TREND MICRO™

# 7.5 InterScan™ Messaging Security Suite

## Installation Guide

Comprehensive threat protection at the Internet messaging gateway

for Windows™

Messaging Security

Document Part No. MSEM76207/131030

Release Date: February 2014

Document Version No.: 1.0

Product Name and Version No.: InterScan™ Messaging Security Suite 7.5

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

The user documentation for Trend Micro InterScan Messaging Security Suite 7.5 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

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

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

# Table of Contents

## About this Manual



## Chapter 1: Introducing InterScan Messaging Security Suite



## Chapter 2: Planning for Deployment

## Chapter 3: Component Descriptions

## Chapter 4: Installing and Uninstalling IMSS 7.5



## Chapter 5: Upgrading from Previous Versions

## Chapter 6: Troubleshooting and Support Information



## Index

# Preface

## About this Manual

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

Refer to the *IMSS 7.5 Administrator's Guide* for information about configuring IMSS settings and the Online Help in the management console for detailed information about each field on the user interface.

Topics include:

# What's New

The following tables provides an overview of new features available in IMSS 7.5.

**TABLE 1. IMSS 7.5 New Features**

| NEW FEATURE | DESCRIPTION |
|---|---|
| Command & Control (C&C) Contact Alert Services | Command & Control (C&C) Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. |
| Smart Scan | Smart Scan facilitates a more efficient scanning process by offloading a large number of threat signatures previously stored on the IMSS server to the cloud. |
| Web Reputation enhancement | The Web Reputation filter has been enhanced to enable detection of URLs that have not been rated by Trend Micro. This functionality helps improve protection against advanced threats that leverage short-lived websites. |
| Advanced threat management | IMSS integrates with the Advanced Threat Scan Engine (ATSE) to detect probable advanced threats in message attachments. IMSS can send a copy of a message to Deep Discovery Advisor for further analysis after the message is handled. |

**TABLE 2. 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:<br>• Address Groups<br>• BATV Keys<br>• Keywords & Expressions<br>• Policy Notifications<br>• Stamps<br>• DKIM Approved List<br>• Web Reputation Approved List |
| Web Reputation | Protect your clients from malicious URLs embedded in email messages with Web reputation. |
| Web Reputation | Protect your clients from malicious URLs embedded in email messages with Web reputation. |
| 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 Domain Keys 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. |
| Expanded File Scanning Support | IMSS now supports scanning Microsoft® Office 2007 and Adobe® Acrobat® 8 documents. |

| New Feature | Description |
|---|---|
| New Migration Tools | New tools have been provided to help customers migrating from previous product versions. |

**Table 3. IMSS 7.0 New Features**

| New Feature | Description |
|---|---|
| Multiple Antivirus and Malware Policies | Multiple IMSS policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria. |
| Centralized Logging and Reporting | A consolidated, detailed report provides top usage statistics and key mail usage data. Centralized logging allows administrators to quickly audit message-related activities. |
| Centralized Archive and Quarantine Management | 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:<br>• Email reputation filters connections from spam senders when establishing SMTP sessions.<br>• IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS).<br>• 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. |

| New Feature | Description |
|---|---|
| Easy Deployment with Configuration Wizard | An easy-to-use configuration wizard to get IMSS up and running. |
| Advance MTA Functions | Opportunistic TLS, domain based delivery, and other MTA functions help IMSS handle email efficiently and securely. |
| Migration | Easy upgrade process ensures that settings will be migrated with minimum effort during setup. |
| Mail Auditing and Tracking | IMSS provides detailed logging for all messages to track and identify message flow related issues. |
| Integration with Trend Micro Control ManagerTM | 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. |

# Audience

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

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

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

# InterScan Messaging Security Suite Documentation

The IMSS documentation consists of the following:

**Administrator's Guide**

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

**Installation Guide**

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

**Online Help**

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

**Readme File**

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

The documentation is available at:

http://docs.trendmicro.com

# Document Conventions

The documentation uses the following conventions:

**TABLE 4. Document Conventions**

| CONVENTION | DESCRIPTION |
|---|---|
| UPPER CASE | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| **Bold** | Menus and menu commands, command buttons, tabs, and options |
| *Italics* | References to other documents |
| `Monospace` | Sample command lines, program code, web URLs, file names, and program output |
| **Navigation** > **Path** | The navigation path to reach a particular screen<br>For example, **File** > **Save** means, click **File** and then click **Save** on the interface |
|  **Note** | Configuration notes |
|  **Tip** | Recommendations or suggestions |
|  **Important** | Information regarding required or default configuration settings and product limitations |
|  **WARNING!** | Critical actions and configuration options |

# Chapter 1

# Introducing InterScan™ Messaging Security Suite

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

Topics include:

# About InterScan Messaging Security Suite

InterScan Messaging Security Suite (IMSS) 7.5 integrates antivirus, anti-spam, anti-phishing, and content filtering technology for complete email protection. This flexible software solution features award-winning antivirus and zero-day protection to block known and potential viruses.

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

# IMSS Main Features and Benefits

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

**TABLE 1-1. Main Features and Benefits**

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

| Feature | Descriptions | Benefits |
|---|---|---|
| Advanced anti-malware protection | The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks. | ATSE identifies both known and unknown advanced threats, protecting your system from new threats that have yet to be added to patterns. |
| Command & Control (C&C) Contact Alert Services | C&C Contact Alert Services allows IMSS to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects. | C&C Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. |
| Smart Scan | Smart Scan facilitates a more efficient scanning process by off-loading a large number of threat signatures previously stored on the IMSS server to the cloud. | Smart Scan leverages the Smart Protection Network to:<br>• Enable fast, real-time security status lookup capabilities in the cloud<br>• Reduce the time necessary to deliver protection against emerging threats<br>• Lower memory consumption on the server |

| 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.<br><br>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.<br><br>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. |
| **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. |

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

| 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.<br><br>When IMSS detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses.<br><br>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.<br><br>The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs℠ ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers. |
| **Protection from spyware and other types of grayware** | | |
| Spyware and other types of grayware | Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see *About Spyware/Grayware on page 1-9*. | IMSS's ability to protect your environment against spyware and other types of grayware enables you to significantly reduce security, confidentiality, and legal risks to your organization. |
| **Integrated anti-spam features** | | |

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| 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.<br><br>SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license. | The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real-time detection that is highly adaptable, even as spam senders change their techniques. |
| Spam Filtering with IP Profiler and Email reputation | IP Profiler is a self-learning, fully configurable feature that proactively blocks IP addresses of computers that send spam and other types of potential threats. Email reputation blocks IP addresses of known spam senders that Trend Micro maintains in a central database.<br><br>**Note**<br>Activate SPS before you configure IP Profiler and Email reputation. | With the integration of IP Filtering, which includes IP Profiler and Email reputation, IMSS can block spammers at the IP level. |
| **Administration and integration** | | |
| LDAP and domain-based policies | You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™ or Microsoft™ Active Directory™ for user-group definition and administrator privileges. | Using LDAP, you can define multiple rules to enforce your company's email usage guidelines. You can define rules for individuals or groups, based on the sender and recipient addresses. |

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Web-based management console | The management console allows you to conveniently configure IMSS policies and settings. | The management console is SSL-compatible. Being SSL-compatible means access to IMSS is more secure. |
| End-User Quarantine (EUQ) | IMSS provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Spam Prevention Solution (SPS) quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete, or approve for delivery. | With the web-based EUQ management console, end-users can manage messages that IMSS quarantines. |
| Delegated administration | IMSS offers the ability to create different access rights to the management console. You can choose which sections of the console are accessible for different administrator logon accounts. | By delegating administrative roles to different employees, you can promote the sharing of administrative duties. |
| 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.<br>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. |

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| POP3 scanning | You can choose to enable or disable POP3 scanning from the management console. | In addition to SMTP traffic, IMSS can also scan POP3 messages at the gateway as messaging clients in your network retrieve them. |
| Clustered architecture | The current version of IMSS has been designed to make distributed deployment possible. | You can install the various IMSS components on different computers, and some components can exist in multiples. For example, if your messaging volume demands, you can install additional IMSS scanner components on additional servers, all using the same policy services. |
| Integration with Trend Micro Control Manager™ | Trend Micro Control Manager™ (TMCM) is a software management solution that gives you the ability to control antivirus and content security programs from a central location regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus and content security policy. | Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available. |

# About Spyware/Grayware

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

**TABLE 1-2. Types of Grayware**

| TYPE | DESCRIPTION |
|---|---|
| Spyware | Gathers data, such as account user names and passwords, and transmits them to third parties |
| Adware | Displays advertisements and gathers data, such as user web surfing preferences, to target advertisements at the user through a web browser |
| Dialers | Change computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem |
| Joke Programs | Cause abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes |
| Hacking Tools | Help hackers enter computers |
| Remote Access Tools | Help hackers remotely access and control computers |
| Password Cracking Applications | Help hackers decipher account user names and passwords |
| Other | Other types not covered above |

## How Spyware/Grayware Gets into your Network

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

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

## Potential Risks and Threats

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

**TABLE 1-3. Types of Risks**

| TYPE | DESCRIPTION |
|---|---|
| Reduced computer performance | To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources. |
| Increased web browser-related crashes | Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot. |
| Reduced user efficiency | By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users can be unnecessarily distracted from their main tasks. |
| Degradation of network bandwidth | Spyware/grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network. |
| Loss of personal and corporate information | Not all data that spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network. |
| Higher risk of legal liability | If hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties. |

# About Web Reputation

Trend Micro web reputation technology helps break the infection chain by assigning websites a "reputation" based on an assessment of the trustworthiness of an URL, derived from an analysis of the domain. Web reputation protects against web-based threats including zero-day attacks, before they reach the network. Trend Micro web

reputation technology tracks the lifecycle of hundreds of millions of web domains, extending proven Trend Micro anti-spam protection to the Internet.

# About Trend Micro Control Manager

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

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

## Control Manager Support

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

**TABLE 1-4. Supported Control Manager Features**

| FEATURE | DESCRIPTION | SUPPORTED? |
|---|---|---|
| Two-way communication | Using 2-way communication, either IMSS or Control Manager may initiate the communication process. | No.<br><br>Only IMSS can initiate a communication process with Control Manager. |

| FEATURE | DESCRIPTION | SUPPORTED? |
|---|---|---|
| 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.<br><br>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 management console. | No.<br><br>You need to first log on to the IMSS management console before you can manage IMSS from Control Manager. |
| Configuration replication | Replicate configuration settings from an existing IMSS server to a new IMSS server from Control Manager. | Yes |
| Pattern update | Update pattern files used by IMSS from Control Manager | Yes |
| Engine update | Update engines used by IMSS from Control Manager. | Yes |

| FEATURE | DESCRIPTION | SUPPORTED? |
|---|---|---|
| Product component update | Update IMSS product components such as patches and hot fixes from Control Manager. | No.<br>Refer to the specific patch or hot fix readme file for instructions on how to update the product components. |
| Configuration by user interface redirect | Configure IMSS through the IMSS management console accessible from Control Manager. | Yes |
| Renew product registration | Renew IMSS product license from Control Manager. | Yes |
| Customized reporting from Control Manager | Control Manager provides customized reporting and log queries for email-related data. | Yes |
| Control Manager agent installation/ uninstallation | Install or uninstall IMSS Control Manager agent from Control Manager. | No.<br>IMSS Control Manager agent is automatically installed when you install IMSS. To enable/disable the agent, do the following from the IMSS management console:<br>1. Go to **Administration** > **Connections**.<br>2. Click the **TMCM Server** tab.<br>3. To enable/disable the agent, select/clear the check box next to **Enable MCP Agent**. |
| Event notification | Send IMSS event notification from Control Manager. | Yes |

| FEATURE | DESCRIPTION | SUPPORTED? |
|---|---|---|
| Command tracking for all commands | Track the status of commands that Control Manager issues to IMSS. | Yes |

# About Trend Micro Smart Protection

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

Smart protection services include:

**File Reputation Services**

File reputation decouples the pattern file from the local scan engine and conducts pattern file lookups to the Trend Micro Smart Protection Network. High performance content delivery networks ensure minimum latency during the checking process and enable more immediate protection.

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

**Web Reputation Services**

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

Web reputation technology prevents users from:

- Accessing compromised or infected sites

- Communicating with Command & Control (C&C) servers used in cybercrime

## The Need for a New Solution

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

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

## Trend Micro™ Smart Protection Network™

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

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

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

The Smart Protection Network provides Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. A client sends web reputation queries to the Smart Protection Network to check the reputation

of websites that a user is attempting to access. The client correlates a website's reputation with the specific web reputation policy enforced on the computer to determine whether access to the site is allowed or blocked.

For more information on the Smart Protection Network, visit:

www.smartprotectionnetwork.com

# About Command & Control (C&C) Contact Alert Services

Trend Micro Command & Control (C&C) Contact Alert Services provides IMSS with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. It leverages the Global Intelligence list compiled, tested, and rated by the Trend Micro Smart Protection Network to detect callback addresses.

With C&C Contact Alert Services, IMSS has the ability to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects. Administrators can configure IMSS to quarantine such messages and send a notification when a message is flagged. IMSS logs all detected email with C&C objects and the action taken on these messages. IMSS sends these logs to Control Manager for query purposes.

# Chapter 2

# Planning for Deployment

This chapter explains how to plan for IMSS deployment.

Topics include:

# Deployment Checklist

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

1. **Identify the location of IMSS**

| TICK WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Select one of the following locations on your network where you would like to install IMSS. | | |
| | Without a firewall | | *Installing without a Firewall on page 2-11* |
| | In front of a firewall | | *Installing in Front of a Firewall on page 2-12* |
| | Behind a firewall | | *Installing Behind a Firewall on page 2-13* |
| | On a former SMTP gateway | | *Installing on a Former SMTP Gateway on page 2-14* |
| | In the De-Militarized Zone | | *Installing in the De-Militarized Zone on page 2-15* |

2. **Plan the scope**

| TICK WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Decide whether you would like to install one IMSS server or multiple servers. | | |
| | Single-server installation | | *Single-Server Installation on page 2-16* |
| | Multiple scanner service | | *Multiple Scanner Service Installation on page 2-18* |
| | Multiple EUQ service | | *Multiple End-User Quarantine Service Installation on page 2-20* |
| | Complex distributed | | *Complex Distributed Installation on page 2-23* |
| | Wide area network | | *Wide-Area Network Installation on page 2-24* |
| | IP filtering<br><br>**Tip**<br>Trend Micro recommends that you consider the failover plan before deciding on the scope. | | *IP Filtering on page 2-28* |

3. **Install or Upgrade**

| TICK WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Perform a fresh installation of IMSS or upgrade from a previous version. | | |
| | Upgrade from a previous version | | *Upgrading from Previous Versions on page 5-1* |

4. **Configure basic IMSS settings**

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

5. **Start services**

| TICK WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Activate IMSS services to start protecting your network against various threats. | | |

| TICK WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Scanner | | IMSS Services section of the Administrator's Guide |
| | Policy | | |
| | EUQ | Yes | |

6. **Configure other IMSS settings**

| TICK WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Configure various IMSS settings to get IMSS up and running. | | |
| | IP Filtering Rules | Yes | IP Filtering Service section of the Administrator's Guide |
| | SMTP Routing | | Scanning SMTP Messages section of the Administrator's Guide |
| | POP3 Settings | Yes | Scanning POP3 Messages section of the Administrator's Guide |
| | 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 |

7. **Back up IMSS**

| Tick when completed | Tasks | Optional | Reference |
|---|---|---|---|
| | 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 . The following table lists each component sub-module.

**Table 2-1. Component and sub-module installation**

| Main Component | Installed Sub-module | Sub-module Description |
|---|---|---|
| IMSS Admin Database | Administrator Database | The main IMSS Admin database that stores all global settings. |
| | Database Server | The server on which the IMSS Admin database runs. |
| Central Controller | Apache® Tomcat® | The web server for the IMSS web console, through which you configure settings. |
| | Named Server | The DNS server for IP Profiler. |
| | FoxDNS | Contains the list of blocked and white IP addresses for IP Profiler and writes the list to the named server. |
| | IMSSMGR | A module that manages IMSS processes. |

| Main Component | Installed Sub-module | Sub-module Description |
|---|---|---|
| Scanner Service | Scanning Services | Performs all email-scanning actions. |
| | Policy Services | A remote store of rules for the scanner services, caching rules that would otherwise require a database look-up |
| | IMSSMGR | A module that manages scanner processes. |
| Scanner Service (Continued) | SMTP Service | Trend Micro MTA/MDA |
| | IP Profiler | Part of Trend Micro MTA |
| | Email reputation | Part of Trend Micro MTA |
| 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 the following table for the ports IMSS uses.

**TABLE 2-2. IMSS Ports**

| PORT NUMBER | COMPONENT AND ROLE | CONFIGURATION LOCATION |
|---|---|---|
| 25 | The MTA service port.<br>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 console, go to **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 console, go to **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 console, go to **Administration** > **IMSS Configuration** > **Connections** > **Components** on the menu. |
| 8005 | Admin Web Server (Tomcat) management port that can handle Tomcat management commands. | `{IMSS}/UI/adminUI/conf/server.xml: Server / port` |
| 8009 | EUQ Console Tomcat AJP port. This port is used to perform load balancing between several Tomcat servers and the Apache HTTP server. | `{IMSS}/UI/euqUI/conf/server.xml: Server / Service / Connector (protocol=AJP/1.3) / port` |
| 8015 | Tomcat management port that can handle Tomcat management commands. | `{IMSS}/UI/euqUI/conf/server.xml: Server/port` |

| 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:<br>`{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.)<br>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 |

| Port Number | Component and Role | Configuration Location |
|---|---|---|
| 15505 | IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the web console. The manager also provides quarantine/archive query results to the web console and the EUQ Web console through this port. | From the web console, go to **Administration** > **IMSS Configuration** > **Connections** > **Components** on the menu. |
| IMSS uses the following ports when you enable related services: | | |
| 389 | LDAP server listening port. | IMSS<br>From the web console, go to **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 console, go to **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu. |
| 443 | Microsoft IIS HTTPS listening port. You need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS. | From the web console, go to **Administration** > **IMSS Configuration** > **Connections** > **TMCM Server** on the menu. |
| 88 | KDC port for Kerberos realm. | Not configurable on the IMSS server. |
| 53 | The Bind service listening port. Do not assign a different port number. | Not configurable on the IMSS server. |

# Network Topology Considerations

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

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

**Note**

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

## Installing without a Firewall

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

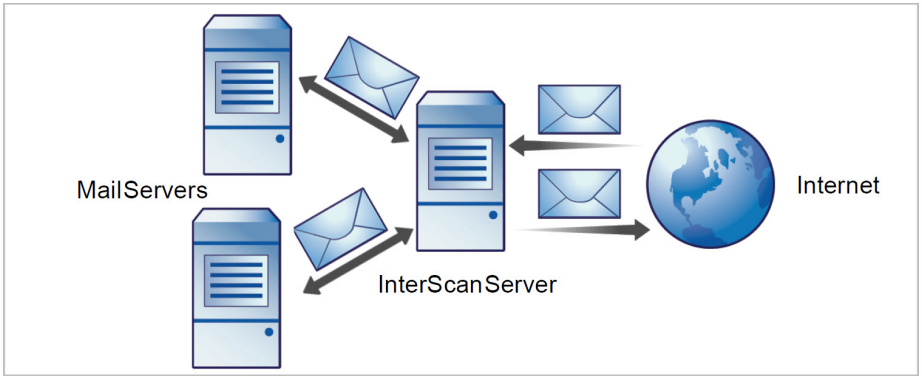



**FIGURE 2-1. Installation topology: no firewall**

**Note**

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

## Installing in Front of a Firewall

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

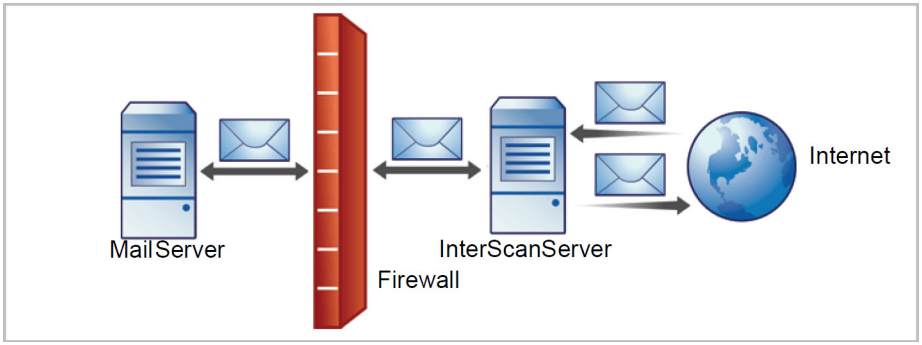



**FIGURE 2-2. Installation topology: in front of the firewall**

### Incoming Traffic

- IMSS should be the first server to receive incoming messages. 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 messages go to IMSS servers.
- Incoming SMTP messages only come from IMSS servers.

