TREND MICRO™

InterScan™ Messaging Security Suite 7

Comprehensive threat protection at the Internet messaging gateway

for Windows™

Installation Guide

Messaging Security

Document Part No. MSEM74176/90727

Release Date: November 2009

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

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

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

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

Contents

Preface

Chapter 1: Introducing InterScan Messaging Security Suite

Chapter 2: Component Descriptions

Chapter 3: Planning for Deployment

Chapter 4: Installing and Uninstalling IMSS 7.1

Chapter 5: Upgrading from Previous Versions

Chapter 6: Troubleshooting, FAQ, and Support Information

Index

Preface

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

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

Topics include:

Audience

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

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

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

InterScan Messaging Security Suite Documentation

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

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

The *Installation Guide, Administrator's Guide* and *readme files* are available at:

http://www.trendmicro.com/download

Document Conventions

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

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

Chapter 1

Introducing InterScan Messaging Security Suite

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

Topics include:

About IMSS

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

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

What's New

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

TABLE 1-1. IMSS 7.1 New Features

NEW FEATURE	DESCRIPTION
Policy Objects	Several information objects that can be used by policies have been removed from policy creation and given their own areas for configuration: • Address Groups • BATV Keys • Keywords & Expressions • Policy Notifications • Stamps • DKIM Approved List • Web Reputation Approved List
Web Reputation	Protect your clients from malicious URLs embedded in email messages with Web reputation.

TABLE 1-1. IMSS 7.1 New Features (Continued)

NEW FEATURE	DESCRIPTION
BATV Support	Bounce Address Tag Validation (BATV) protects your clients from bounced email message attacks.
NRS Terminology Change	Network Reputation Service (NRS) has been changed to **Email reputation**.
Detection Capability Enhancement	Use DomainKeys Identified Mail (DKIM) enforcement, with the DKIM Approved List, in policies to assist in phishing protection and to reduce the number of false positives regarding domains.
X-Header Support	Insert X-Headers into email messages to track and catalog the messages.
Expanded File Scanning Support	IMSS now supports scanning Microsoft® Office 2007 and Adobe® Acrobat® 8 documents.
New Migration Tools	New tools have been provided to help customers migrating from previous product versions.

IMSS 7.0 New Features

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

TABLE 1-2. IMSS 7.0 New Features

NEW FEATURE	DESCRIPTION
Multiple Antivirus and Malware Policies	Multiple IMSS policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria.

TABLE 1-2. IMSS 7.0 New Features (Continued)

NEW FEATURE	DESCRIPTION
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	IMSS provides an easy way to search multiple IMSS quarantine and archive areas for messages.
Scalable Web End-User Quarantine (Web EUQ)	Multiple Web EUQ services offer end-users the ability to view quarantined email messages that IMSS detected as spam. Together with EUQ notification, IMSS will help lower the cost of helpdesk administrative tasks.
Multiple Spam Prevention Technologies	Three layers of spam protection: • Email reputation filters spam senders at the connection layer. • IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS). • Trend Micro Anti-spam engine detects and takes action on spam.
IntelliTrap	IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus in a compressed file will enter your network through email.
Delegated Administration	LDAP-integrated account management allows users to assign administrative rights for different configuration tasks.
Easy Deployment with Configuration Wizard	An easy-to-use configuration wizard to get IMSS up and running.

TABLE 1-2. IMSS 7.0 New Features (Continued)

NEW FEATURE	DESCRIPTION
Advance MTA Functions	Opportunistic TLS, domain based delivery, and other MTA functions help IMSS handle email efficiently and securely.
Migration	Easy upgrade process ensures that settings will be migrated with minimum effort during setup.
Mail Auditing and Tracking	IMSS provides detailed logging for all messages to track and identify message flow related issues.
Integration with Trend Micro Control Manager™	Perform log queries on Email reputation detections from Control Manager, in addition to other supported features.
Supports 8 bit to 7 bit-MIME transformation	IMSS 7.0 Service Pack 1 supports the transformation of 8 bit to 7 bit-MIME according to the standard defined in RFC 1652 SMTP Service Extension for 8bit-MIME transport. In the event that the next hop of the SMTP server does not support 8 bit MIME, IMSS will convert the message from 8 bit MIME to 7 bit MIME.

IMSS Main Features and Benefits

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

TABLE 1-3. Main Features and Benefits

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

TABLE 1-3. Main Features and Benefits (Continued)

FEATURE	DESCRIPTIONS	BENEFITS
IntelliTrap	Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files. Because there is the possibility that IntelliTrap may identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature. By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be classified as security risks.	IntelliTrap helps reduce the risk that a virus compressed using different file compression schemes will enter your network through email.
Content management	IMSS analyzes email messages and their attachments, traveling to and from your network, for appropriate content.	Content that you deem inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using IMSS.

TABLE 1-3. Main Features and Benefits (Continued)

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

TABLE 1-3. Main Features and Benefits (Continued)

FEATURE	DESCRIPTIONS	BENEFITS
Legal liability and business integrity	Improper use of email can also put a company at risk of legal liability. Employees may engage in sexual or racial harassment, or other illegal activity. Dishonest employees can use a company messaging system to leak confidential information. Inappropriate messages that originate from a company's mail server damage the company's reputation, even if the opinions expressed in the message are not those of the company.	IMSS provides tools for monitoring and blocking content to help reduce the risk that messages containing inappropriate or confidential material will be allowed through your gateway.

TABLE 1-3. Main Features and Benefits (Continued)

FEATURE	DESCRIPTIONS	BENEFITS
Mass mailing virus containment	Email-borne viruses that may automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users. When IMSS detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses. For example, if IMSS detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if IMSS detects a mass-mailing virus, the program can automatically delete the entire message.	By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value. The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs[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.
Protection from 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 1-14	IMSS's ability to protect your environment against spyware and other types of grayware enables you to significantly reduce security, confidentiality, and legal risks to your organization.

TABLE 1-3. Main Features and Benefits (Continued)

FEATURE	DESCRIPTIONS	BENEFITS
Integrated spam		
Spam Prevention Solution (SPS)	Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam detection services to other Trend Micro products. To use SPS, obtain an SPS Activation Code. For more information, contact your sales representative. SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license. **Note:** Activate SPS before you configure IP Profiler and Email reputation.	The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real-time detection that is highly adaptable, even as spam senders change their techniques.
Spam Filtering with IP Profiler and Email reputation	IP Profiler is a self-learning, fully configurable feature that proactively blocks IP addresses of computers that send spam and other types of potential threats. Email reputation blocks IP addresses of known spam senders that Trend Micro maintains in a central database.	With the integration of IP Filtering, which includes IP Profiler and Email reputation, IMSS can block spammers at the IP level.

TABLE 1-3. Main Features and Benefits (Continued)

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

TABLE 1-3. Main Features and Benefits (Continued)

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

TABLE 1-3. Main Features and Benefits (Continued)

FEATURE	DESCRIPTIONS	BENEFITS
Integration with Trend Micro™ Control Manager™	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 1-16.	Outbreak Prevention Services delivered through Control Manager reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available.

About Spyware and Other Types of Grayware

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

TABLE 1-4. Types of spyware/grayware

TYPES OF SPYWARE/GRAYWARE	DESCRIPTIONS
Spyware/Grayware	Gathers data, such as account user names and passwords, and transmits them to third parties.
Adware	Displays advertisements and gathers data, such as user Web surfing preferences, through a Web browser.
Dialers	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem.

TABLE 1-4. Types of spyware/grayware (Continued)

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

About Web Reputation

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

About Trend Micro Control Manager

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

Control Manager consists of the following components:

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

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

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

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

- **Entity**—An entity is a representation of a managed product on the Product Directory link. Each entity has an icon in the directory tree. The directory tree on the Control Manager console displays all managed entities, and IMSS can be one of the entities.

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

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

Integrating with Control Manager

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

TABLE 1-5. Supported Control Manager features

FEATURES	DESCRIPTIONS	SUPPORTED?
2-way communication	Using 2-way communication, either IMSS or Control Manager may initiate the communication process.	No. Only IMSS can initiate a communication process with Control Manager.
Outbreak Prevention Policy	The Outbreak Prevention Policy (OPP) is a quick response to an outbreak developed by TrendLabs that contains a list of actions IMSS should perform to reduce the likelihood of the IMSS server or its clients from becoming infected. Trend Micro ActiveUpdate Server deploys this policy to IMSS through Control Manager.	Yes
Log Upload for Query	Uploads IMSS virus logs, Content Security logs, and Email reputation logs to Control Manager for query purposes.	Yes
Single Sign-On	Manage IMSS from Control Manager directly without first logging on to the IMSS Web management console.	No. You need to first log on to the IMSS Web management console before you can manage IMSS from Control Manager.
Configuration Replication	Replicate configuration settings from an existing IMSS server to a new IMSS server from Control Manager.	Yes

TABLE 1-5. Supported Control Manager features (Continued)

FEATURES	DESCRIPTIONS	SUPPORTED?
Pattern Update	Update pattern files used by IMSS from Control Manager	Yes
Engine Update	Update engines used by IMSS from Control Manager.	Yes
Product Component Update	Update IMSS product components such as patches and hot fixes from Control Manager.	No. Refer to the specific patch or hot fix readme file for instructions on how to update the product components.

TABLE 1-5. Supported Control Manager features (Continued)

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

TABLE 1-5. Supported Control Manager features (Continued)

FEATURES	DESCRIPTIONS	SUPPORTED?
Control Manager Agent Installation /Uninstallation	Install or uninstall IMSS Control Manager Agent from Control Manager.	No. IMSS Control Manager agent is automatically installed when you install IMSS. To enable/disable the agent, do the following from the IMSS Web management console: 1. Choose **Administration > Connections** from the menu. 2. Click the **TMCM Server** tab. 3. To enable/disable the agent, select/clear the check box next to **Enable TMCM Agent** .
Event Notification	Send IMSS event notification from Control Manager.	Yes
Command Tracking for All Commands	Track the status of commands that Control Manager issues to IMSS.	Yes

Chapter 2

Component Descriptions

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

Topics include:

About IMSS Components

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

You can install IMSS components on a single computer or on multiple computers. For graphical representations of how these components work together, see Understanding Installation Scenarios on page 3-16.

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 SQL Server Express database or use an existing database.

Central Controller

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

Scanner Services

Servers configured as scanner services do the following:

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

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

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

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

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

Policy Services

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

Policy Synchronization

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

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

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

End-User Quarantine Service

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

Primary and Secondary End-User Quarantine Services

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

End-User Quarantine Server Components

The EUQ Server includes the following software components:

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

Apache Web Server and mod_jk

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

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

Tomcat

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

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

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

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

Struts Framework

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

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

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

End-User Quarantine Application

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

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

The EUQ Application is implemented as a set of Java classes in the `com.trendmicro.imss.ui` package stored in the `{IMSS}\ui\euqui\webapps\ROOT\WEB-INF\classes` directory and set of Java Server Pages stored in the `{IMSS}\ui\euqui\webapps\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 the Trend Micro IMSS End-User Quarantine Console service using the Microsoft Management Console.

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 SQL database server to install the EUQ database.

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

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

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

IP Filtering

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

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

  IP profiler detects any of these four potential Internet threats:

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

How IP Profiler Works

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

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

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

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

Email Reputation

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

Types of Email Reputation

There are two types of Email reputation: Standard and Advanced.

Email Reputation: Standard

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

Email reputation: Standard is a DNS single-query-based service. Your designated email server makes a DNS query to the standard reputation database server whenever an incoming email message is received from an unknown host. If the host is listed in the standard reputation database, Email reputation reports that email message as spam. You can set up your MTA to take the appropriate action on that message based on the spam identification from Email reputation.

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

Email Reputation: Advanced

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

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

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

How Email Reputation Technology Works

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

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

Figure 2-1 illustrates how Email reputation works.

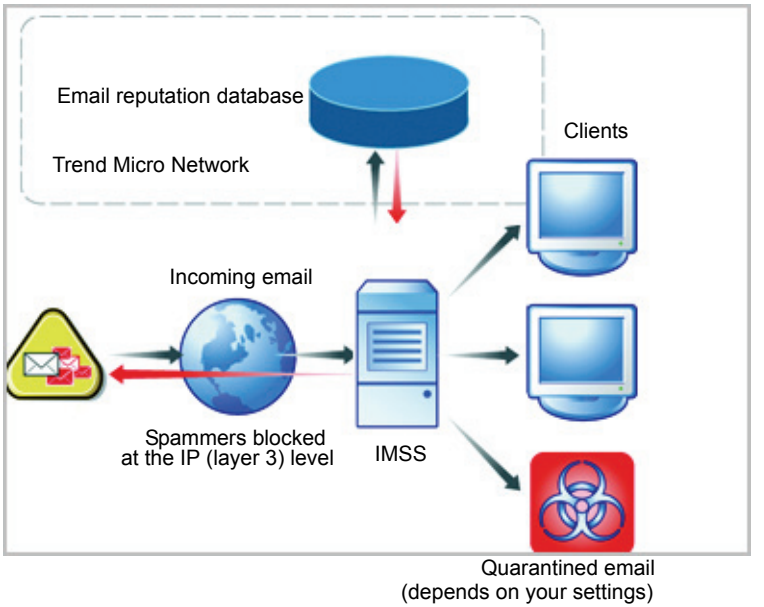


FIGURE 2-1. How Email reputation works

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

Using the Email Reputation Management Console

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

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

To open the Email reputation management console:

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

   https://tmspn.securecloud.com/

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

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

TABLE 2-1. ISP Spam List

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

TABLE 2-1. ISP Spam List (Continued)

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

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

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

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

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

TABLE 2-2. Report Types

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

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

b. Click one of the following:

TABLE 2-3. Policy Settings

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

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

About End-User Quarantine (EUQ)

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

About Centralized Reporting

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

Chapter 3

Planning for Deployment

This chapter explains how to plan for IMSS deployment.

Topics include:

Deployment Checklist

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

TABLE 3-1. Deployment Checklist

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

TABLE 3-1. Deployment Checklist (Continued)

TICK ✓ WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	• Single-server installation		Single-Server Installation on page 3-16
	• Multiple scanner service		Multiple Scanner Service Installation on page 3-18
	• Multiple EUQ service		Multiple End-User Quarantine Service Installation on page 3-20
	• Complex distributed		Complex Distributed Installation on page 3-23
	• Wide area network		Wide-Area Network Installation on page 3-25
	• IP filtering **Tip:** Trend Micro recommends that you consider the failover plan before deciding on the scope.		IP Filtering on page 3-28
	Step 3 - Install or Upgrade		
	Perform a fresh installation of IMSS or upgrade from a previous version.		

TABLE 3-1. Deployment Checklist (Continued)

TICK ✓ WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	• Install IMSS components		Multiple Scanner and EUQ Service/Database Installation on page 4-20
	• Upgrade from a previous version		Upgrading from Version 5.7 to Version 7.1 on page 5-5
	Step 4 - Configure basic IMSS settings		
	Go through the 8 steps of configuring the Central Controller through the Configuration Wizard.		
	Configure settings using the Configuration Wizard		Performing Basic Configuration with the Configuration Wizard section of the *Administrator's Guide*.
	Step 5 - Start services		
	Activate IMSS services to start protecting your network against various threats.		
	• Scanner		IMSS Services section of the *Administrator's Guide*.
	• Policy		
	• EUQ	Yes	
	Step 6 - Configure other IMSS settings		
	Configure various IMSS settings to get IMSS up and running.		

TABLE 3-1. Deployment Checklist (Continued)

TICK ✓ WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	• IP Filtering Rules	Yes	IP Filtering Service section of the *Administrator's Guide*.
	• SMTP Routing		Scanning SMTP Messages section of the *Administrator's Guide*.
	• POP3 Settings	Yes	Scanning POP3 Messages section of the *Administrator's Guide*.
	• Policy and scanning exceptions		Managing Policies section of the *Administrator's Guide*.
	• Perform a manual update of components and configure scheduled updates		Updating Scan Engine and Pattern Files section of the *Administrator's Guide*.
	• Log settings		Configuring Log Settings section of the *Administrator's Guide*.
	Step 7 - Back up IMSS		
	Perform a backup of IMSS as a precaution against system failure		
	Back up IMSS Admin database		Backing Up IMSS section of the *Administrator's Guide*.

Component and Sub-module Installation

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

TABLE 3-2. Component and sub-module installation

MAIN COMPONENT	INSTALLED SUB-MODULE	SUB-MODULE DESCRIPTION
IMSS Admin Database	Administrator Database	The main IMSS Admin database that stores all global settings.
	Database Server*	The server on which the IMSS Admin database runs.
Central Controller	Apache® Tomcat®	The Web server for the IMSS Web management console, through which you configure settings.
	Named Server	The DNS server for IP Profiler.
	FoxDNS	Contains the list of blocked and white IP addresses for IP Profiler and writes the list to the named server.
	IMSSMGR	A module that manages IMSS-related processes.
Scanner Service	Scanning Services	Performs all email-scanning actions.
	Policy Services	A remote store of rules for the scanner services, caching rules that would otherwise require a database look-up
	IMSSMGR	A module that manages scanner processes.
	SMTP Service	Trend Micro MTA/MDA
	IP Profiler	Part of Trend Micro MTA
	Email reputation	Part of Trend Micro MTA

TABLE 3-2. Component and sub-module installation (Continued)

MAIN COMPONENT	INSTALLED SUB-MODULE	SUB-MODULE DESCRIPTION
EUQ Service	Apache Tomcat	The Web server for the EUQ Web console, though which your users can access the email messages that IMSS quarantined as spam.
	Apache Service	Install this module with the primary EUQ services for load balancing purposes when you choose to install multiple EUQ services.
	IMSSMGR	A module that manages EUQ processes.
EUQ Database	EUQ Database	The database that contains all email messages that IMSS quarantined as spam.
	Database Server*	The server on which the EUQ database runs.

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

IMSS Ports

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

TABLE 3-3. IMSS Ports

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
25	The MTA service port. The mail server will listen at this port to accept messages. This port must be opened at the firewall, or the server is not able to accept mails.	From the Web management console, click **Administration > IMSS Configuration > SMTP Routing > Connections** on the menu.
110	IMSS scanner generic POP3 port. The scanner uses this port to accept POP3 request and scan POP3 mails.	From the Web management console, click **Administration > IMSS Configuration > Connections > POP3** on the menu.
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 Web Server (Tomcat) management port that can handle Tomcat management commands.	{IMSS}/UI/adminUI/conf/server.xml: Server / port
8009	EUQ Console Tomcat AJP port. This port is used to perform load balancing between several Tomcat servers and the Apache HTTP server.	{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector (protocol=AJP/1.3) / port
8015	Tomcat management port that can handle Tomcat management commands.	{IMSS}/UI/euqUI/conf/server.xml: Server/port

TABLE 3-3. IMSS Ports (Continued)

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
8445	IMSS Web console listening port. Open this port to log on to the Web management console using a Web browser.	Tomcat listening port: {IMSS}/UI/adminUI/conf/server.xml: Server / Service / Connector / port
8446	EUQ service listening port.	{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector / port
8447	EUQ service listening port with load balance.	{IMSS}/UI/euqUI/conf/EUQ.conf: Listen / VirtualHost / ServerName
10024	IMSS scanner reprocessing port. Messages released from the central quarantine area in the Admin database and from the EUQ database will be sent through this port for reprocessing.	imss.ini / [socket_2]/ proxy_port
10026	The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSS.) All messages sent through this port will not be scanned by IMSS. Due to security considerations, the port is only bound at IMSS server's loopback interface (127.0.0.1). It is therefore not accessible from other computers. You are not required to open this port at the firewall.	tsmtpd.ini

TABLE 3-3. IMSS Ports (Continued)

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
15505	IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the Web 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 services:		
389	LDAP server listening port.	IMSSFrom the Web management console, click **Administration > IMSS Configuration > Connections > LDAP** on the menu.
80	Microsoft IIS HTTP listening port. You need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu.
443	Microsoft IIS HTTPS listening port. You need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu
88	KDC port for Kerberos realm.	Not configurable on the IMSS server.

TABLE 3-3. IMSS Ports (Continued)

PORT NUMBER	COMPONENT AND ROLE	CONFIGURATION LOCATION
53	The Bind service listening port. Do not assign a different port number.	Not configurable on the IMSS server.

