	Step1 - Identify the location of IMSS		
	Choose one of the following locations on your network where you would like to install IMSS.		
	• Without a firewall		*Installing without a Firewall* on page 3-12
	• In front of a firewall		*Installing in Front of a Firewall* on page 3-13
	• Behind a firewall		*Installing Behind a Firewall* on page 3-14
	• On a former SMTP gateway		*Installing on a Former SMTP Gateway* on page 3-15
	• In the De-Militarized Zone		*Installing in the De-Militarized Zone* on page 3-15
	Step 2 - Plan the scope		
	Decide whether you would like to install IMSS on a single server or multiple servers.		
	• Single-server installation		*Single-Server Installation* on page 3-23

Tick ☑ when completed	Tasks	Optional	Reference
	• Multiple scanner service		*Multiple Scanner Service Installation* on page 3-25
	• Multiple EUQ service		*Multiple End-User Quarantine Service Installation* on page 3-27
	• Complex distributed		*Complex Distributed Installation* on page 3-30
	• Wide area network		*Wide-Area Network Installation* on page 3-33
	Note: Trend Micro recommends that you consider the failover plan before deciding on the scope.		*IP Filtering* on page 3-36
	Step 3 - Install or Upgrade		
	Perform either a fresh installation of IMSS or upgrade from a previous version.		
	• Prepare MTA		*Preparing Message Transfer Agents* on page 4-2
	• Install IMSS components		*Installation Steps* on page 4-14
	• Install IP Filtering	Yes	*Installing IP Filtering Components* on page 4-16

Tick ☑ when completed	Tasks	Optional	Reference
	• Upgrade from a previous version		*Upgrade Steps* on page 4-31
	• Verify that installation is successful		*Verifying the Installation* on page 4-22
	Step 4 - Configure basic IMSS settings		
	Go through the 7 steps of configuring the Central Controller via the Configuration Wizard.		
	Configure settings using the Configuration Wizard		Performing Basic Configuration with the Configuration Wizard section of the Administrator's Guide.
	Step 5 - Start services		
	Activate IMSS services to start protecting your network against various threats.		
	• Scanner		IMSS Services section of the Administrator's Guide.
	• Policy		
	• EUQ	Yes	
	Step 6 - Configure other IMSS settings		
	Configure various IMSS settings to get IMSS up and running.		
	• IP Filtering Rules	Yes	IP Filtering Service section of the Administrator's Guide.
	• SMTP Routing		Scanning SMTP Messages section of the Administrator's Guide.

Tick ☑ when completed	Tasks	Optional	Reference
	• POP3 Settings	Yes	Scanning POP3 Messages section of the Administrator's Guide.
	• Policy and scanning exceptions		Managing Policies section of the Administrator's Guide.
	• Perform a manual update of components and configure scheduled updates		Updating Scan Engine and Pattern Files section of the Administrator's Guide.
	• Log settings		Configuring Log Settings section of the Administrator's Guide.
	Step 7 - Back up IMSS		
	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 automatically. Table 3-1 lists each component sub-module.

Main Component	Installed Sub-module	Sub-module Description
IMSS Admin Database	Administrator Database	The main IMSS admin database that stores all global settings.
	Database Server*	The server on which the IMSS admin database runs.
Central Controller	Apache® Tomcat®	The Web server for the IMSS Web management console, through which you configure settings.
	Named Server*	The DNS server for IP Profiler.
	FoxDNS	Contains the list of blocked and white IP addresses for IP Profiler and writes the list to the named server.
	IMSSMGR	A module to manage IMSS-related 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
	Control Manager Agent	The software component required for Control Manager to manage IMSS.
	IMSSMGR	A module to manage scanner processes.
EUQ Service	Apache Tomcat	The Web server for the EUQ Web console, though which your users can access the email messages that IMSS quarantined as spam.
	Apache Service	You install this module with the primary EUQ services for load balancing purposes when you choose to install multiple EUQ services.
	IMSSMGR	A module to manage EUQ processes.

TABLE 3-1. Component and sub-module installation

Main Component	Installed Sub-module	Sub-module Description
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.
NRS	Maillog Parser	A module to parse NRS-related mail logs.
Sub-module(s) marked with an asterisk (*) are the sub-components that you can choose to install when you install the main component.		

TABLE 3-1. Component and sub-module installation

IMSS Ports

See Table 3-2 for the ports IMSS uses. Items with an asterisk (*****) are configurable from the IMSS Web management console.

Port Number	Component and Role	Configuration Location
25	The Postfix mail service port. The mail server will listen at this port to accept messages. This port must be opened at the firewall, or the server is not able to accept mails.	`master.cf`
110	IMSS scanner generic POP3 port. The scanner uses this port to accept POP3 request and scan POP3 mails for all POP3 servers.	`imss.ini / [Socket_2]/ proxy_port`
5060	Policy Server listening port. The scanner will connect to this port to query matched rules for every message.	From the Web management console, click **Administration > IMSS Configuration > Connections > Components** on the menu.
8005	Admin UI Web Server (Tomcat) management port that can handle Tomcat management command.	`{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 command.	`{IMSS}/UI/euqUI/conf/server.xml:` `Server/port`

TABLE 3-2. IMSS Ports

Port Number	Component and Role	Configuration Location
8445	Admin UI listening port. You need to open this port to log on to the Web management console using a Web browser.	`Tomcat listen port: {IMSS}/UI/adminUI/conf/server.xml : Server / Service / Connector / port`
8446	EUQ service listening port.	`{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector / port`
8447	EUQ service listening port with load balance.	`{IMSS}/UI/euqUI/conf/EUQ.conf: Listen / VirtualHost / ServerName`
10024	IMSS scanner reprocessing port. Messages released from the central quarantine area in the admin database and from the EUQ database will be sent to this port for reprocessing.	`imss.ini / [Socket_3]/ proxy_port`
10025	IMSS scanner scanning port. All messages that are sent to this port will be scanned by the scanner.	`imss.ini / [Socket_1]/ proxy_port`

TABLE 3-2. IMSS Ports

Port Number	Component and Role	Configuration Location
10026	The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSS.) All messages sent to this port will not be scanned by IMSS. Due to security considerations, the port is only bound at IMSS server's loopback interface (127.0.0.1). It is therefore not accessible from other computers. You are not required to open this port at the firewall.	`master.cf`
15505	IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the Web management console. The manager also provides quarantine/archive query results to the Web management console and the EUQ Web console through this port.	From the Web management console, click **Administration > IMSS Configuration > Connections > Components** on the menu.
IMSS uses the following ports when you enable related service:		
389	LDAP server listening port.	Not configurable on the IMSS server.
5432	PostgreSQL database listening port. Please do not change this port.	You cannot change this port.

TABLE 3-2. IMSS Ports

Port Number	Component and Role	Configuration Location
80	Microsoft IIS http listening port. You would need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu.
443	Microsoft IIS https listening port. You would need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu
88	KDC port for Kerberos realm.	Not configurable on the IMSS server.
53	The Bind service listening port. Please do not change the port.	Not configurable on the IMSS server.

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

TABLE 3-2. IMSS Ports

Considering Network Topology

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

Installing without a Firewall

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

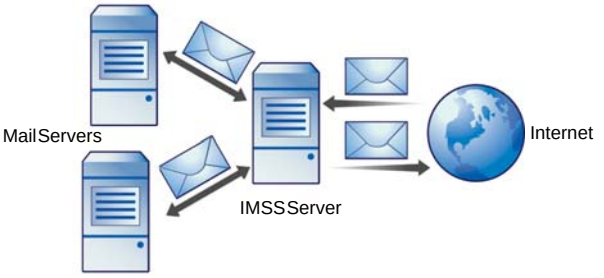


FIGURE 3-1 Installation topology: no firewall

Installing in Front of a Firewall

Figure 3-2 illustrates the installation topology when you install IMSS in front of your firewall:

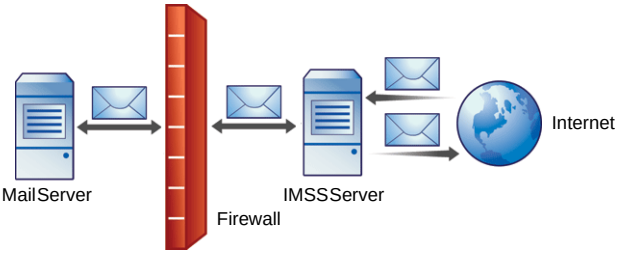


FIGURE 3-2 Installation topology: in front of the firewall

Incoming Traffic

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

Outgoing Traffic

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

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

Installing Behind a Firewall

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

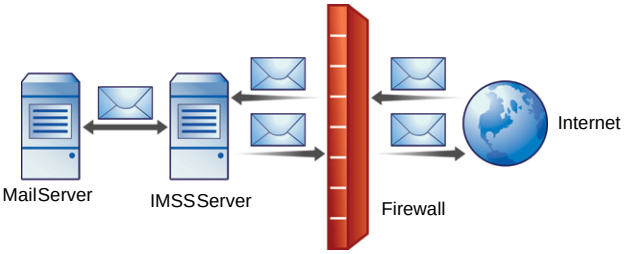


FIGURE 3-3 Installation scenario: behind a firewall

Incoming Traffic

- Configure your proxy-based firewall, so:
  - Outgoing SMTP email goes to Postfix first and then to IMSS.
  - Incoming SMTP email goes first to Postfix, then to IMSS, and then to the SMTP servers in the domain.
- Configure your packet-based firewall.
- Configure IMSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server.
- Configure relay restriction to only allow relay for local domain(s).

Outgoing Traffic

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

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

Installing on a Former SMTP Gateway

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

On the SMTP gateway:

- Allocate a new TCP/IP port to route SMTP mail to IMSS. It must be a port unused by any other services.
- Configure IMSS to bind to the newly allocated port, which frees port 25.

Note: The existing SMTP gateway binds to port 25.

Incoming Traffic

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

Outgoing Traffic

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

Installing in the De-Militarized Zone

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

Incoming Traffic

- Configure your proxy-based firewall, so that incoming and outgoing SMTP email can only go from the DMZ to the internal email servers.
- Configure your packet-based firewall.

- Configure Postfix and IMSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server.

Outgoing Traffic

- Configure Postfix to route all outgoing email (destined to other than the local domains) to the firewall or deliver 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, through Postfix and IMSS, to any domain.