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

**Tip**

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

## Installing Behind a Firewall

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

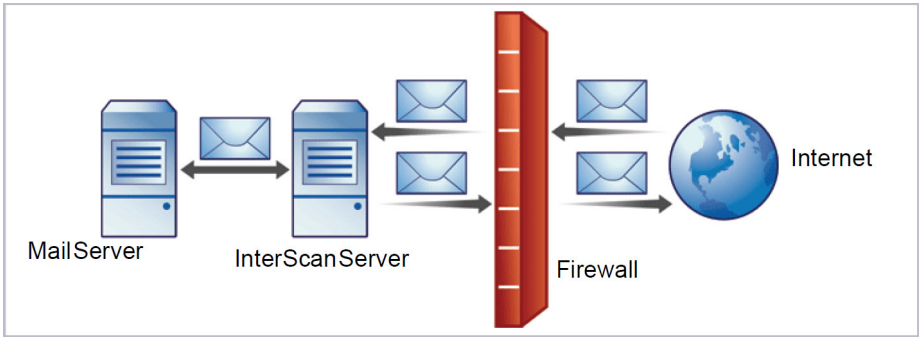



**FIGURE 2-3. Installation scenario: behind a firewall**

### Incoming Traffic

- Configure your proxy-based firewall, as follows:
  - Outgoing SMTP messages go to the IMSS server or the switch performing load balancing between scanners.
  - Incoming SMTP messages 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 messages destined for your local domain(s) to the SMTP gateway or your internal mail server.
- Configure relay restriction to only allow relay for local domain(s).

### Outgoing Traffic

- Configure all internal SMTP gateways to send outgoing messages to IMSS servers.
- If you are replacing your SMTP gateway with IMSS, configure your internal mail server to forward outgoing messages to IMSS servers.
- Configure IMSS to route all outgoing messages (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 the **Configuring SMTP Routing** section of the *IMSS 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 messages to the SMTP gateway and the newly allocated port.

### Outgoing Traffic

- Configure the SMTP gateway to route outgoing email messages to the IMSS port 25.
- Configure IMSS to route all outgoing email messages (destined for 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 messages 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 messages destined for your local domain(s) to the SMTP gateway or your internal mail server.

### Outgoing Traffic

- Configure IMSS to route all outgoing messages (destined for domains 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 the **Configuring SMTP Routing** section of the *IMSS Administrator's Guide*.

# Understanding Installation Scenarios

IMSS allows you to install either a single instance of each component on a single server (single-server installation) or several IMSS components on multiple servers (distributed deployment installation). Use the following information as a guide to choose a scenario.

## Single-Server Installation

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

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

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

**Note**

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

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

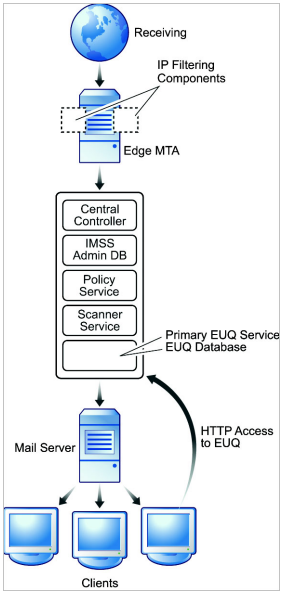



**FIGURE 2-4. Single server deployment**

## Performing Single-Server Installation

### Procedure

1. Install IMSS and End-User Quarantine.

## Multiple Scanner Service Installation

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

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

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

The following figure shows how a single-server installation of IMSS with two additional scanner services fits into standard messaging network topology.

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

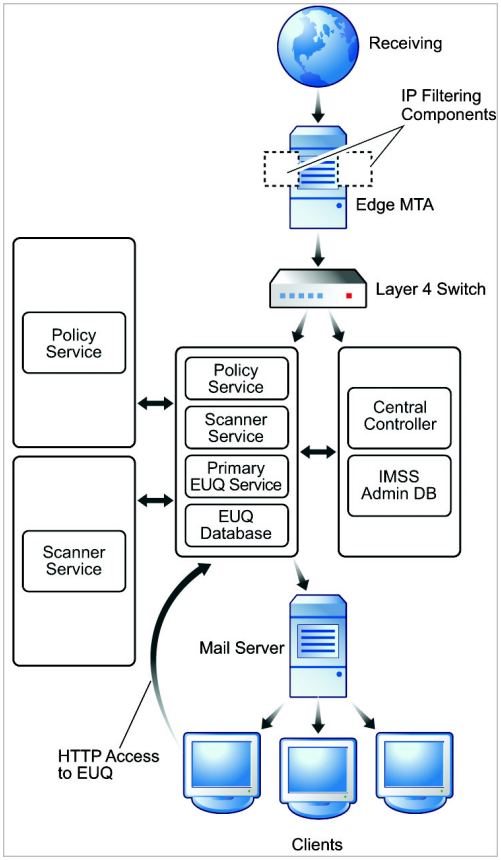



**FIGURE 2-5. Multiple scanner service and policy service deployment**

## Performing Multiple Scanner Service Installation

### Procedure

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

See *Complex Distributed Installation on page 2-23*.

2. After you open the IMSS web console and perform the initial configuration (see *Using the Configuration Wizard* chapter of the *Administrator's Guide*), go to the **System Summary** screen.

3. 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.

The following figure shows how a single-server installation of IMSS with a separate primary EUQ service and additional secondary EUQ services (with Apache services for

load balancing) and distributed EUQ databases fit into a standard messaging network topology.

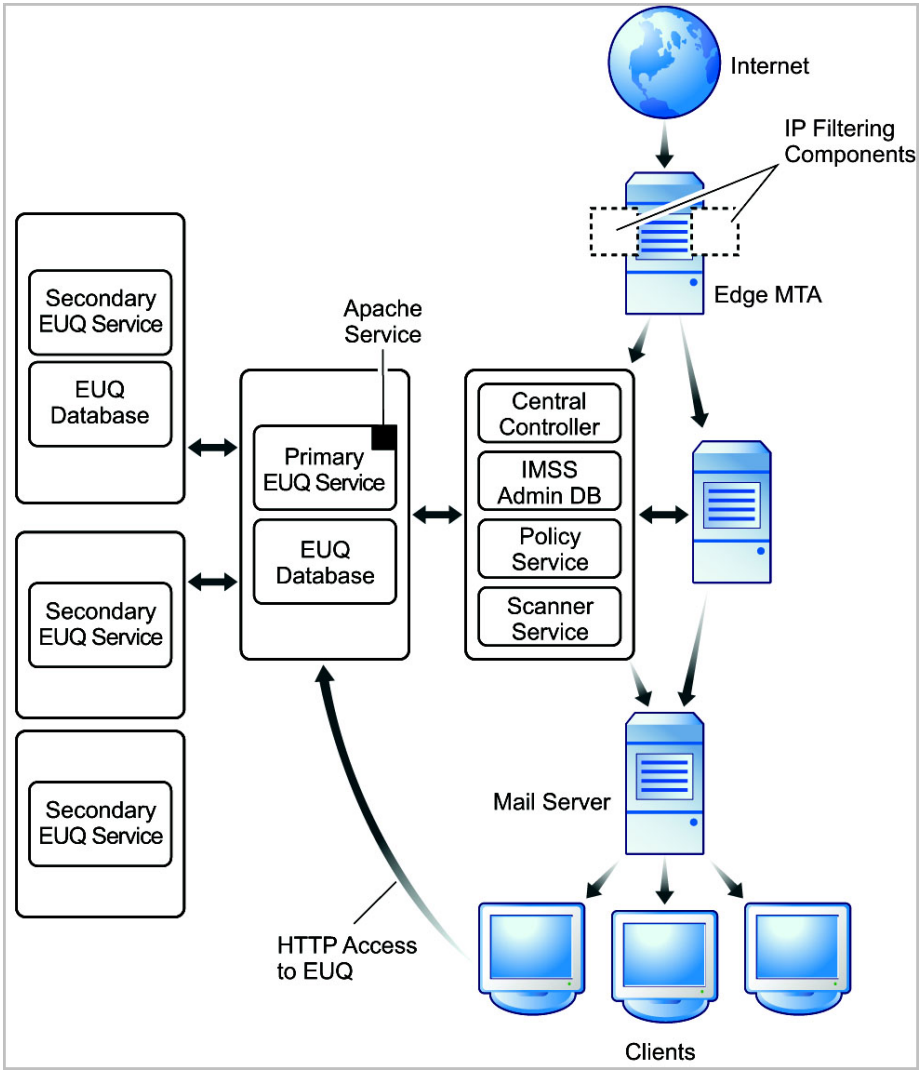



**FIGURE 2-6. Multiple EUQ service deployment**

## Performing Multiple EUQ Service Installation

**Procedure**

1. On one computer, install IMSS.

   See *Single-Server Installation on page 2-16* or *Complex Distributed Installation on page 2-23*.

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**

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

4. After you open the IMSS web console and perform initial configuration (see *Performing Basic Configuration with the Configuration Wizard* and *Configuring IMSS Settings* sections of the *Administrator's Guide*), go to the **System Summary** screen.

5. Click **Start** for the EUQ services you want to enable.

   **Note**

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

## Other Considerations When Deploying End-User Quarantine

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

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

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

For more information, see *Single-Server Installation on page 2-16* or *Complex Distributed Installation on page 2-23*.

### Communication Between Servers

If you have an internal firewall, configure it to allow communication between IMSS, the EUQ service, and the database. For instance, if you install the EUQ service on one server, and the database on another, configure any firewall between the two servers to allow communication on port 5432 for database connections.

## Complex Distributed Installation

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

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

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

**Note**

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

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

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

**Note**

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

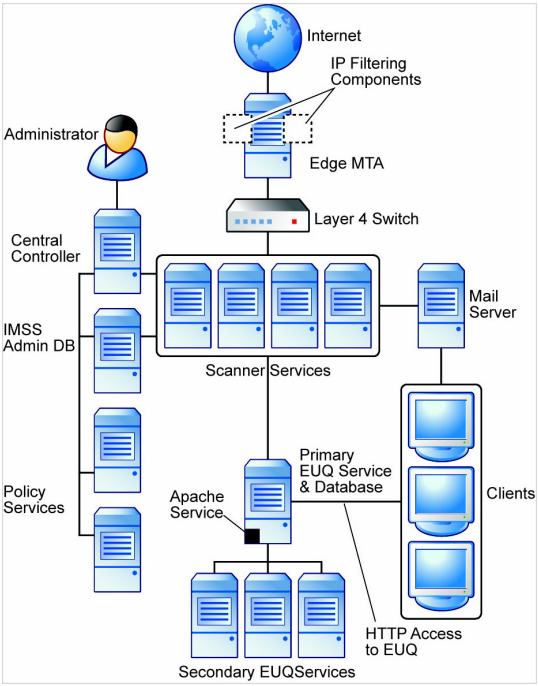



**FIGURE 2-7. Complex architecture deployment**

## 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 Trend Micro Control Manager (TMCM) servers that manage all sites. Each Control Manager server can replicate database information between IMSS scanners registered to Control Manager.

**Tip**

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

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

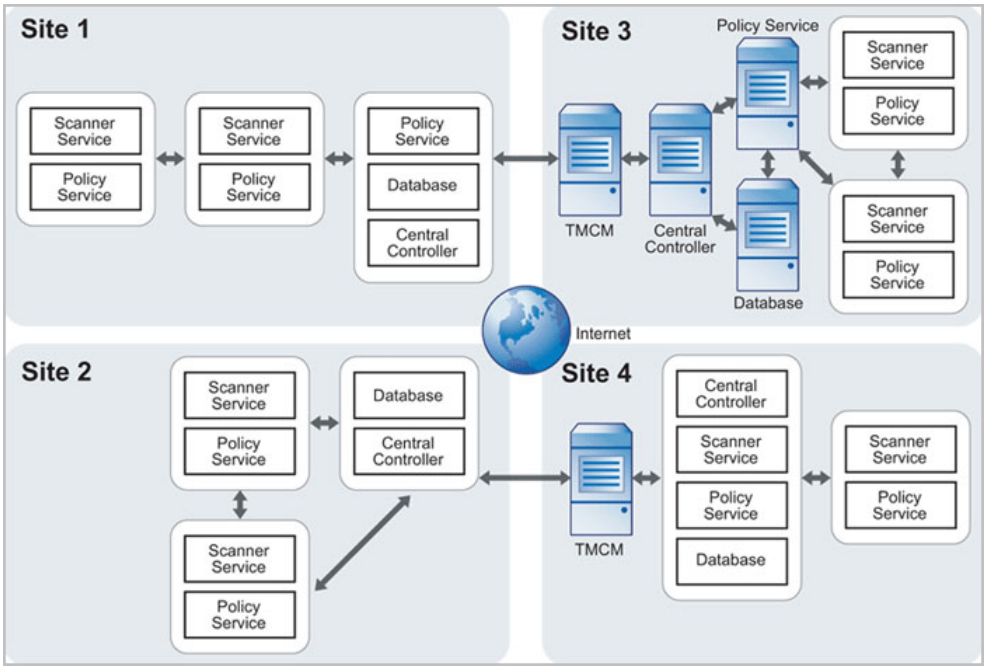



**FIGURE 2-8. WAN deployment**

**Site 1**

An IMSS server with a Central Controller, IMSS Admin database, and policy service + two IMSS scanner services with policy services enabled.

**Site 2**

An IMSS server with a Central Controller, IMSS Admin database, and policy service + two IMSS scanner services with policy services enabled (for fault tolerance).

**Site 3**

An IMSS Central Controller + IMSS Admin database + a single policy service only + two IMSS scanner services with policy services enabled (for fault tolerance).

**Site 4**

An IMSS server with a Central Controller and IMSS Admin database + one IMSS scanner services with policy services enabled.

## Fault Tolerance and Failover in a WAN Scenario

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

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

**Note**

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

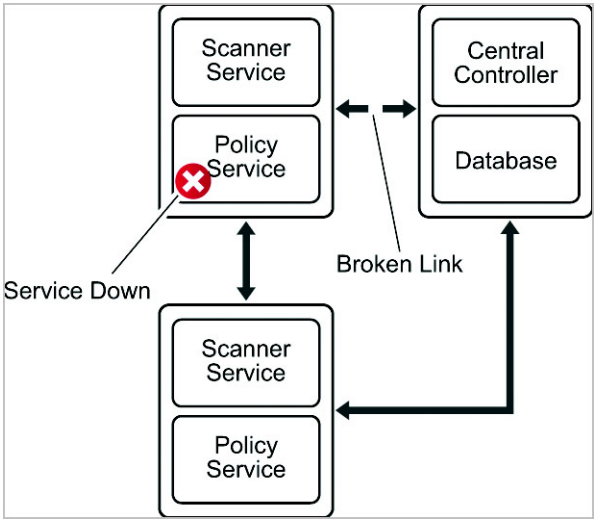



**FIGURE 2-9. Failover**

# IP Filtering

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

## Deployment with IP Filtering

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

**Note**

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

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

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

# About Failover

The following table shows what happens when certain IMSS components malfunction, and how you can plan for failover to keep your IMSS protection up and running. For more information about failover in a WAN deployment scenario, see *Fault Tolerance and Failover in a WAN Scenario on page 2-27*.

**TABLE 2-3. Failover Scenarios**

| COMPONENT THAT MALFUNCTIONS | EXPECTED RESULT | RECOMMENDED FAILOVER PLAN |
|---|---|---|
| Scanner service is not running or becomes disconnected | 1. IMSS tries to restart the scanner service<br>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 2-18*. |

| 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).<br>2. IMSS tries to restart the policy service.<br>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 2-18*. |
| IMSS Admin database is not running | 1. The IMSS server will continue to operate.<br>2. The IMSS web console is unavailable. | Back up the Admin database periodically. |
| EUQ service database is not running | An error message appears on the EUQ Web console. | Back up the EUQ Database periodically. |

| 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.<br>2. Foxhunter will not use the LDAP settings.<br>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**.<br><br>**Note**<br>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:<br>1. Go to **Administration** > **Connections**.<br>2. Click the **LDAP** tab.<br>3. Select the check box next to **Enable LDAP2** and provide the required information.<br><br>**Tip**<br>Trend Micro recommends that you enable the fault tolerance feature on the LDAP server. |

# Chapter 3

# Component Descriptions

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

Topics include:

# About IMSS Components

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

You can install IMSS components on a single computer or on multiple computers. For graphical representations of how these components work together, see *Understanding Installation Scenarios on page 2-16*.

# 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 existing databases.

# Central Controller

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

# Scanner Services

Servers configured as scanner services do the following:

- Accept SMTP and POP3 messaging traffic
- Request policy from a policy service

- Evaluate the message based on the applicable policies
- Take the appropriate action on the message based on the evaluation outcome
- Store quarantined and archived messages locally
- Log policy and system activity locally, and automatically update the log portion of the IMSS database at scheduled intervals, providing indexing to allow users to search through quarantined items and logs

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

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

**Note**

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

# Policy Services

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

## Policy Synchronization

The IMSS Admin database schema includes a versioning mechanism. The policy service checks the database version periodically. If the version number in the database is different from the version cached on the policy service, the policy service performs a database query and retrieves the latest version. This keeps the cached version of the database synchronized with the database, without the need to check the entire database for new or changed entries.

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

# End-User Quarantine Service

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

## Primary and Secondary End-User Quarantine Services

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

## End-User Quarantine Server Components

The EUQ Server includes the following software components:

**Apache HTTP Server**
: Accepts the HTTP requests from end users and distributes them across all installed EUQ Servers. The Apache Web server is only installed on the Primary EUQ Server.

**Tomcat Application Server**
: Accepts the HTTP requests from end users and passes them to Struts.

**Struts Framework**

Controls the page presentation flow for end users.