Network Topology Considerations

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

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

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

Installing without a Firewall

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

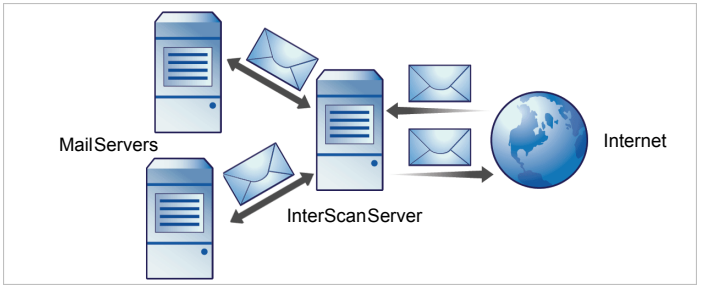


FIGURE 3-1. Installation topology: no firewall

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

Installing in Front of a Firewall

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

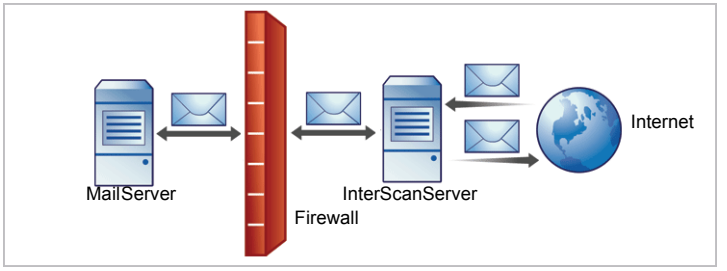


FIGURE 3-2. Installation topology: in front of the firewall

Incoming Traffic

- IMSS should be the first server to receive incoming email. Configure the MX records on the DNS servers that currently reference your SMTP gateway or firewall to reference the address of the IMSS server, or the switch that performs load balancing between scanners.
- 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 can only go to IMSS servers.
  - Incoming SMTP email can only come from IMSS servers.
- Configure IMSS to allow internal SMTP gateways to relay to any domain through IMSS.

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

Installing Behind a Firewall

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

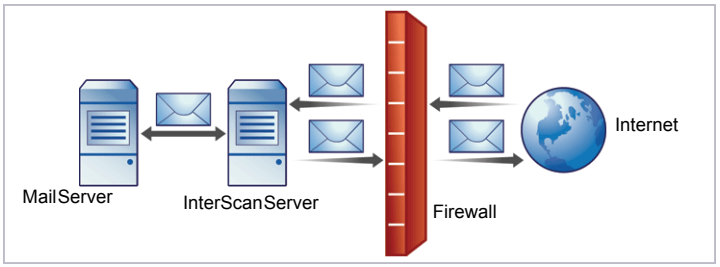


FIGURE 3-3. Installation scenario: behind a firewall

Incoming Traffic

- Configure your proxy-based firewall, as follows:
  - Outgoing SMTP email goes to the IMSS server or the switch performing load balancing between scanners.
  - Incoming SMTP email can only come from IMSS servers.
- Configure your packet-based firewall, as follows:
  - Change the MX records on the DNS server that currently reference your SMTP gateway to reference the address of the server hosting IMSS.
  - Point your MX records to IMSS or the firewall, if you configured it to manage a secure subnet.
- Configure IMSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server.
- Configure relay restriction to only allow relay for local domain(s).

Outgoing Traffic

- Configure all internal SMTP gateways to send outgoing mail to IMSS servers.
- If you are replacing your SMTP gateway with IMSS, configure your internal mail server to forward outgoing email to IMSS servers.
- Configure IMSS to route all outgoing email (to domains other than local), to the firewall, or deliver the messages using an external DNS server.
- 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 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 the gateway. Ensure the port is not used by any other services.

- Configure the existing SMTP gateway to bind to the newly allocated port, which frees port 25.
- Install IMSS—and it binds to port 25.

Incoming Traffic

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

Outgoing Traffic

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

Installing in the De-Militarized Zone

You can also install IMSS 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.
- Reconfigure your packet-based firewall so that the mail exchange (MX) records on the DNS server that currently reference your SMTP gateway reference the address of the server hosting IMSS or the switch performing load balancing between scanners.
- Configure IMSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server.

Outgoing Traffic

- Configure IMSS to route all outgoing email (destined to other than the local domains) to the firewall or deliver them using an external DNS server.
- Configure all internal SMTP gateways to forward outgoing mail to then to IMSS.
- Configure IMSS to allow internal SMTP gateways to relay to any domain, through IMSS.

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

Understanding Installation Scenarios

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

Single-Server Installation

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

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

- Central Controller
- IMSS Admin Database
- Policy Service
- Scanner Service
- Primary EUQ Service and EUQ Database
- MTA Services
- IP Filtering Services

Note: To use IP filtering services, you must deploy IMSS as the Edge MTA.

Figure 3-4 shows how a single-server installation of IMSS fits into a standard messaging network topology.

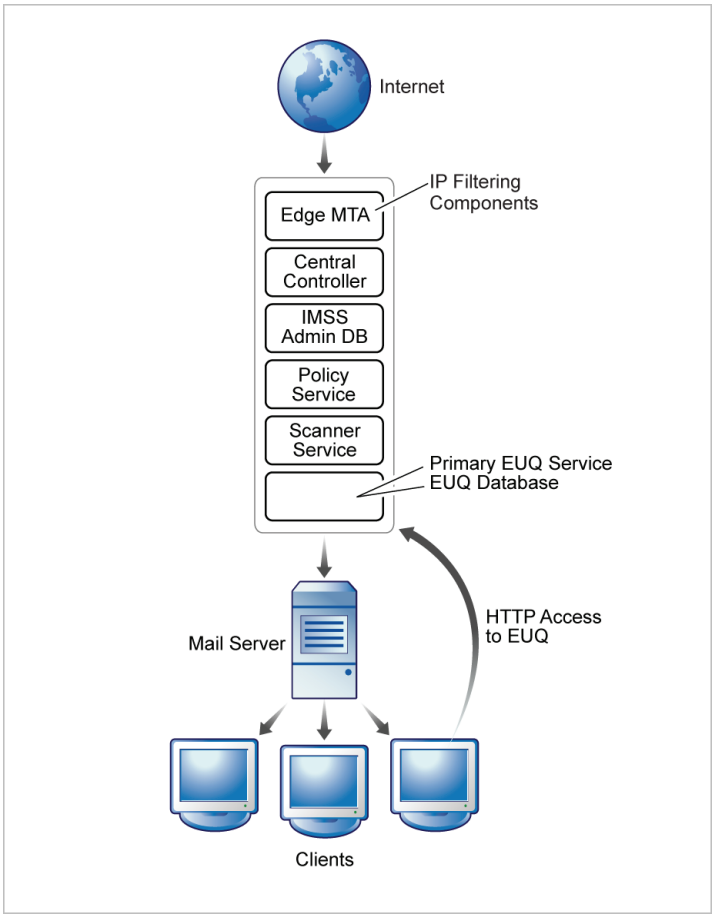


FIGURE 3-4. Single server deployment

To perform a single-server installation:

1. Install IMSS and End-User Quarantine (see Single-Server Installation on page 4-3).

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 3-5 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.

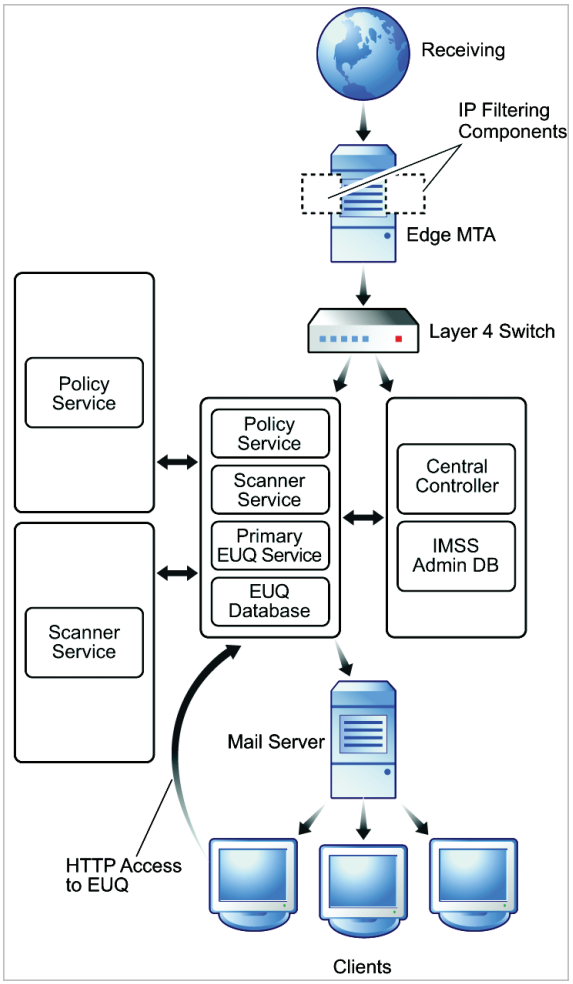


FIGURE 3-5. Multiple scanner service and policy service deployment

To perform a multiple scanner service installation:

1. On one computer, install IMSS and End-User Quarantine (see Complex Distributed Installation on page 4-36).
2. On other computers, install the necessary scanner service and policy services.

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

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

Multiple End-User Quarantine Service Installation

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

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

Note: You can install up to eight EUQ servers and EUQ databases.

Figure 3-6 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.

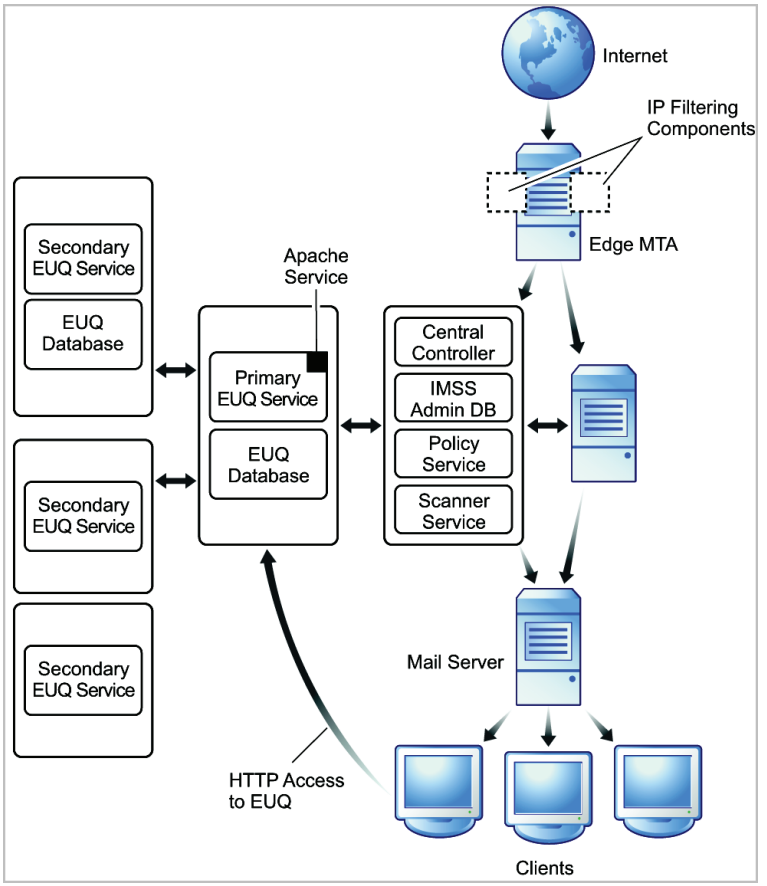


FIGURE 3-6. Multiple EUQ service deployment

To perform a multiple EUQ service installation:

1. On one computer, install IMSS (see Single-Server Installation on page 4-3 or Complex Distributed Installation on page 4-36).
2. On another computer, install a single instance of the EUQ service. This will be the primary EUQ service.
3. 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.

---

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

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

Other Considerations When Deploying End-User Quarantine

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

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

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

For more information, see Single-Server Installation on page 4-3 or Complex Distributed Installation on page 4-36.

Communication Between Servers

If you have an internal firewall, configure it to allow communication between IMSS, the EUQ service, and the database. For instance, if you install the EUQ service on one server, and the database on another, configure any firewall between the two servers to allow communication on the port for database connection.

Complex Distributed Installation

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

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

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

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

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

Figure 3-7 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.

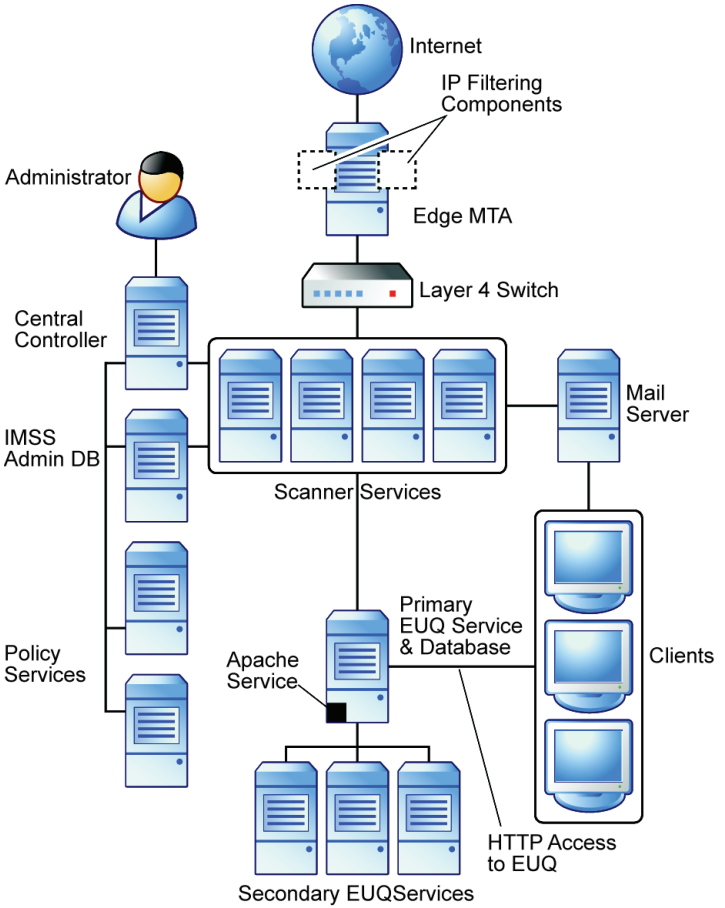


FIGURE 3-7. Complex architecture deployment

Wide-Area Network Installation

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

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

Trend Micro Control Manager

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

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

Figure 3-8 shows a multi-site WAN deployment.

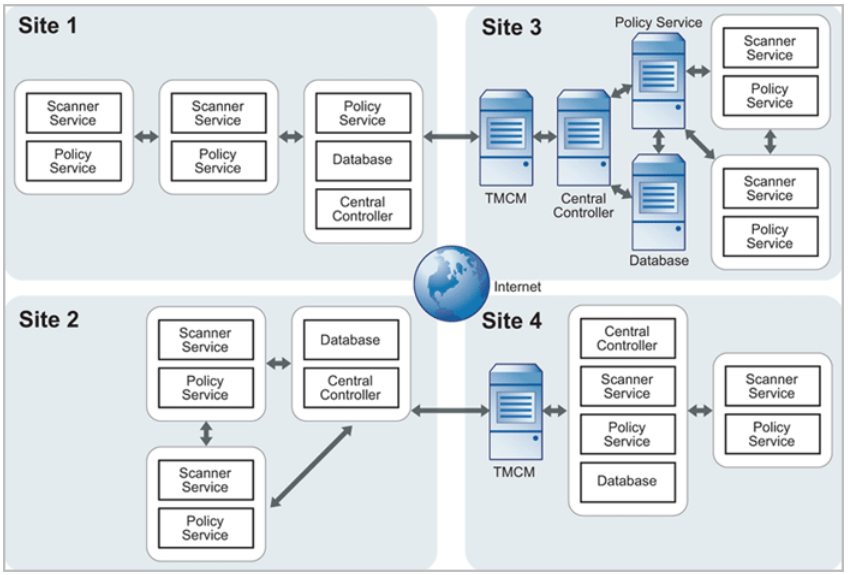


FIGURE 3-8. WAN deployment

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 3-9*.

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

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

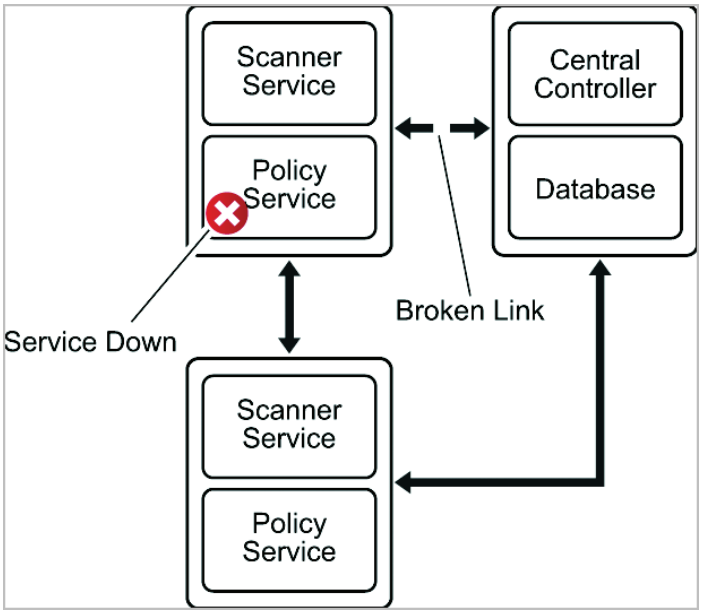


FIGURE 3-9. Failover

IP Filtering

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

Deploying IMSS with IP Filtering

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

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

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

About Failover

Table 3-4 shows what happens when certain IMSS components malfunction, and how you can plan for failover to keep your IMSS protection up and running. For more information about failover in a WAN deployment scenario, see Fault Tolerance and Failover in a WAN Scenario on page 3-27.

TABLE 3-4. Failover Scenarios

COMPONENT THAT MALFUNCTIONS	EXPECTED RESULT	RECOMMENDED FAILOVER PLAN
Scanner service is not running or becomes disconnected	1. IMSS tries to restart the scanner service 2. IMSS sends an event notification if the service cannot be started within the time you specify for notifications.	Install multiple scanners for load balancing and failover. For details, see Multiple Scanner Service Installation on page 3-18.

TABLE 3-4. Failover Scenarios (Continued)

COMPONENT THAT MALFUNCTIONS	EXPECTED RESULT	RECOMMENDED FAILOVER PLAN
Policy service is not running or a communication problem with the IMSS server occurs	1. Scanner services using the stopped policy service switch to an active policy service (if available). 2. IMSS tries to restart the policy service. 3. IMSS sends an event notification if the service cannot be started or reconnected within the time you specify for notifications.	Install multiple scanners for load balancing and failover. For details, see Multiple Scanner Service Installation on page 3-18.
IMSS Admin database is not running	1. The IMSS server will continue to operate.	Back up the Admin database periodically. http://www.microsoft.com/Sqlserver/2005/en/us/express.aspx
EUQ service database is not running	1. An error message appears on the EUQ Web console.	Back up the EUQ Database periodically. http://www.microsoft.com/Sqlserver/2005/en/us/express.aspx

TABLE 3-4. Failover Scenarios (Continued)

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

Chapter 4

Installing and Uninstalling IMSS 7.1

This chapter explains how to install IMSS under different scenarios.

Topics include:

System Requirements

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

TABLE 4-1. System Requirements

HARDWARE/SOFTWARE	DESCRIPTION
Operating System	• Microsoft™ Windows™ Server 2008 SP 2 (X86 and X64) • Microsoft Windows Server 2003 R2, SP2 (X86 and X64) • Microsoft Windows Server 2003 SP2 (X86 and X64) **Note:** IMSS is a 32-bit program. When installing on a 64-bit operating system, use the commands "perfmon.msc -32" or "mmc /32 perfmon.msc" to start IMSS Monitor.
Recommended CPU	Quad-Core Intel™ Xeon™ CPU 1.6GHz or above
Minimum CPU	Two Intel Xeon 3GHz processors
Recommended Memory	4GB RAM
Minimum Memory	2GB RAM
Recommended Disk Space	250GB total The following recommendations are based on 500,000 email messages/day, a 50% quarantine rate, and logs preserved for a month. • 10GB for mail storage • 50GB or more for the Admin database • 20GB or more for the EUQ database • 40GB or more for the working quarantine folder

TABLE 4-1. System Requirements (Continued)

HARDWARE/SOFTWARE	DESCRIPTION
Minimum Disk Space	80GB total
Browser	• Microsoft Internet Explorer 6 SP1 and above, 7, or 8 • Mozilla™ Firefox™ 3.0
Monitor	Monitor that supports 800 x 600 resolution with 256 colors or higher
Microsoft SQL Server	• Microsoft SQL Server 2005 SP1, SP2 • Microsoft SQL Server 2000 SP4 • Microsoft SQL Server 2005 Express SP1, SP2 **Note:** IMSS does not support Windows Authentication Mode for databases.
Microsoft Data Access Components	Microsoft Data Access Components (MDAC) 2.8 SP1 or above
LDAP server	• Microsoft™ Active Directory 2000 or 2003 • IBM Lotus™ Domino™ 6.0 or above • Sun™ One LDAP 5.2 or above

Note: The default location for the IMSS Admin DB and EUQ DB is C:\Program Files\Trend Micro\SQL Express if you have installed these databases using SQL Express. The default IMSS Quarantine working folder is C:\Program Files\Trend Micro\IMSS\queue\.