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

About Operating Models

You can deploy IMSS in different ways with relation to 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 NRS).

The Standalone Model

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

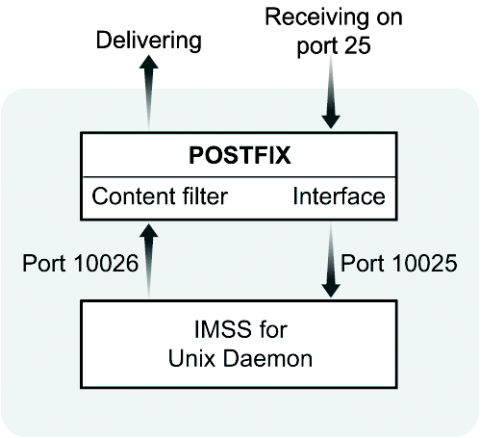


FIGURE 3-4 Standalone model

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.imss70
-o smtpd_client_restrictions=
-o smtpd_enforce_tls=no
```

The Sandwich Model

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

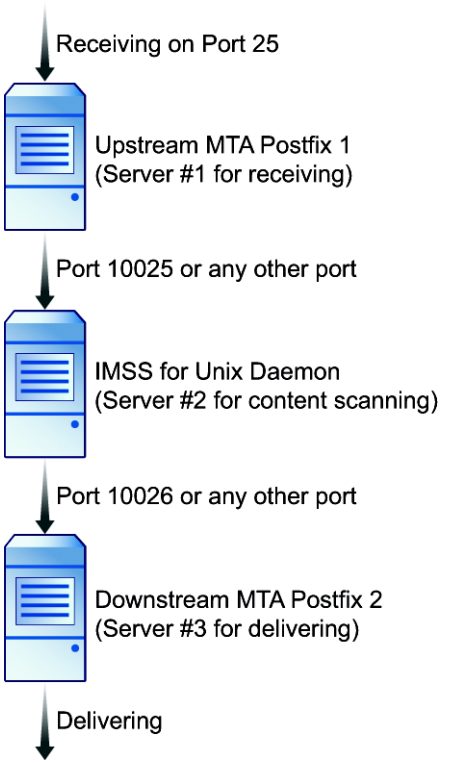


FIGURE 3-5. Sandwich model

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

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

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

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