**End-User Quarantine Application**

Communicates with the other IMSS components to implement the EUQ Console logic.

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

**Email Reputation**

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

## How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email messages containing threats mentioned in the section *IP Filtering on page 3-7*. You can customize several criteria that determine when IMSS starts taking a specified action on an IP address. The criteria differ depending on the potential threat, but commonly include a duration during which IMSS monitors the IP address and a threshold.

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 on page 3-9* and *Advanced on page 3-9*.

### Email Reputation: Standard

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

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

**Tip**

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

### Email Reputation: Advanced

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

This is a dynamic, real-time antispam solution. To provide this service, Trend Micro continuously monitors network and traffic patterns and immediately updates the

dynamic reputation database as new spam sources emerge, often within minutes of the first sign of spam. As evidence of spam activity ceases, the dynamic reputation database is updated accordingly.

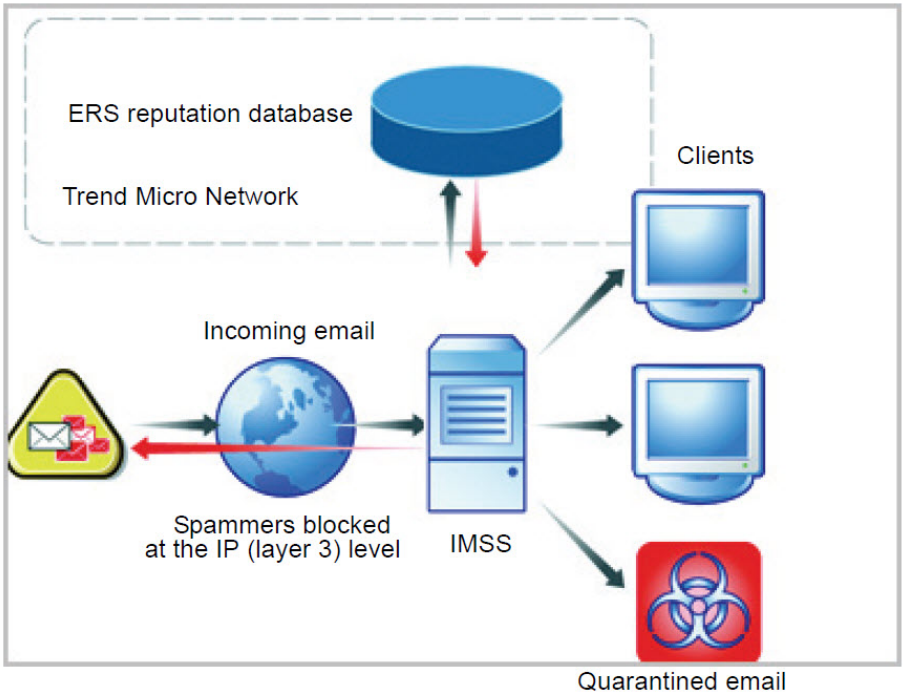
Like Email reputation: Standard, Email reputation: Advanced is a DNS query-based service, but two queries can be made to two different databases: the standard reputation database and the dynamic reputation database (a database updated dynamically in real time). These two databases have distinct entries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

## How Email Reputation Technology Works

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

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

The figure below illustrates how Email reputation works.




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

# About End-User Quarantine (EUQ)

IMSS provides web-based EUQ to improve spam management. The Web-based EUQ service allows end users to manage their own spam quarantine. Messages that Spam Prevention Solution (licensed separately from IMSS), or administrator-created content filters, determine to be spam, are placed into quarantine. These messages are indexed

into a database by the EUQ agent and are then available for end users to review and delete or approve for delivery.

## About Centralized Reporting

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

# Chapter 4

# Installing and Uninstalling IMSS 7.5

This chapter explains how to install IMSS under different scenarios.

Topics include:

# System Requirements

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

**TABLE 4-1. System Requirements**

| SPECIFICATION | DESCRIPTION |
|---|---|
| Operating System | • Microsoft™ Windows™ Server 2012 (X64)<br>• Microsoft™ Windows™ Server 2008 R2 SP1 (X64)<br>• Microsoft Windows Server 2008 SP2 (X86 and X64)<br>• Microsoft Windows Server 2003 R2 SP2 (X86 and X64)<br>• Microsoft Windows Server 2003 SP2 (X86 and X64) |
| CPU | • Recommended:<br>Intel™ Quad Core 2.0GHz or above<br>• Minimum:<br>Intel™ Dual Pentium™ IV 3GHz or above |
| Memory | • Recommended:<br>8GB<br>• Minimum:<br>2GB |

| SPECIFICATION | DESCRIPTION |
|---|---|
| Disk Space | • Recommended:<br>250GB total<br>The following recommendations are based on 500,000 messages/day, a 50% quarantine rate, and logs preserved for a month.<br>  • 10GB for mail storage<br>  • 50GB or more for the Admin database<br>  • 20GB or more for the EUQ database<br>  • 40GB or more for the working quarantine folder<br>• Minimum:<br>80GB total |
| Browser | • Microsoft™ Internet Explorer™ 7, 8, 9, 10<br>  **Note**<br>For Internet Explorer™ 8, 9, and 10, only the Compatibility View mode is supported.<br>• Mozilla™ Firefox™ 22 |
| Monitor | Monitor that supports 800 x 600 resolution with 256 colors or higher |
| Microsoft SQL Server | • Microsoft SQL Server 2008, 2008 SP3<br>• Microsoft SQL Server 2008 R2, R2 SP1, R2 SP2<br>• Microsoft SQL Server 2005 SP3, SP4<br>• Microsoft SQL Server 2008 Express SP3<br>  **Note**<br>IMSS does not support Windows Authentication Mode for databases. |

| SPECIFICATION | DESCRIPTION |
|---|---|
| LDAP server | • IBM™ Lotus Domino 8.0, 8.5<br>• Microsoft Active Directory 2000, 2003, 2008 R2, 2012 |
| Trend Micro Control Manager™ | • Version 5.5 (Service Pack 1 Patch 4 with Hotfix 1921 or later version)<br>• Version 6.0 (Patch 4 or later version) |
| Deep Discovery Advisor | Version 3.0 (Service Pack 1 or later version) |

**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`.

## Performing a Basic Installation

To install the SQL Server Express database on this server, make sure that the following system requirements are met:

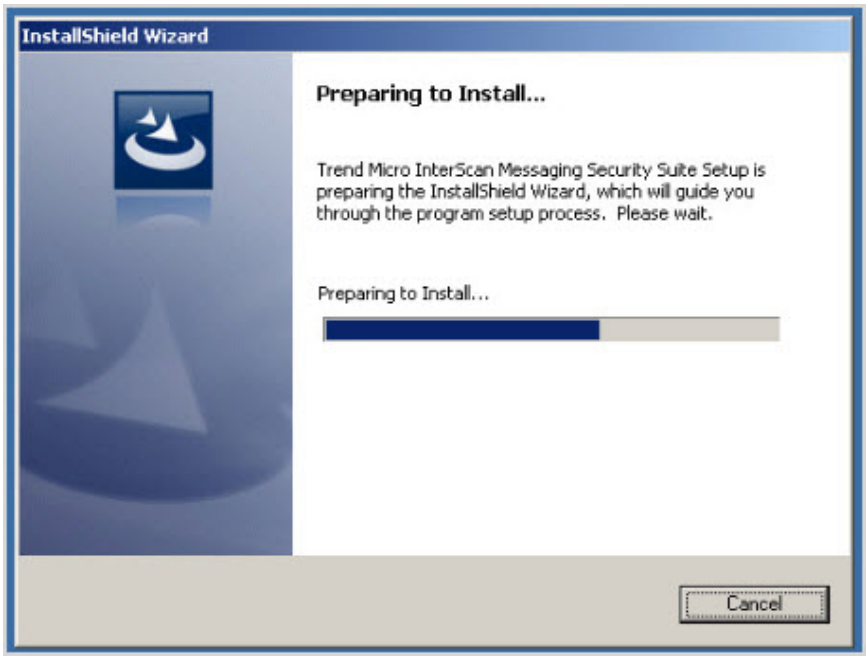
- Windows Installer 4.5
- Microsoft .Net Framework 2.0 SP2

For details about the system requirements, see *System Requirements on page 4-2*.

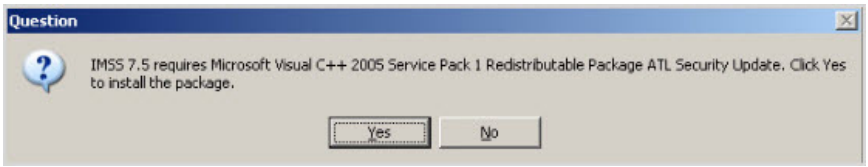
**Procedure**

1. Double-click `Setup.exe`.

   The **Preparing to Install...** screen appears.

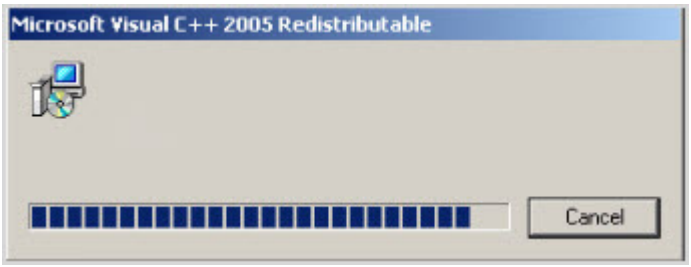



   If Microsoft Visual C++ 2005 has not been installed on the server, a dialog box appears.

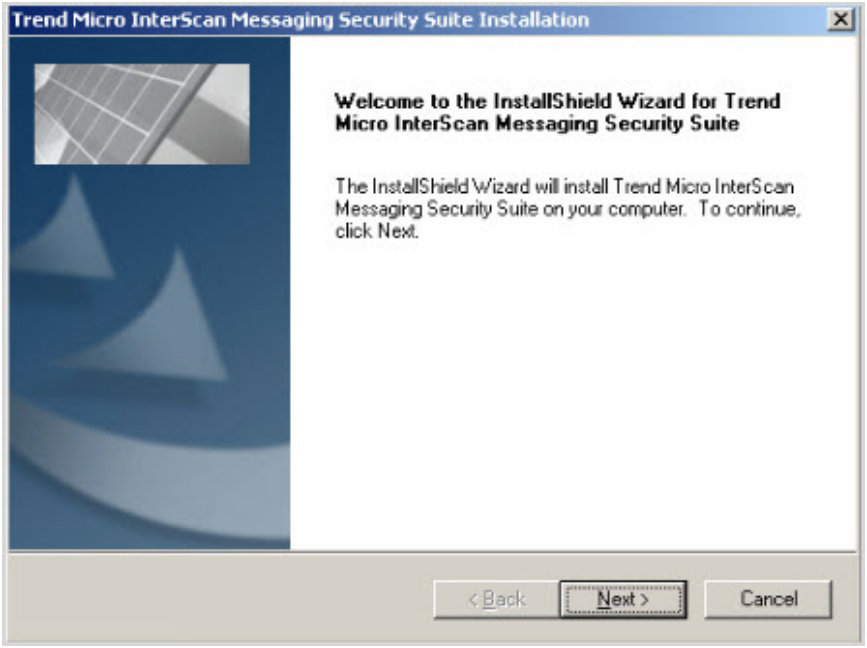



2. Click **Yes**.

Installation of Microsoft Visual C++ 2005 begins.

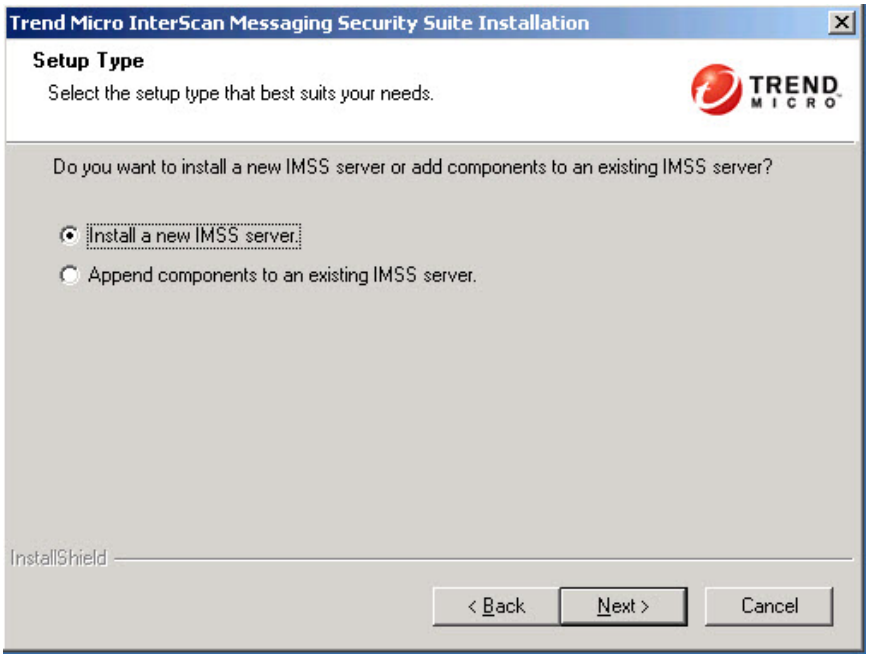



When the installation completes, the InstallShield Wizard for IMSS appears.



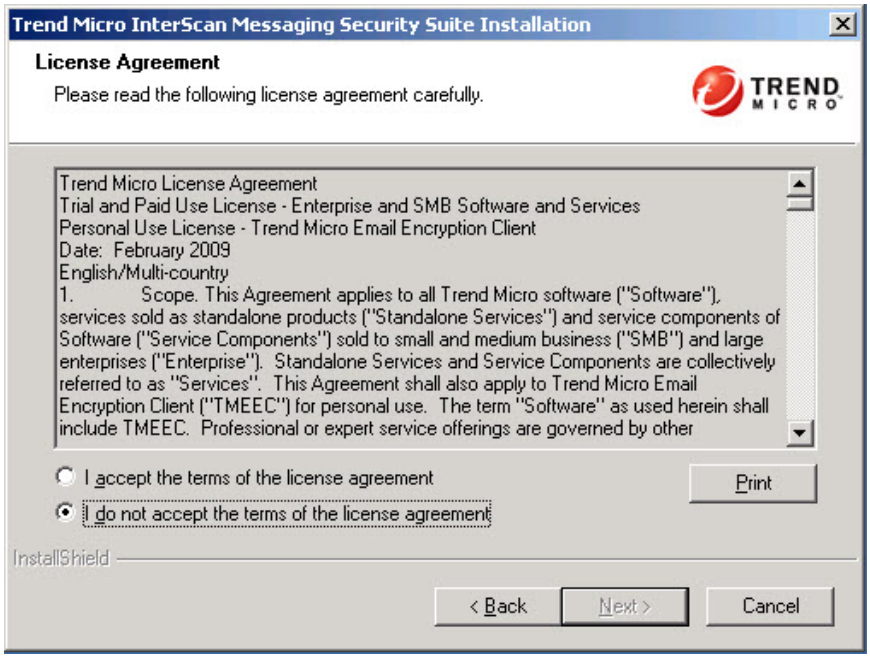

3. Click **Next**.

The **Setup Type** screen appears.




4. Select **Install a new IMSS server**.
5. Click **Next**.

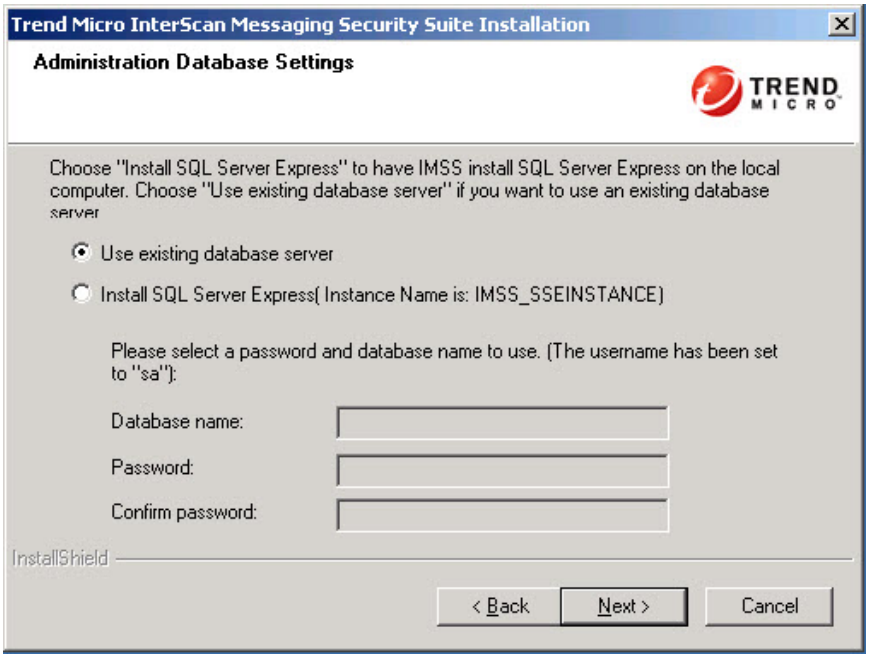
The **License Agreement** screen appears.




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

7. Click **Next**.

The **Administration Database Settings** screen appears.

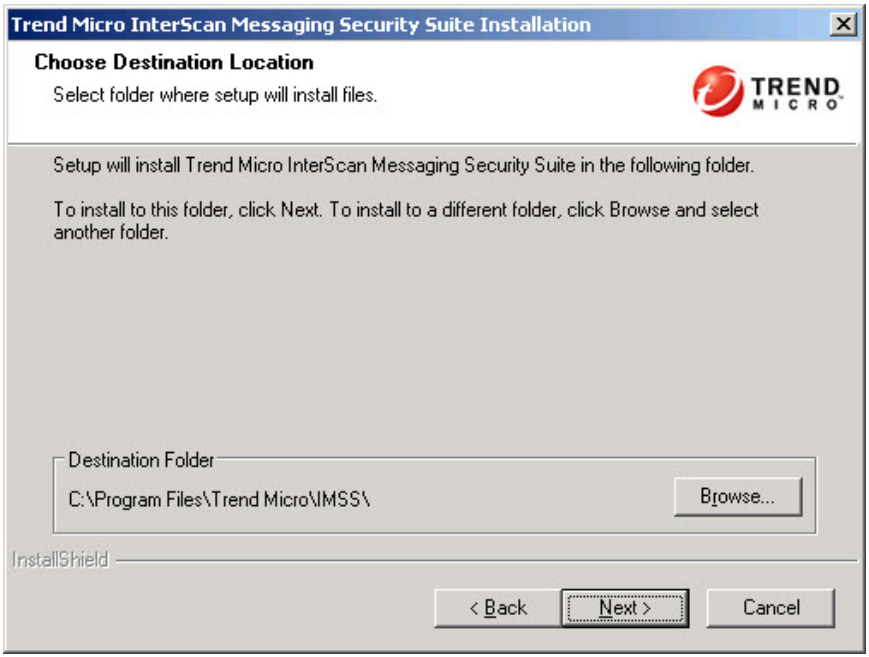



8. Select the database configuration.

   - To configure the existing database server, see *Using the Existing Database Server on page 4-17*.
   - To install SQL Server Express, see *Installing SQL Server Express on page 4-19*.