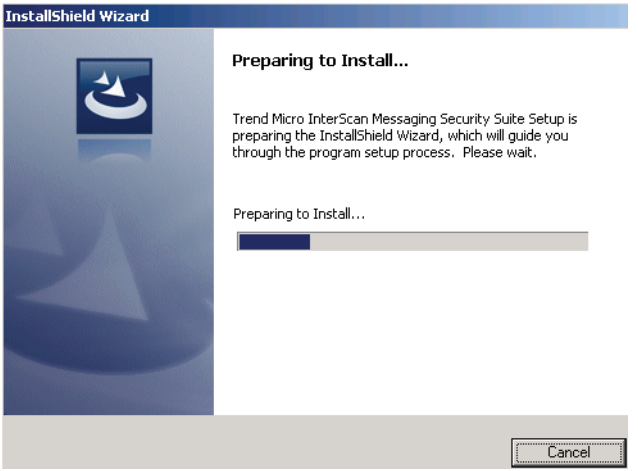
Single-Server Installation

Single server installation means installing all IMSS components on one server.

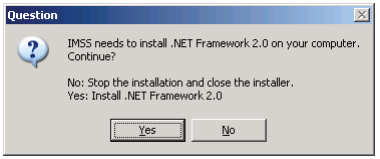
If the installation cannot complete and the message "cannot overwrite xxx.xxx" appears, manually remove all files in the destination folder and retry installation. You might need to stop all running applications under the destination folder. For example, a terminal service instance might be running statmon.exe.

To perform a basic installation:

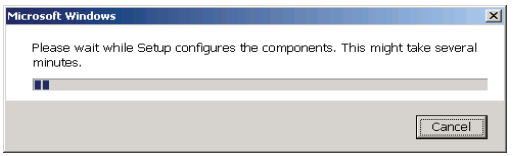
1. Double-click **Setup.exe**. The Preparing to Install... screen appears.



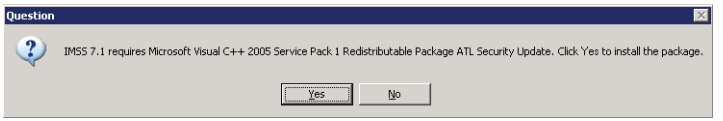
If Microsoft .NET Framework 2.0 has not been installed on the server, a dialog box appears.



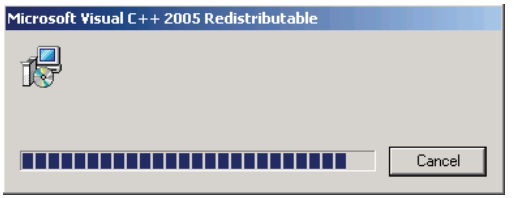
2. Click **Yes**. Installation of Microsoft .NET Framework 2.0 begins.

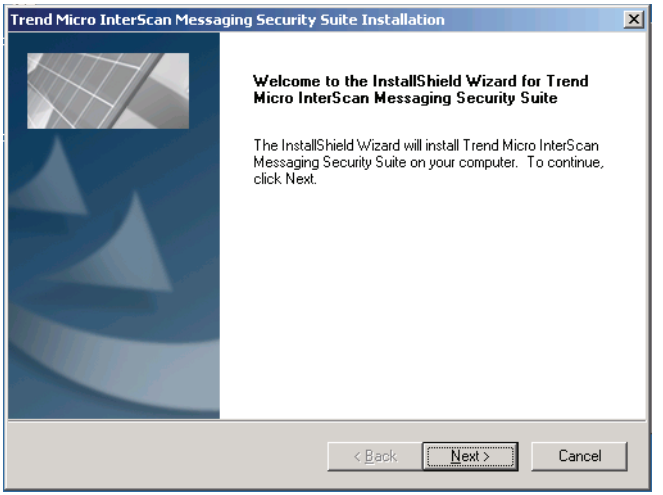


If Microsoft Visual C 2005 is not installed, a dialog box appears.

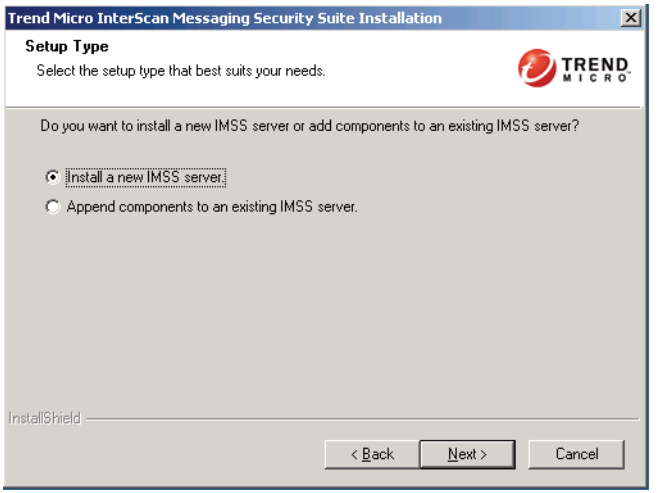


3. Click **Yes**. Microsoft Visual C++ 2005 installation begins.



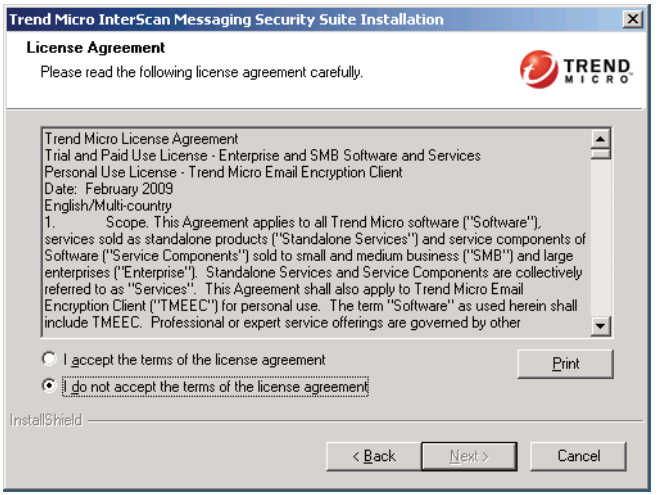


4. Click **Next**. The Setup Type screen appears.



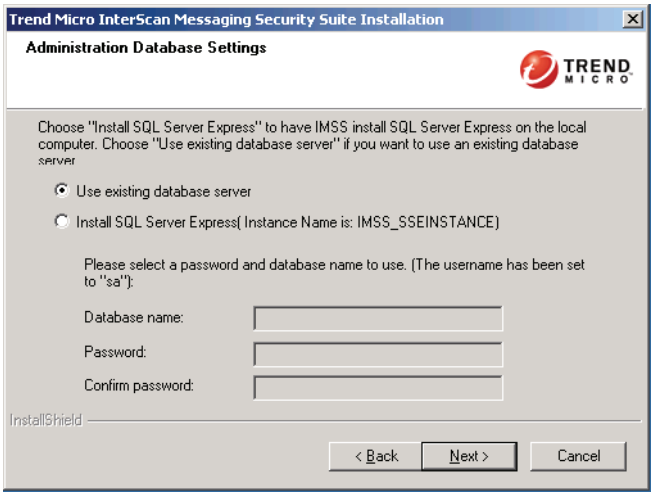
5. Select **Install a new IMSS server**.

6. Click **Next**. The License Agreement screen appears.



7. Read the license agreement carefully before selecting **I accept the terms of the license agreement**.

8. Click **Next**. The Administration Database Settings screen appears.



To use an existing database server:

If an external database is specified, enable the remote connections of the external SQL Server.

After enabling remote connections, start the SQL Server Browser service because SQL Servers with default configurations listen on a dedicated port. If the port is already occupied by a program, the SQL Server will choose another port. External programs need to communicate with the SQL Server Browser service to determine the new SQL Server listening port.

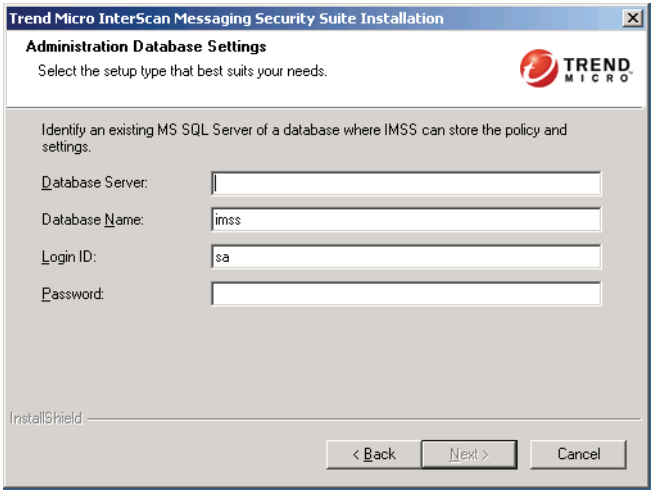
When selecting an external database, a DNS record for the server, where the database resides, must exist in the DNS server. You can specify the IP address or hostname of the server. If the IMSS Setup program cannot query the DNS record of the server where the external database resides, IMSS cannot connect to the external database.

Note: IMSS does not support databases using "Windows Authentication Mode".

a. Select **Use existing database server**.

b. Click **Next**. Type the required information for the existing database server.

Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.



Note: If you have multiple database instances on the target computer, type the IP address or hostname with the instance name.

If you have one database server on the target computer, but the instance name is not the default name, add the instance name after the IP address or hostname.

To install the SQL Server Express database on this server:

Cancelling the installation of SQL Server Express requires some manual cleanup. Certain components cannot be automatically removed:

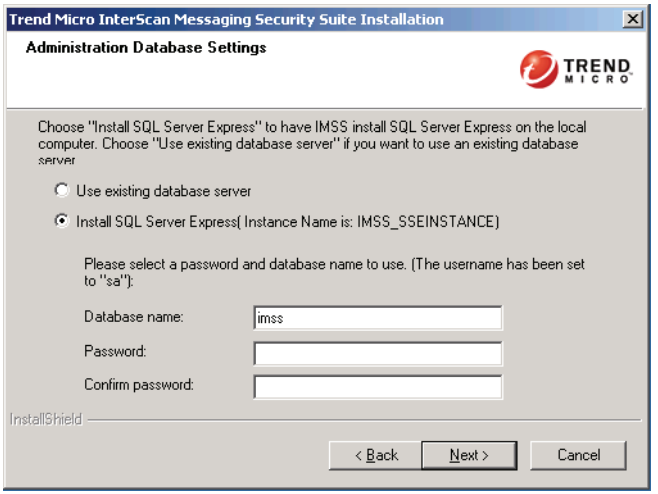
- Microsoft SQL Server Native Client
- Microsoft SQL Server Setup Support Files
- Microsoft SQL Server VSS Writer

When SQL Server Express installs, the database settings are configured for local connections by default. If external connections to the database are required, enable the remote connections of the SQL server.

a. Select **Install SQL Server Express**.

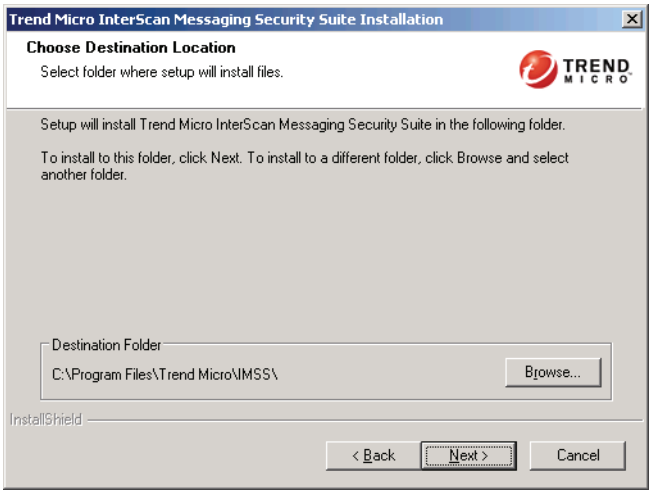
b. Type a **Database name** and **Password** for the "sa" user account.

Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.



The instance of the database that installs is `IMSS_SSEINSTANCE`. When appending a scanner to this IMSS installation, provide the following: `hostname(IP address)\IMSS_SSEINSTANCE`.

9. Click **Next**. The Choose Destination Location screen appears.



10. To change the destination directory, click **Browse** and locate the desired directory.

    On Windows Server 2003 x64 platforms, IMSS 7.1 cannot install in the directory `C:\Program Files\Trend Micro\imss.`

    Only x64 programs can deploy to that directory on Windows Server 2003 x64 platforms.

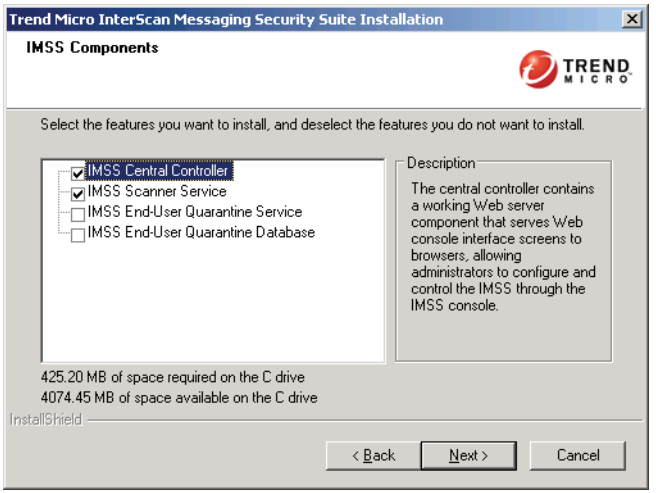
    Install IMSS in the following directory on Windows Server 2003 x64 platforms `C:\Program Files(x86)\Trend Micro\imss.`

WARNING! **Do not install IMSS in a directory that has double-byte characters. IMSS will not function correctly when installed under a directory that uses double-byte characters.**

Do not install IMSS in a directory that has the following feature enabled: "Encrypt contents to secure data". IMSS will not function correctly when installed under a directory that has this feature enabled.

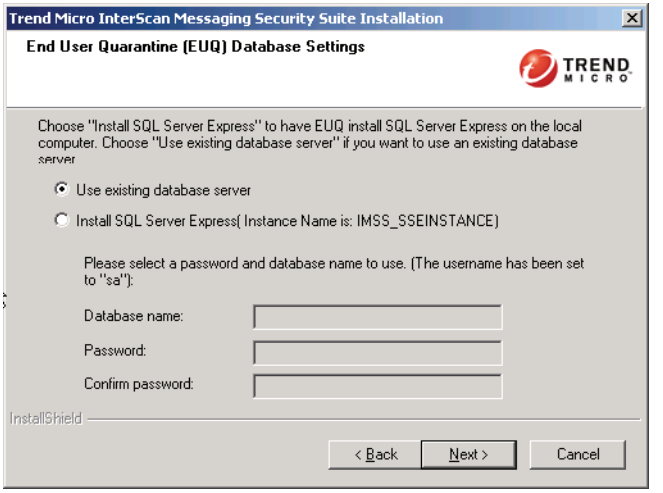
---

11. Click **Next**. The **IMSS Components** screen appears.



12. Select the required components:
    - **IMSS Central Controller:** The Central Controller contains a working Web server component that serves Web console interface screens to browsers. The Web management console allows administrators to configure and control IMSS.
    - **IMSS Scanner Service:** Scanners accept SMTP and POP3 messaging traffic, request policy from a policy server, evaluate the message based on the applicable policies, and take the appropriate action on the message based on the evaluation result.
    - **IMSS End-User Quarantine Service:** The primary EUQ Server hosts a Web-based console similar to the IMSS Web management console so your users can view, delete, or resend spam addressed to them.
    - **IMSS End-User Quarantine Database:** The EUQ database stores quarantined spam email information and the end user approved sender list. If you install EUQ, you must also install the EUQ database (or multiple databases for scalability).

13. Click **Next**. The End-user Quarantine (EUQ) Database Settings screen appears if you have selected the **IMSS End-user Quarantine Database** option.



To use an existing database server:

If an external database is specified, enable the remote connections of the external SQL Server.

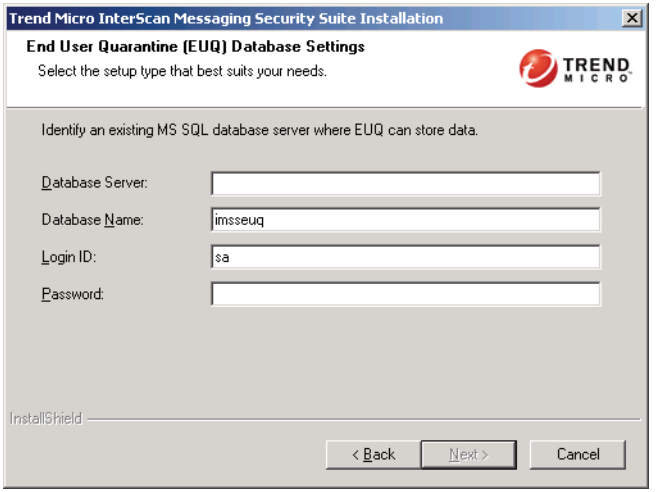
After enabling remote connections, start the SQL Server Browser service because SQL Servers with default configurations listen on a dedicated port. If the port is already occupied by a program, the SQL Server will choose another port. External programs need to communicate with the SQL Server Browser service to determine the new SQL Server listening port.

Note: IMSS does not support databases using "Windows Authentication Mode".

a. Select **Use existing database server**.

b. Click **Next**. Type the information for the existing database server.

Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.



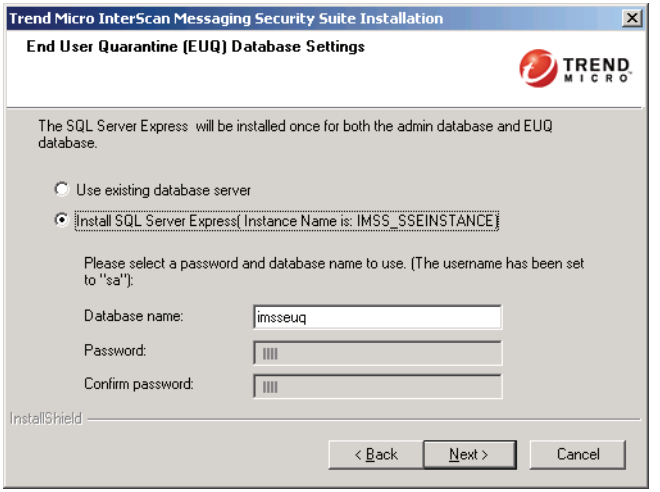
To install an SQL Server Express database on this server:

Cancelling the installation of SQL Server Express requires some manual cleanup. Certain components cannot be automatically removed.

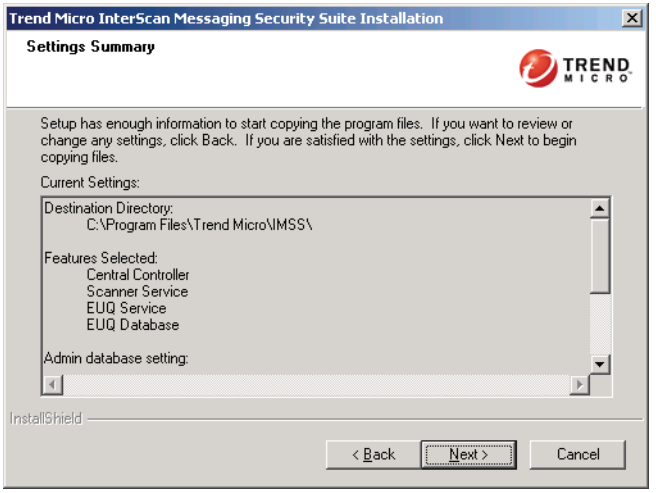
a. Select **Install SQL Server Express.**

b. Type the **EUQ database name** and a **Password** for the SQL Server Express "sa" user account.