  ```
  relayhost=smtp:[ip_of_server2]:10025
  ```

```
default_destination_recipient_limit=100
default_destination_concurrency_limit=50
```

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

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

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

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

The Proxy Model

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

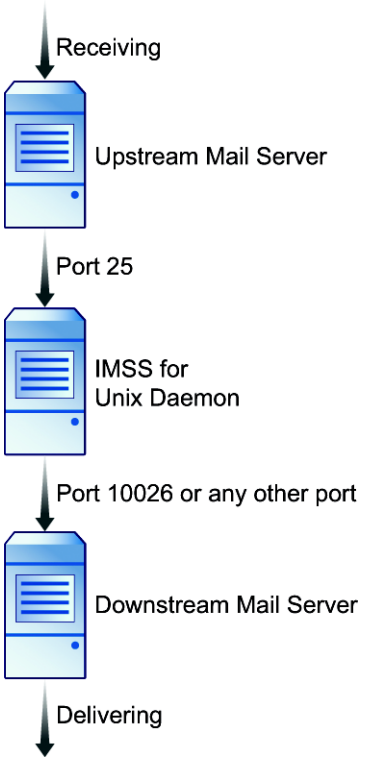


FIGURE 3-6. Proxy model

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

Understanding Installation Scenarios

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

Single-Server Installation

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

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

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

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

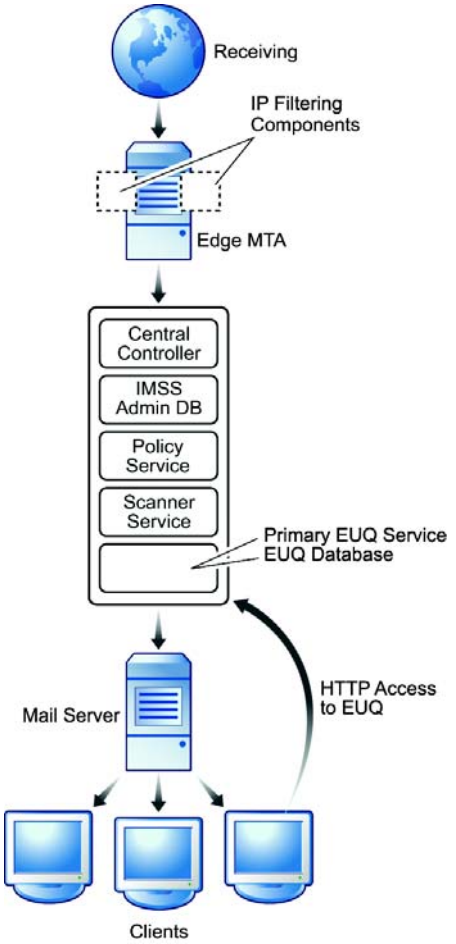


FIGURE 3-7 Single server deployment

To perform a single-server installation:

1. Install IMSS and End-User Quarantine (see *Installing IMSS Components and End-User Quarantine* on page 4-13).
2. On the edge MTA server, install all IP Filtering components (see *Installing IP Filtering Components* on page 4-16).

Multiple Scanner Service Installation

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

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

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

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

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

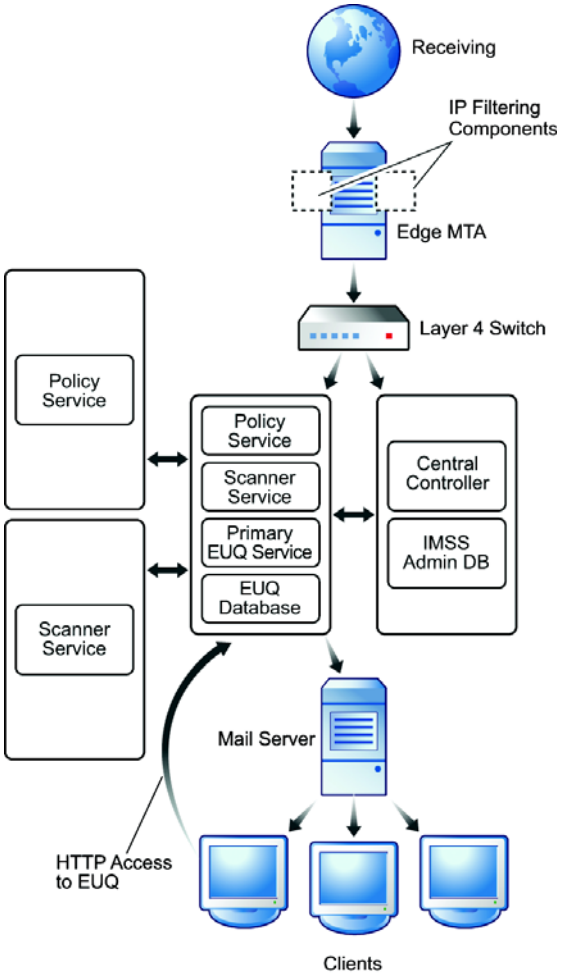


FIGURE 3-8 Multiple scanner service and policy service deployment

To perform a multiple scanner service installation:

1. On one computer, install IMSS and End-User Quarantine (see *Installing IMSS Components and End-User Quarantine* on page 4-13).

2. On other computers, install the necessary scanner service and policy services. On the edge MTA server, install all IP Filtering components (see *Installing IP Filtering Components* on page 4-16).

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

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

Multiple End-User Quarantine Service Installation

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

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

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

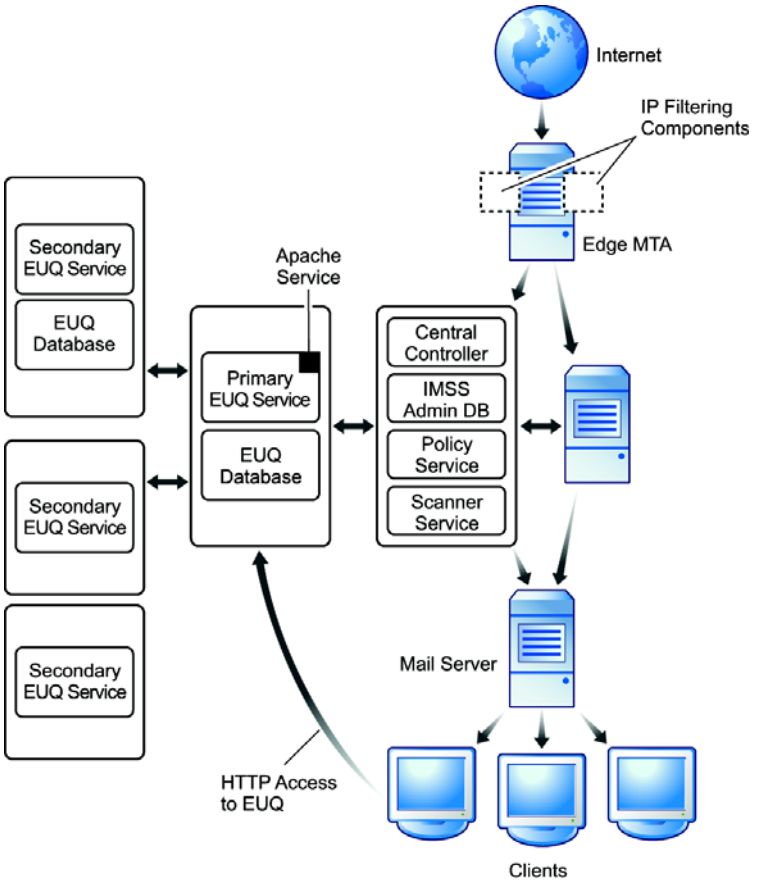


FIGURE 3-9 Multiple EUQ service deployment

To perform a multiple EUQ service installation:

1. On one computer, install IMSS (see *Installing IMSS Components and End-User Quarantine* on page 4-13).

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

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

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

3. On the edge MTA server, install all IP Filtering components (see *Installing IP Filtering Components* on page 4-16).
4. After you have opened the IMSS Web management console and performed 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. For the EUQ services you want to enable, click **Start**.

   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 HTTP 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 be of a type that does not prevent HTTP 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 4-13.

Communication Between Servers

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

Complex Distributed Installation

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

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

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

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

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

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

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

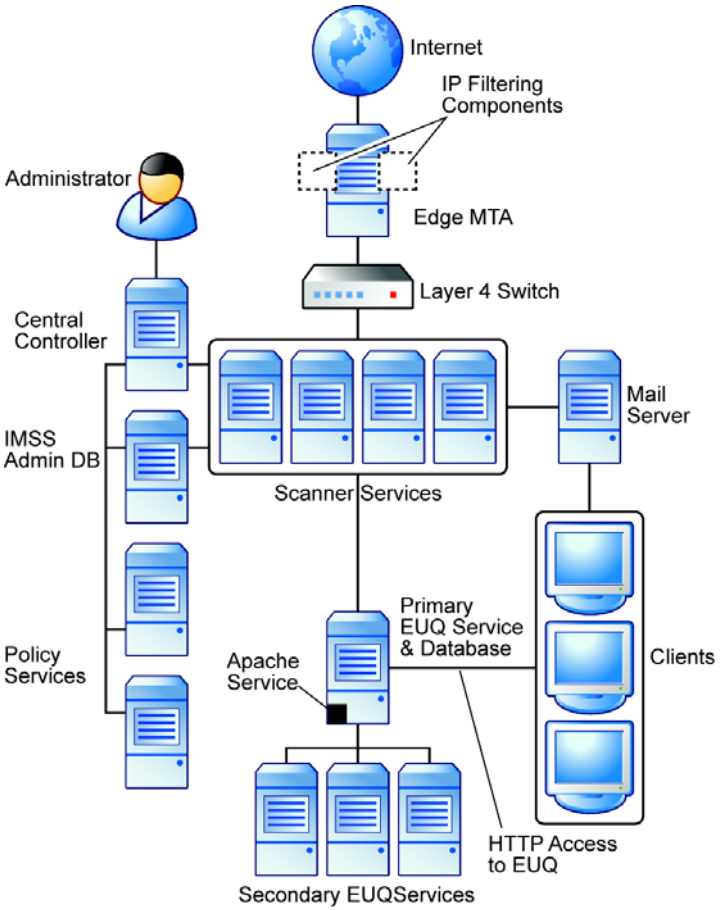


FIGURE 3-10 Complex architecture deployment

Wide-Area Network Installation

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

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

Trend Micro Control Manager

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

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

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

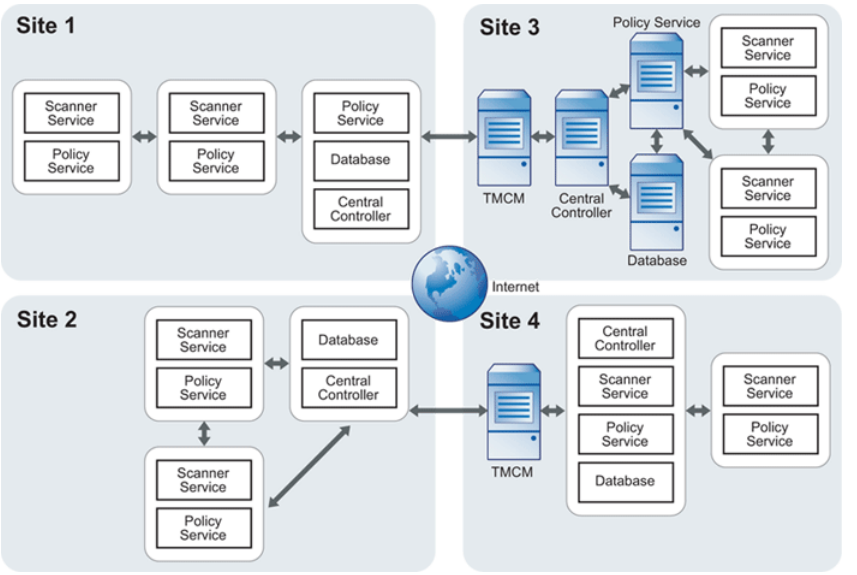


FIGURE 3-11 WAN deployment

The following describes how each site differs in this scenario:

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

Fault Tolerance and Failover in a WAN Scenario

Three out of the four sites in this scenario use multiple scanner services with policy services installed. Policy services can access cached IMSS settings from the IMSS

admin database. Any scanner service that goes down can use another active policy service. Therefore, if one policy service stops or if communication between the central database is interrupted, both scanner services will remain operational and continue processing mail by using the active policy service that has a connection to the IMSS server. See Figure 3-12.

Each site has its own Central Controller and database server, all of which are reporting back to two Control Manager servers. A Control Manager server can replicate IMSS admin databases that directly report to it. If one of the IMSS admin databases become corrupt or unoperational, you can use the replica for restoration.

Note: Control Manager servers cannot replicate IMSS admin database information between them.

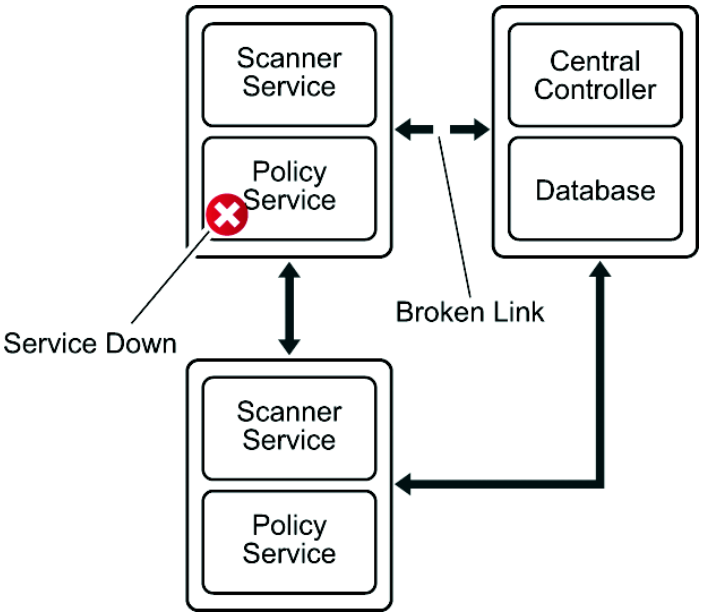


FIGURE 3-12 Failover

IP Filtering

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

Deploying IMSS with IP Filtering

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

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

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

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

About Failover

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

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 3-25.
Policy service is not running or a communication problem occurs with the IMSS server	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 3-25.
IMSS admin database is not running	1. The IMSS server will continue to operate. 2. IMSS sends an event notification if it is unable to start the service within the time you specify for notifications.	Back up the admin database periodically. For more information on backup and restore, visit www.postgresql.org.
EUQ service database is not running	1. An error message appears on the EUQ Web console. 2. IMSS sends an event notification if it is unable to start the service within the time you specify for notifications.	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 login. 2. Foxhunter will not use the LDAP settings. 3. If LDAP is disconnected and you have specified LDAP groups in the policy route, IMSS will continue to run normally using the cached LDAP entities (if available) when performing a policy match. IMSS will also automatically send an event notification regarding the disconnection to the addressees specified in **Administration** > **Notifications** > **Delivery Settings**. **Note:** IMSS automatically sends the LDAP disconnection notification in the backend and you cannot configure the notification settings from the Web management console.	Enable a secondary LDAP server as follows: 1. Choose **Administration** > **Connections**. 2. Click the **LDAP** tab. 3. Select the check box next to **Enable LDAP2** and provide the required information. Trend Micro also recommends that you enable the fault tolerance feature on the LDAP server.

TABLE 3-3. Failover Scenarios

Chapter 4

Installing and Upgrading

This chapter explains how to install IMSS under different scenarios.

Topics include:

Preparing Message Transfer Agents

IMSS supports three (3) types of Message Transfer Agents (MTA), namely, Postfix, Sendmail and Qmail. This section explains how to prepare these MTAs for use with IMSS before installing IMSS components.

Preparing Postfix

If you will install IMSS on the same computer that has a Postfix installation, configure Postfix as listed in this section. This step is applicable for both Linux and Solaris platforms.

Note: 1. **IMSS 7.0 Linux:** The installer does not install an MTA during IMSS server installation. You should already have your MTAs installed and operational. If you install Postfix on the same computer on which you will install IMSS, verify that the Postfix settings are correct.
Trend Micro strongly recommends that you install and use the Postfix distributed with your version of Linux. See www.postfix.org for details.

2. **IMSS 7.0 Solaris**: The installer can install Postfix for you during IMSS server installation if there is no MTA on the target computer. If you already have your MTAs installed and operational, verify that the MTA settings are correct.

Installing Postfix with IMSS 7.0 Solaris

The following steps show how you can install Postfix during IMSS server installation if there is no existing Postfix on the target computer:

1. Type **`./isinst.sh`** to install IMSS. For details on installing IMSS components, see *Installation Steps* on page 4-14.

   After you have chosen the option to Start Installation, the installer will check the available free disk space, memory, swap space and BIND server. If no Postfix is detected on the target computer, the installer will prompt you to install Postfix.

2. Type **Y** to install Postfix 2.3.8.

```
Checking Postfix ...
./isinst.sh: postconf: not found
*******************************************************************************
No Postfix was found on your computer. IMSS requires Postfix.
Do you want to install Postfix 2.3.8 now? [y/n] y
```

3. The installer will check for an existing domain name on the target computer. If the domain name is detected as null, the installer will prompt you to enter the correct domain name.

   Type a valid domain name and press **Enter**.