9. Click **Next**.

The **Choose Destination Location** screen appears.




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

**Note**

For Windows Server x64 platforms, note the following:

- IMSS 7.5 cannot install to `C:\Program Files\Trend Micro\imss`. Only x64 programs can deploy to this directory.
- To install IMSS on x64 platforms, use the following directory `C:\Program Files(x86)\Trend Micro\imss`.

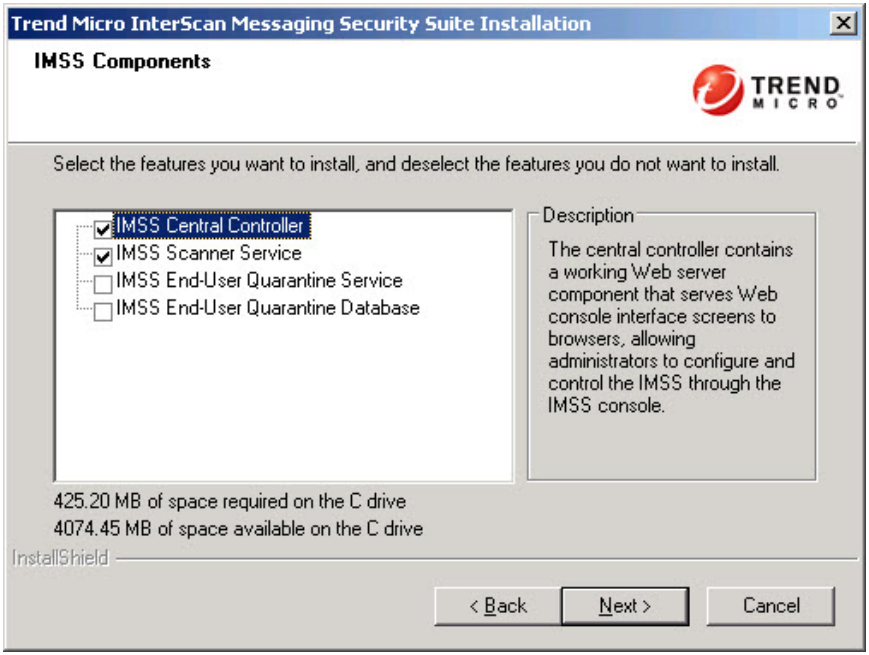
**WARNING!**

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.



**Note**

The IMSS Central Controller installs the BIND Service (ISC BIND) for IP Profiler. It is recommended that you do not use a DNS server to install a Central Controller because the DNS service and ISC BIND both listen on port 53. If a DNS server is used, IMSS delivers a "Port 53 is used by another service. Stop the service before you enable IP Profiler." message.

If you must use the DNS server, ignore this message and proceed with the installation. After the installation is completed, stop the DNS service before enabling IP Profiler. Other IMSS functions are not affected.

12. Select the required components.

- **IMSS Central Controller**
- **IMSS Scanner Service**
- **IMSS End-User Quarantine Service**
- **IMSS End-User Quarantine Database**

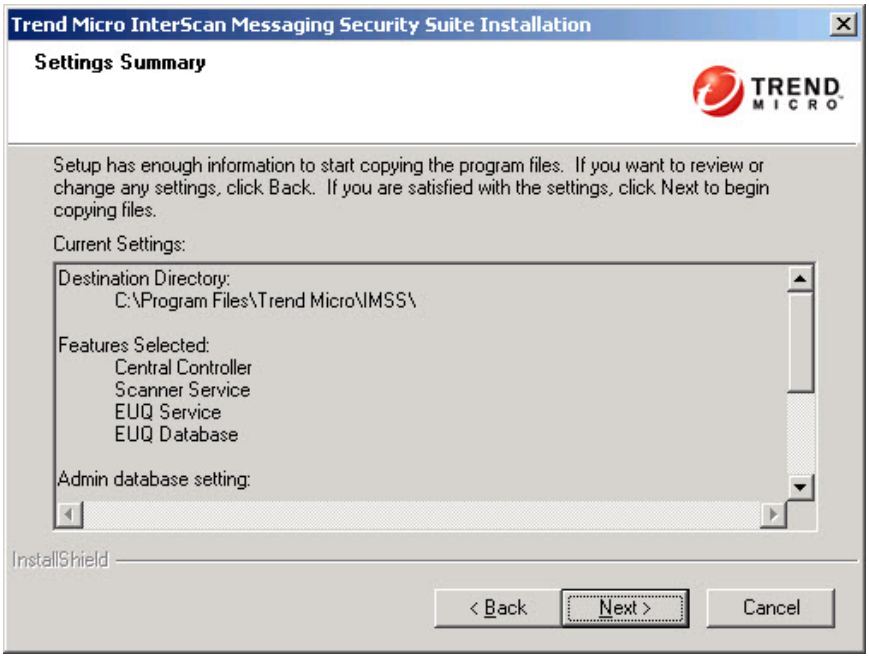
**Note**

For component descriptions, see *Component Descriptions on page 3-1*.

13. Click **Next**.

If you selected the **IMSS End-user Quarantine Database** option, the **End-user Quarantine (EUQ) Database Settings** screen appears. For details, go to *Configuring EUQ Database Settings on page 4-20*.

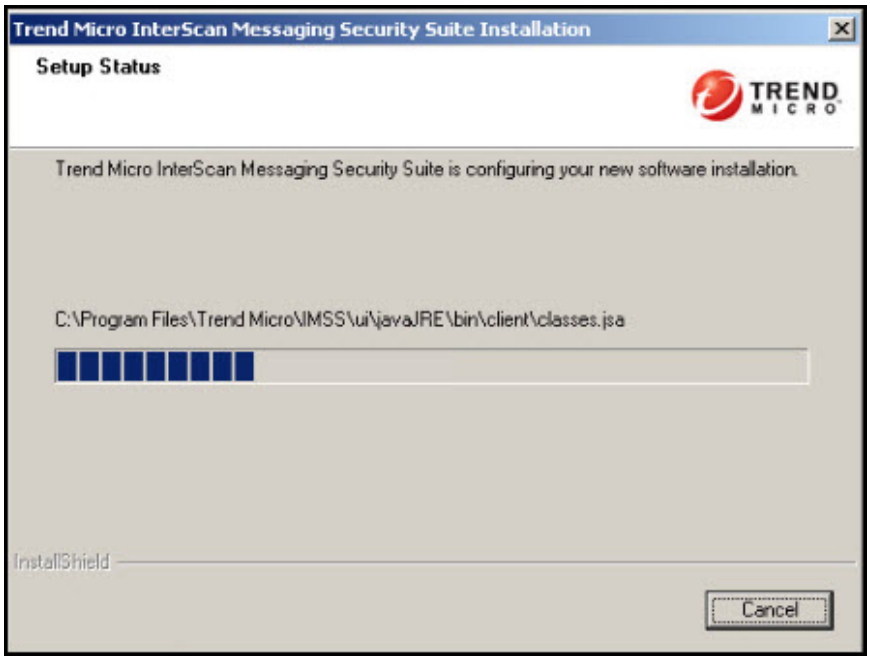
If you selected other components, the **Settings Summary** screen appears.



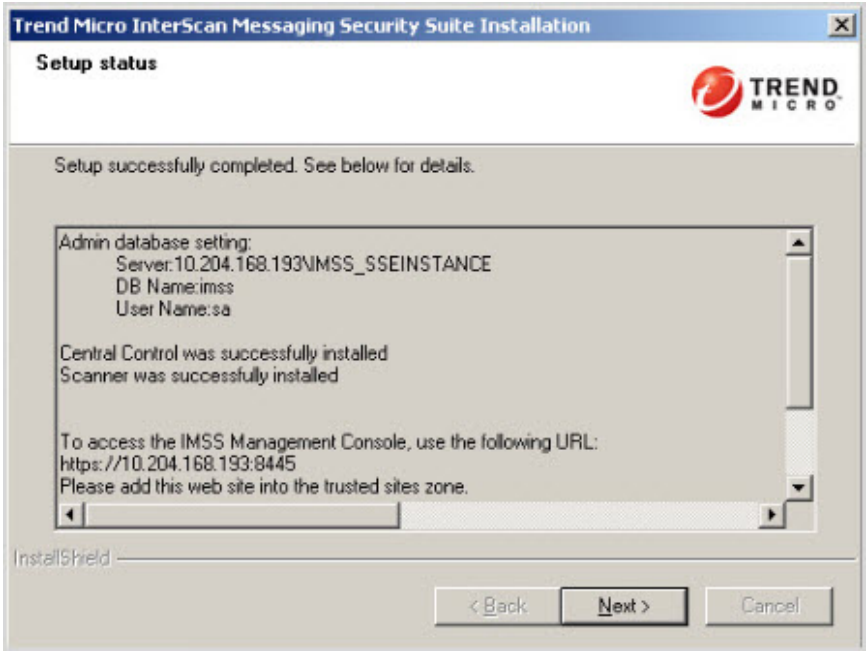

14. Verify that the selected components and the defined settings are correct.

15. Click **Next**.

If the system requirements are met, the **Setup Status** screen appears, and installation begins.

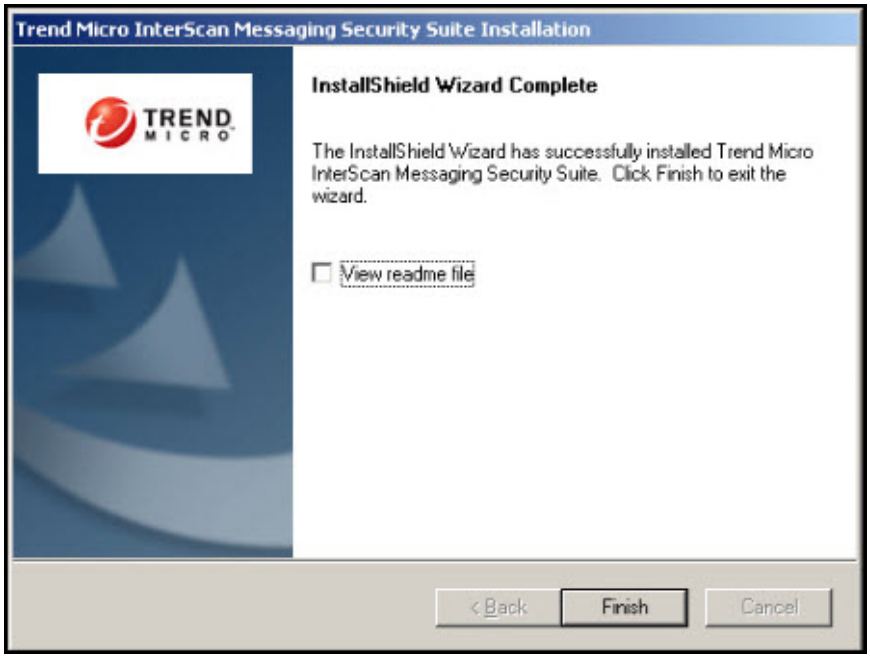



**16.** Wait for the installation to complete.



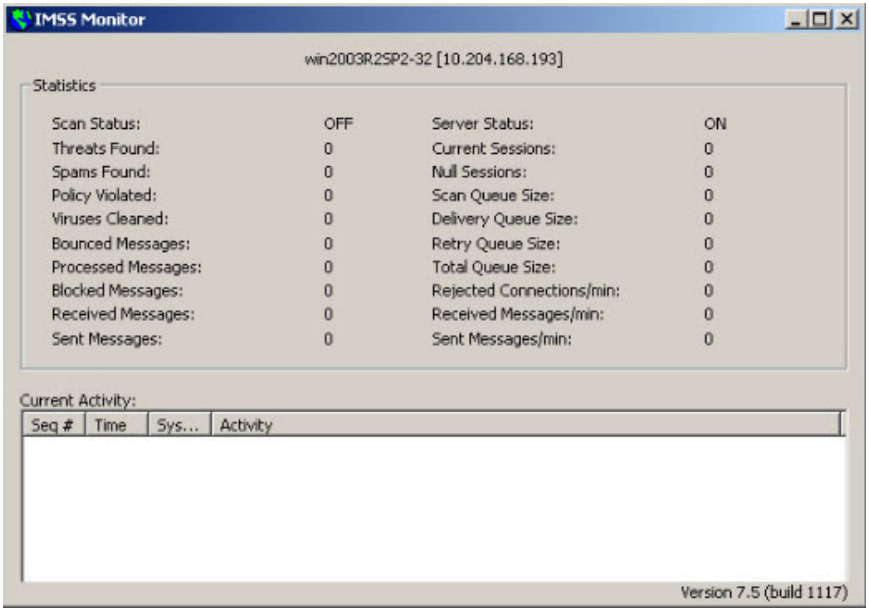

**17.** Click **Next**.

The **InstallShield Wizard Complete** screen appears.




18. Click **Finish**.

The IMSS Monitor appears.




## Using the 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.

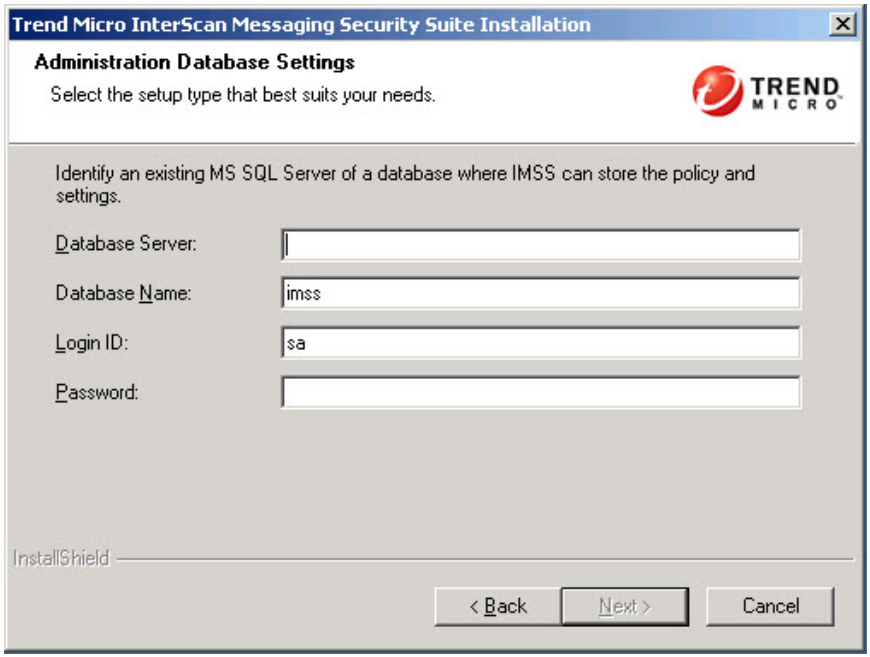
**Note**

IMSS does not support databases using *Windows Authentication Mode*.

### Procedure

1. Select **Use existing database server**.
2. Click **Next**.

   The **Administration Database Settings** screen appears.




3. Specify the required information for the existing database server.

**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.

## Installing SQL Server Express

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.

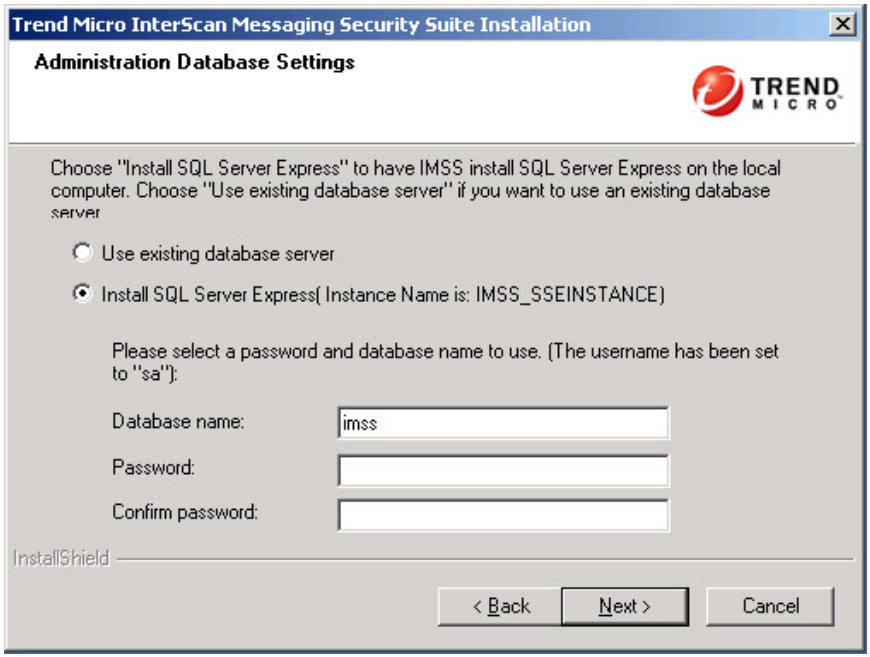
**Procedure**

1. Select **Install SQL Server Express**.

**Note**

For details about the system requirements, see *System Requirements on page 4-2*.

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



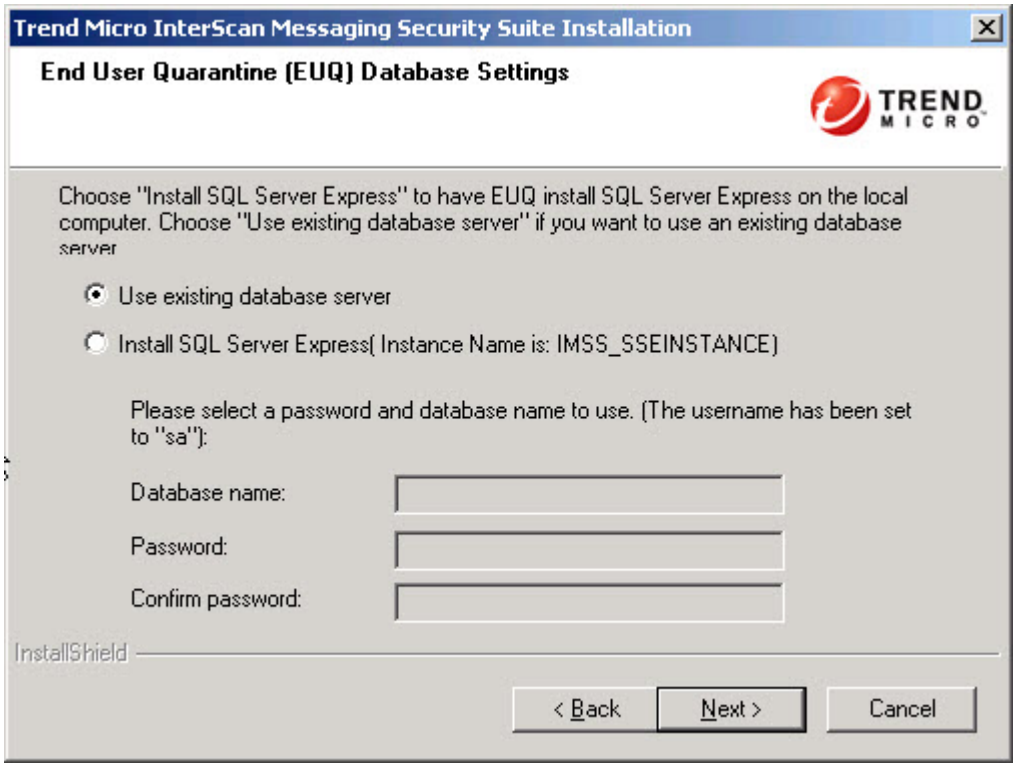

**Note**

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.`

## Configuring EUQ Database Settings

The **End-user Quarantine (EUQ) Database Settings** screen appears when you select **IMSS End-User Quarantine Database** as a component to install.