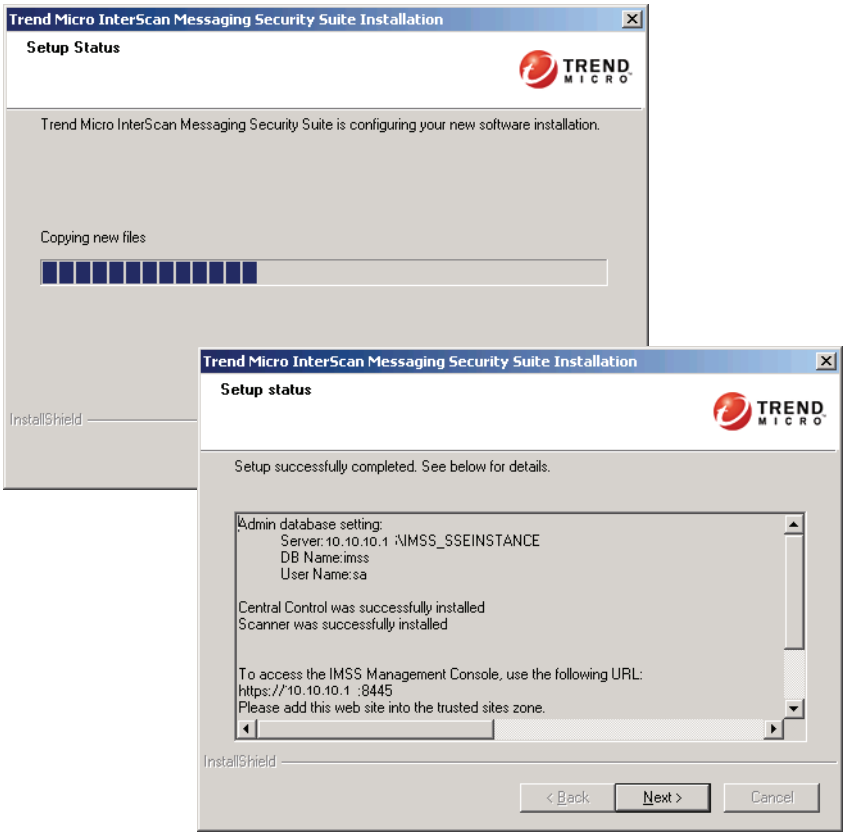
Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.



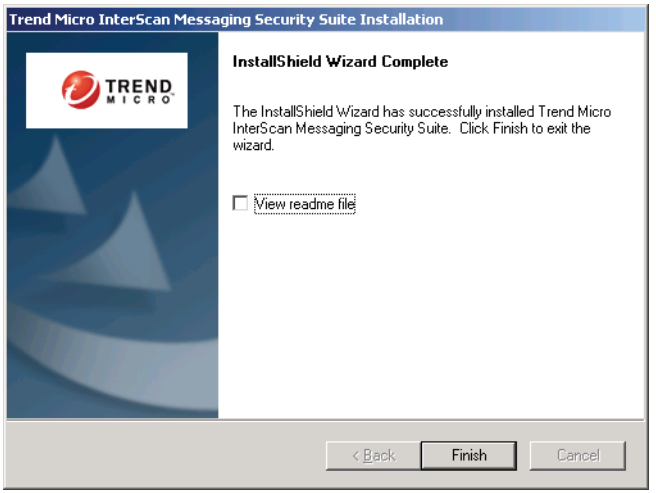
14. Click **Next**. The Settings Summary screen appears. Verify the selected components and the defined settings are correct.



15. Click **Next**. The Setup Status screen appears and installation begins.

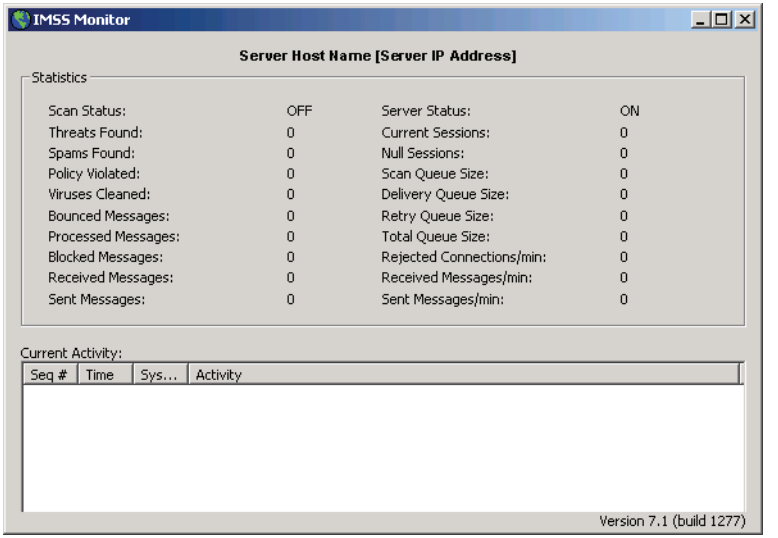


16. Click **Next**. The InstallShield Wizard Complete screen appears.



17. Click **Finish**. The IMSS Monitor appears.

Note: IMSS is a 32-bit program. After installing on a 64-bit operating system, use the commands "perfmon.msc -32" or "mmc /32 perfmon.msc" to start IMSS Monitor.



Multiple Scanner and EUQ Service/Database Installation

This section describes how to install multiple scanner and EUQ services. It also addresses the differences between appending additional components on computers where IMSS components already exist and installing new components on computers where there are no existing IMSS components.

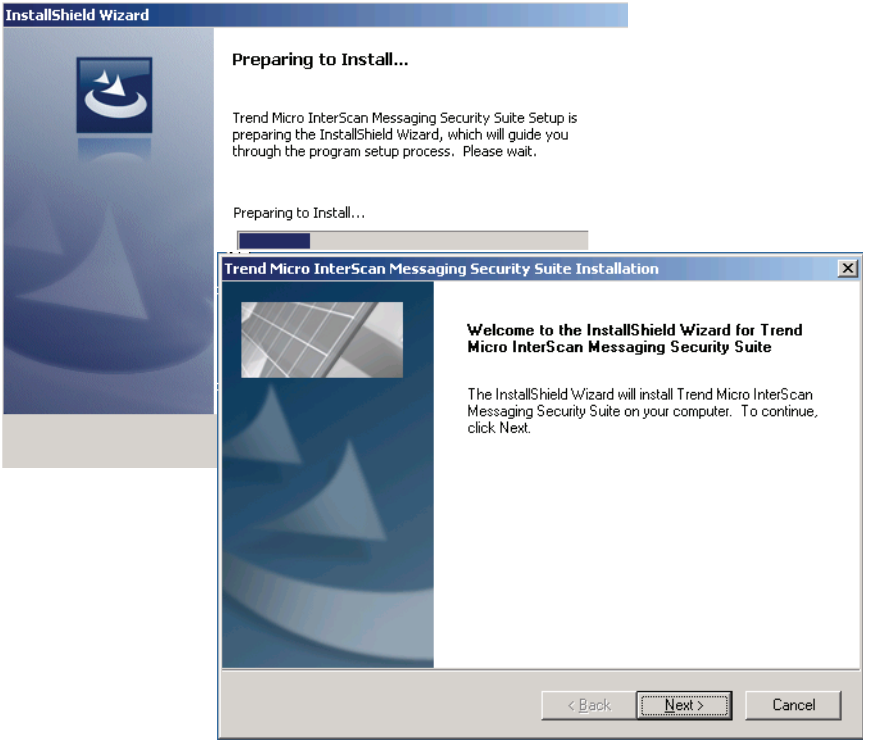
If the installation cannot complete and the message "cannot overwrite xxx.xxx" appears, manually remove all files under the destination folder and retry installation. You might need to stop all running applications under the destination folder. For example, a terminal service instance might be running statmon.exe.

Appending Components When No Previously Installed Components Exist

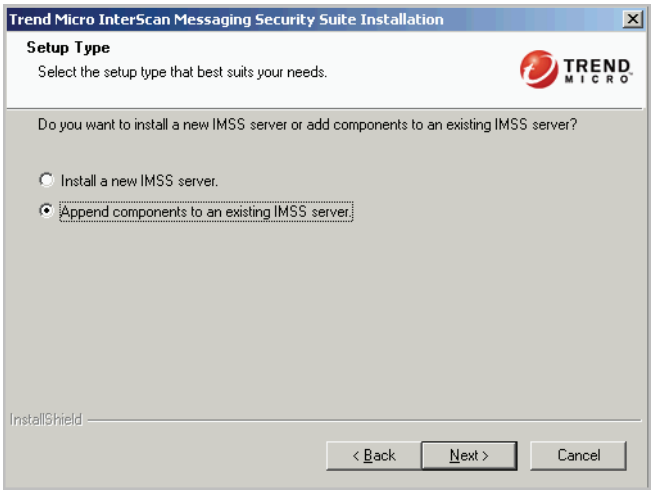
Add IMSS components to servers where no IMSS components existed.

To append a scanner or EUQ service/database on a computer where no previously installed components exist:

1. Double-click on **Setup.exe**. The Preparing to Install... screen appears.

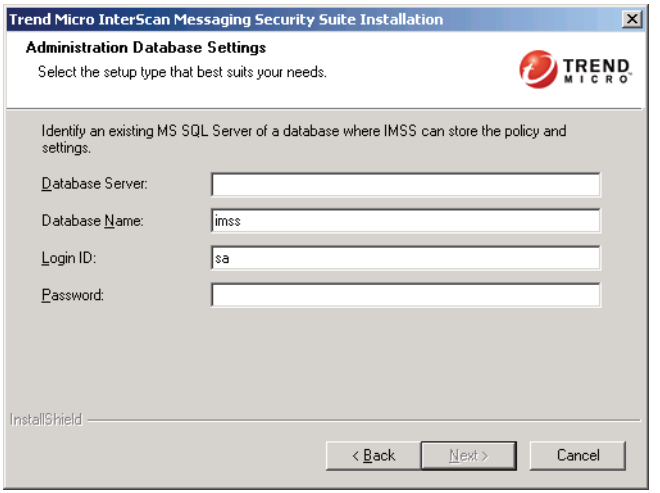


2. Click **Next**. The Setup Type screen appears.



3. Select **Append components to an existing IMSS Server**.

4. Click **Next**. The Administration Database Settings screen appears.

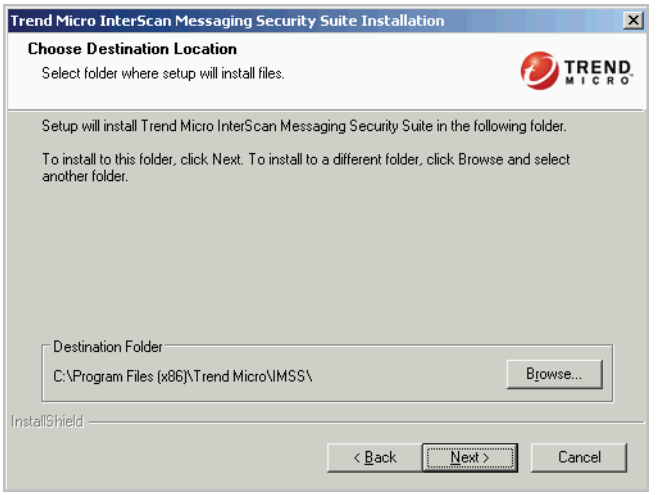


5. Type the required information for the administration database.

   Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.

   When appending a scanner to this IMSS installation and the database was installed from the IMSS installation package, provide the following for Database Server: `hostname(IP address)\IMSS_SSEINSTANCE`.

6. Click **Next**. The Choose Destination Location screen appears.



7. Specify the destination path.

   IMSS 7.1 cannot install on Windows 2003 x64 platforms in the directory `C:\program Files\Trend Micro\imss`.

   Only x64 programs can deploy to that directory on Windows 2003 x64 platforms.

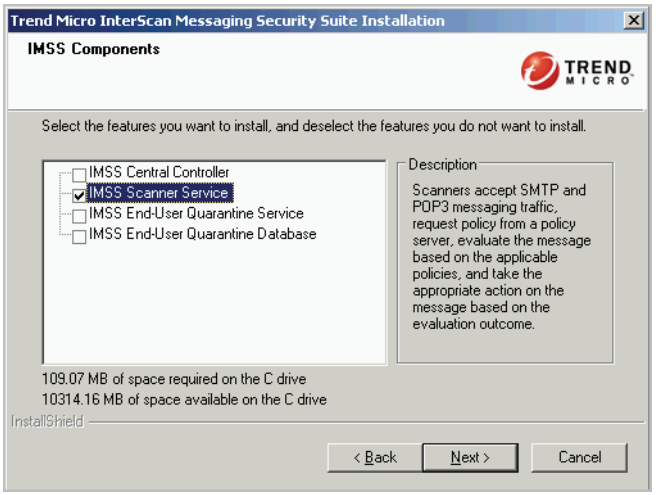
   To install IMSS in the following directory on x64 platforms use `C:\program Files(x86)\Trend Micro\imss`.

WARNING! **Do not install IMSS in a directory that has double-byte characters. IMSS will not function correctly when installed under a directory that uses double-byte characters.**

Do not install IMSS in a directory that has the following feature enabled: "Encrypt contents to secure data". IMSS will not function correctly when installed under a directory that has this feature enabled.

---

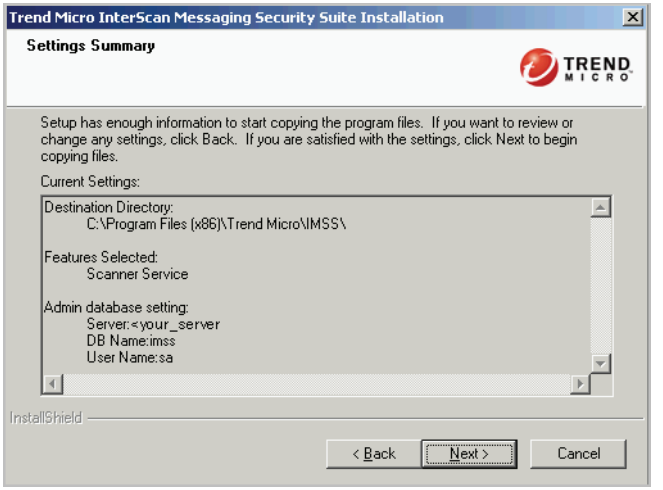
8. Click **Next**. The IMSS components screen appears.



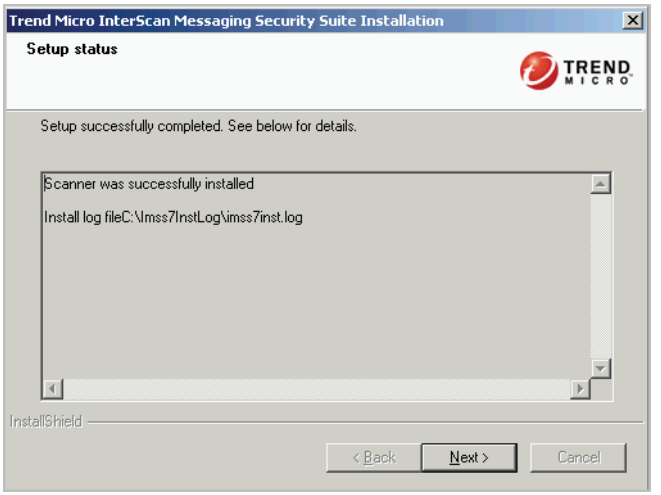
To install additional IMSS Scanner Service:

a. Select the **IMSS Scanner Service** component.

b. Click **Next**. The Settings Summary screen appears.

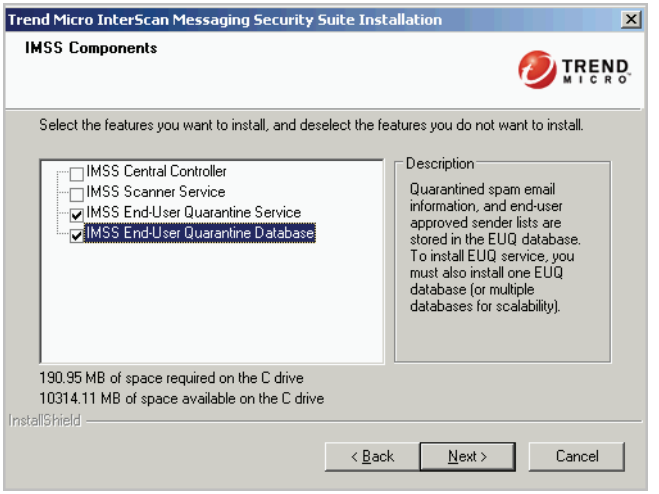


c. Verify the settings and click **Next**. The Setup Status screen appears.



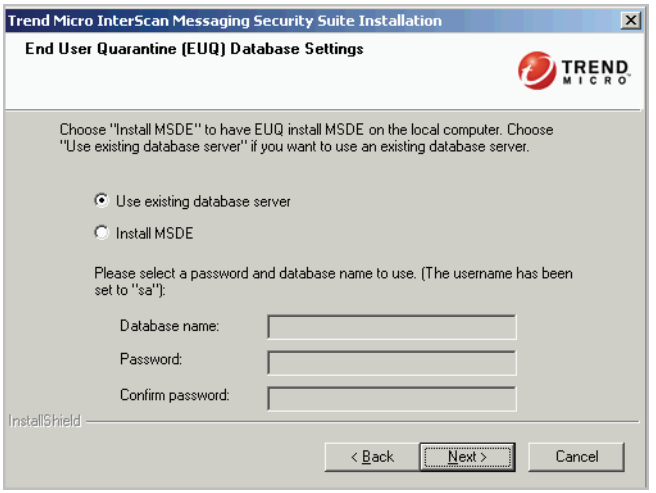
d. Click **Next**. The files install.

To install additional EUQ Service and/or EUQ Database:



a. Select **IMSS End-user Quarantine Service** and/or **IMSS End-user Quarantine Database**.

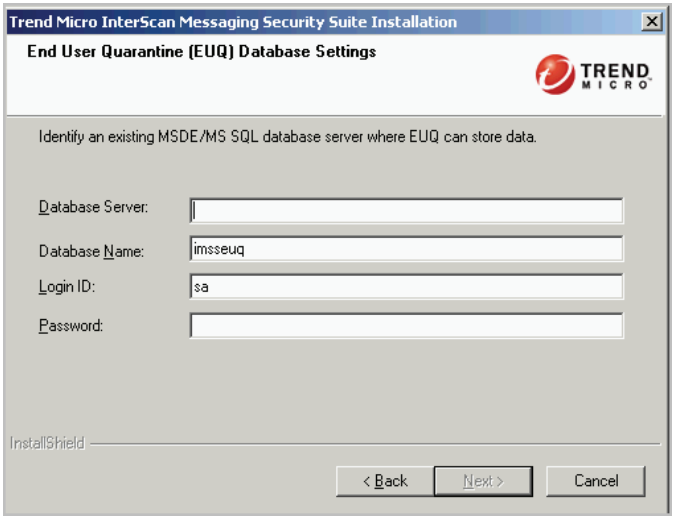
b. Click **Next**. The End-user Quarantine Database Settings screen appears.



To install EUQ database on an existing database server:

i. Select **Use existing database server**.

ii. Click **Next**. The End-user Quarantine Database Settings screen appears.



iii. Type the information for the existing database server.

Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.

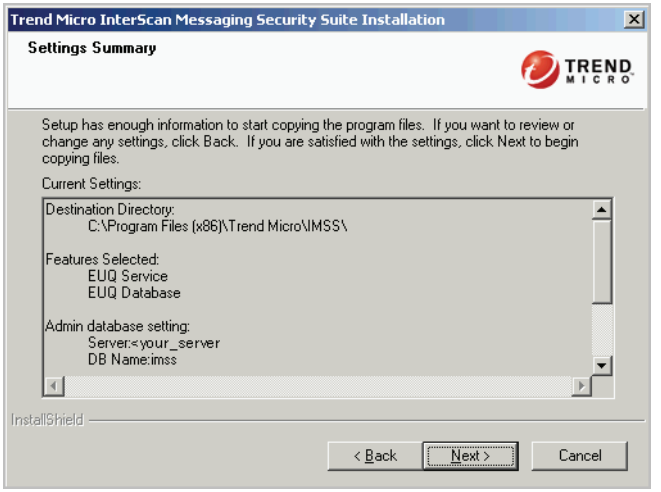
To install an SQL Server Express database on this server:

i. Select **Install SQL Server Express**.

ii. Type the **EUQ database name** and a **Password** for the "sa" user account.

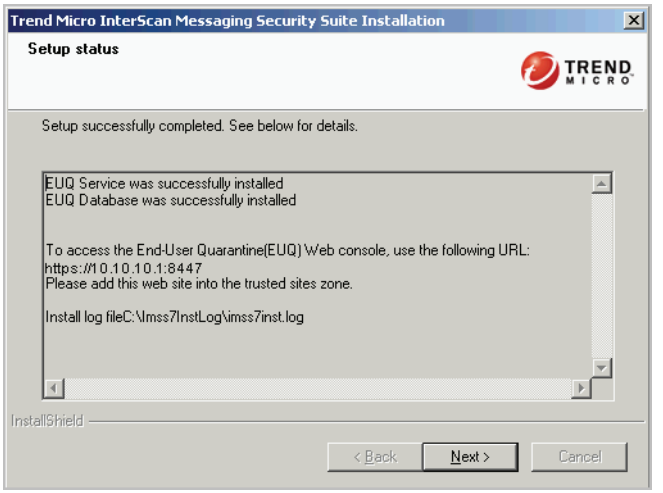
Passwords can contain letters, numbers and the following characters: `~!@#$%^&*()[]{}+-|:'<>?/,.= _.

c. Click **Next**. The Settings Summary screen appears.