```
x postfix-2.3.8/README_FILES/SCHEDULER_README, 5372 bytes, 11 tape blocks
x postfix-2.3.8/README_FILES/SMTPD_ACCESS_README, 15789 bytes, 31 tape blocks
x postfix-2.3.8/README_FILES/SMTPD_POLICY_README, 18078 bytes, 36 tape blocks
x postfix-2.3.8/README_FILES/SMTPD_PROXY_README, 10576 bytes, 21 tape blocks
x postfix-2.3.8/README_FILES/STANDARD_CONFIGURATION_README, 25704 bytes, 51 tape blocks
x postfix-2.3.8/README_FILES/TLS_README, 88135 bytes, 173 tape blocks
x postfix-2.3.8/README_FILES/TUNING_README, 22370 bytes, 44 tape blocks
x postfix-2.3.8/README_FILES/ULTRIX_README, 2002 bytes, 4 tape blocks
x postfix-2.3.8/README_FILES/UUCP_README, 5265 bytes, 11 tape blocks
x postfix-2.3.8/README_FILES/VERP_README, 7163 bytes, 14 tape blocks
x postfix-2.3.8/README_FILES/VIRTUAL_README, 23675 bytes, 47 tape blocks
x postfix-2.3.8/README_FILES/XCLIENT_README, 9207 bytes, 18 tape blocks
x postfix-2.3.8/README_FILES/XFORWARD_README, 7677 bytes, 15 tape blocks
x postfix-2.3.8/COMPATIBILITY, 2961 bytes, 6 tape blocks
x postfix-2.3.8/COPYRIGHT, 1922 bytes, 4 tape blocks
x postfix-2.3.8/LICENSE, 11942 bytes, 24 tape blocks
x postfix-2.3.8/postfixinstall, 5475 bytes, 11 tape blocks
x postfix-2.3.8/postfixinstallutil, 23673 bytes, 47 tape blocks
x postfix-2.3.8/RELEASE_NOTES, 36337 bytes, 71 tape blocks
x postfix-2.3.8/RELEASE_NOTES-1.1, 50071 bytes, 98 tape blocks
x postfix-2.3.8/RELEASE_NOTES-2.0, 38863 bytes, 76 tape blocks
x postfix-2.3.8/RELEASE_NOTES-2.1, 26781 bytes, 53 tape blocks
x postfix-2.3.8/RELEASE_NOTES-2.2, 19753 bytes, 39 tape blocks
x postfix-2.3.8/TLS_ACKNOWLEDGEMENTS, 2315 bytes, 5 tape blocks
x postfix-2.3.8/TLS_CHANGES, 106588 bytes, 209 tape blocks
x postfix-2.3.8/TLS_LICENSE, 1629 bytes, 4 tape blocks
x postfix-2.3.8/TLS_TODO, 1065 bytes, 3 tape blocks
x postfix-2.3.8/US_PATENT_6321267, 5633 bytes, 12 tape blocks
Detected domain name is [], is it right[y/n]: y
Domain name can not be empty. Please enter the correct domain name: imsstest.com
```

4. The installer will then prompt you to enter some definitions before installing the Postfix files. Type the paths for the various files as desired.

Tip: Trend Micro recommends that you accept the default paths.

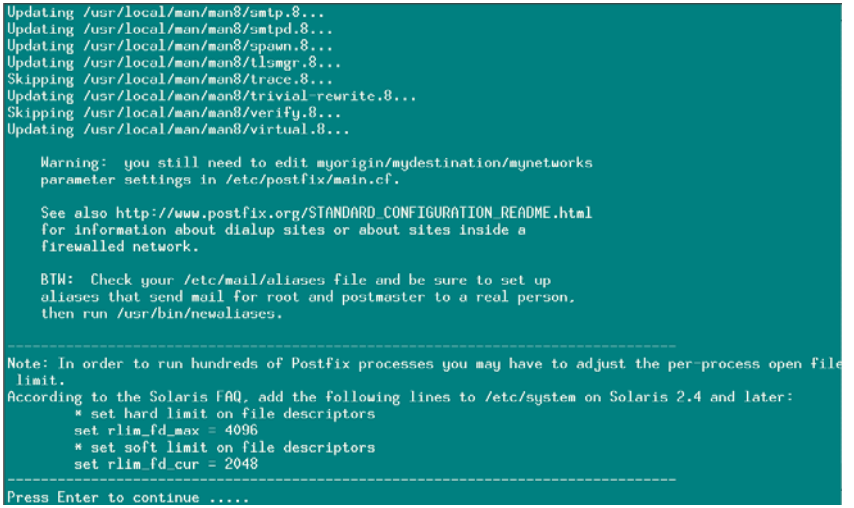
```
x postfix-2.3.8/US_PATENT_6321267, 5633 bytes, 12 tape blocks
Detected domain name is [], is it right[y/n]: y
Domain name can not be empty. Please enter the correct domain name: imsstest.com

    Warning: if you use this script to install Postfix locally, this
    script will replace existing sendmail or Postfix programs.  Make
    backups if you want to be able to recover.

    Before installing files, this script prompts you for some
    definitions.  Most definitions will be remembered, so you have to
    specify them only once. All definitions should have a reasonable
    default value.

Please specify a directory for scratch files while installing Postfix.
You must have write permission in this directory.
tempdir: [/IMSS70_TEMP_FOR_UnpackTmp/postfix-2.3.8]

Please specify the final destination directory for Postfix queues.
queue_directory: [/var/spool/postfix]

Please specify the final destination pathname for the installed Postfix
sendmail command. This is the Sendmail-compatible mail posting
interface.
sendmail_path: [/usr/lib/sendmail]

Please specify the final destination pathname for the installed Postfix
newaliases command. This is the Sendmail-compatible command to build
alias databases for the Postfix local delivery agent.
newaliases_path: [/usr/bin/newaliases]
```

5. After you have specified the required paths, Postfix installation begins.

```
newaliases_path: [/usr/bin/newaliases]

Please specify the final destination pathname for the installed Postfix
mailq command. This is the Sendmail-compatible mail queue listing
command.
mailq_path: [/usr/bin/mailq]

Please specify the destination directory for the Postfix on-line manual
pages. You can no longer specify "no" here.
manpage_directory: [/usr/local/man]

Please specify the destination directory for the Postfix README files.
Specify "no" if you do not want to install these files.
readme_directory: [no]
Updating /usr/libexec/postfix/anvil...
Updating /usr/libexec/postfix/bounce...
Updating /usr/libexec/postfix/cleanup...
Updating /usr/libexec/postfix/discard...
Updating /usr/libexec/postfix/error...
Updating /usr/libexec/postfix/flush...
Updating /usr/libexec/postfix/local...
Updating /usr/libexec/postfix/master...
Updating /usr/libexec/postfix/oqmgr...
Updating /usr/libexec/postfix/pickup...
Updating /usr/libexec/postfix/pipe...
Updating /usr/libexec/postfix/proxymap...
Updating /usr/libexec/postfix/qmgr...
Updating /usr/libexec/postfix/qmqpd...
Updating /usr/libexec/postfix/scache...
Updating /usr/libexec/postfix/showq...
```

6. After installing Postfix, the installer will prompt you to configure Postfix later. For details on how to configure Postfix, see *Insert or modify the following settings to /etc/postfix/main.cf* on page 4-5 and *Insert the following settings to /etc/postfix/master.cf* on page 4-6.

   Press **Enter** to continue with the installation of IMSS components.



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=20
```

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 – 20 smtpd
  –o content_filter=
  –o smtpd_timeout=$imss_timeout
  –o local_recipient_maps=
  –o myhostname=postfix.imss70
  –o smtpd_client_restrictions=
```

Using Sendmail

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

Sendmail Daemons

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

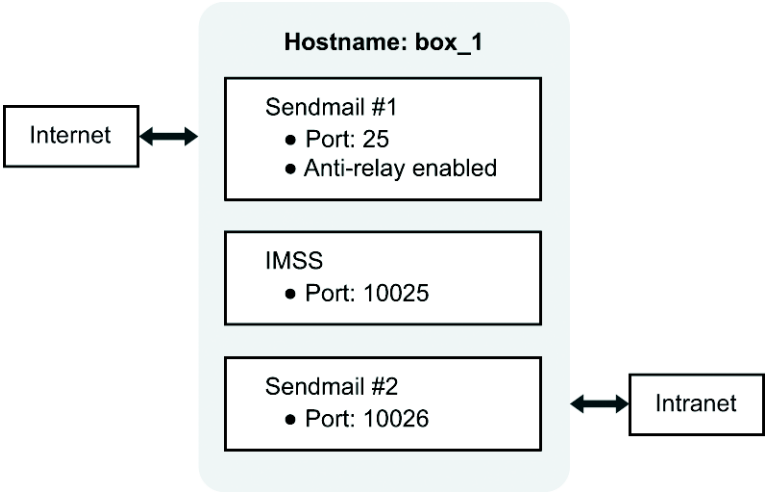


FIGURE 4-1. Sendmail daemons on one server

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

Configuring Sendmail #1

To configure Sendmail #1:

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

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

   Msmtp Before:

   ```
   P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,
   T=DNS/RFC822/SMTP,
   A=TCP $h
   ```

Msmtp After:

```
P=[IPC], F=kmDFMuX, S=11/31, R=21, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=TCP localhost.your_domain_name 10025
```

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

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

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

Mlocal Before:

```
P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9, S=10/30,
R=20/40,
T=DNS/RFC822/X-Unix,
A=mail.local -d $u
```

Mlocal After:

```
P=[IPC], F=klsDFMAw5:/|@qSmn9, S=10/30, R=20/40,
T=DNS/RFC822/X-Unix,
A=TCP localhost.your_domain_name 10025
```

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