**Procedure**

- To configure the existing database server, see *Using the Existing Database Server on page 4-17*.
- To install SQL Server Express, see *Installing SQL Server Express on page 4-19*.

# 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.

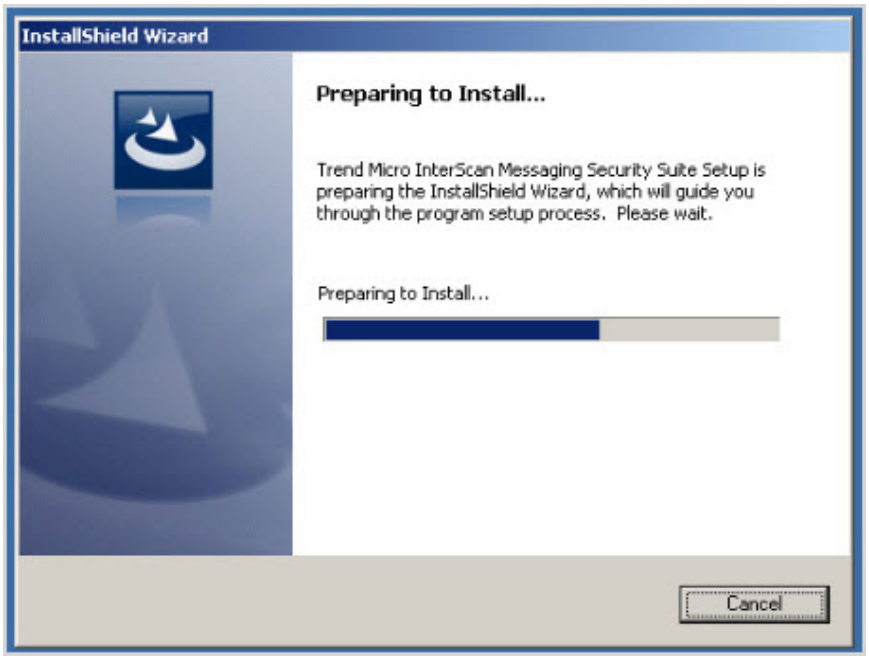
## Appending Components When No Previously Installed Components Exist

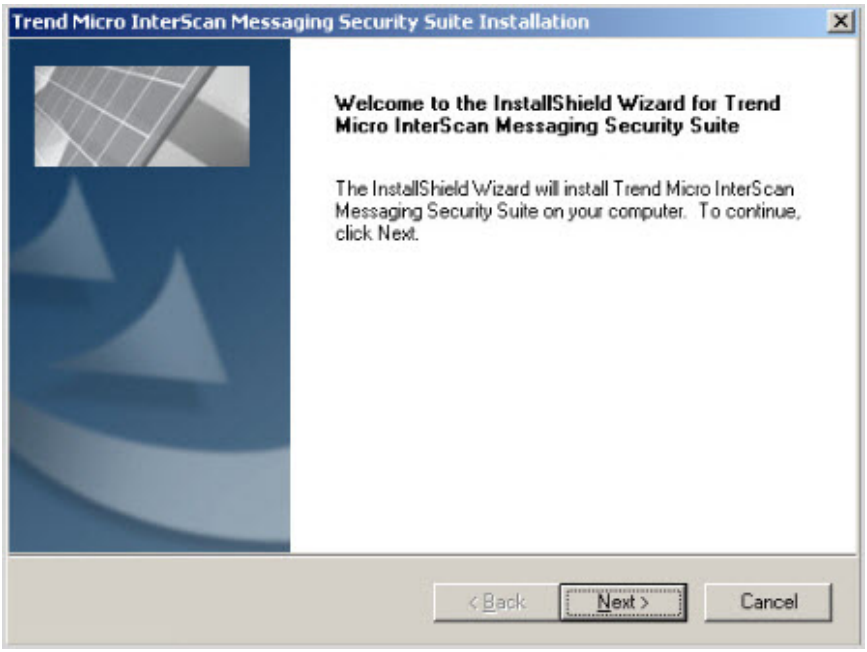
Add IMSS components to servers where no IMSS components existed.

**Procedure**

1. Double-click on `Setup.exe`.

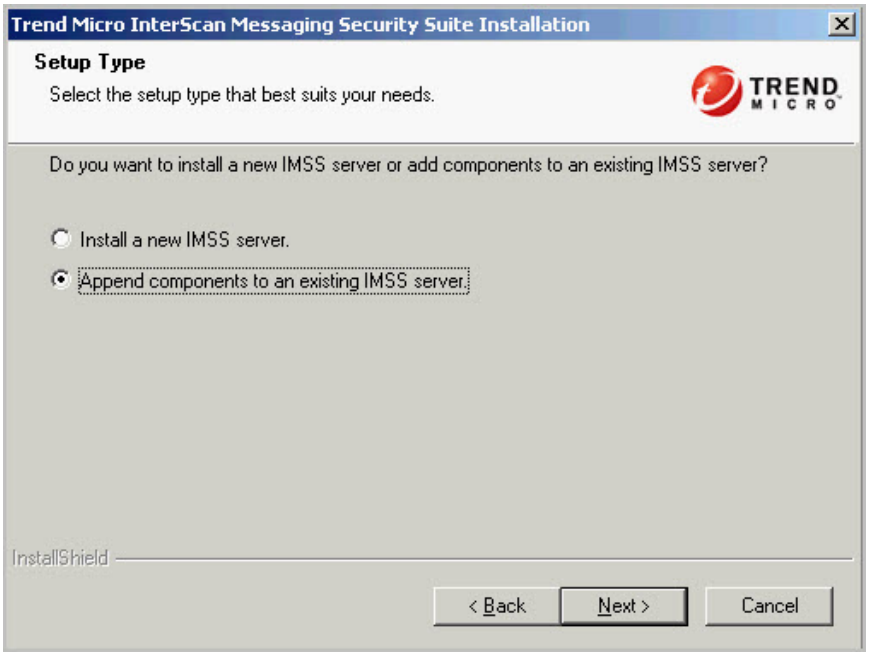
The **Preparing to Install...** screen appears.




Trend Micro InterScan Messaging Security Suite Installation
Welcome to the InstallShield Wizard for Trend Micro InterScan Messaging Security Suite
The InstallShield Wizard will install Trend Micro InterScan Messaging Security Suite on your computer. To continue, click Next.
< Back
Next >
Cancel

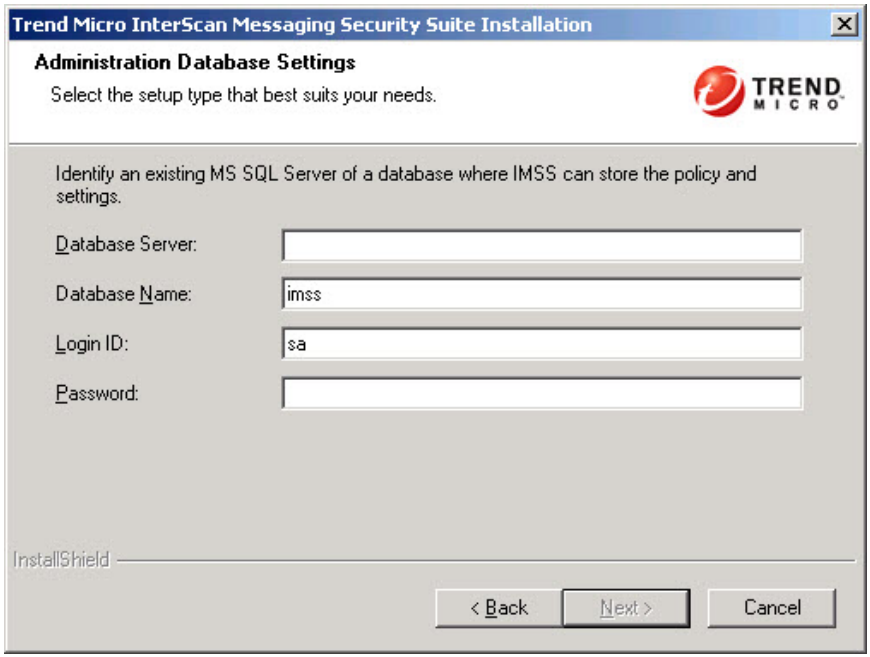
2. Click **Next**.

The **Setup Type** screen appears.




3. Select **Append components to an existing IMSS Server**.
4. Click **Next**.

The **Administration Database Settings** screen appears.



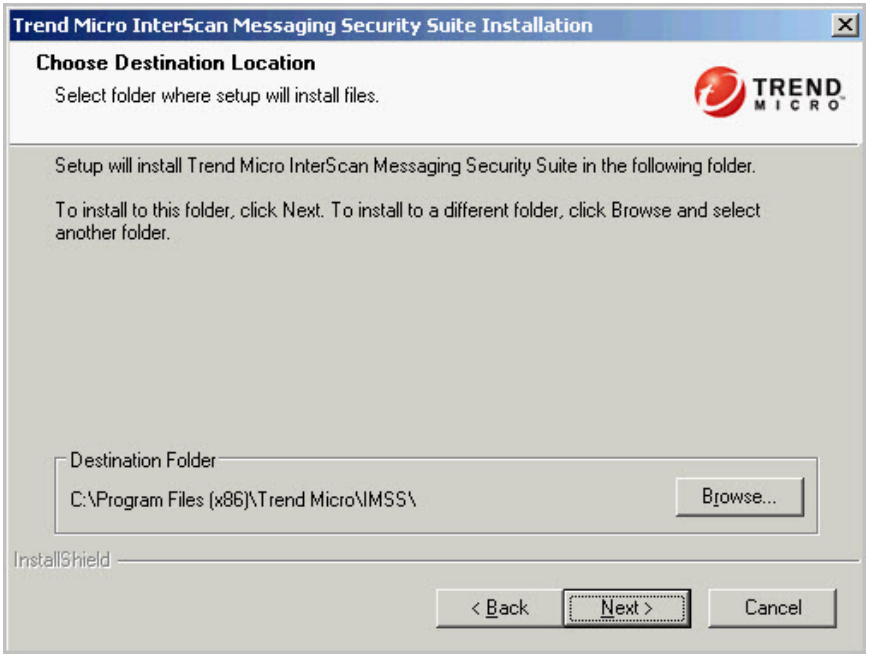

5. Type the required information for the administration database.

   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.

**Note**

For Windows Server x64 platforms, note the following:

- IMSS 7.5 cannot install to `C:\Program Files\Trend Micro\imss`. Only x64 programs can deploy to this directory.
- To install IMSS on x64 platforms, use the following directory `C:\Program Files(x86)\Trend Micro\imss`.

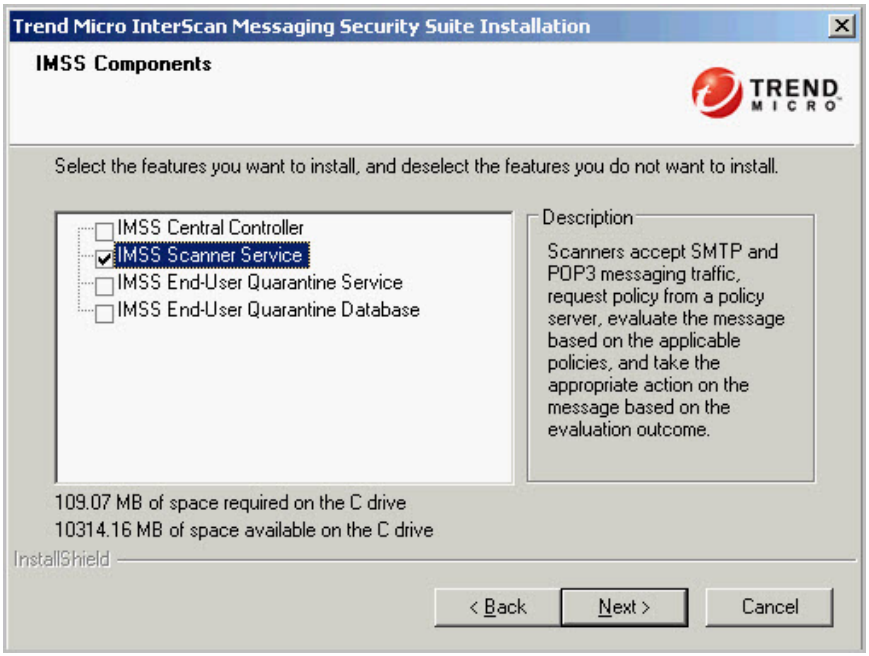
**WARNING!**

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.



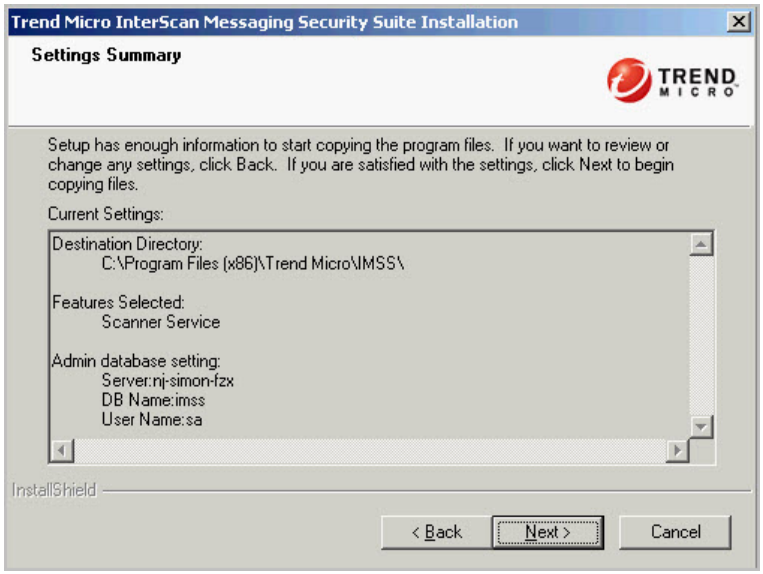

9. Select the components to install.

- To install additional IMSS Scanner Service:

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

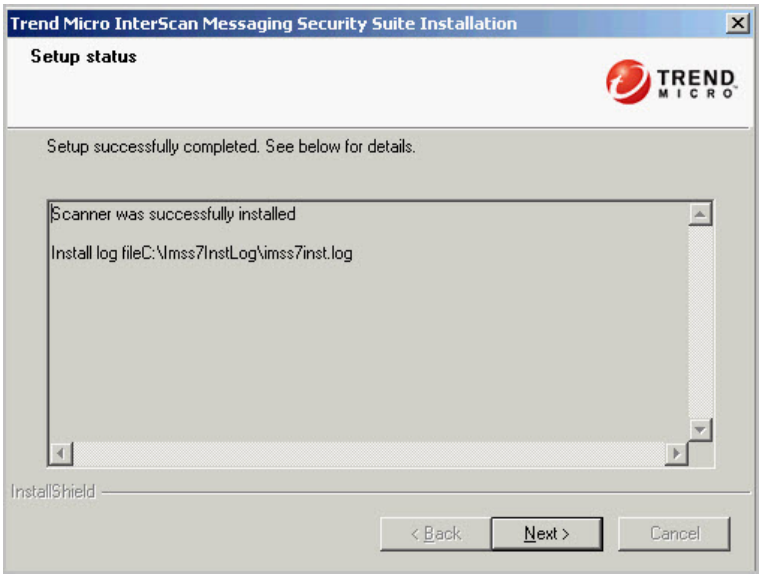
  b. Click **Next**.

The **Settings Summary** screen appears.




c. Verify the settings and click **Next**.

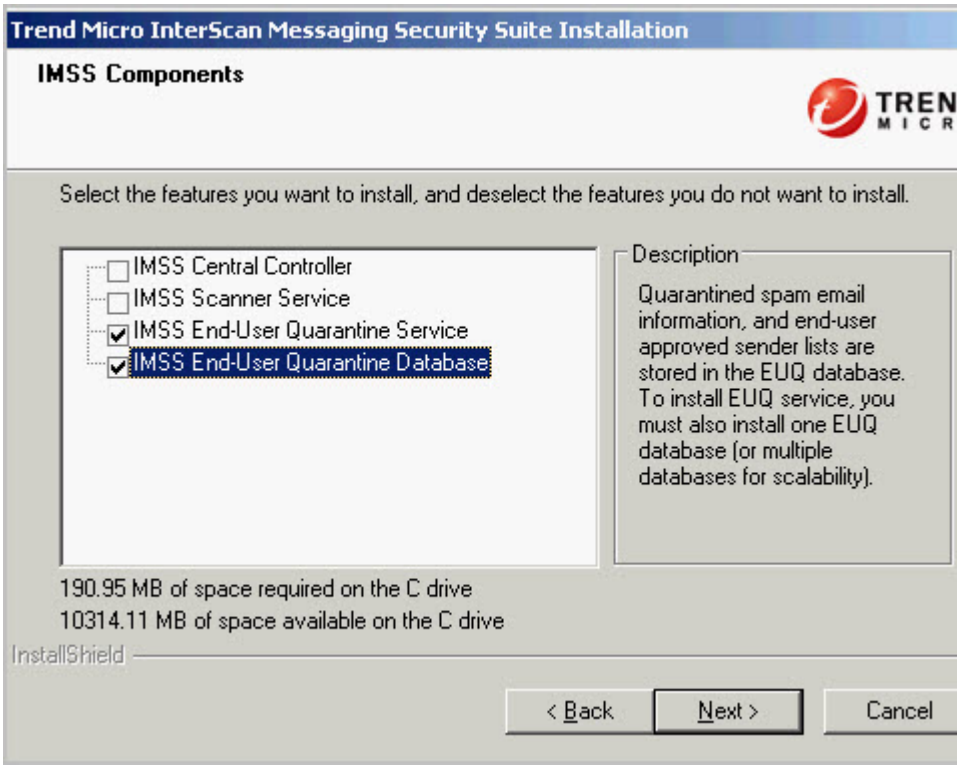
The **Setup Status** screen appears.




d. Click **Next**.

The files install.

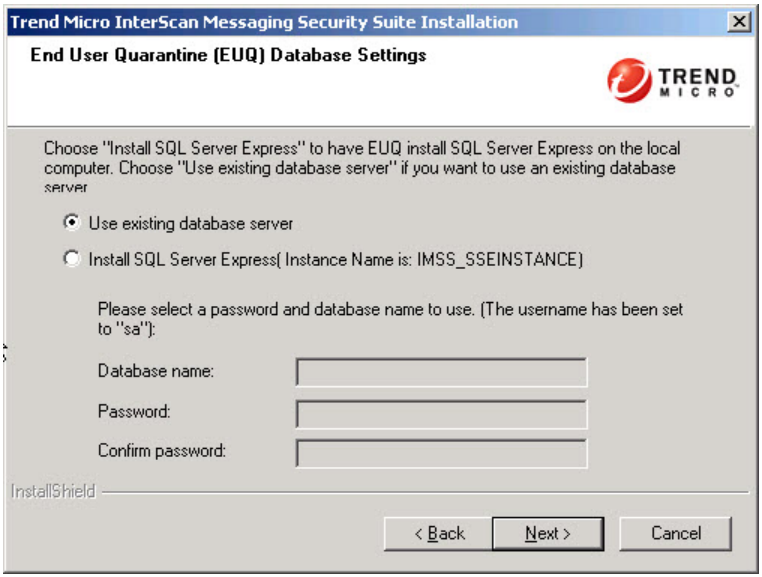
- To install additional EUQ Service and/or EUQ Database:




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.