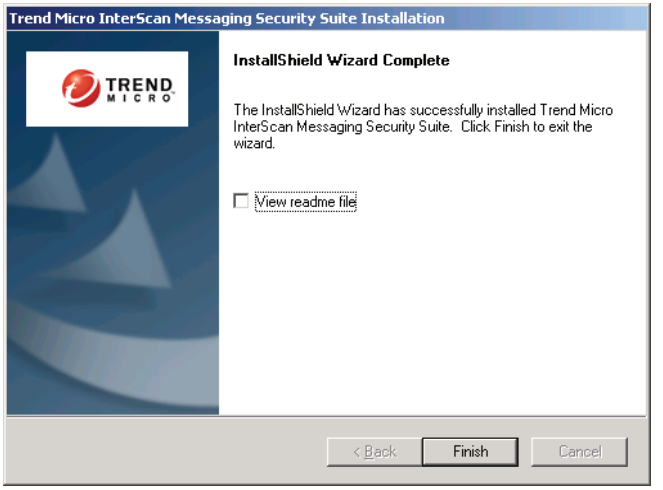


d. Verify the selected components and the defined settings.

e. Click **Next**. The Setup Status screen appears.



9. Click **Next**. The InstallShield Wizard Complete screen appears.



10. Click **Finish**.

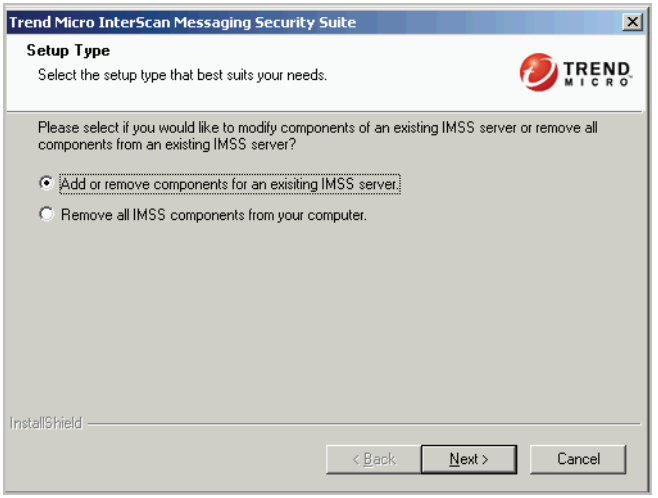
Note: If you have chosen to install additional EUQ database, go to the `$IMSS_HOME\bin\` directory of the Central Controller and run `euqtrans.bat` at the command line to distribute data from the original EUQ databases to all databases.

Appending Components When Previously Installed Components Exist

Add IMSS components to servers that have existing IMSS components.

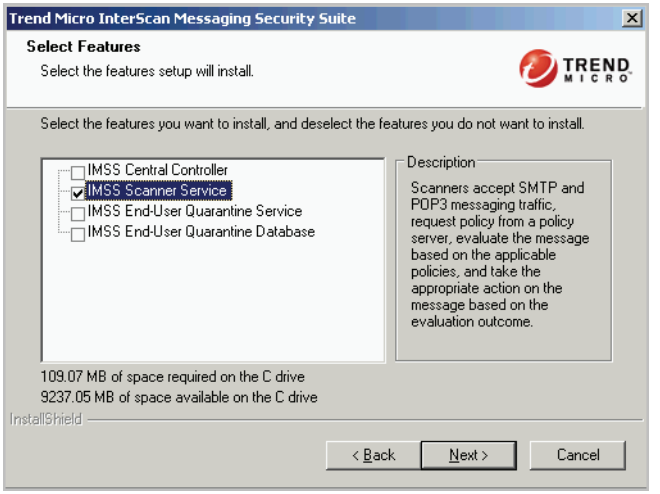
To append a scanner or EUQ service/database on a computer where IMSS components already exist:

1. Double-click **Setup.exe**. The Preparing to Install... screen appears, followed by the Welcome screen.
2. Click **Next**. The Setup Type screen appears.



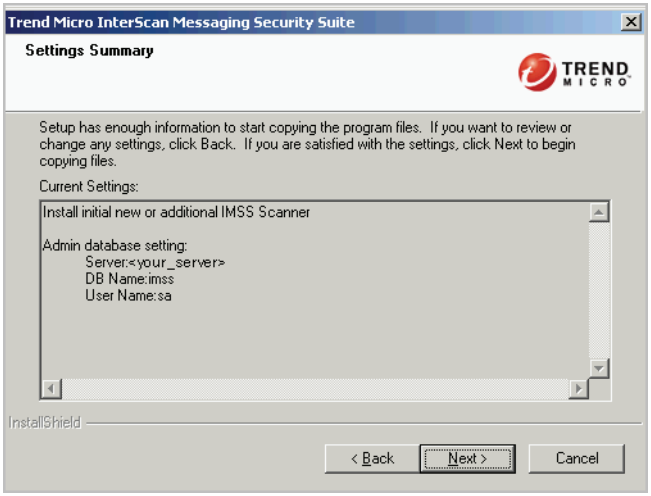
3. Select **Add or remove components for an existing IMSS Server**.

4. Click **Next**. The Select Features screen appears.



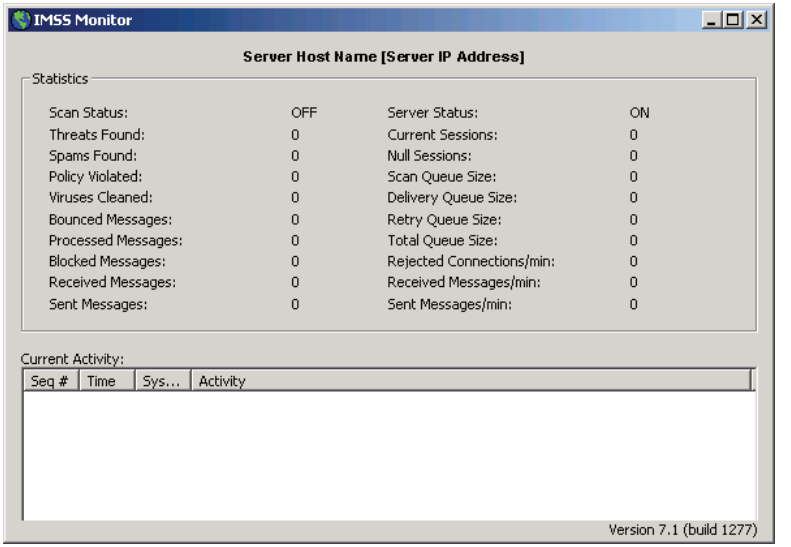
5. Choose the component to add.

6. Click **Next**. The Settings Summary screen appears. If you have chosen to install additional EUQ Service or Database, you will be prompted to provide the EUQ database information before you see the Settings Summary screen.



7. Click **Next**. The Setup Status screen appears.

   After installation, the IMSS Monitor appears.



Complex Distributed Installation

If the installation cannot complete and the message "cannot overwrite xxx.xxx" appears, manually remove all files in the destination folder and retry the installation. You might need to stop all running applications in the destination folder. For example, a terminal service instance might be running `statmon.exe`.

To perform a complex distributed installation, complete the following:

1. Install IMSS on a single server (see Single-Server Installation on page 4-3).
2. Append additional IMSS scanner services, EUQ services or EUQ databases (see Multiple Scanner and EUQ Service/Database Installation on page 4-20) as required.

Silent Installation

Silent installation enables you to install multiple scanners, EUQ services and EUQ databases of the same settings without having to reconfigure the settings manually every time you run `Setup.exe` on other computers.

You can perform silent installation by recording the installation steps in a script and running this script to install additional IMSS components subsequently. Similarly, you can also record uninstallation steps in a script and then run the recorded script to perform silent uninstallation.

Silent installation includes two main steps:

Step 1. Recording the installation steps.

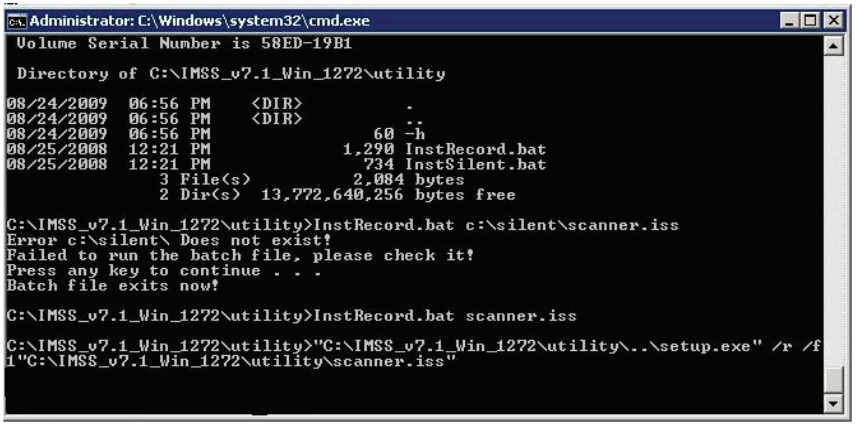
Step 2. Running the script to install additional components.

Recording the Installation Steps

Silent installation records the configuration settings specified during installation.

To record the installation steps:

1. Open a command window and change the directory to the folder where the Setup program is stored.



2. Change to a sub folder called `utility`.
3. Run the `InstRecord.bat` file to record the installation steps in the specified script. For example:

   ```
   InstRecord.bat scanner.iss
   ```

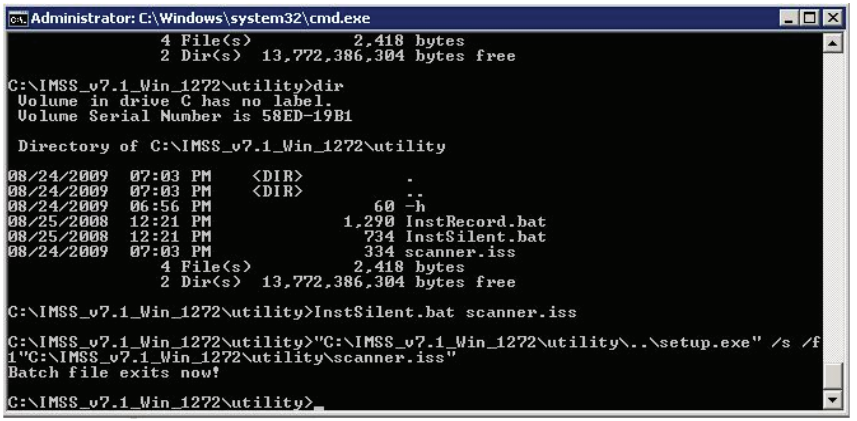
4. Type `setup.exe` to run the Setup program. See Single-Server Installation on page 4-3.

Note: 1. You can specify the path where you want to store the script. However, the path must already exist before you run `InstRecord.bat`.
2. The script file must have an `.iss` extension.
3. If you do not specify the path, the script will be created under the current folder.

Running the Silent Installation Script

To install additional components using the silent installation script:

1. Open a command window and change to the folder where the setup program is stored.



2. Change to a sub folder called `utility`.
3. Run the `InstSilent.bat` file to install components using the silent installation script created earlier. See Recording the Installation Steps on page 4-37. For example:

   ```
   InstSilent.bat scanner.iss
   ```

   The installation proceeds silently in the background without pop-up installation pages.
4. To verify that installation has been completed successfully, click **Summary** > **System** on the Web management console and check the **Managed Server Settings**.

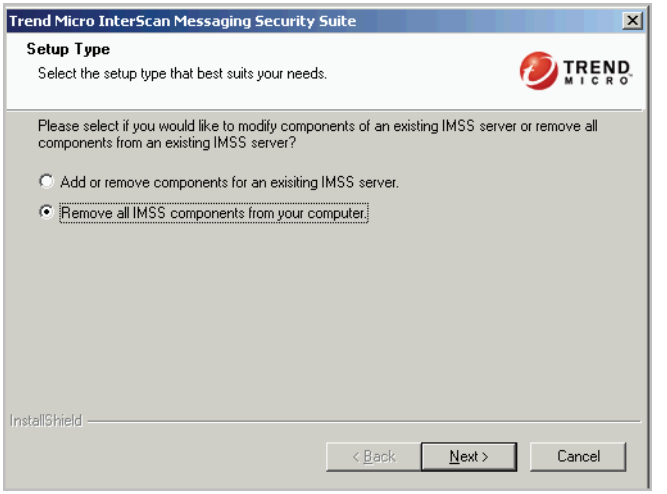
Performing Uninstallation

This section describes how to remove IMSS components.

Uninstalling IMSS Components

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

1. Click **Setup.exe**. The Setup Type screen appears.

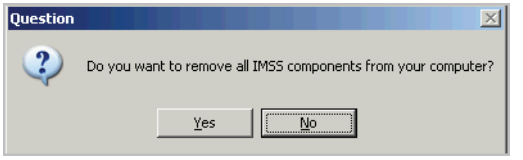


2. Select the components to remove:

   To remove all IMSS components from the computer:

   a. Select **Remove all IMSS components from your computer**.

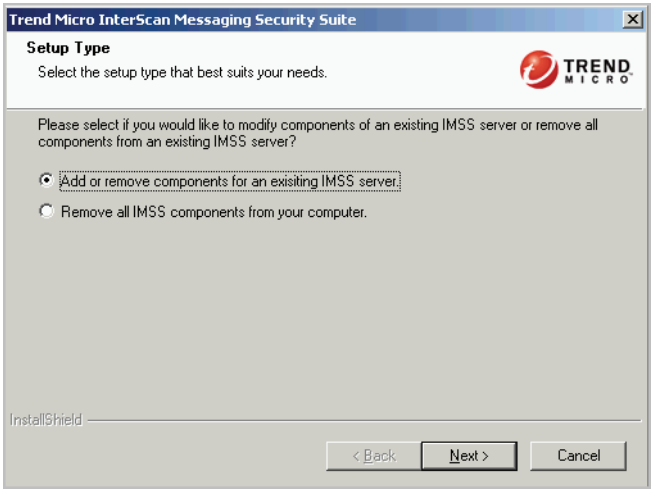
   b. Click **Next**. A confirmation screen appears.



   c. Click **Yes** to confirm.

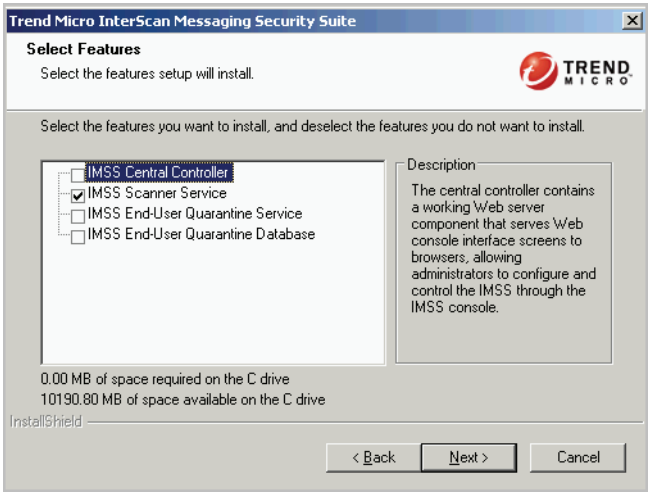
To remove selected IMSS components:

a. To uninstall selected components individually, select **Add or remove components for an existing IMSS server**.

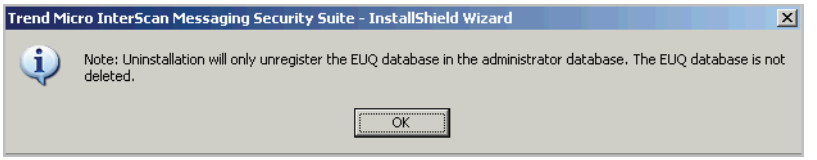


b. Click **Next**. The Select Features screen appears.

c. Clear check box for the component to be uninstalled.



d. Click **Next**. The following message appears if you chose to uninstall the EUQ database.

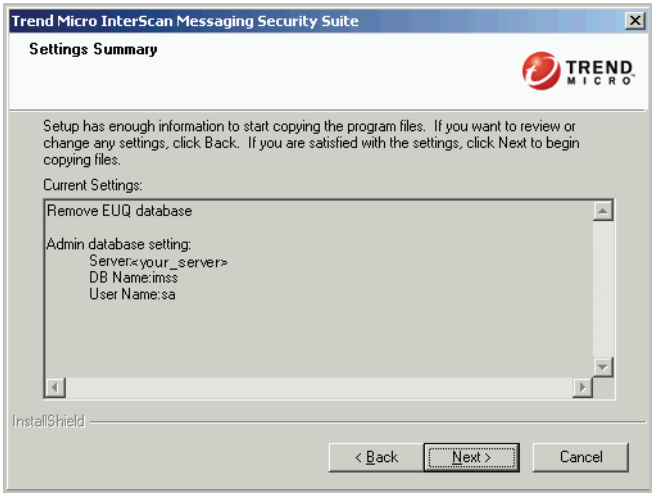


e. Click **OK**.

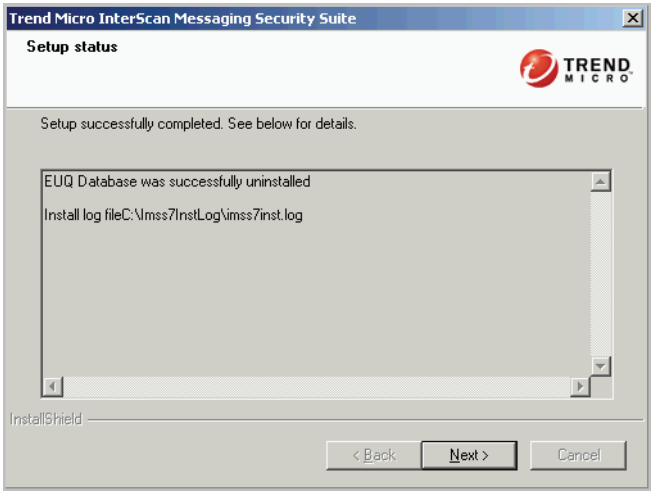
Note: Selecting to uninstall the EUQ Database only unregisters the database from the Admin database. After removing all other components, manually remove the EUQ database.

---

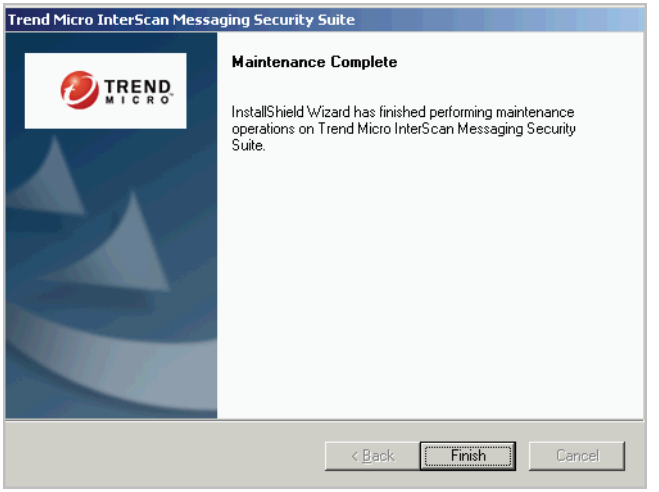
3. Click **Next**. The Settings Summary screen appears.



4. Click **Next**. The component uninstalls. The Setup Status screen appears.



5. Click **Next**. The Maintenance Complete screen appears.



6. Click **Finish**.

Silent Uninstallation

The steps for silent uninstallation are similar to the steps in Silent Installation on page 4-37.

Note: Run the silent uninstallation on the computer that has a similar environment as the computer where you recorded the silent installation script.
Close all Microsoft Management Console screens when you record the silent installation script or execute a silent installation.