```
define('LOCAL_MAILER_PATH','[IPC]')dnl
define('LOCAL_MAILER_FLAGS','k')dnl
define('LOCAL_MAILER_ARGS','TCP [127.0.0.1] 10025')dnl
```

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

Configuring Sendmail #2

To configure Sendmail #2:

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

   Before:

   ```
   O DaemonPortOptions=Name=MTA-v4, Family=inet
   O DaemonPortOptions=Name=MTA-v6, Family=inet6
   O DaemonPortOptions=Port=587, Name=MSA, M=E
   ```

   After:

   ```
   #O DaemonPortOptions=Name=MTA-v4, Family=inet
   #O DaemonPortOptions=Name=MTA-v6, Family=inet6
   #O DaemonPortOptions=Port=587, Name=MSA, M=E
   O DaemonPortOptions=Port=10026
   ```

   Corresponding macro-file change:

   ```
   DAEMON_OPTIONS('Port=10026')dnl
   ```

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

   Before:

   ```
   O QueueDirectory=/var/spool/mqueue
   ```

   After:

   ```
   O QueueDirectory=/var/spool/mqueue1
   ```

   Corresponding macro-file change:

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

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

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

   The macro-file changes are:

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

Restarting Sendmail services

To finish Sendmail setup, restart Sendmail services:

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

   ```
   /usr/lib/sendmail –bd –q1h
   ```

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

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

Using Qmail

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

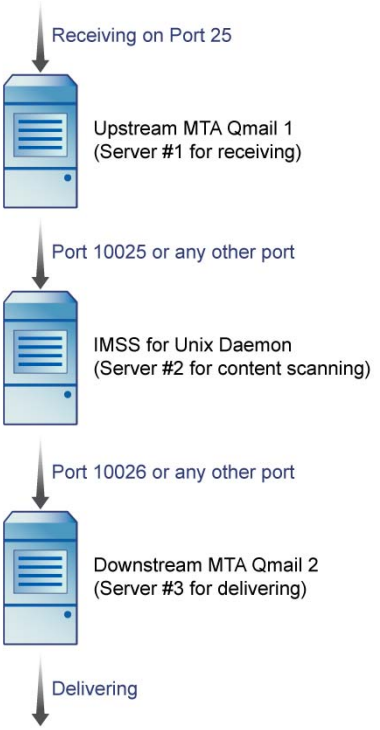


FIGURE 4-2. Deploying Qmail with IMSS

For detailed information on installing and configuring Qmail, visit

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

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

Configuring Qmail

To configure Qmail:

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

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

Installing IMSS Components and End-User Quarantine

This section shows you how to configure the Solaris system file and provides the steps to install IMSS components and End-User Quarantine.

Configuring Solaris System File

IMSS 7.0 Solaris will perform a system IPC check prior to installation on Solaris versions 8 and 9. The system will prompt you if the IPC values in Solaris are set too low. Configure the following IPC values in the system file if you encounter memory issue and restart the system before proceeding with the installation.

Insert the following settings to /etc/system

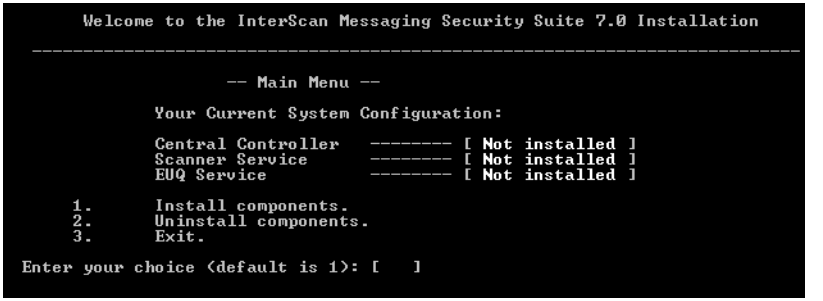
```
set shmsys:shminfo_shmmax=0x2000000
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=256
set shmsys:shminfo_shmseg=256

set semsys:seminfo_semmap=256
set semsys:seminfo_semmni=512
set semsys:seminfo_semmns=512
set semsys:seminfo_semmsl=50
set semsys:seminfo_semopm=30
set semsys:seminfo_semmnu=100
```

Note: The above modification to the Solaris system file is only necessary on Solaris 8 and Solaris 9 but is not required on Solaris 10.

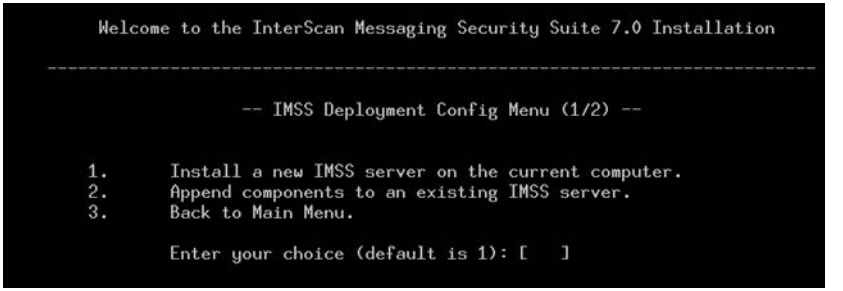
Installation Steps

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

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

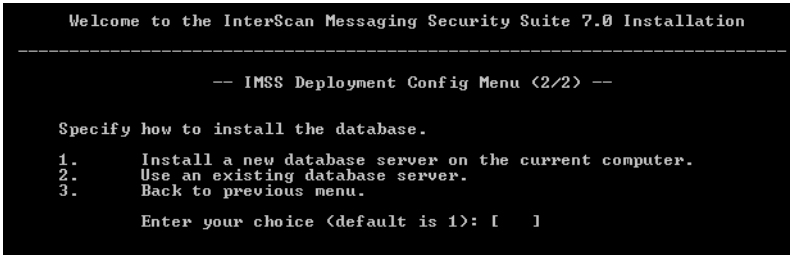


3. Type **1** to begin installation.
4. Read and accept the license agreement.
5. On the IMSS Deployment Config Menu, decide whether to install a new IMSS server or append to an existing installation. To append a scanner service or EUQ service to an existing IMSS server, you will need the database information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

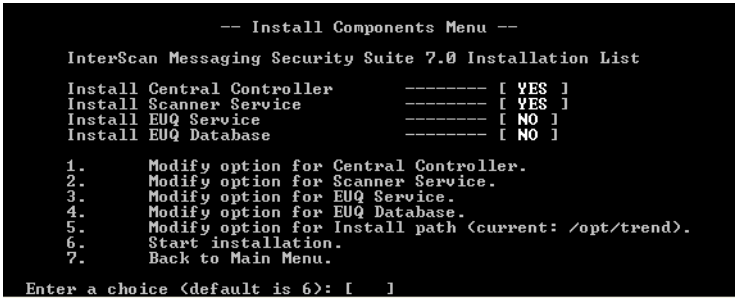


6. Do one of the following:

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



The Install Components Menu screen appears showing the status of the InterScan 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.



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

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

If you want to install the EUQ service, the installer will verify whether an EUQ service already exists on the current computer and whether it is a primary or secondary service. The installer will install a primary service if no EUQ service

exists or if the existing service is a secondary 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 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 4-2.

Note: 1. The installer can install Postfix for you if there is no Postfix on the target computer. You must however, configure Postfix after the installation. See *Preparing Postfix* on page 4-2.

2. 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 9.4.0 (provided with the IMSS install package).

---

9. Press `Enter` to continue. The installer provides a note on whether the DNS server on your computer is active. To use IP Profiler, which you can install later, the DNS server must be active and running properly. For instructions on how to install IP Profiler, see *Installing IP Filtering Components* on page 4-16.
10. Press `Enter` to begin installing the components you selected.

Installing IP Filtering Components

Trend Micro IP Filtering consists of two components:

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

Installing Network Reputation Services and IP Profiler

The Trend Micro Network Reputation Service runs on a modified Postfix installation. The NRS 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 NRS Activation Code and for information about your IMSS Admin Database. You should install the database before installing Network Reputation Services and IP Profiler.

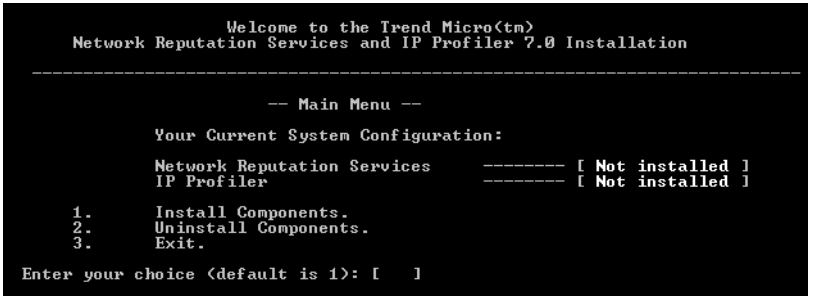
The server on which you install NRS must already have an instance of Postfix installed. It must also be able to connect to the IMSS Admin Database and the server that is processing your messaging (most likely the IMSS server). Trend Micro recommends running NRS and IP Profiler on a gateway/edge server.

Note: You must activate NRS 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 Network Reputation Service using the same SPS Activation Code.

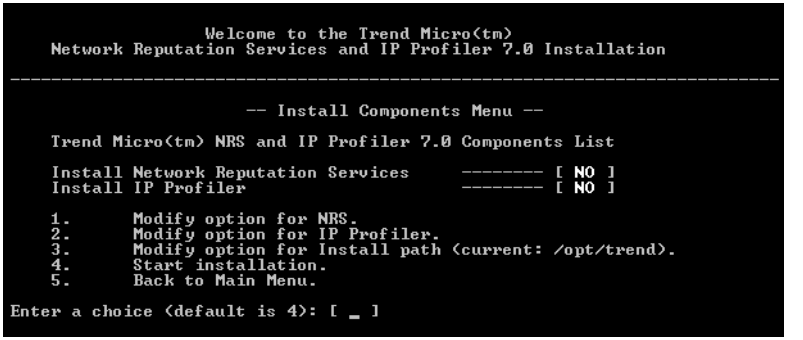
To install IP Profiler and NRS:

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 NRS. If you are installing these products for the first time, **[Not Installed]** appears.



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 **NRS**.



5. Choose to install IP Profiler or NRS:

   To install NRS:

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

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

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

   d. Accept the change.

   e. Type the path for the mail log.

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

Note: If you install NRS on Suse 10, the installer will detect the current mail log path and display it as the default setting. If the detected path is incorrect, you may modify the path manually. Please ensure that the modified mail log path is correct, as incorrect specification of this path may cause NRS to malfunction.

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, enter **3**, and then enter 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 NRS.

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:

- 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
  ```

- Collect information about Sendmail:
  - Use the `which` command to find the Sendmail program file:

    ```
    # which sendmail
    /usr/sbin/sendmail
    ```

  - 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)

  - 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)
- Modify the `foxlibd` script in the `/opt/trend/ipprofiler/script` directory:
  - Set the `TM_FOX_UID` parameter to the user id:

    ```
    TM_FOX_UID=0
    ```

  - Set the `TM_FOX_GID` parameter to the group id:

    ```
    TM_FOX_GID=0
    ```

    - 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
      ```
- 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"
- Use the `foxlibd` script instead of **sendmail** to start Sendmail:
  `/opt/trend/ipprofiler/script/foxlibd start/stop`
- Restart FoxProxy:
  `/opt/trend/ipprofiler/script/foxproxyd start/stop`