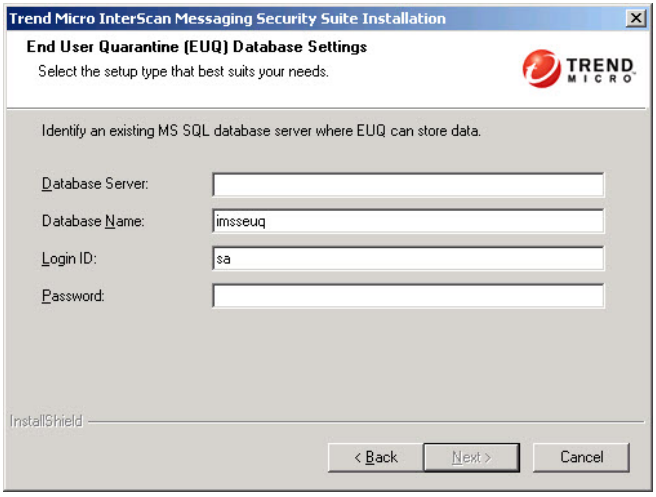



- To install EUQ database on an existing database server:

  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.

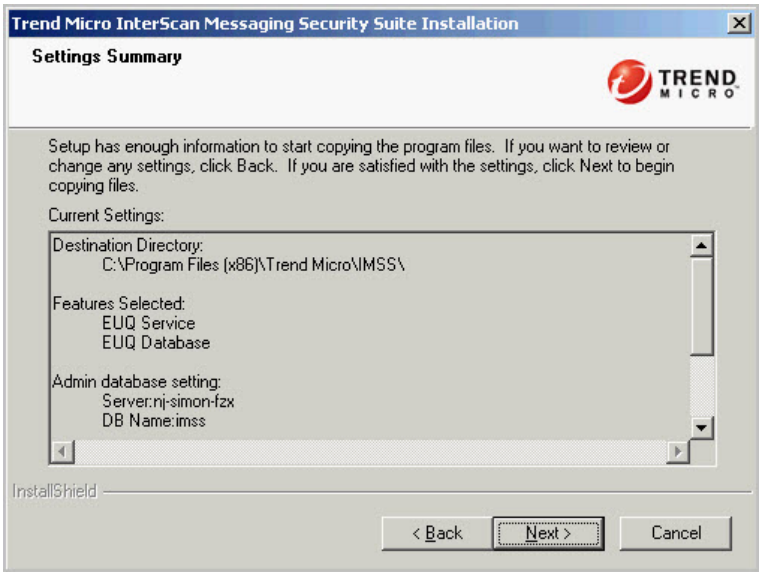
- To install an SQL Server Express database on this server:

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

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

c. Click **Next**.

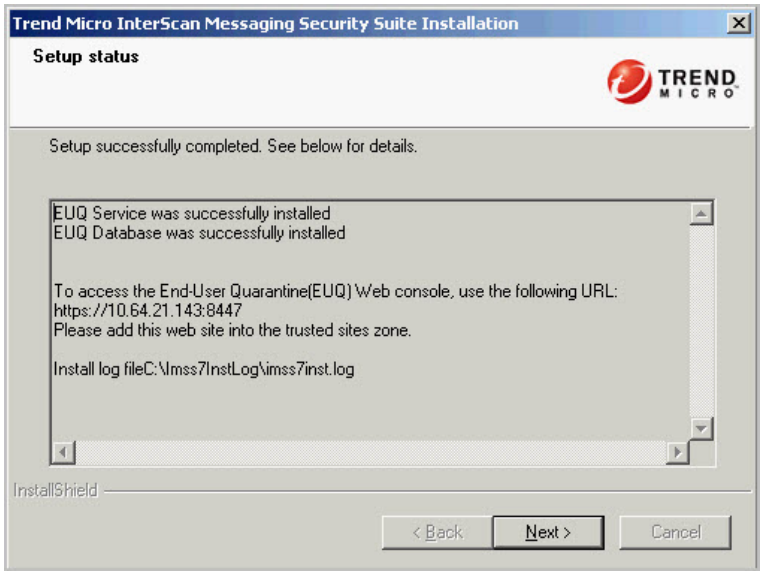
The **Settings Summary** screen appears.




d. Verify the selected components and the defined settings.

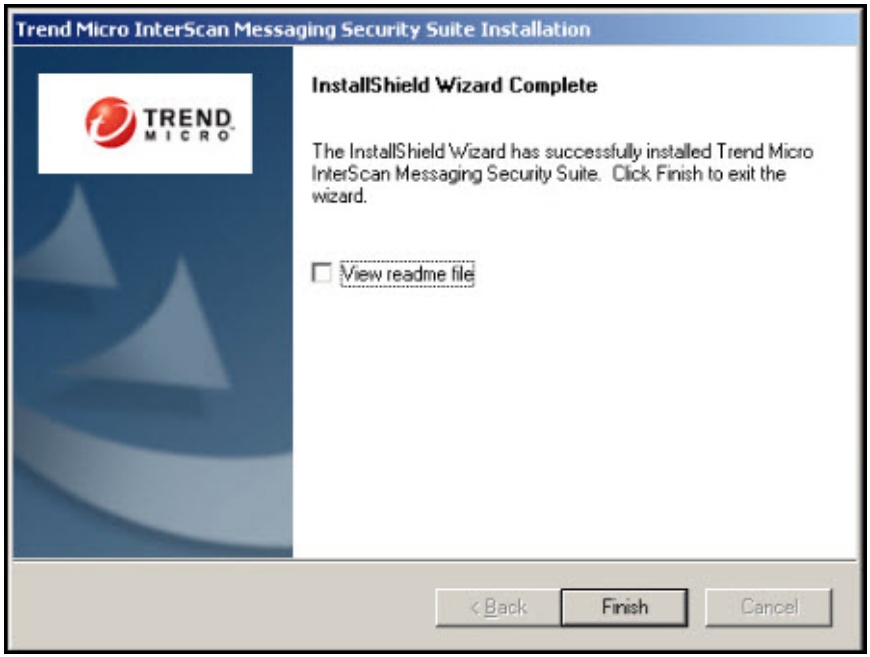
e. Click **Next**.

The **Setup Status** screen appears.




**10.** Click **Next**.

The **InstallShield Wizard Complete** screen appears.




11. 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.

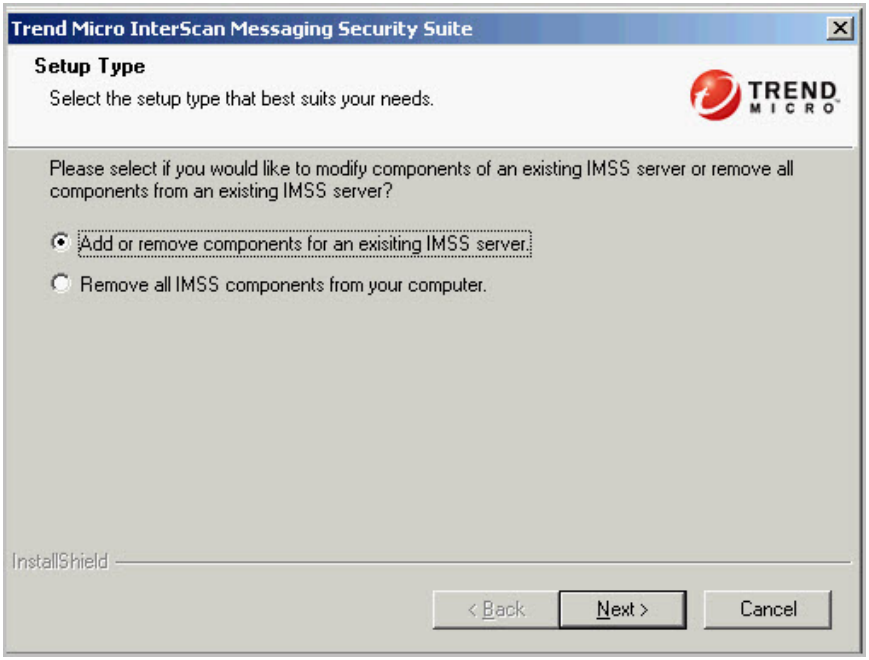
**Procedure**

1. Double-click `Setup.exe`.

   The **Preparing to Install...** screen appears, followed by the **Welcome** screen.

2. Click **Next**.

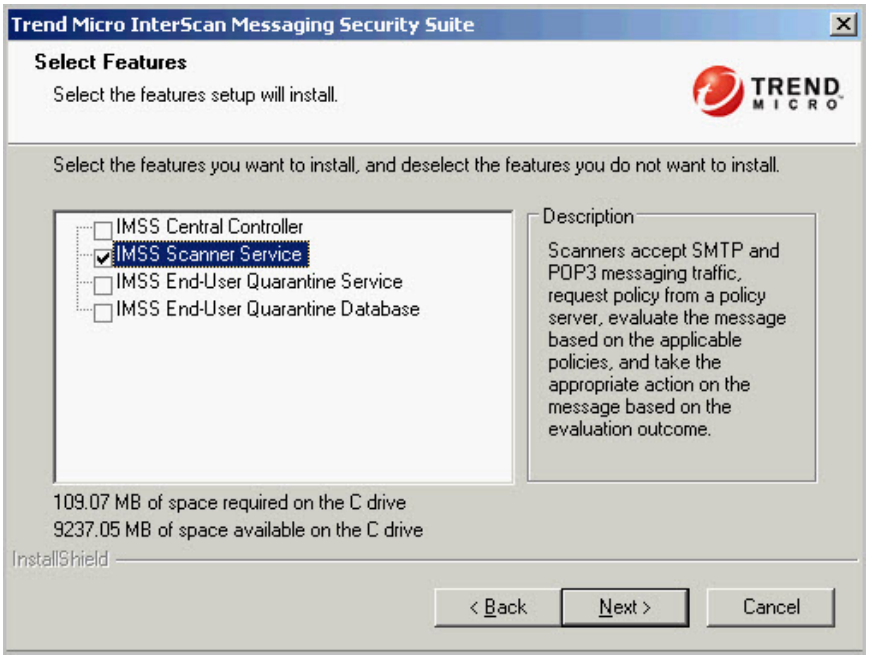
   The **Setup Type** screen appears.




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

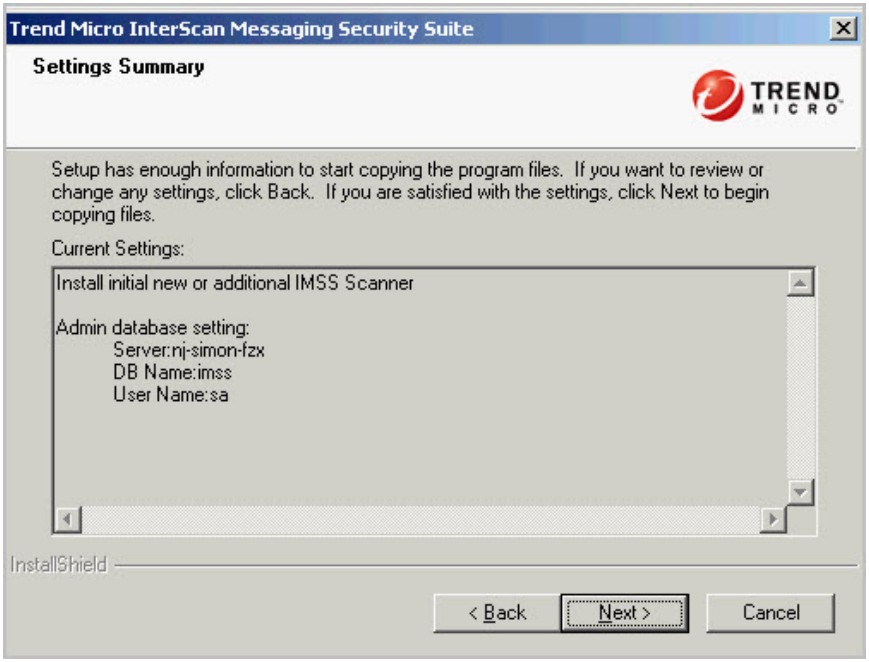
4. Click **Next**.

The **Select Features** screen appears.



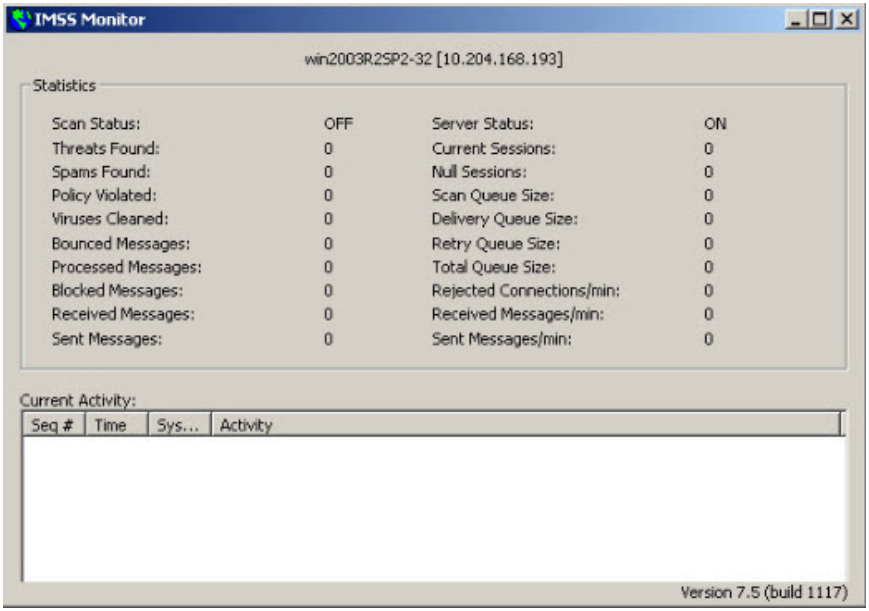

5. Select the component to add.
6. Click **Next**.

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.

# Performing a 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`.

**Procedure**

1. Install IMSS on a single server.

   See *Single-Server Installation on page 4-4*.

2. Append additional IMSS scanner services, EUQ services or EUQ databases as required.

   See *Multiple Scanner and EUQ Service/Database Installation on page 4-22*.

# 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.

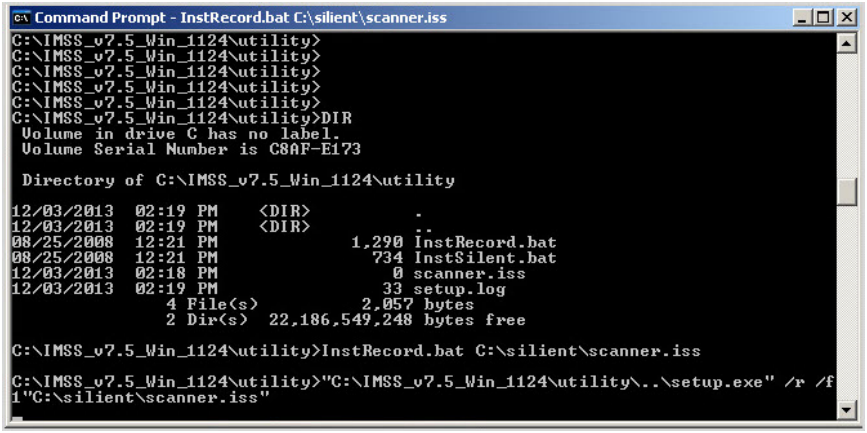
Silent installation includes two main steps:

## Recording the Installation Steps

Silent installation records the configuration settings specified during installation.