Chapter 5

Upgrading from Previous Versions

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

Topics include:

Upgrading from an Evaluation Version

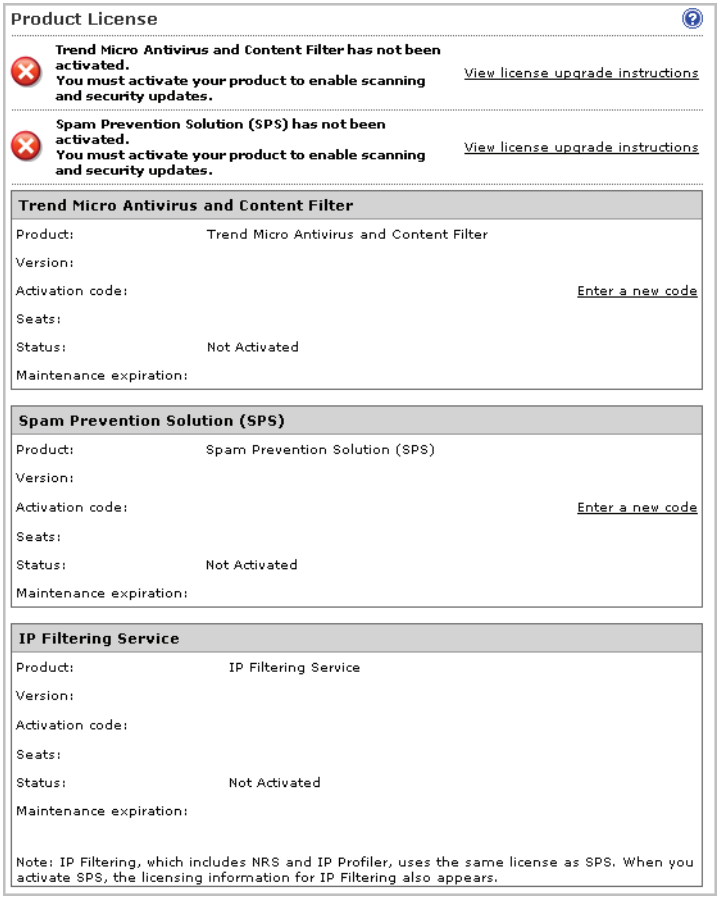
If you provided an evaluation Activation Code to activate IMSS previously, you have started an evaluation period that allows you to try the full functionality of the product. The evaluation period varies depending on the type of Activation Code used.

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

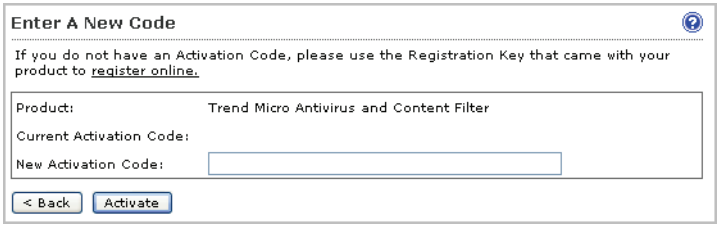
To continue using IMSS, purchase the full version license for the product. You will then be provided a new Activation Code.

To upgrade from the evaluation period:

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



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



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

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

4. Click **Activate**.

Upgrading from Version 5.7 to Version 7.1

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

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

WARNING! **1. The Setup program does not support automatic rollback to IMSS 5.7. If the installation encounters issues, a manual rollback is the only option. See** Rolling Back the Upgrade on page 5-43 **for more information.**

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

IMSS 5.7 Upgrade Considerations

Consider the following before migrating or installing over IMSS 5.7:

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

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

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

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

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

Upgrading IMSS 5.7: Policy Recommendations

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

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

Removing Unused Policy Objects

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

TABLE 5-1. Unused Policy Objects to Remove

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

Merging Policy Objects

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

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

Modifying Policy Objects

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

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

Upgrading IMSS 5.7: Process Recommendations

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

Perform a Fresh Installation of IMSS 7.1

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

Tip: 1. Prepare the system environment according to Trend Micro recommended system requirements. See System Requirements on page 4-2 for more information.

2. Carefully plan your deployment strategy for IMSS 7.1.

Become Familiar with IMSS 7.1 Before Upgrading

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

Tip: 1. Study the Administrator's Guide.

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

General IMSS 5.7 Migration Tasks

Perform the following tasks to simplify migration:

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

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

Verify IMSS 7.1 Operation after Migration

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

- Open the Summary screen to verify all services can start successfully.

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

IMSS 5.7 Settings that Cannot be Migrated

Certain IMSS 5.7 settings cannot migrate to IMSS 7.1:

TABLE 5-2. IMSS 5.7 Settings that cannot migrate

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

TABLE 5-2. IMSS 5.7 Settings that cannot migrate (Continued)

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

TABLE 5-2. IMSS 5.7 Settings that cannot migrate (Continued)

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

IMSS 5.7 Settings that Change After Migration

Certain IMSS 5.7 settings change after migrating to IMSS 7.1:

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

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

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

SETTING	SETTINGS THAT CHANGE
Configuration Settings	Maximum log file size: If the minimum log size is less than 100MB, migration changes this setting to 100MB. If the maximum log size exceeds 99999MB, migration changes this setting to 99999MB. Specifying "0" (meaning there is no limit to the log file size) is no longer supported. The maximum value is specified.
	Number of days to keep log: If IMSS 5.7 settings specify keeping logs less than 150 days, migration changes the setting to 150 days. Specifying "0" (meaning there is no limit to the length of time to keep files) is no longer supported. The maximum value is specified.
	Notifications: If the SMTP server setting specifies "default", migration changes the value to "127.0.0.1".
NRS	NRS in IMSS 5.7 supports an approved list and a block list. In IMSS 7.1, IP Filtering contains the components: Email reputation (NRS) and IP Profiler. The block list for IMSS 5.7 migrates and works correctly when IP Profiler is enabled. However, during migration from IMSS 5.7 to IMSS 7.1, IP Profiler is disabled by default. This means the NRS block list will not work because IP Profiler is disabled.

Upgrade Options for Multiple Scanner Deployment

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

Single Admin Database

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

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

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

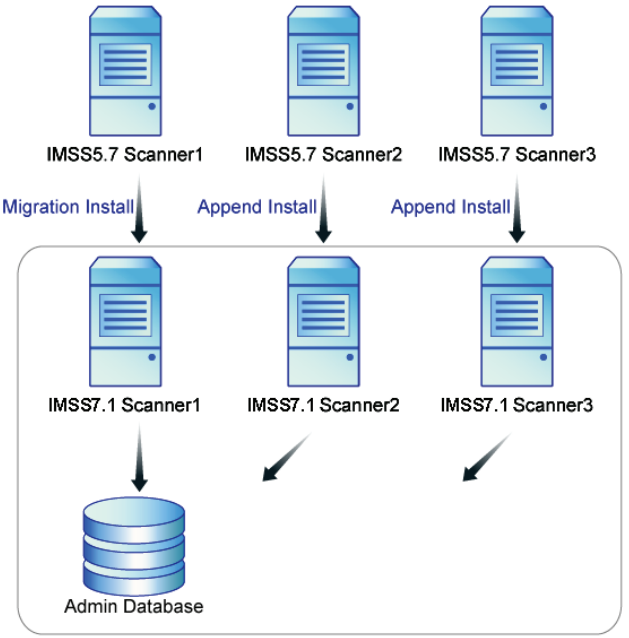


FIGURE 5-1. Single Admin database

Multiple Admin Databases

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

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

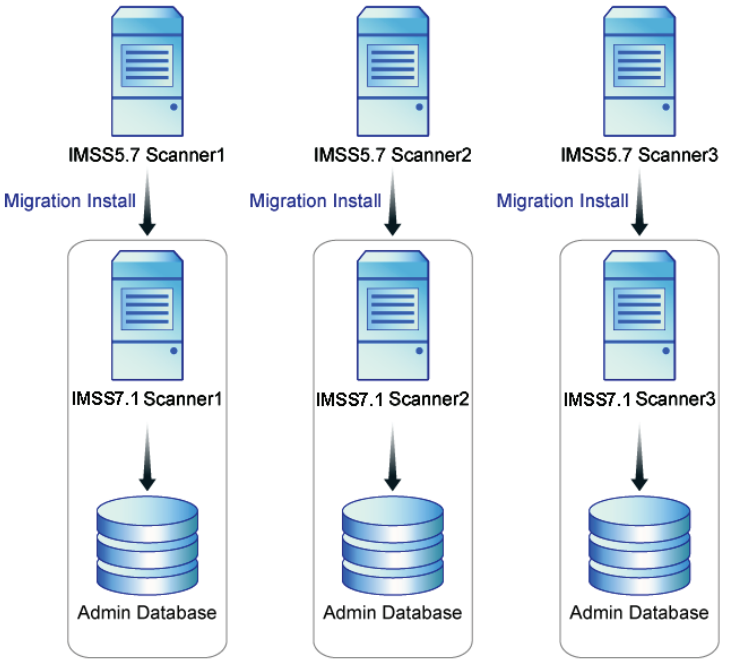


FIGURE 5-2. Multiple Admin databases

Backing Up IMSS 5.7 Settings

See the following sections:

- Backing up IMSS 5.7 Data for a Single-server Deployment on page 5-17
- Backing up IMSS 5.7 Data for a Distributed Deployment on page 5-19

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

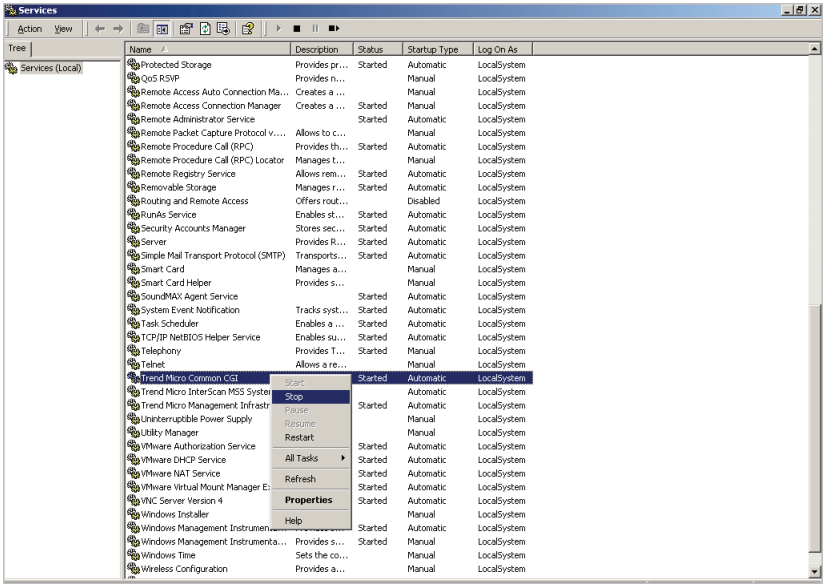
Backing up IMSS 5.7 Data for a Single-server Deployment

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

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

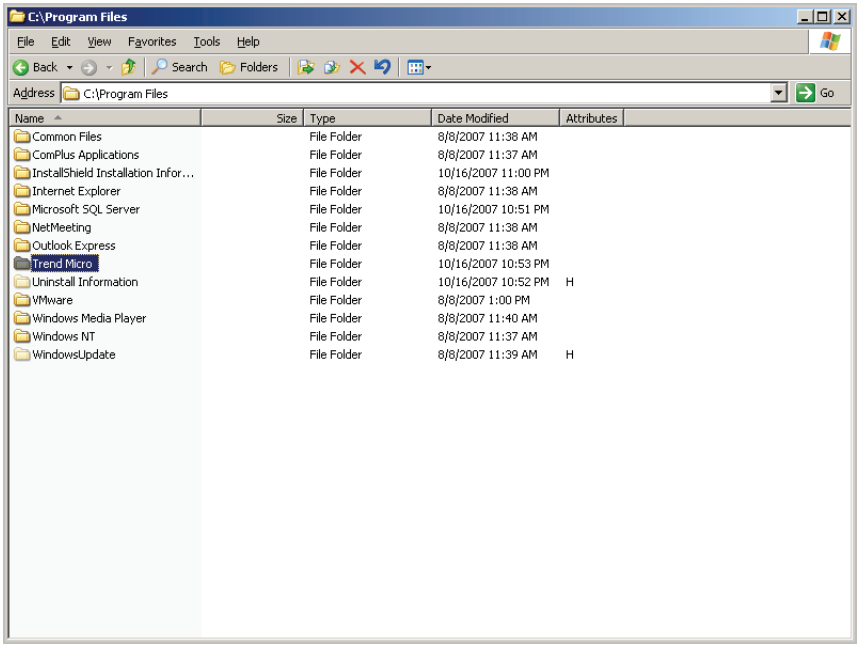
To back up IMSS 5.7 data:

1. Stop all IMSS 5.7 services from the Microsoft Management Console.

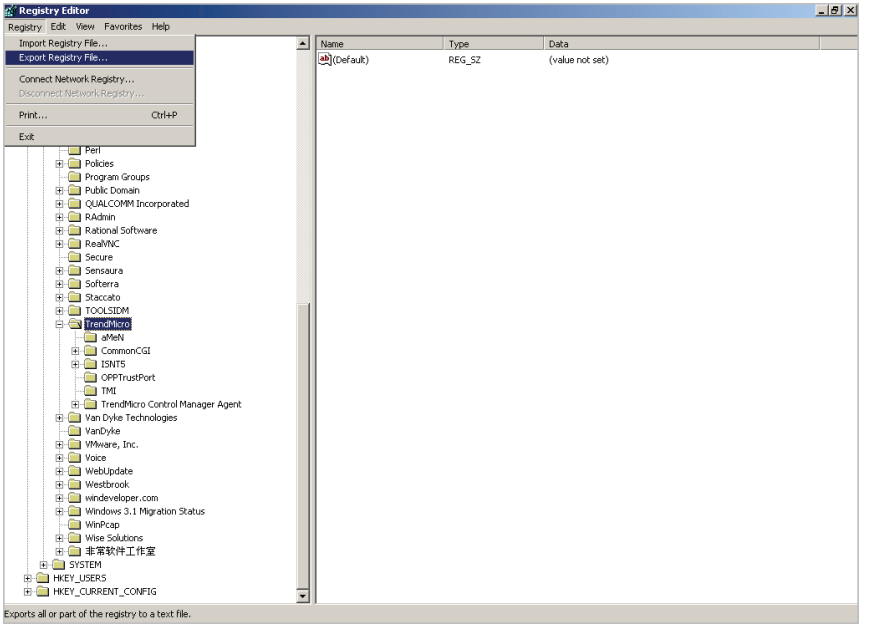


2. Back up IMSS on the database server using the Microsoft SQL management tool.
3. Stop the database service from the Microsoft Management Console.
4. Stop IIS services from the Microsoft Management Console.

5. Back up the installation folder of IMSS 5.7.



6. Export the policy settings from the registry:
   HKEY_LOCAL_MACHINE>SOFTWARE>TrendMicro



Backing up IMSS 5.7 Data for a Distributed Deployment

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

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

To back up IMSS 5.7 data for a distributed deployment:

On Server 1:

1. Stop all IMSS 5.7 services from the Microsoft Management Console.
2. Stop IIS services from the Microsoft Management Console.

3. Back up the IMSS 5.7 installation folder.
4. Export IMSS 5.7 policy settings from the registry:

   `HKEY_LOCAL_MACHINE>SOFTWARE>TrendMicro`

On Server 2:

1. Back up the IMSS database on the server hosting the IMSS database, using the Microsoft SQL Management tool.
2. Stop the database service.

On Server 3:

1. Stop all IMSS 5.7 services from the Microsoft Management Console.
2. Stop the IIS Admin Service from the Microsoft Management Console.
3. Back up the installation folder of IMSS 5.7.

Migrating from IMSS 5.7 to IMSS 7.1

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

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

The migration process requires the following tasks:

Step 1. Exporting IMSS 5.7 settings

Step 2. Importing IMSS 5.7 settings to IMSS 7.1

Exporting IMSS 5.7 Settings

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

You can obtain the latest migration tool at:

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

WARNING! **If you are exporting the configuration settings from InterScan Messaging Security Suite 5.7 Windows version and it contains Double Byte Character Settings (DBCS), please make sure that the locale of the Windows is also in DBCS. Otherwise, the DBCS setting will not be migrated correctly.**

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

1. Clean up IMSS 5.7 configuration settings. See Upgrading IMSS 5.7: Policy Recommendations on page 5-6 and Upgrading IMSS 5.7: Process Recommendations on page 5-7 for detailed information.
2. Copy `migration_tool_57to71.zip` to a directory on the IMSS 5.7 server.
3. Extract the Export Tool.
4. Change the name of the directory where the tool extracts to the following:

   `migration_tool_57to71`
5. Run the script `export_tool_57.bat` to export the configuration settings from IMSS 5.7.

Importing IMSS 5.7 Settings to IMSS 7.1

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

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

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

To migrate settings from IMSS 5.7 to IMSS 7.1:

1. Install IMSS 7.1 on a server. See Single-Server Installation on page 4-3 or Complex Distributed Installation on page 4-36 for more information.
2. Use the IMSS 5.7 Export Tool to obtain the IMSS 5.7 migration package.
3. Extract the migration_tool_57to71.zip on the server where the IMSS 7.1 Central Controller is installed.
4. Change the name of the directory where the tool extracts to the following:

   `migration_tool_57to71`
5. Retrieve the IMSS 5.7 migration package from the `migration_tool_57to71` directory on the IMSS 5.7 server.
6. Put the migration package on the server, where the IMSS 7.1 Central Controller is installed, at the following location:

   `migration_tool_57to71`

   Note: Read the Migration Tool's scope and limitations carefully before continuing.
7. Launch `migration_tool_57.bat`.
8. Follow the instructions that display to use the Migration Tool.

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

   `C:\Imss7InstLog\migrationfrom57\MigrationReport` and `C:\Imss7InstLog\migrationfrom57` with the logs formatted as `migration_57.yyyymmdd.log`
9. Perform the following post-migration tasks to verify the results of the migration:
   a. Check for items that did not migrate. Add missing items manually to IMSS 7.1.
   b. Check the results for migrated items. This helps to gain a basic understanding about the mapping relationship between IMSS 5.7 filters and IMSS 7.1 rules.
   c. Verify that all services can be started, especially the policy server.
   d. Verify that all policies can be accessed on the Web console.

Installing IMSS 7.1 Over IMSS 5.7

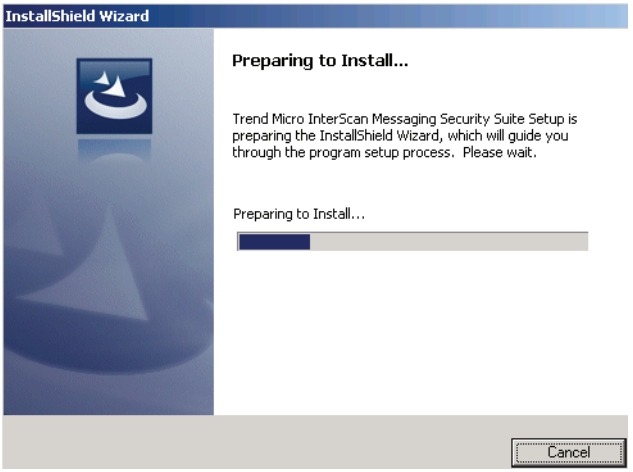
Installing IMSS 7.1 over an installation of IMSS 5.7 requires IMSS 5.7 with patch 4 installed.

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

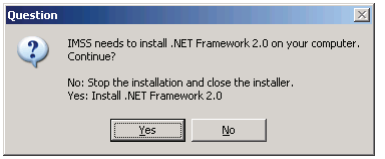
The Setup program does not unregister the current IMSS server from Control Manager. That means that all logs from the old server can still be queried by Control Manager.

To upgrade to IMSS 7.1:

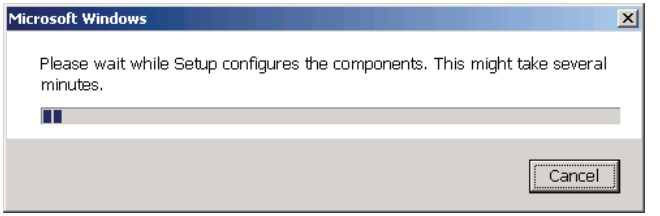
1. Double-click **Setup.exe**, on the IMSS 5.7 server. The Preparing to Install... screen appears.



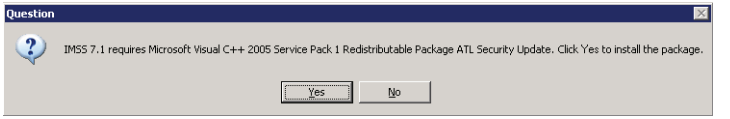
If Microsoft .NET Framework 2.0 has not been installed on the server, a dialog box appears.



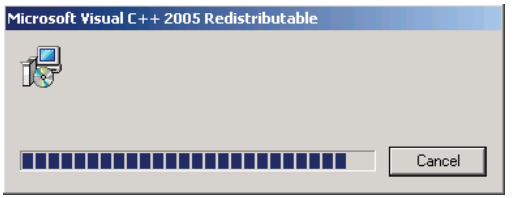
2. Click **Yes**. Installation of Microsoft .NET Framework 2.0 begins.