Integrating FoxLib with Qmail

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

- Modify the Qmail start script.
    - If you have installed the daemon tool to start Qmail, the smtpd start script should be located at `/service/qmail-smtpd/run`.
    - 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
      ```
- Get the qmail user and group, then copy the correct `.so` file.
    - Run the following commands to check user and group:
      ```
      #id qmaild
      uid=101(qmaild) gid=100(nofiles)
      ```
    - We can see that the smtp user is qmaild, group is nofiles.
    - 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
```

- 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"

- Run the following script to restart foxproxyd:

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

- Type the following command to start Qmail:

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

  Alternatively, reboot 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.

Upgrading from an Evaluation Period

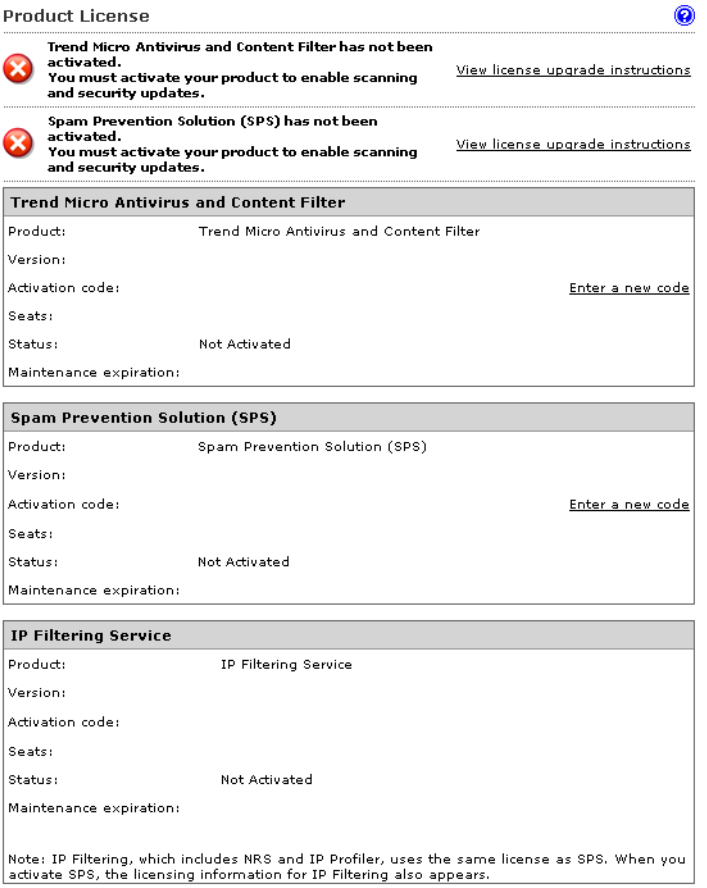
If you entered an evaluation Activation Code to activate IMSS previously, you have started an evaluation period that allows you to try the full functionality of the product. The evaluation period varies depending on the type of Activation Code used.

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

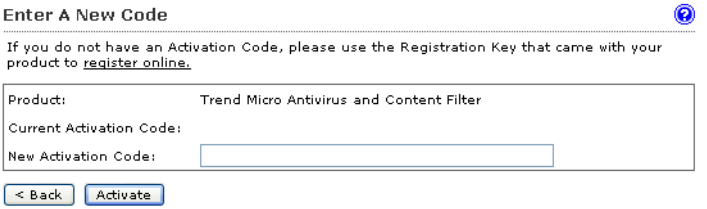
To continue using IMSS, please purchase the full licensed product. You will then be assigned a new licensed Activation Code.

To upgrade from the evaluation period:

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



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



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

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

4. Click **Activate**.

Upgrading from Version 5.7 to Version 7.0

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

- Back up your old IMSS settings
- Uninstall the previous version of IMSS
- Install IMSS 7.0
- Migrate the existing settings

Note: 1. 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 Your Settings* on page 4-29). If problems occur during migration, you can roll back to version 5.7 (see *Rolling Back the Migration* on page 4-38).

2. If you are currently running IMSS 5.5 or lower versions, please refer to the IMSS 5.7 Getting Started Guide for the instructions on upgrading to version 5.7 first. Thereafter, you may follow the instructions in this section to upgrade from version 5.7 to version 7.0

3. If you choose not to migrate your old IMSS settings, Trend Micro recommends that you completely uninstall IMSS 5.7 and then do a fresh install, rather than installing IMSS 7.0 over an existing installation.

Upgrade Options for Multiple Scanner Deployment

If you have installed multiple scanner services in IMSS 5.7, you may need to perform the upgrade differently depending on whether you want to install a single admin database shared by all the scanners or one admin database for each scanner in IMSS 7.0.

Single Admin Database

If you want all the IMSS scanners to access the same admin database in IMSS 7.0, do the following to upgrade from IMSS 5.7:

1. For the first scanner, run the IMSS 7.0 installer and perform a migration install.
2. For subsequent scanners, run the IMSS 5.7 installer to uninstall the existing IMSS, then run IMSS 7.0 installer and choose append install.

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

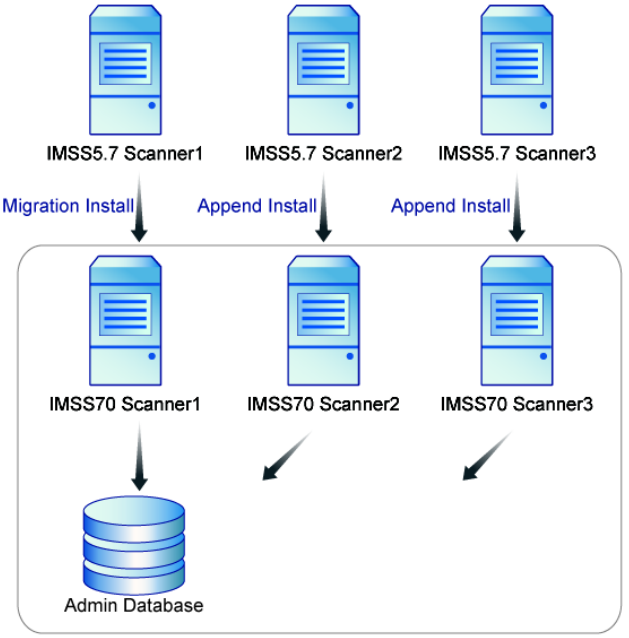


FIGURE 4-3. Single admin database

Multiple Admin Databases

If you want each IMSS scanner to access a different admin database in version 7.0, perform migration install for each scanner as illustrated below.

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

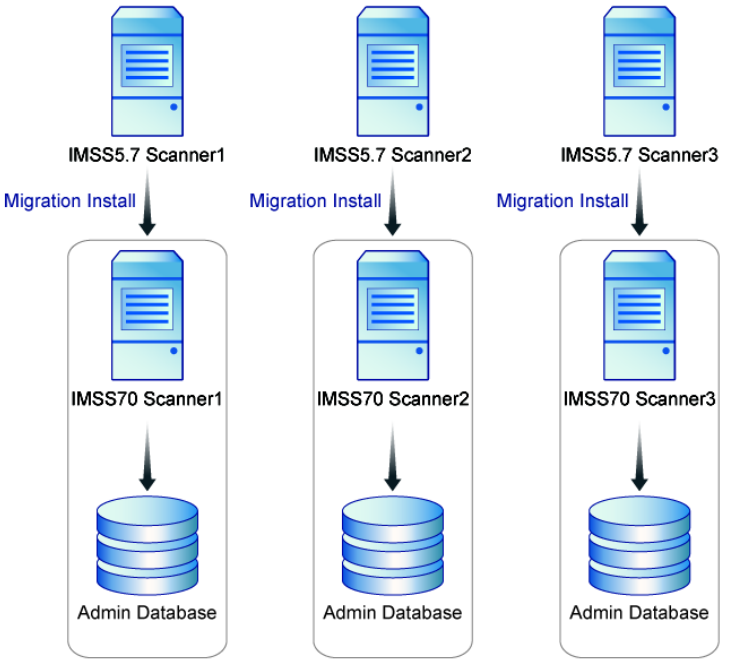


FIGURE 4-4. Multiple admin databases

Backing Up Your Settings

See the following sections:

- *Backing up IMSS 5.7 Data for a Single-server Deployment* on page 4-29
- *Backing up IMSS 5.7 Data for a Distributed Deployment* on page 4-30

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

Backing up IMSS 5.7 Data for a Single-server Deployment

First, back up your IMSS 5.7 data before migration.

To back up IMSS 5.7 data:

1. 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
   ```

2. Stop postfix using the command:

   ```
   # postfix stop
   ```

3. Backup the home folder of IMSS 5.7 using the command:

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

4. Backup the database-related data using the command:

   ```
   # tar cvf imss57_db_data.tar /var/imss
   ```

5. Backup the Postfix configuration files using the command:

   ```
   # tar cvf postfix_config.tar /etc /postfix/main.cf
   /etc/postfix/master.cf
   ```

Backing up IMSS 5.7 Data for a Distributed Deployment

First, back up your IMSS 5.7 data before migration. This scenario assumes four types of servers:

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

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

To back up your IMSS 5.7 data:

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

   On computers with scanner services:

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

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

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

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

   On computers with only an IMSS 5.7 database:

   a. Back up the database using the command:

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

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

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

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

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

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

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

   On computers with EUQ and central reporting:

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

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

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

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

On computers with NRS:

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

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

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

c. Stop Postfix using the command:

```
# postfix stop
```

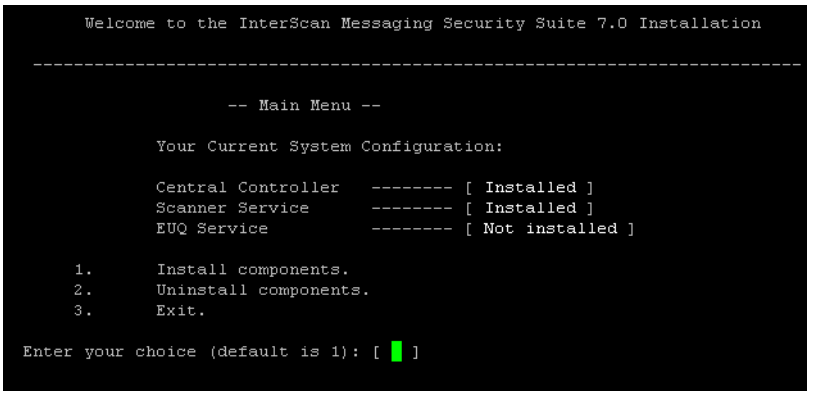
d. Back up the Postfix configuration files using the command:

```
# tar cvf s4_postfix_config.tar /etc/postfix/main.cf
/etc/postfix/master.cf
```