**Procedure**

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
   ```

   **Note**

   a. You can specify the path where you want to store the script. However, the path must already exist before you run `InstRecord.bat`.

   b. The script file must have an `.iss` extension.

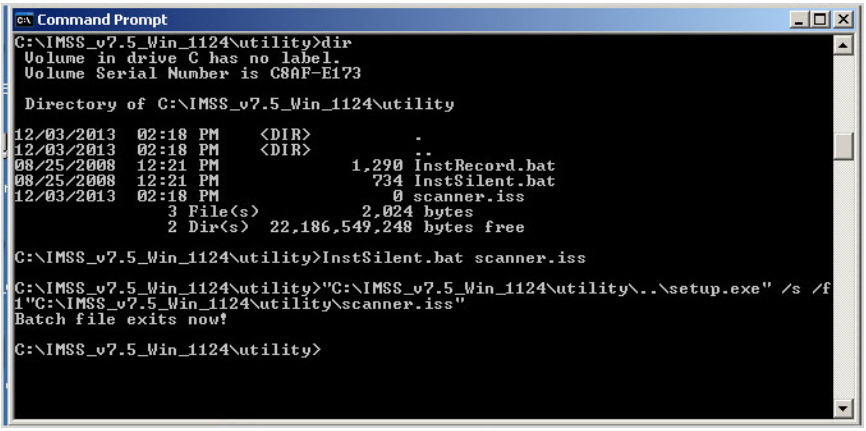
   c. If you do not specify the path, the script will be created under the current folder.

   The installation proceeds automatically. For details about the installation, see *Single-Server Installation on page 4-4*.

# Running the Silent Installation Script

**Procedure**

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 4-41*. 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, go to **Summary** > **System** on the web 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.

**Procedure**

1. Click `Setup.exe`.

   The **Setup Type** screen appears.

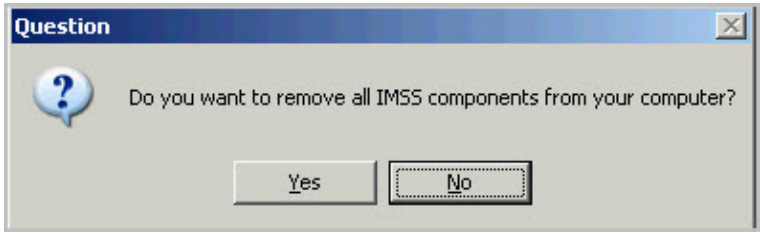

2. Select the components to remove:

- To remove all IMSS components from the computer:

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

  b. Click **Next**.

     A confirmation screen appears.



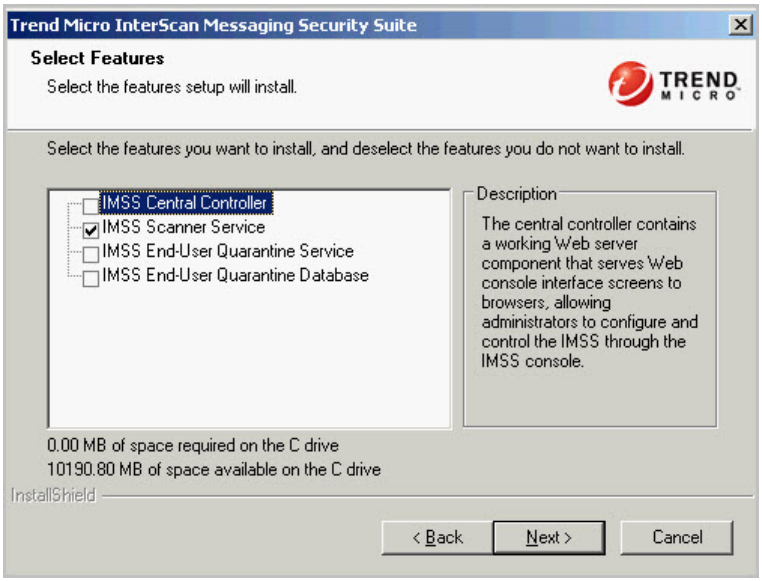

  c. Click **Yes** to confirm.

- 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 the check box for the component to be uninstalled.

d. Click **Next**.

The following message appears if you chose to uninstall the EUQ database.

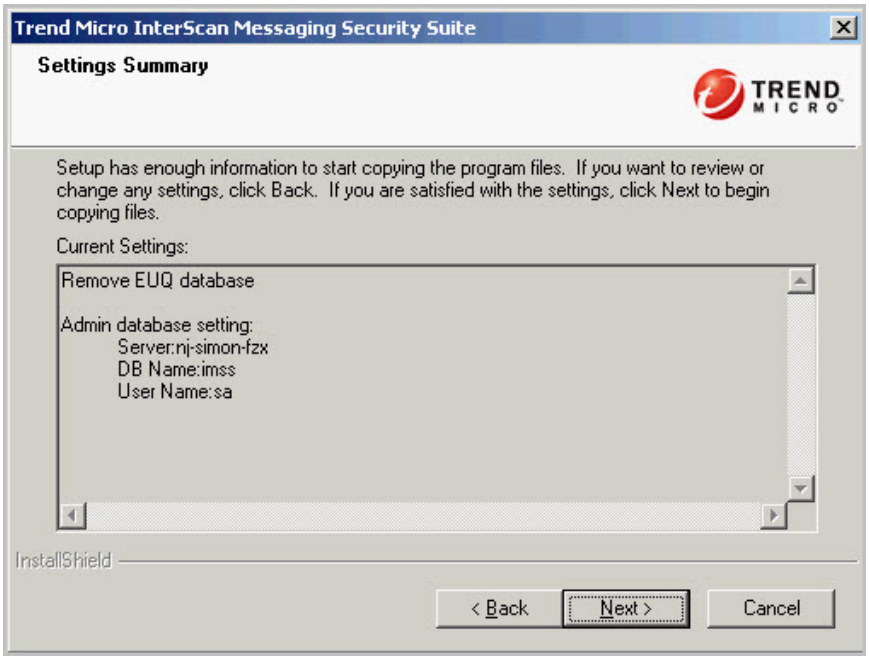

e. Click **OK**.

**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.

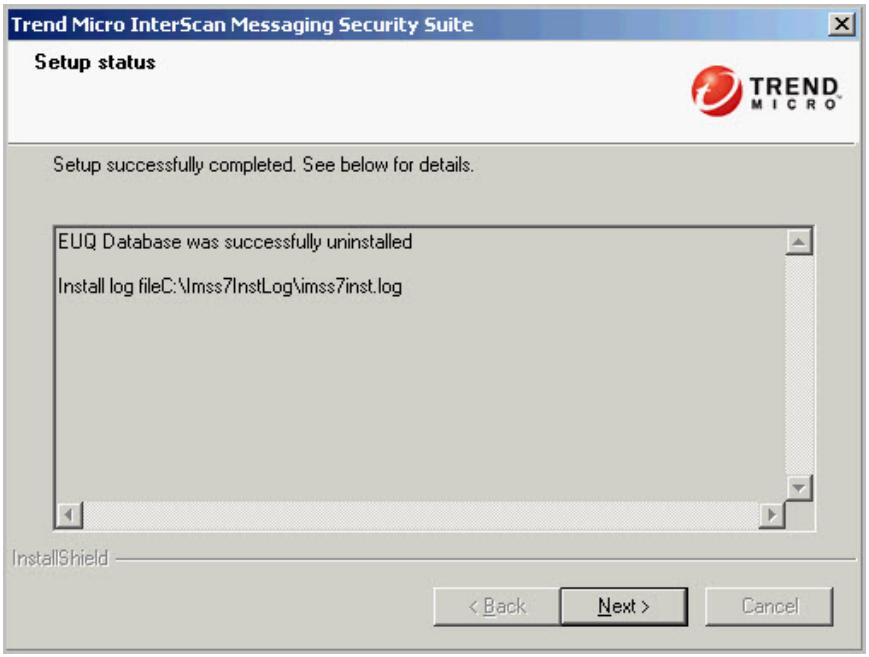
3. Click **Next**.

   The **Settings Summary** screen appears.



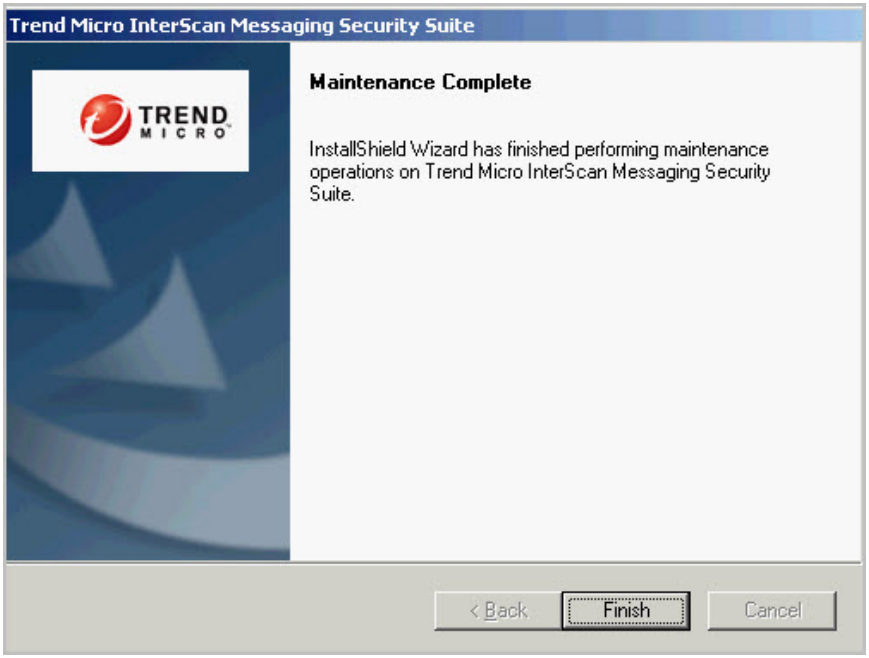

4. Click **Next**.

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 4-41*.

**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.

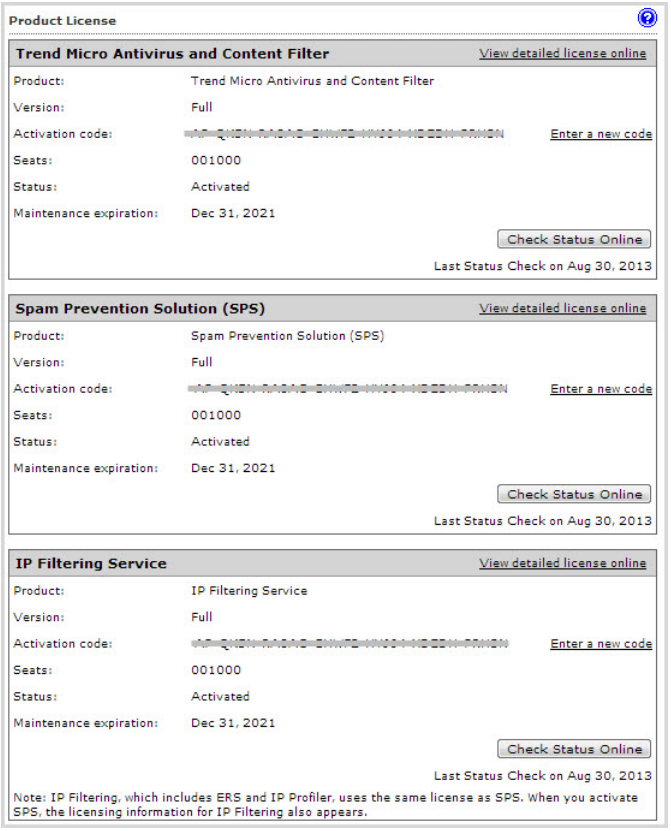
Fourteen (14) days prior to the expiry of the evaluation period, IMSS will display a warning message on the management console alerting you of the impending expiration.

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

**Procedure**

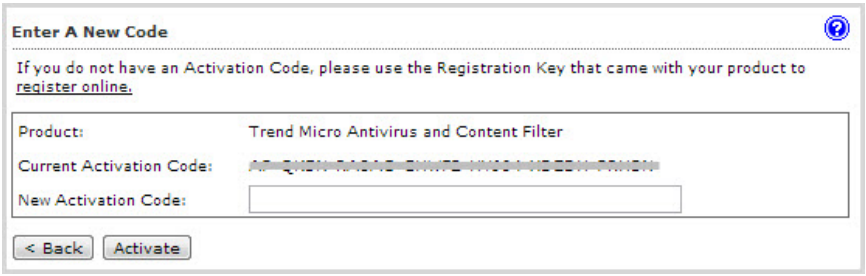
1. Go to **Administration** > **Product Licenses**.

The **Product License** screen appears.




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

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




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

**Note**

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

4. Click **Activate**.

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

# Upgrading IMSS Windows 7.1 to IMSS Windows 7.5

Upgrade IMSS Windows 7.1 to IMSS Windows 7.5 in either of the following ways:

- Migrating from IMSS Windows 7.1 to IMSS Windows 7.5

  In this way, you can export all IMSS settings, excluding the data generated, such as logs and reports, from IMSS 7.1 and import them to IMSS 7.5.

  For more information, see *Migrating from IMSS Windows 7.1 to IMSS Windows 7.5 on page 5-5*.

- Installing IMSS Windows 7.5 Over IMSS Windows 7.1 Patch 3

  In this way, you can retain all IMSS 7.1 settings, including the generated data, such as logs and reports.

  For more information, see *Installing IMSS Windows 7.5 Over IMSS Windows 7.1 Patch 3 on page 5-7*.

## Migrating from IMSS Windows 7.1 to IMSS Windows 7.5

The migration process requires the following tasks:

- **Step 1**: Exporting IMSS 7.1 Windows settings
- **Step 2**: Importing IMSS 7.1 Windows settings to IMSS 7.5

**Important**

IMSS Windows 7.1 patch 3 is required when upgrading or migrating.

**Note**

Trend Micro recommends only migrating settings. Migrating from IMSS Windows 7.1 to IMSS Windows 7.5 using the export/import feature only migrates settings. To maintain all legacy data, install IMSS Windows 7.5 over IMSS Windows 7.1. For more information, see *Installing IMSS Windows 7.5 Over IMSS Windows 7.1 Patch 3 on page 5-7*.

### Exporting IMSS Windows 7.1 Settings

**Procedure**

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

   The **Import/Export** screen appears.

2. Under **Export Configuration Files**, click **Export** to export the settings
3. Wait a moment for the configuration files to generate.

4. Save the exported configuration file to local storage on the server.

## Importing IMSS Windows 7.1 Patch 3 Settings to IMSS Windows 7.5

After migration, IMSS Windows 7.5 settings are overwritten and all services are restarted.

**WARNING!**

During migration do not perform any database operations.

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

**Procedure**

1. Install the IMSS Windows 7.5 server.

   See one of the following installation scenarios:

   - *Single-Server Installation on page 4-4*
   - *Performing a Complex Distributed Installation on page 4-40*

2. Log on to the IMSS Windows 7.5 web console.
3. Verify that no services are starting or stopping. If any service is starting or stopping, wait until the operation has completed.
4. Go to **Administration** > **Import/Export**

   The **Import/Export** screen appears.

5. Under **Import Configuration Files**, click **Choose File**.
6. Select the previously exported settings file, then click **Open**.
7. Click **Import**.
8. Click **OK** to confirm.
9. Wait a moment for the configuration import to complete.

10. Click **Return** to go back to the **Import/Export** screen.

## Installing IMSS Windows 7.5 Over IMSS Windows 7.1 Patch 3

The IMSS Windows 7.5 Setup program does not unregister the current IMSS server from Control Manager. All logs from the old server can still be queried by Control Manager. Trend Micro recommends that you back up the Admin Database and applications before proceeding. For more information, see *Backing Up IMSS on page 5-13*.

**Tip**

Trend Micro recommends migrating instead of installing over a previous version. For more information, *Migrating from IMSS Windows 7.1 to IMSS Windows 7.5 on page 5-5*

- When IMSS Windows 7.1 is deployed on distribute servers, make sure to close all IMSS services on all servers, then install IMSS Windows 7.5 on Central Controller Server first. After installation on Central Controller, install IMSS Windows 7.5 on other servers one by one or at the same time.
- When IMSS Windows 7.1 is deployed on a single server, install IMSS Windows 7.5 directly.
- To stop IMSS related services manually, you can go to Services management console. Then find and stop the following services:
  - Trend Micro IMSS CMAgent Services
  - Trend Micro IMSS End User Quarantine Console
  - Trend Micro IMSS EUQ Load Balancer
  - Trend Micro IMSS IPProfiler
  - Trend Micro IMSS Manager
  - Trend Micro IMSS Policy Service
  - Trend Micro IMSS Scan Service

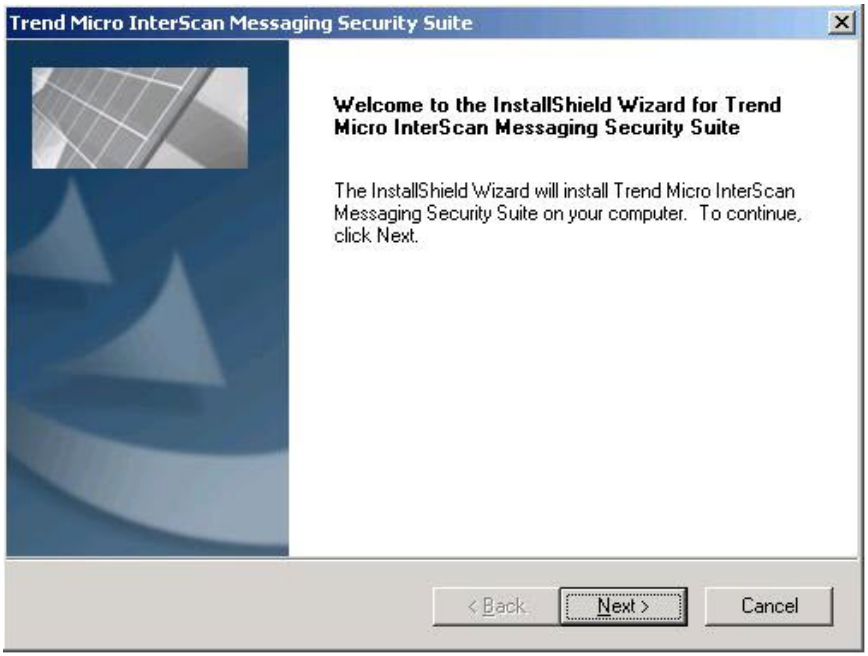
- Trend Micro IMSS SMTP Service
- Trend Micro IMSS Task Services
- Trend Micro IMSS Web Console

**Procedure**

1. Double-click `Setup.exe` on the IMSS 7.1 server.

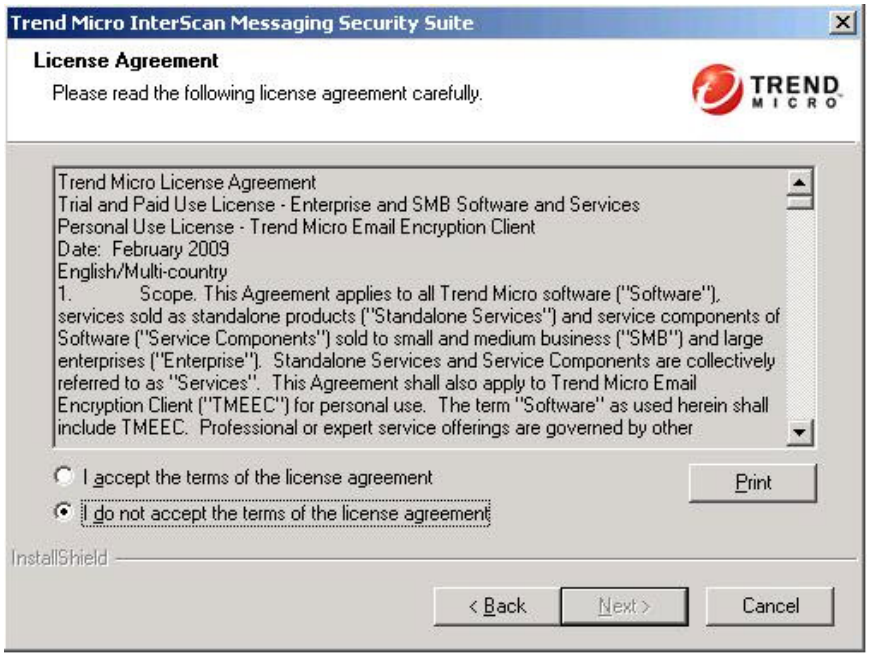
   The **Preparing to Install...** screen appears.

After the Setup program is ready, the **Welcome** screen appears.

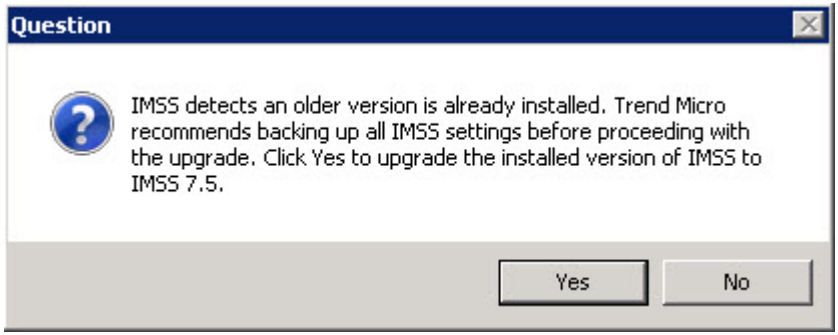



2. Click **Next**.

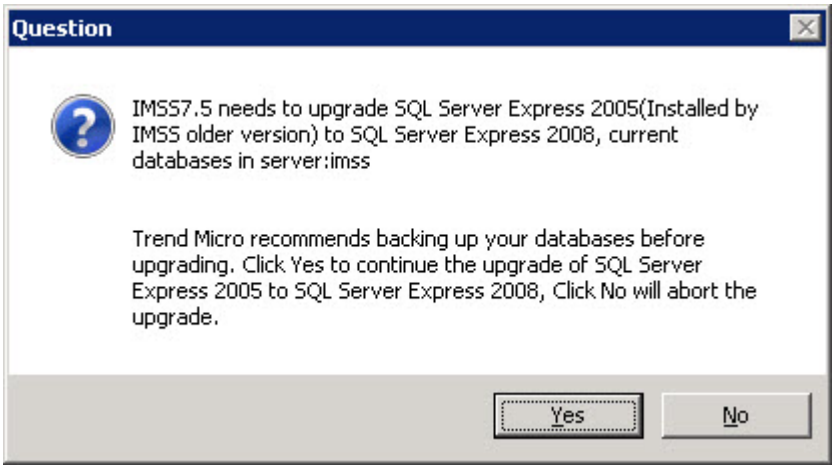
The **License Agreement** screen appears.




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



5. At the message, click **Yes** to install IMSS 7.5 over IMSS 7.1.




6. At the message, click **Yes** to upgrade SQL Server 2005 to SQL Server 2008.

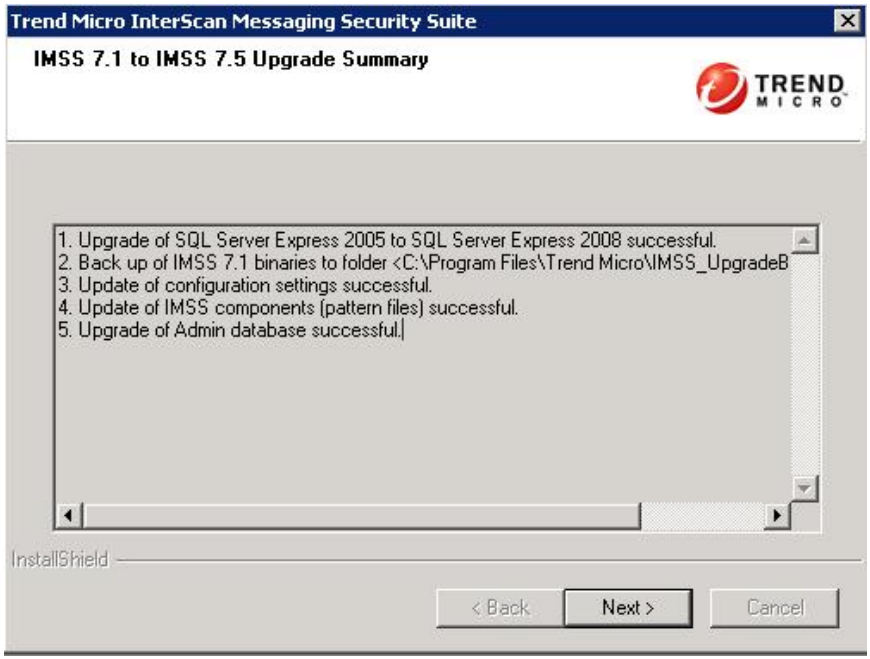
**Note**

If the endpoint does not meet the minimum system requirements, the Setup program requests you to first install all required programs.

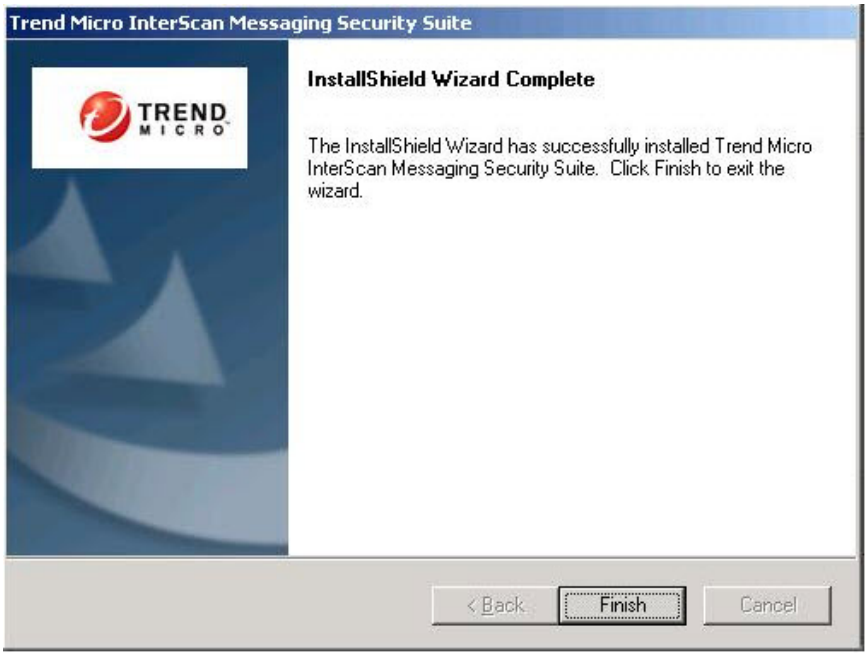
For more information, see *System Requirements on page 4-2*.

If all requirements are met, the installation begins with the Setup program stopping services. The IMSS upgrade takes about 15 minutes.

7. At the **IMSS 7.1 to IMSS 7.5 Upgrade Summary** screen, click **Next**.


Trend Micro InterScan Messaging Security Suite
IMSS 7.1 to IMSS 7.5 Upgrade Summary
TREND MICRO
1. Upgrade of SQL Server Express 2005 to SQL Server Express 2008 successful.
2. Back up of IMSS 7.1 binaries to folder <C:\Program Files\Trend Micro\IMSS_UpgradeB
3. Update of configuration settings successful.
4. Update of IMSS components (pattern files) successful.
5. Upgrade of Admin database successful.
InstallShield
< Back
Next >
Cancel

The **Installation Complete** screen appears.




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

**Note**

If IMSS Windows 7.1 is deployed on distribute servers, repeat *1 on page 5-8* to *8 on page 5-13* on each server.