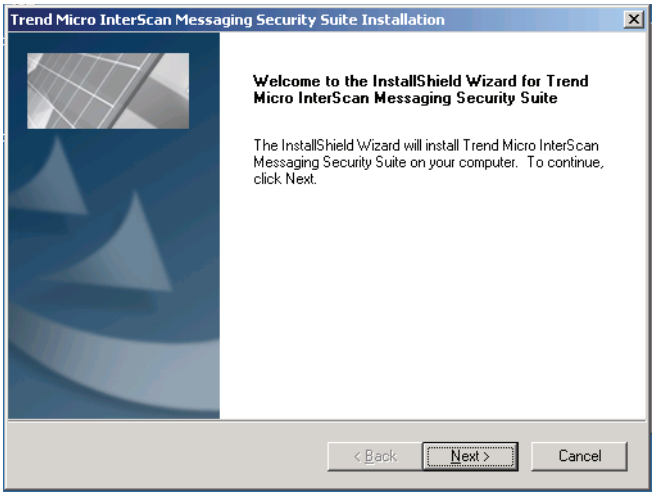


If Microsoft Visual C++ 2005 is not installed, a dialog box appears.

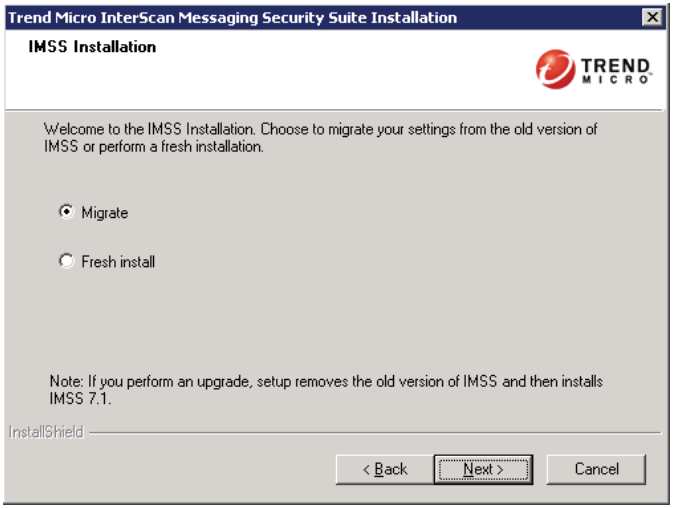


3. Click **Yes**. Microsoft Visual C 2005 installation begins.





4. Click **Next**. The Migrate option appears if the installation package detects IMSS 5.7.

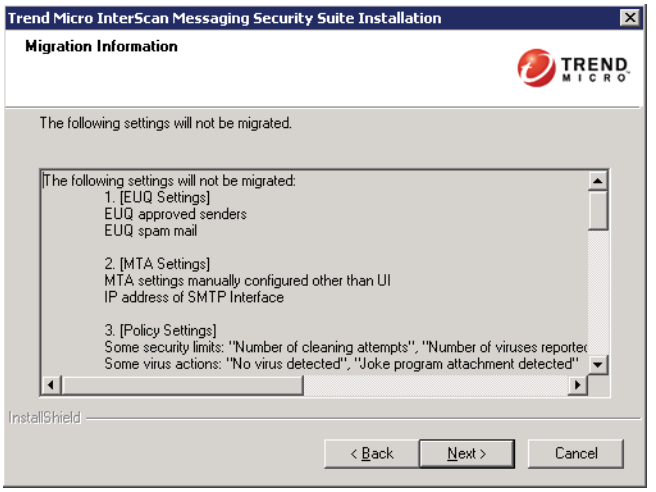


If you select **Migrate**, the Setup program installs IMSS 7.1 over the IMSS 5.7 installation.

If you select **Fresh Install**, the Setup program uninstalls IMSS 5.7, and then installs IMSS 7.1.

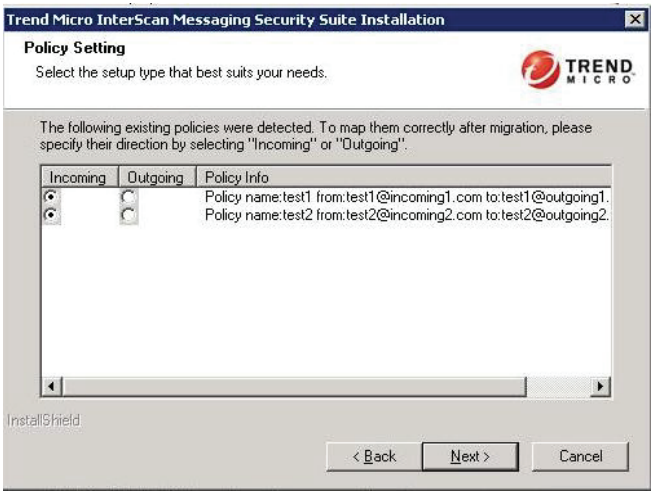
5. Select **Migrate**.

6. Click **Next**. The Migration Information screen appears.

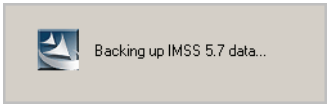


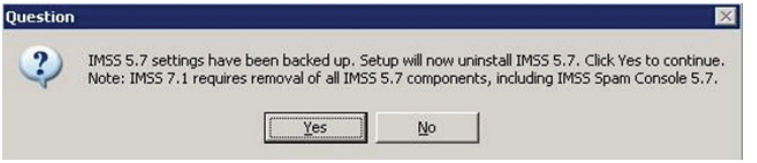
Note: All settings that will not migrate display in this screen. You can also check these settings from `C:\Imss7InstLog\migrationfrom57\MigrationReport\GeneralReport.txt`.

7. Click **Next**. The Policy Setting screen appears if you have policies with special routes in IMSS 5.7.

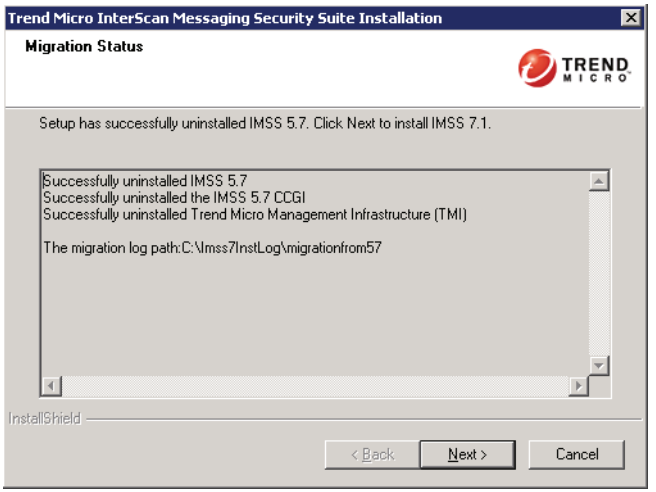


8. Select the policy directions by clicking **Incoming** or **Outgoing**.
9. Click **Next**. Migration data backs up and a setup confirmation screen appears.





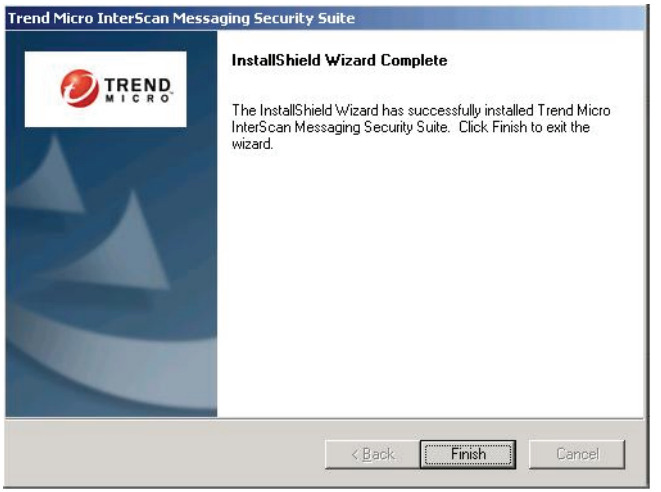
10. Click **Yes**. IMSS 5.7 uninstalls.



11. Click **Next**. Configure and install IMSS 7.1 (as in Single-Server Installation on page 4-3). As installation completes, the Setup program imports IMSS 5.7 data to IMSS 7.1.

The Migration Results screen appears.

12. Click **Next**. The Installation Complete screen appears.



13. Click **Finish** to complete the upgrade.

Note: After upgrading, IMSS detects invalid x-filter rules and saves the result to `C:\Imss7InstLog\migrationfrom57\InvalidRule.txt`. IMSS 5.7 accepts expressions preceded by an asterisk, such as `*aaabbb`, but IMSS 7.1 cannot accept such expressions. To avoid syntax errors, replace the asterisks with "*" or ".*".

Installing Over IMSS 5.7 Encounters Issues

During installation the Setup program attempts to perform an automatic migration of IMSS 5.7 settings to IMSS 7.1. The Setup program saves IMSS 5.7 settings in the following folder:

```
%SYSTEM DIS%/Imss7InstLog/migrationfrom57/
```

If an issue occurs during the installation the Setup program launchs a pop up message. The message may prompt a manual migration of IMSS 5.7 settings to IMSS 7.1.

To perform a manual migration of IMSS 5.7 settings, if automatic migration is unsuccessful:

1. Verify that the following folder exists and that it contains the IMSS 5.7 settings data:

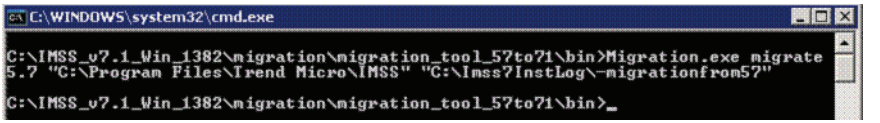
   `%SYSTEM DIS%/Imss7InstLog/migrationfrom57/`

2. Manually migrate IMSS 5.7 settings using the migration tool `migration_tool_57to71.zip`.

   Tip: While the migration tool is located in the IMSS 7.1 installation package (`migration\migration_tool_57to71.zip`), Trend Micro recommends downloading the latest migration tool from the Trend Micro website: http://www.trendmicro.com/download/

3. Use the command line console to run the migration tool from the `bin` subdirectory using the command:

   ```
   migrate.exe migrate <old imss version>  "<IMSS HOME>"
   "<Backup path>"
   ```



4. Use the migration report log to check the migration details:

   `C:\Imss7InstLog\migrationfrom57\MigrationReport\`

Upgrading from IMSS 7.0 to IMSS 7.1

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

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

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

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

Migrating or Installing Over IMSS 7.0

Consider the following before migrating or installing over IMSS 7.0:

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

IMSS 7.1 Settings That Cannot be Migrated

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

Backing Up IMSS 7.0 Settings

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

Backing Up Configuration Settings

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

You can also manually back up the contents of the `C:\Program Files\Trend Micro\IMSS\config` folder.

Backing Up IMSS 7.0 Databases

The IMSS 7.1 Setup program does not perform a full Admin database backup, and does not support backup for the EUQ database.

When installing IMSS 7.1 over an existing IMSS 7.0 installation:

1. The IMSS 7.1 Setup program upgrades MSDE to SQL Server Express 2005, if it detects that MSDE was installed by IMSS 7.0. A message appears displaying the database list for the MSDE server.
2. The IMSS 7.1 Setup program needs to upgrade the Admin database, if the IMSS 7.1 Central Controller is installed.

Tip: Trend Micro recommends performing a full manual backup of the following databases to prevent data loss if an error occurs during installation.

- Admin database before upgrading the Central Controller

- Any databases in the MSDE server, if MSDE is installed with IMSS 7.0.

Before copying the database's data and log files, verify the following:

- The database is not currently in use
- There are no remote connections to the database

If the database's data and logs cannot be copied, after verifying the above, stop the database service from the Microsoft Management Console and try again.

To determine the location of the database's data and log files using osql.exe or sqlcmd.exe:

`osql.exe` and `sqlcmd.exe` can be found in the SQL Server's installation path, under the `Tools\bin` folder.

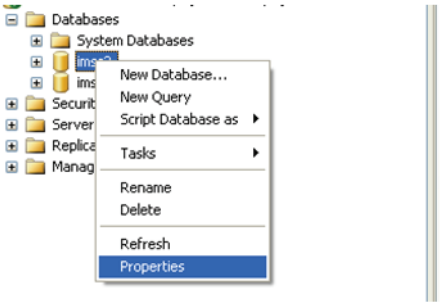
1. Open the command line interface, and change the directory to the location for `osql.exe` or `sqlcmd.exe`.
2. Connect to the database server using the following command:
   - For `osql.exe`:
     ```
     osql -S database server -U user name -P password
     ```
   - For `sqlcmd.exe`:
     ```
     sqlcmd -S database server -U user name -P password
     ```
3. Specify a database to back up. When successfully connected to the database server, the SQL command line console appears.
4. Type the following SQL command in the SQL command line console:
   ```
   SELECT filename FROM database name.dbo.sysfiles
   ```
5. Press `Enter`, and type `GO` to execute the command. Wait for its completion.

   The query will return results similar to the following:
   - Data file: `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\imss.mdf`
   - Log file: `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\imss_log.ldf`
6. Copy these files to the directory designated to backup the IMSS database.

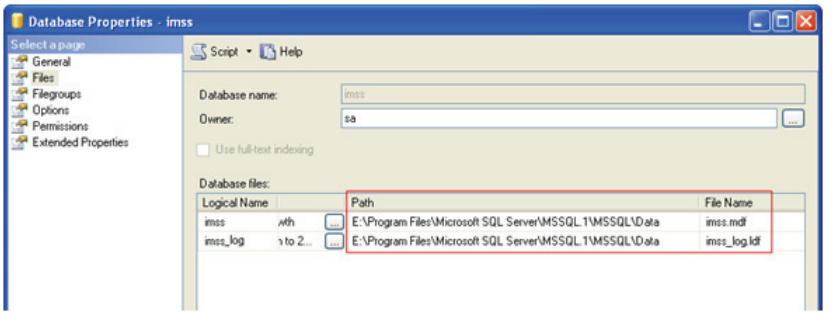
To determine the location of the database's data and log files using SQL Server Management Studio Express:

1. Log on to the database server.
2. Select the database from the list of databases.

3. Right-click the selected database. A pop up menu appears.



4. Select **Properties** from the pop up menu. A dialog box appears.
5. Click **Files** from the Select a page list. The right hand pane changes to display a table.



6. Move the horizontal bar until the **Path** column appears.
7. Copy these files to the directory designated to backup the IMSS database.

Upgrading an IMSS 7.0 Single Server Deployment

Upgrading a single server deployment is very similar to upgrading a distributed deployment. Install over the previous installation or perform a fresh installation of IMSS 7.1 and migrate all settings.

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

Upgrading an IMSS 7.0 Distributed Deployment

Upgrading a distributed deployment is very similar to upgrading a single server deployment. Install over the previous Central Controller installation or perform a fresh installation of the IMSS 7.1 Central Controller and migrate all settings.

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

Migrating from IMSS 7.0 to IMSS 7.1

The migration process requires the following tasks:

Step 1. Exporting IMSS 7.0 settings

Step 2. Importing IMSS 7.0 settings to IMSS 7.1

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

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

Exporting IMSS 7.0 Settings

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

You can obtain the latest migration tool at:

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

To export IMSS 7.0 configuration settings:

1. Copy `migration_tool_70to71.zip` to the IMSS 7.0 server.
2. Extract the Export Tool.

3. Change the name of the directory where the tool extracts to the following:

   `migration_tool_70to71`

4. Run the script `export_tool_70.bat` to export the configuration settings from IMSS 7.0.

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

Importing IMSS 7.0 Settings to IMSS 7.1

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

WARNING! During migration do not perform any database operations.

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

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

To migrate settings from IMSS 7.0 to IMSS 7.1:

1. Install IMSS 7.1 on a server. See Single-Server Installation on page 4-3 or Complex Distributed Installation on page 4-36 for more information.
2. For distributed deployments, stop all IMSS remote services manually before migrating settings.
3. Extract `migration_tool_70to71.zip` on the server where the IMSS 7.1 Central Controller is installed.
4. Change the name of the directory where the tool extracts to the following:

   `migration_tool_70to71`

5. Retrieve the IMSS 7.0 migration package from the `migration_tool_70to71` directory on the IMSS 7.0 server.
6. Put the migration package on the server, where the IMSS 7.1 Central Controller is installed, at the following location:

   `migration_tool_70to71`

7. Start the migration tool.

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

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

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

   `C:\Imss7InstLog\migration\MigrationReport` and `C:\Imss7InstLog\migration` with the logs formatted as `migration_70.yyyymmdd.log`

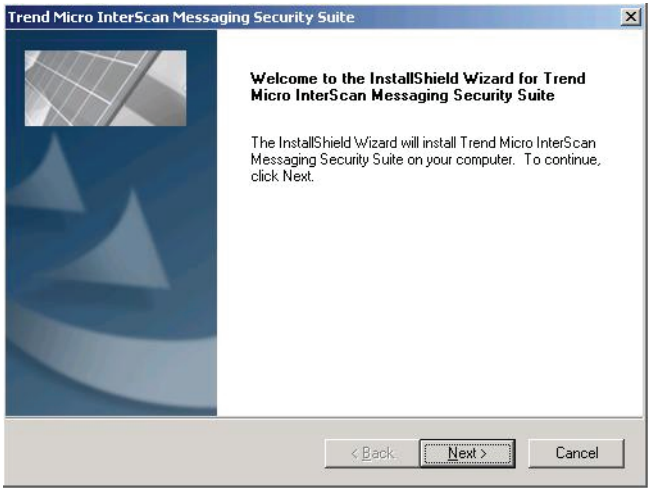
9. Perform the following post-migration tasks to verify the results of the migration:
   a. Check the results for migrated items.
   b. Verify that all services can be started, especially the policy server.
   c. Verify that all policies can be accessed on the Web console.

Installing IMSS 7.1 Over IMSS 7.0

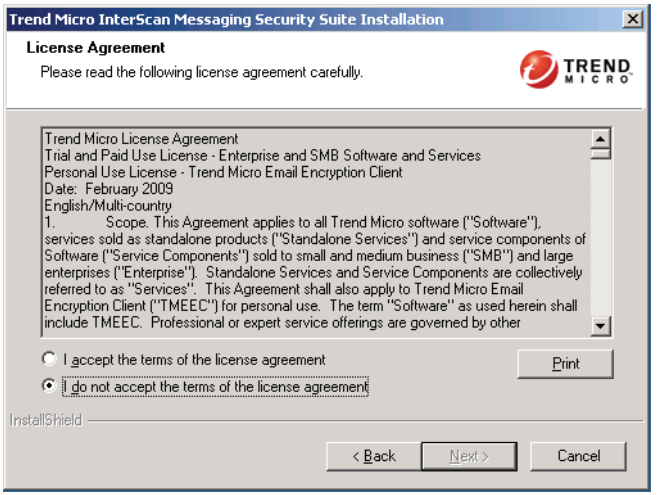
IMSS 7.0 SP1 with patch 2 or above is required when upgrading or migrating.

To install IMSS 7.1 over IMSS 7.0:

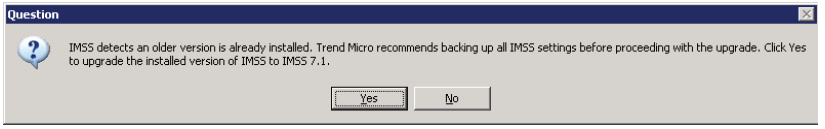
1. Double-click on **Setup.exe**. The Welcome screen appears.



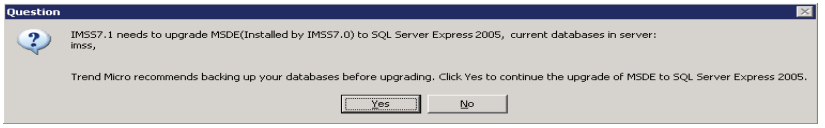
2. Click **Next**.



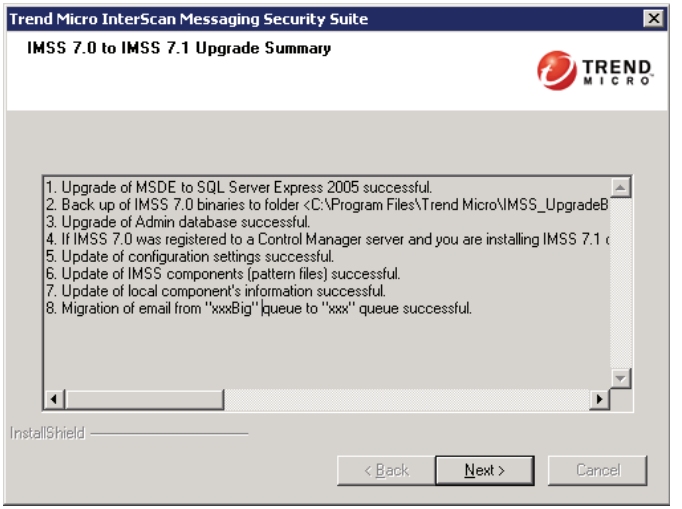
3. Read the license agreement carefully before selecting **I accept the terms of the license agreement**.
4. Click **Next**.