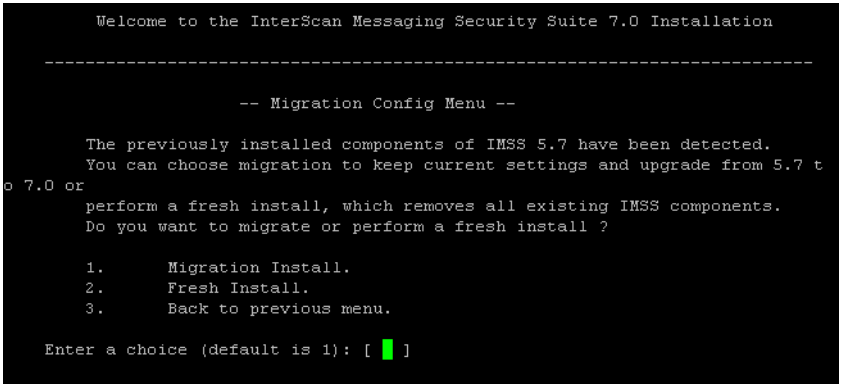
Upgrade Steps

To upgrade to IMSS 7.0:

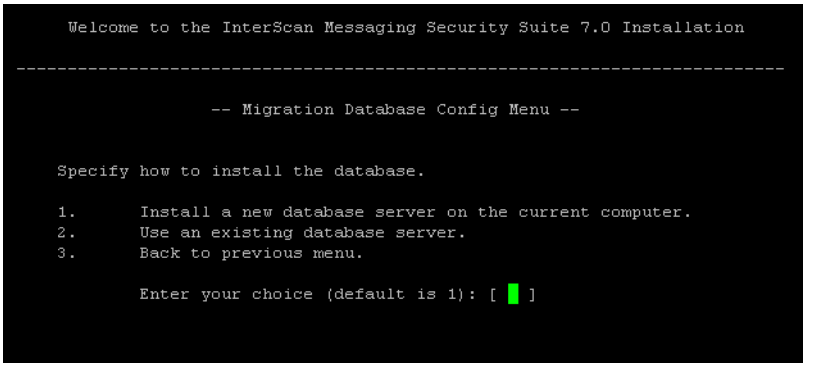
1. Log on as a superuser on the computer where you installed version 5.7 and go to the installation package directory.
2. Type `./isinst.sh`. The Main Menu appears.



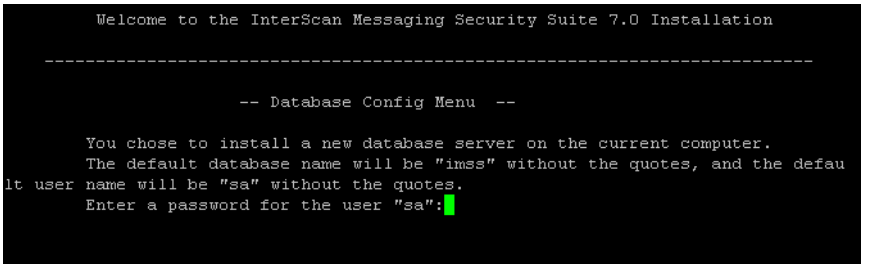
3. Type 1 to migrate your settings and upgrade to version 7.0. The Migration Config Menu appears indicating that previous IMSS 5.7 components have been detected.



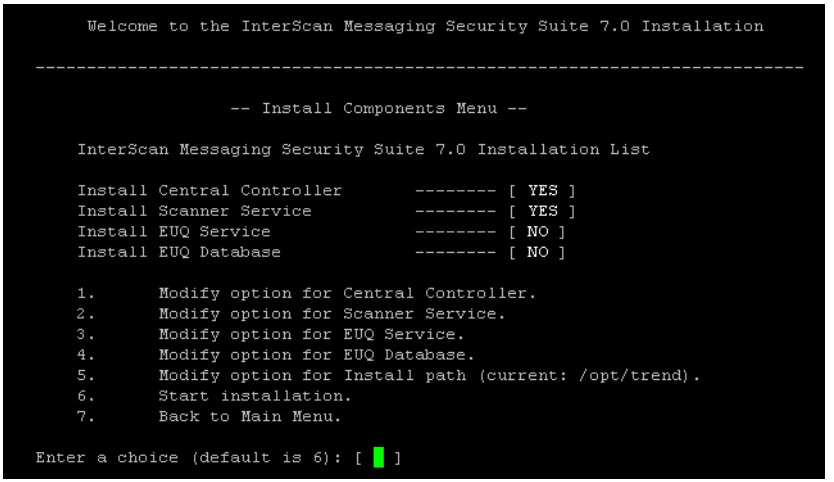
4. Type 1 to perform a migration install. The Migration Database Config Menu appears. The installer will back up the old IMSS settings before uninstalling IMSS 5.7 and installing IMSS 7.0.



5. Select whether to install a new IMSS admin database server or use an existing server. Type the database server details. If you choose to use an existing server, the installer connects to the server.



6. 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 7.0 admin database or EUQ database, you need to modify the access control of PostgreSQL as follows:

1. `vi /var/imss/pgdata/pg_hba.conf`
2. Modify "`255.255.255.255`" on line 60 to "`255.255.255.0`"
3. Modify "`ffffff00`" on line 63 to "`255.255.255.0`"
4. Save the changes
5. `/opt/trend/imss/script/dbctl.sh stop`
6. `/opt/trend/imss/script/dbctl.sh start`

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.

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 **6** to start installation. The following occurs:
   a. 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.
   b. 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 7.0 Linux is bundled with BIND 9.3.2.
IMSS 7.0 Solaris is bundled with BIND 9.4.0.

   c. Next, you will see a list of the settings that cannot be migrated.

d. The installer backs up the old settings, uninstalls IMSS 5.7 and then installs IMSS 7.0.

Note: 1. Filters under your version 5.7 policies and sub-policies will appear as rules in version 7.0. The installer will automatically detect and migrate your policies to rules. For more information on IMSS 7.0 rules, see the Online Help from the Web console.

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

3. Please uninstall the old version of NRS in IMSS 5.7 manually if you want to install NRS of IMSS 7.0 later after migration.

Activation of Supported Services

After upgrade, the Activation Code for IMSS 5.7 will be retained if it has not expired. Otherwise, you need to enter the new Activation Code to use the following:

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

However, to use NRS you must type the Activation Code during installation.

Settings That Cannot be Migrated

IMSS will not migrate the following settings:

EUQ Settings

- EUQ approved senders
- EUQ spam mail

Report Settings

- Pearl reports
- SPS reports

Configuration Settings

- Quarantine area and archive folder paths
- Email messages in queue folder

Note: The entire queue folder of IMSS 5.7 will be renamed as `queue_backup_yy-mm-dd-HH-MM-SS` during migration. You need to handle the backed up messages manually after migration.

- Log paths
- Limits on notifications for processes per hour
- Web console password
- Database settings in `odbc.ini` and `database.ini`

Policy Settings

- Security settings: number of clean attempts, number of viruses reported, and message size criteria
- User-defined virus filters in sub-policies
- Customized actions for “No virus” in the virus filter
- Virus scanning settings for “Extensions to Exclude” for “Specified File Types”
- Global spam scanning mode
- Additional sensitivity for SPS filtering
- Action settings for graymail
- Advanced action settings for spam
- Expression list matching for attachments or file type in the advanced content filter
- Actions for “Archive Original”
- Notifications with original mail attachments
- Forwarding original email message attachments

NRS Settings

All NRS settings cannot be migrated.

Using Migration Reports

You can view two types of migration reports under `$IMSS_Home/installlog/MigrationReport`:

- `GeneralReport.txt`—View all items that IMSS did not migrate.
- `DetailReport.txt`—View the relationship between IMSS 5.7 and IMSS 7.0 for both migrated and non-migrated settings.

Rolling Back the Migration

If any problems occur with the migration to version 7.0, you can roll back to version 5.7. For more information about IMSS 5.7 installation-related questions, see your IMSS 5.7 documentation for more information. This section explains how to perform the roll back for the following deployment scenarios for version 5.7:

- Single-server deployment—Install all components of IMSS 5.7 on a single server before migration (see *Rolling Back in a Single-Server Deployment Scenario* on page 4-38).
- Complex distributed deployment—Install each component of IMSS 5.7 on different servers (see *Rolling Back in a Complex Distributed Deployment Scenario* on page 4-39).

Rolling Back in a Single-Server Deployment Scenario

If you deployed version 5.7 on a single IMSS computer, follow these instructions.

To roll back to version 5.7 in a single-server deployment scenario:

1. Uninstall the 7.0 version that you just installed (see *Performing Uninstallation* on page 4-42).
2. Reinstall IMSS 5.7.
3. Stop all running IMSS 5.7 processes by typing the following:

   ```
   # $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
   ```

4. Stop Postfix by typing the following:

   ```
   # postfix stop
   ```

5. Restore the IMSS 5.7 home folder by unpacking the file `imss57.tar` under the root directory. To do this, type the following:

   ```
   # tar vxf imss57.tar
   ```

6. Restore IMSS 5.7 database data by unpacking the file `imss57_db_data.tar` under the root directory. This replaces the data folder of IMSS 5.7 database. To do this, type the following:

   ```
   # tar vxf imss57_db_data.tar
   ```

7. Restore Postfix configuration by unpacking the file `postfix_config.tar` under the root directory. This replaces the configuration files of Postfix. To do this, type the following:

   ```
   # tar vxf postfix_config.tar
   ```

8. Start all IMSS 5.7 processes by typing the following commands:

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

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

   ```
   # $IMSS_HOME/imss/script/S99ADMINUI start
   ```

   ```
   # $IMSS_HOME/imss/script/S99EUQ start
   ```

9. Start Postfix by typing the following command:

   ```
   # postfix start
   ```

Rolling Back in a Complex Distributed Deployment Scenario

If you deployed version 5.7 components on multiple computers, follow these instructions.