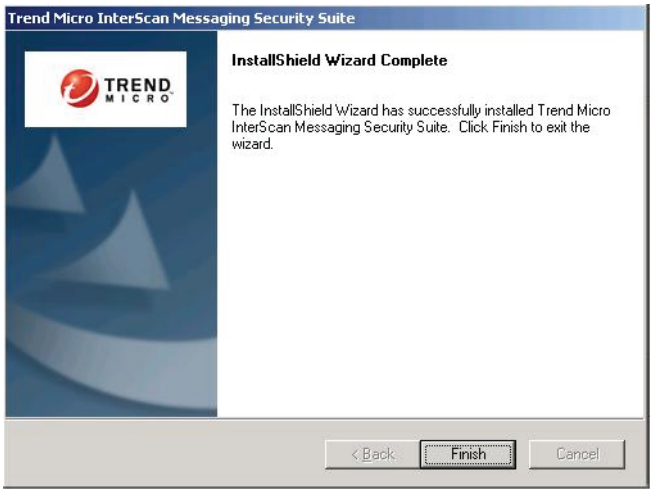
5. Click **Yes** to install IMSS 7.1 over IMSS 7.0.



6. Click **Yes** to upgrade MSDE to SQL Server Express 2005. A summary of the upgrade appears.



7. Click **Next**. The Installation Complete screen appears.



8. Click **Finish** to complete the upgrade.

Activation of Supported Services

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

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

To use Email reputation, type the Activation Code from the Web console after installation completes.

Rolling Back the Upgrade

If any problems occur with the migration to version 7.1, you can roll back to version 5.7/7.0. For more information about IMSS 5.7 installation-related questions, see your IMSS 5.7 documentation. 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 5-43).
- Complex distributed deployment—Install each component of IMSS 5.7 on different servers (see Rolling Back in a Complex Distributed Deployment Scenario on page 5-44).

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 all IMSS 7.1 components using the uninstallation program.
2. Perform a fresh installation for IMSS 5.7.
3. Stop all IMSS 5.7 services from the Microsoft Management Console.
4. Start the database service.
5. Restore the database data for IMSS 5.7 using the Microsoft SQL Management tool.

6. Stop the database service.
7. Stop IIS services from the Microsoft Management Console.
8. Restore the IMSS 5.7 installation folder.
9. Delete the registry key "TrendMicro" under `[HKEY_LOCAL_MACHINE\SOFTWARE]`.
10. Import the old IMSS 5.7 policy settings into the registry.
11. Start IIS services, including World Wide Web Publishing Service.
12. Start the database service.
13. Start all services of IMSS 5.7 in the following sequence:
    a. Start TMI.
    b. Start CCGI.
    c. Start all other IMSS-related services.

Note: TMI and CCGI must start before other IMSS services.

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 Email reputation)

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

1. Uninstall all IMSS 7.1 components using the uninstallation program.
2. Perform a fresh installation of IMSS 5.7. Follow the previous IMSS 5.7 deployment.
3. Stop all IMSS 5.7 services:
    a. On Server 1: Stop all IMSS-related services and the IIS service.

b. On Server 3: Stop all IMSS-related services.

4. Restore IMSS 5.7-related data on Server 1:
   a. Restore the IMSS 5.7 installation folder.
   b. Delete the registry key "TrendMicro" under `[HKEY_LOCAL_MACHINE\SOFTWARE]`.
   c. Import the old IMSS 5.7 policy settings into the registry.
5. On Server 2: Restore IMSS 5.7 database data using the Microsoft SQL Management tool.
6. On Server 3: Restore the IMSS 5.7 installation folder.
7. On Server 2: Restart the database service.
8. On Server 1:
   a. Start IIS services, including the World Wide Web Publishing Service.
   b. Start all IMSS-related services in the following sequence:
      i. Start TMI.
      ii. Start CCGI.
      iii. Start all other IMSS-related services.

Note: TMI and CCGI MUST start before other IMSS services.

---

9. On Server 3: Start all IMSS-related services.

Chapter 6

Troubleshooting, FAQ, and Support Information

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

Topics include:

Troubleshooting

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

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

TABLE 6-1. Installation Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Installation stopped and the following message appears: "can not overwrite xxx.xxx"	Manually remove all files in the destination folder and retry the installation. **Note:** You might need to stop all running applications in the destination folder. For example, a terminal service instance might be running statmon.exe.
Cannot append components to an existing installation because the database information is not correct.	When appending a scanner to an IMSS installation, provide the following for Database Server (when the server does not use the default instance name): hostname (IP address)\IMSS_SSEINSTANCE.

.Frequently Asked Questions

Mail Transfer Agent

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

You can modify the MTA configuration file which will be applied to the local MTA component after you restart the component.

1. Open and edit the MTA configuration file

   `%IMSS_HOME%\config\tsmtpd.ini`.

2. Using the command line interface, stop and restart the scanner and MTA components to apply the changes:

   ```
   net stop TmImssScan

   net stop TmImssMTA

   net start TmImssMTA

   net start TmImssScan
   ```

3. Check that the settings are applied to the MTA component.

How does IMSS process a partial email?

IMSS rejects partial email as a malformed message if `BypassMessagePartial=no` in the `imss.ini` file (default setting).

If the key is set to `yes`, IMSS will bypass the partial mails. Trend Micro does not recommend changing the item `BypassMessagePartial` to `yes` as this may cause virus leak.

How do I replace a self-signed MTA SSL certification?

Do the following:

1. Write a configuration file. For more information, see http://www.openssl.org/docs/apps/req.html
2. Run the following command:

   ```
   openssl req -new -x509 -days 1460 -nodes -config

   tsmtpd.cfg -out tsmtpd.pem -keyout tsmtpd.pem
   ```

3. Upload `tsmtpd.pem` from the Web management console.
4. The OpenSSL utility command line. For more information go to the following Web site:

   http://www.openssl.org/docs/apps/req.html

Is the SMTP AUTH feature for "Domain-based relay" and "Default relay" supported? If yes, which authentication method does IMSS support?

IMSS supports the CRAM-MD5, PLAIN and LOGIN SMTP AUTH authentication methods for "Domain-based relay" and "Default relay". However, you cannot configure the settings from the Web management console. To configure the settings, set `<auth>=1` to use the AUTH function and manually edit `tsmtpd.ini` as follows:

Syntax:

```
[SmtpClient]

# for Domain-based delivery

RelayHostCount=1

RelayHost0=trend.com:guid0

[D_guid0]

UseMethod=1

SmartHostCount=1

SmartHost0=<hostname_or_ip>:<port>:<auth>:<username>:<passwo
rd>


# for Default delivery

[DefaultRelay]

UseMethod=1

SmartHostCount=1

SmartHost0=<hostname_or_ip>:<port>:<auth>:<username>:<passwo
rd>
```

Example:

```
[SmtpClient]

# for Domain-based delivery

RelayHostCount=1
```

```
RelayHost0=trend.com:guid0

[D_guid0]

UseMethod=1

SmartHostCount=1

SmartHost0=192.168.1.1:25:1:user1:@trend.com:!CRYPT!66AE674C
2079B2CD00CAB0D02E765970

# for Default delivery

[DefaultRelay]

UseMethod=1

SmartHostCount=1

SmartHost0=192.168.1.2:25:1:user2@trend.com:
!CRYPT!66AE674C2079B2CD00CAB0D02E765970
```

Note: Type the following command to encrypt the password before adding the encrypted password into `tsmtpd.ini`:
`C:\Program Files\Trend Micro\IMSS\bin\password.exe <password text>`

SMTP Settings

Is IMSS an open relay mail server by default?

No, IMSS is not an open relay mail server by default. However, some administrative tools may incorrectly report that IMSS is an open relaymail server as IMSS allows some special characters such as the percent mark (%) and exclamatory mark (!) in email addresses. This causes some third-party administrative tools to misidentify IMSS as an open relay because some old UNIX mail server implementations treat such characters embedded in an email address as tricky source routings. You may do one of the following to prevent IMSS from being misidentified as an open relay mail server:

- Apply the settings to all IMSS servers under one central database

  If you have deployed IMSS in a distributed environment, run the following SQL statements to add new settings to the `tb_mta_config` table in the central database:

```
insert into tb_mta_config (section, name, value, inifile)
values ( 'SmtpServer', ' RestrictInDomain', '1',
'tsmtpd.ini');

insert into tb_mta_config (section, name, value, inifile)
values ( 'SmtpServer', ' RestrictInDomainMeta', ' !#$%',
'tsmtpd.ini');
```

- Apply the settings to one IMSS server

  Edit `tsmtpd.ini` (located in `IMSS_INSTALL_ROOT\config\`) and remove the comments for the following keys:

  ```
  RestrictInDomain=1

  RestrictInDomainMeta=!#$%
  ```

Installation / Uninstallation

Can the IMSS Admin database be installed separately?

Yes. You can install the IMSS Admin database separately in two ways

- Run the Setup program and configure the IMSS database. Do not select any other IMSS components.
- Run the Setup program at the command interface, if you have an existing database server on the target machine:
  - Go to the setup folder.
  - Run the Setup program using the following command:

    ```
    setup.exe /zOnlyInstDB
    ```

  - Follow the installation screens to install the IMSS Admin database.

Note: After installing the IMSS Admin database, run the Setup program and install any other components using the account created database to connect to the IMSS database.

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. During uninstallation, the IMSS EUQ database is only unregistered from the Admin database. The IMSS EUQ database can be re-registered through the Web management console.

Can the old IMSS database be removed during installation?

No, because an application is connecting to the database when the Setup program tries to remove the database. Remove all connections to the old database, drop the database, and create a new database.

Must IMSS 7.1 be installed in the default path?

No. You can specify any install path except `X:\Program Files` in 64-bit operating system, where X is the system disk. This folder is reserved for 64-bit programs.

Why doesn't the shortcut for the Web management console on the target computer work?

If the target computer is running Windows Server 2003, add the shortcut address to the trusted zone for the browser.

If the database process is

- **Not running:** Start the database service and restart the IMSS Web management console service.
- **Running:** If the Web management console starts up before the database, restart the IMSS Web management console service.

Can IMSS use a domain account to access a database?

No. IMSS 7.1 does not support Windows authentication.

Can the database server be referenced by hostname?

Yes. You can specify the "Hostname\Instance" or "IP address\Instance" to reference the database server.

Can the IP address for IMSS or IMSS components be changed?

Yes.

To change the IP address for IMSS (Central Controller + Scanner):

1. Stop all IMSS services as follows:

   Open Windows **Control Panel** > **Administrative Tools** > **Services**. Stop the following services in sequence:

   `Trend Micro IMSS Web Console`

   `Trend Micro IMSS IPProfiler`

   `Trend Micro IMSS Task Services`

   `Trend Micro IMSS CMAgent Service`

   `Trend Micro IMSS Policy Service`

   `Trend Micro IMSS Scan Service`

   `Trend Micro IMSS SMTP Service`

   `Trend Micro IMSS Manager`

2. Change the server IP address.
3. Change the IP address in `ODBC.ini` and `EUQ.ini` in the IMSS configuration folder.
4. Change the database URL and user name/password in `%IMSS_HOME%\ui\adminUI\webapps\ROOT\WEB-INF\struts-config-common.xml`
5. Change the following database data:
   - `tb_component_list`: Specify the computer name and all scanner IP addresses.
   - `tb_euq_db_info`: Specify the EUQ database computer settings.
   - `tb_global_setting`: In section [cmagent] name [ConfigUrl], change the Web management console URL.

6. Modify the SQL Server's IP settings and restart the Microsoft SQL Server services.
7. Restart all IMSS services as follows:

   Open Windows **Control Panel** > **Administrative Tools** > **Services**. Restart the following services in sequence:

   ```
   Trend Micro IMSS Manager
   Trend Micro IMSS SMTP Service
   Trend Micro IMSS Scan Service
   Trend Micro IMSS Policy Service
   Trend Micro IMSS CMAgent Service
   Trend Micro IMSS Task Services
   Trend Micro IMSS IPProfiler
   Trend Micro IMSS Web Console
   ```

To change the IP address for a Scanner:

New IP addresses for scanners are automatically updated in the `tb_component_list` by the IMSS service `TmImssManager` when the service restarts. To update the IP address on a scanner, restart the `TmImssManager` service.

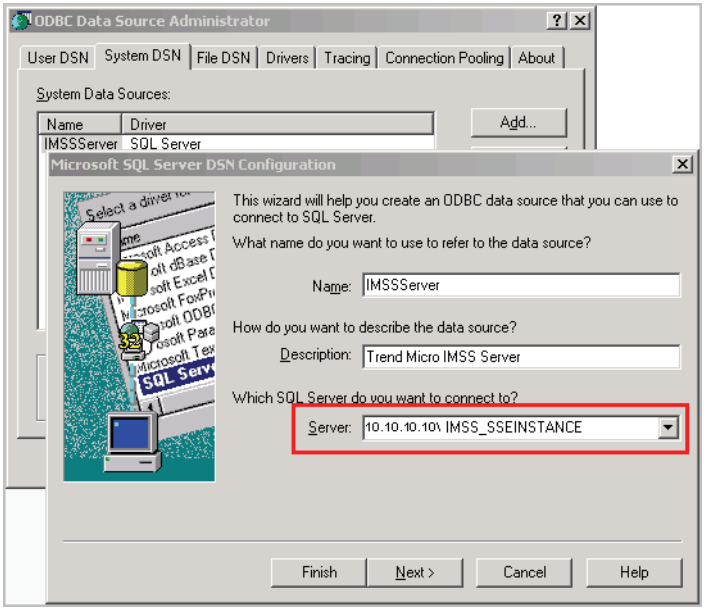
To change the IP address for the Central Controller:

1. Restart the IMSS service `TmImssManager`.
2. Specify the new IP address of the Central Controller in the `[cmagent]/ConfigUrl` parameter in the `tb_global_setting table`.
3. If IP Profiler was installed:
   - Restart the BIND Service (ISC BIND) on the Central Controller.
   - Update the IP address for the `[SmtpServer]/IPProfilerDNSServerIP` parameter in the `tsmtpd.ini` file on each scanner.
4. Restart the SMTP service on each scanner to use the new IP Profiler DNS server IP address.
5. To access the Web management console, change the IP address to the new IP address in the `adminui` file. The file is located in the IMSS installation directory.

To change the IP address of the Admin database:

1. Stop all IMSS components.
2. On all scanners and EUQ servers, set the server parameter to the new IP address of the database server in the ODBC System DSN settings.

   Modify the setting from the ODBC Data Source Administrator dialog box, located at **Start > Administrative Tools > Data Sources (ODBC)**.



Note: On 64-bit platforms, run `%systemdrive%\Windows\SysWOW64\Odbcad32.exe` to change the DSN Setting for IMSS.

3. On all scanners and EUQ servers, set the ServerName parameter to the new IP address of the database server in the `odbc.ini` file, located at `IMSS\config\`.

4. On the Central Controller, set the database URL to the new IP address of the database server in the `struts-config-common.xml` file, located at `IMSS\ui\adminUI\webapps\ROOT\WEB-INF\`. To change the setting, locate the string similar to the following and modify the IP address:

   ```
   <set-property
   property="url"
   value="jdbc:sqlserver://10.100.10.31;DatabaseName=imss" />
   ```

5. On all servers, start all IMSS components.

To change the IP address of primary EUQ servers:

1. Change the "ServerName" to the new IP address in the `EUQ.conf` file, located at `/opt/trend/imss/UI/euqUI/conf/`.
2. Change the IP address in the following files to the new IP address:
   - `euqbalance`
   - `euqui`

   Both files are located in the IMSS installation directory.
3. Set the `admin_cmd` parameter in `tb_global_setting` for the primary EUQ server to **12288**.
4. Restart the IMSS Manager service on the primary EUQ server. This changes the IP address in the `tb_component_list` to the new IP address, updates the load balance configuration, and restarts the TmImssEuqLoadBalancer service.
5. Restart the EUQ service on the primary EUQ server.

To change the IP address of secondary EUQ servers:

1. Change the IP address in the `euqui` file to the new IP address. The file is located in the IMSS installation directory.
2. Restart the IMSS Manager service on the secondary EUQ server. This changes the IP address in the `tb_component_list` to the new IP address.
3. Set the `admin_cmd` parameter in `tb_global_setting` for the primary EUQ server to **12288**.
4. Restart the IMSS Manager service on the primary EUQ server to update the `worker.properties` configuration file.

To remove or add EUQ servers into an IMSS group:

The Setup program notifies the IMSS Manager service on the primary EUQ server to update the load-balancing configuration for the Apache Web server. The IMSS Manager service on the Primary EUQ Server detects the `admin_cmd` command and updates the `workers.properties` configuration file to include or remove an EUQ server from the pool of EUQ servers used by the Apache Web server to distribute the End User requests.

To add an EUQ database:

Use the IMSS Web management console or Setup program to add a new EUQ database. Once installation completes, use the `euqtrans.bat` script, from the `<IMSS>\bin` directory of the Central Controller, to re-balance the EUQ databases.

To remove an EUQ database:

1. Use the IMSS Web management console to unregister (not delete) the EUQ database.
2. Run the `euqtrans.bat` script to move the Approved Sender list and quarantined message information to another database, and re-balance the databases based on the new deployment.

To change the EUQ database IP address:

1. Change the IP address in the `euq.ini` file to the new IP address. The file is located at `<IMSS>\config\`.
2. Use the IMSS Web management console to change the IP address of the EUQ database to the new IP address for the database.

   After configuring the EUQ Database Settings, IMSS automatically notifies all the services to restart. On restart, the services automatically check for updated EUQ database connection settings from the `tb_euq_db_info` table and updates the local ODBC User DSN settings in the Windows registry.

Where is the MIB file for SNMP notification?

The file `IMSS_win.mib` is located in top level folder of the extracted IMSS installation package.

How can I migrate DBCS settings in IMSS 5.7?

Before migration, ensure that the language settings are correct.

1. Install East Asian language files. For Windows Server 2003, click **Control Panel** > **Regional and Language Options** > **Languages** and select **Install files for East Asian languages**.
2. Change the **Language for non-Unicode programs** setting to Chinese/Japanese as required by the DBCS language used in IMSS 5.7.
3. Perform a migration installation.

Upgrading

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

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

`C:\Imss7InstLog\migrationfrom57\MigrationReport\GeneralReport.txt`.

What is the mapping relationship between IMSS 5.7 policies and IMSS 7.1 rules?

The mapping relationship is described in the detailed migration report:

`C:\Imss7InstLog\migrationfrom57\MigrationReport\DetailReport.txt`.

How do I upgrade IMSS 5.7 scanners?

To upgrade from multiple IMSS 5.7 scanners:

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

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

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

Is rollback to IMSS 5.7 possible after upgrading?

Yes. See Rolling Back the Upgrade on page 5-43 for detailed rollback instructions.

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

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

How do I simplify SPS rules after an upgrade?

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

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

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

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

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

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

    For example: A virus filter with the routes (a->b; c->d; e->b) will be migrated to two virus rules with the routes (a,e->b; c->d).
  - There will be two rules for one virus filter after migration if it was "active" in IMSS 5.7 for both SMTP and POP3 traffic.
  - There will be only one rule for one virus rule after migration if it is "inactive" in IMSS 5.7 for both SMTP and POP3 traffic. The rule direction is for "all routes".

- **SPS filter(s) —** The migration module maps each SPS filter to one SPS rule after migration or several SPS rules depending on the Routes and Filter Actions. There will normally be one SPS rule after migration. The following are exceptions when there will be several SPS rules:
  - **If there are multiple routes with different "To" or "From" addresses**.

    For example: SPS filter with the routes (a->b; c->d; e->b) will be migrated to two SPS rules with the routes (a,e->b; c->d).
  - **If three filter actions are different**.

    For example, SPS filter with the following filter actions will be migrated to two SPS rules named "Spam Filter (SPS) BlackWhiteList And Phish >Global Policy" and "Spam Filter (SPS) Spam >Global Policy":
    - "Tag and Deliver" for "Blocked senders"
    - "Delete" for "Phishing emails"
    - "Quarantine" for "Spam"
- eManager filter
  - There will be several rules for one eManager filter after migration if there are multiple routes with different "To" or "From" addresses.

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

For the detailed mapping relationship of each policy, check:

`C:\Imss7InstLog\migration\MigrationReport\DetailReport.txt`.

Using the Knowledge Base

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

http://esupport.trendmicro.com

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

Contacting Support

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

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

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

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

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

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

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

Fax: +1 (408) 257-2003

Web address: www.trendmicro.com

Email address: support@trendmicro.com

Index

V

W

X