This scenario assumes four types of servers:

- Server 1—running scanner services and central controllers
- Server 2—running the IMSS admin database
- Server 3—running the EUQ service and EUQ database
- Server 4—running IP Filtering (IP Profiler and NRS)

To roll back to version 5.7 in a complex distributed deployment scenario:

1. Uninstall the 7.0 version that you just installed (see *Performing Uninstallation* on page 4-42).
2. Reinstall IMSS 5.7 (see your IMSS 5.7 documentation).

3. Stop all running IMSS 5.7 processes and component processes by typing the following:
   - On computers with scanner services:
     ```
     # $IMSS_HOME/imss/script/S99ISIMSS stop
     ```
   - On computers with only an IMSS 5.7 admin database:
     ```
     # $IMSS_HOME/imss/script/dbctl.sh stop
     ```
   - On computers with Central Controllers only:
     ```
     # $IMSS_HOME/imss/script/S99ADMINUI stop
     ```
   - On computers with EUQ:
     ```
     # $IMSS_HOME/imss/script/S99EUQ stop
     ```
4. On computers running NRS, kill the `maillogParser` process.
5. Stop Postfix by typing the following:
   ```
   # postfix stop
   ```
6. Restore the IMSS 5.7 home folder by unpacking the file `imss57.tar` under the root directory. To do this, type the following:
   - On computers with scanner services:
     ```
     # tar vxf imss57_s1_scanner.tar
     ```
   - On computers with only an IMSS 5.7 database:
     ```
     # tar vxf imss57_s2_db.tar
     # tar vxf imss57_s2_db_data.tar
     ```
   - On computers with Central Controllers or EUQ:
     ```
     # tar vxf imss57_s3_euq.tar
     ```
   - On computers with NRS:
     ```
     # tar vxf imss57_s4_nrs.tar
     # tar vxf imss57_s4_postfix_config.tar
     ```
7. Start all IMSS 5.7 processes by typing the following commands:
   - On computers with scanner services:
     ```
     # $IMSS_HOME/imss/script/S99ISIMSS start
     ```
   - On computers with only an IMSS 5.7 database:
     ```
     # $IMSS_HOME/imss/script/dbctl.sh start
     ```

- On computers with EUQ and central reporting:

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

8. Start Postfix by typing the following command:

```
# postfix start
```

Performing Uninstallation

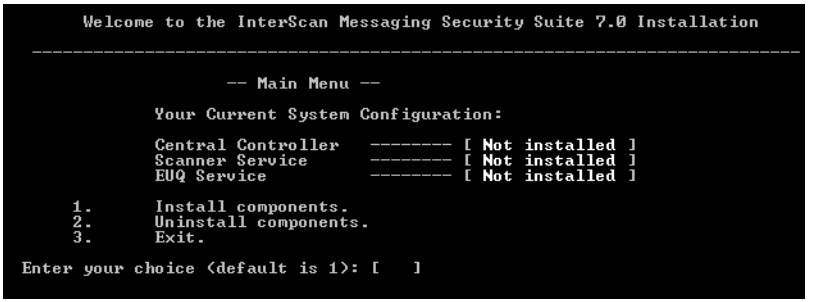
Uninstalling IMSS Components

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

Note: If you have performed a core-installation of Solaris, install the following before uninstalling IMSS:
- SUNWipc
- SUNWipx

---

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



3. Type **2**.

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

5. After you have changed the uninstallation status to **[YES]** for the components that you want to uninstall, type **4**.
6. 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 Network Reputation Services and IP Profiler

To uninstall NRS and IP Profiler:

1. Log on as a superuser and go the installation package directory.
2. Type `./ipfilterinst.sh`. The Main Menu displays showing the status of IP Profiler and NRS. 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.
6. If you are uninstalling NRS, select whether to remove the mail log file. If you do not remove the file, the Postfix mail log will still be written to this file.

   The installer also unregisters IP Profiler and NRS from the IMSS admin database if the database is running.

Performing Manual Uninstallation

Uninstalling IMSS Manually

To uninstall IMSS manually:

1. Stop all IMSS related processes using the command:
   `$Home_IMSS/script/imssstop.sh stop`
2. Stop postgres related processes using the command:
   `$Home_IMSS/script/dbctl.sh stop`
3. Remove the IMSS package as follows:
   ```
   rpm -e imss-7.0-1
   rpm -e imsseuq-7.0-1
   rpm -e imsscctrl-7.0-1
   ```
   If some components have not been installed, the uninstall command may not work.
4. Remove `$Home_IMSS`, such as `/opt/trend/imss`.
5. Remove daemon start/stop scripts.
   - Start scripts run automatically upon system reboot. Remove these scripts from `/etc/rc2.d/ /etc/rc3.d /etc/rc5.d`.
     `S99IMSS, S98dbctl, S99CMAGENT, S99POLICY, S99bindctl, S99IMSSUI, S99FOXDNS, S99SCHEDULED, S99MONITOR, S99MANAGER`
   - Stop scripts kill the processes automatically upon system shutdown. Remove these scripts from `/etc/rc0.d /etc/rc6.d`.
     `K98dbctl, K97CMAGENT, K97IMSS, K97POLICY, K97EUQ, K97bindctl, K97IMSSUI, K97FOXDNS, K97SCHEDULED, K96MONITOR, K96MANAGER, K99IMSSSTOP`

Uninstalling Database Manually

To uninstall database manually:

1. Stop postmaster processes using the command:
   `$Home_IMSS/script/dbctl.sh stop`
   OR
   Kill the processes forcefully using the command:
   `kill -9 pid`

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

Uninstalling Postfix Manually

To uninstall Postfix manually:

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

Uninstalling IP Profiler Manually

To uninstall IP Profiler manually:

1. Stop IP Profiler related processes using the command:
   `/opt/trend/ipprofiler/script/foxproxyd stop`
2. Remove IP Profiler and NRS packages using the command:
   ```
   rpm -e ipprofiler-7.0-1
   rpm -e nrs-7.0-1
   ```
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

Troubleshooting, FAQ, and Support

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

Topics include:

Troubleshooting

Table 5-1 shows common troubleshooting issues that you might encounter when installing IMSS. Read through the solutions below. If you have additional problems, check the Trend Micro Knowledge Base.

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

Issue	Suggested Resolution
The NRS installation does not validate the NRS Activation Code	To validate the Activation Code, the NRS installation script accesses Trend Micro through the Internet. Verify that your DNS server is operating correctly and that the computer on which you are installing NRS has access to the Internet.
When installing NRS, the following error message appears: "Applying change to Postfix failed"	Postfix is not running. The NRS installation script writes configuration information into the Postfix configuration files. Verify that Postfix is running, and then run the NRS installer again.

TABLE 5-1. Troubleshooting issues

Frequently Asked Questions

Postfix MTA Settings

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

If you want to control all the Postfix computers from the Web management console, you should enable the "**Apply settings to all scanners**" option. Choose **Administrator** > **SMTP Routing** > **SMTP** from the menu.

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

```
detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:queue_directory
```

How can I change my MTA settings without using the Web management console?

You can modify the IMSS configuration file and add the following key.

1. Open `imss.ini`.
2. Make the following modification:

```
detach_key_postfix=smtpd_use_tls:queue_directory:{Parameter1:{Parameter2}:…::{Parameter n}
```

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

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 install program and configure the IMSS database only without selecting any other IMSS components.

How many scanners can be installed?

Any number of scanners can be installed.

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 can't I remove the old IMSS database during installation?

This is because 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 7.0 on a computer with an external DNS server?

Basically, there should be no functional problem integrating IMSS 7.0 with DNS server. Functionally, it is alright to 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 7.0 on a computer with an existing Apache Server?

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

Upgrading

Are all IMSS 5.7 settings maintained during migration?

No. Due to architectural changes in IMSS 7.0, some settings cannot be kept. The IMSS 7.0 installer will ask for the new values of these settings during migration and the settings can also be found in the general migration report:

`$IMSS_Home/installlog/MigrationReport/GeneralReport.txt`

How do I migrate multiple IMSS 5.7 scanners?

To migrate from multiple IMSS 5.7 scanners:

- Migrate 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 4-26.

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

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

Is a smooth rollback to IMSS 5.7 possible after migration?

Yes. See *Rolling Back the Migration* on page 4-38 for detailed rollback instructions.

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

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

How do I simplify SPS rules after migration?

In order to keep all SPS filter settings for all policies of IMSS 5.7, IMSS 7.0 migrates each SPS filter to one or multiple SPS rule(s) in IMSS 7.0. If you want to reduce the number of SPS rules after migration, perform the following:

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

What is the source of internal addresses during migration?

To maintain IMSS 5.7 internal domains, IMSS 7.0 extracts all domains from the following fields:

- Domains in the "To" field of incoming policy routes
- Domains in the "From" field of outgoing policy routes

Note: If there are address groups in the two fields above, all domains in the address groups are extracted.

How are filters and policies mapped during migration?

The architectures of IMSS 5.7 and IMSS 7.0 are very different. Therefore, the migration module maps all IMSS 5.7 filters to related rules in IMSS 7.0 in the following ways:

- **Virus filter(s) —** There is only one virus rule for all messages after migration (regardless of the number of virus filters in IMSS 5.7).
  - The status of virus rules will be "Enable" if one of the virus filters is "active" in IMSS 5.7.
  - Otherwise, the status of the virus rule will be "disable" after migration.
- **SPS filter(s) —** The migration module maps each SPS filter into one or multiple SPS rules after migration.
- **eManager filter**
  - There will be two rules for one eManager filter after migration if it is "active" in IMSS 5.7 for both SMTP and POP3 traffic.
  - There will be only 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 direction in IMSS 7.0 if necessary.

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

Others

What is the difference between the Sandwich model and the Proxy model?

In the Sandwich model, you install the upstream MTA, IMSS and the downstream MTA on different computers within the intranet. External messages from the Internet first arrive at the upstream MTA which then passes them to IMSS. In the Proxy model, however, external messages arrive at IMSS directly as there is no upstream MTA to relay them.

Does IMSS listen to port 25 if the Proxy model is deployed?

As there is no upstream MTA to relay messages to IMSS in the Proxy model, the default IMSS listening port is set to 25 in order for IMSS to receive incoming messages directly from the Internet.

Using the Knowledge Base

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

`http://esupport.trendmicro.com`

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

Contacting Support

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

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

`http://www.trendmicro.com/support`

Get the latest Trend Micro product documentation:

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

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

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

Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: www.trendmicro.com
Email address: support@trendmicro.com

Index