# Backing Up IMSS

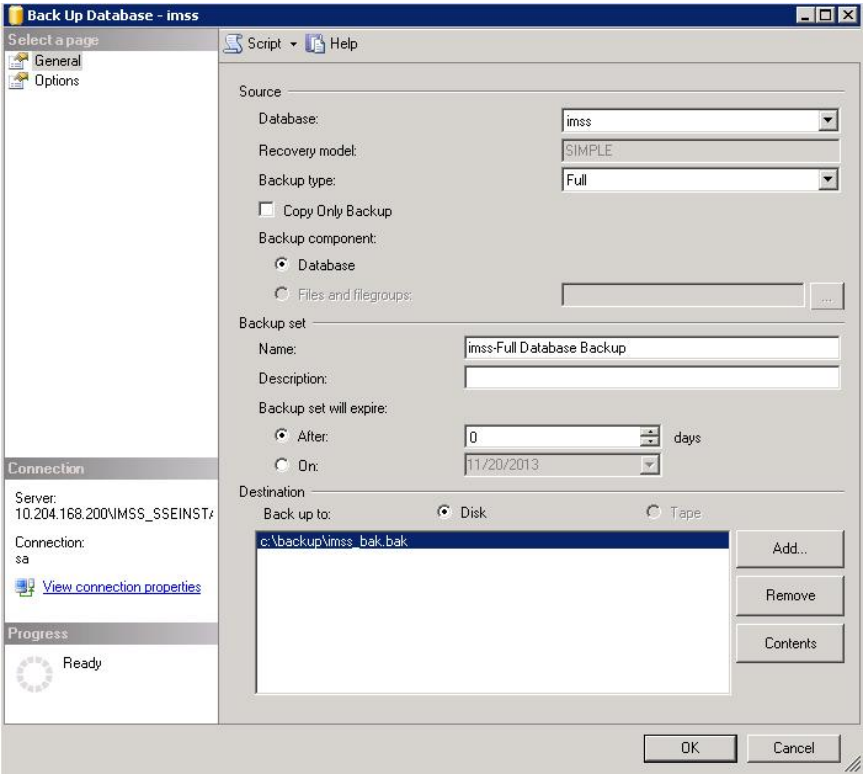
IMSS stores all configuration settings in the admin database (default database "imss"). This section describes how to back up the configurations in the admin database, as well as how to restore all settings.

## Backing Up the Admin Database

**Procedure**

1. Log on as the Database Administrator.
   a. Open Microsoft SQL Management Studio.
   b. Connect to the database server where IMSS **Admin** database is installed.
   c. Log on as user "sa".
2. Find the **Admin** database (default: **imss**), right-click and then go to **Tasks** > **Back up...**.

The **Back Up Database** window appears.




3. Back up the Admin Database to disk.

4. Wait for the database backup to finish.

   The following message appears:

   ```
   The backup of database "imss" completed successfully.
   ```

5. Click **OK**.

6. Repeat steps to back up additional databases (example: EUQ database).

## Backing Up IMSS Applications

The default installation paths:

- 32-bit environments: `C:\Program Files\Trend Micro\IMSS`
- 64-bit environments: `C:\Program Files(x86)\Trend Micro\IMSS`

---

**Procedure**

1. Find the Application where IMSS Windows 7.1 installed.
2. Save it as “IMSS_backup”.

---

# Activating Supported Services

After upgrading, IMSS 7.5 retains the Activation Code from the previous product version. If the Activation Code has expired, provide a new Activation Code to use the following:

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

To use Email reputation, specify the Activation Code from the web console after installation completes.

# Rolling Back the Upgrade

If any problems occur with the migration to version 7.5, you can roll back to version 7.1. For more information about IMSS 7.1 installation-related questions, see your IMSS 7.1 documentation. This section explains how to perform the rollback for the following deployment scenarios for version 7.1:

**Single-server deployment**

If all components of IMSS 7.1 are installed on a single server, roll back the upgrade by referring to *Rolling Back in a Single-Server Deployment Scenario on page 5-17*.

**Complex distributed deployment**

If each component of IMSS 7.1 is installed on different servers, roll back the upgrade by referring to *Rolling Back in a Complex Distributed Deployment Scenario on page 5-19*.

## Rolling Back in a Single-Server Deployment Scenario

The following procedure explains how to roll back an environment that deployed IMSS Windows 7.1 on a single IMSS computer.

Before proceeding, do the following:

- Back up the `IMSS` folder to the `IMSS_Backup` folder.
- Back up the **Admin** database to `C:\backup\imss.bak`.
- Back up the EUQ database to `C:\backup\imsseuq.bak` if the EUQ database has been installed.

---

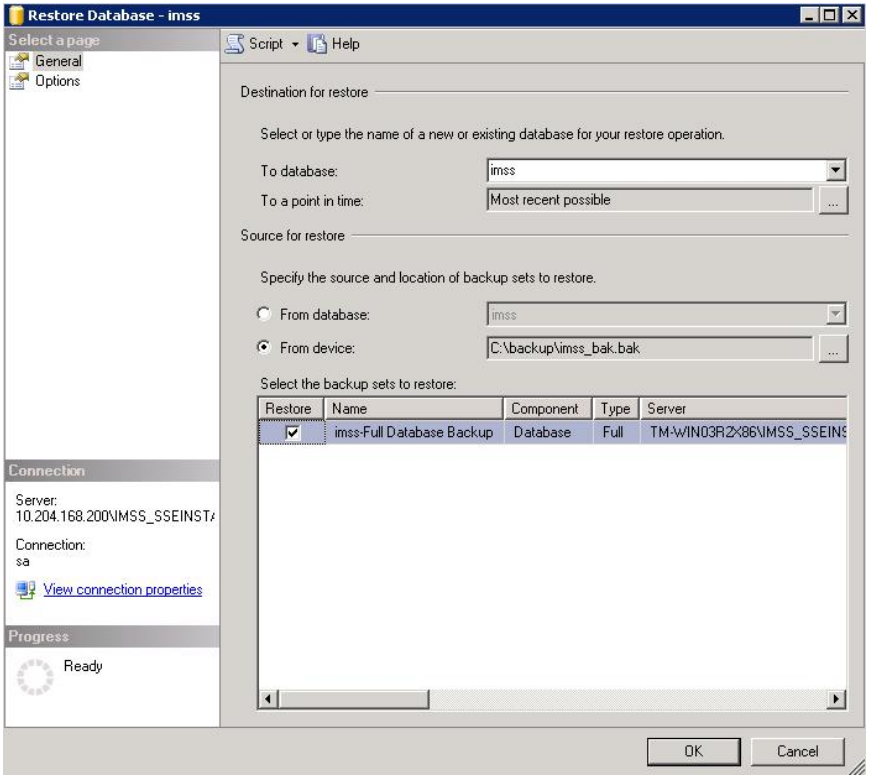
**Procedure**

1. Uninstall all IMSS 7.5 components using the uninstallation program.
2. Perform a fresh installation for IMSS 7.1.
3. Stop all IMSS 7.1 services from the Microsoft Management Console.
4. Start the database service.
5. Restore the database data for IMSS 7.1 using the Microsoft SQL Management tool.
   a. Log on as the Database Administrator.
      - Open Microsoft SQL Management Studio.
      - Connect to the database server where IMSS **Admin** database is installed.

- Log on as user "sa".

b. Find the **Admin** database (default: **imss**), right-click and then go to **Tasks** > **Restore** > **Database**.

The **Restore Database** window appears.




6. Click **OK** to restore IMSS **Admin** database.

7. Go to IMSS installation path and rename `IMSS` to `IMSS_7.1backup`.

8. Rename `IMSS_Backup` to `IMSS`.

9. Restart all IMSS Windows 7.1 services.

## Rolling Back in a Complex Distributed Deployment Scenario

The following procedure explains how to roll back an environment that deployed IMSS Windows 7.1 components on multiple computers.

This scenario assumes three servers:

- Server 1: Running IMSS Scanner and Central Controller services
- Server 2: Running the IMSS Admin database (SQL Server is not installed by IMSS)
- Server 3: Running the EUQ service and EUQ database

Before proceeding, make sure to complete the following:

- On Server 1, back up a copy of the folder `IMSS` to the folder `IMSS_Backup`
- On Server 2, back up the **Admin** database to `C:\backup\imss.bak`
- On Server 3, back up the EUQ database to `C:\backup\imsseuq.bak` and make a copy of the folder `IMSS` to the folder `IMSS_Backup`

**Note**

For information about making a backup, see *Backing Up IMSS on page 5-13*.

**Procedure**

1. Uninstall all IMSS components using the uninstallation program for Server 1 and Server 3.
2. Rename the IMSS **Admin** database to "imss_bak" on Server 2
3. Perform a fresh installation of IMSS 7.1. Follow the previous IMSS 7.1 deployment.
4. Stop all IMSS 7.1 services:

a. On Server 1: Stop all IMSS-related services and the IIS service.

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

5. On Server 1: Restore IMSS 7.1-related data.

   a. Rename the folder `IMSS` to "IMSS_71Backup".

   b. Rename the folder `IMSS_Backup` to "IMSS".

> **Note**
>
> `IMSS_Backup` is the folder where you backed up all your applications.

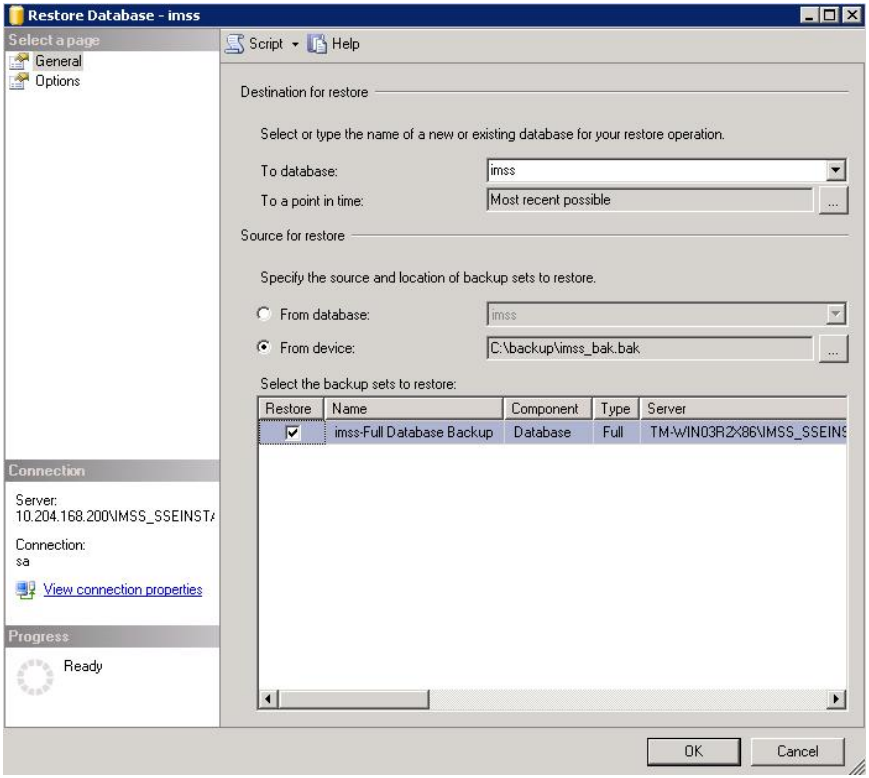
6. On Server 2: Restore IMSS 7.1 database data using the Microsoft SQL Management tool.

   a. Log on as the Database Administrator.

      - Open Microsoft SQL Management Studio.
      - Connect to the database server where IMSS **Admin** database is installed.
      - Log on as user "sa".

   b. Find the **Admin** database (default: **imss**), right-click and then go to **Tasks** > **Restore** > **Database**.

The **Restore Database** window appears.




7. On Server 3: Restore the EUQ database.

   See *5 on page 5-20*.

8. On Server 3: Restore applications.

   See *4 on page 5-19*

9. On Server 2: Restart the database service.

   See *4 on page 5-19*.

10. 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. Trend Micro IMSS CMAgent Services

   ii. Trend Micro IMSS IPProfiler

   iii. Trend Micro IMSS Manager

   iv. Trend Micro IMSS Policy Service

   v. Trend Micro IMSS Scan Service

   vi. Trend Micro IMSS SMTP Service

   vii. Trend Micro IMSS Task Services

   viii. Trend Micro IMSS Web Console

**11.** On Server 3: Start all IMSS services, include the database service.

# Chapter 6

# Troubleshooting and Support Information

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

Topics include:

# Troubleshooting

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

## Installation Troubleshooting Issues

| Issue | Suggested Resolution |
|---|---|
| Installation stopped and the following message appears: "can not overwrite xxx.xxx" | Manually remove all files in the destination folder and retry the installation.<br><br>**Note**<br>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):<br><br>`hostname (IP address)\IMSS_SSEINSTANCE.` |

# Frequently Asked Questions About Installation

## 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:

1. Go to the setup folder.
2. Run the Setup program using the following command:

   ```
   setup.exe /zOnlyInstDB
   ```

3. 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 7.5 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 7.5 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.

### Changing the IP Address for IMSS (Central Controller + Scanner)

**Procedure**

1. Go to **Control Panel** > **Administrative Tools** > **Services** and stop all services in the following sequence:
   a. `Trend Micro IMSS Web Console`
   b. `Trend Micro IMSS IPProfiler`
   c. `Trend Micro IMSS Task Services`
   d. `Trend Micro IMSS CMAgent Service`
   e. `Trend Micro IMSS Policy Service`
   f. `Trend Micro IMSS Scan Service`
   g. `Trend Micro IMSS SMTP Service`
   h. `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 your SQL Server's IP settings and restart your Microsoft SQL Server services.

7. Go to **Control Panel** > **Administrative Tools** > **Services** and restart all services in the following sequence:

   a. `Trend Micro IMSS Manager`

   b. `Trend Micro IMSS SMTP Service`

   c. `Trend Micro IMSS Scan Service`

   d. `Trend Micro IMSS Policy Service`

   e. `Trend Micro IMSS CMAgent Service`

   f. `Trend Micro IMSS Task Services`

   g. `Trend Micro IMSS IPProfiler`

   h. `Trend Micro IMSS Web Console`

---

### Changing the IP address for a Scanner

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

### Changing the IP address for the Central Controller

---

**Procedure**

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.

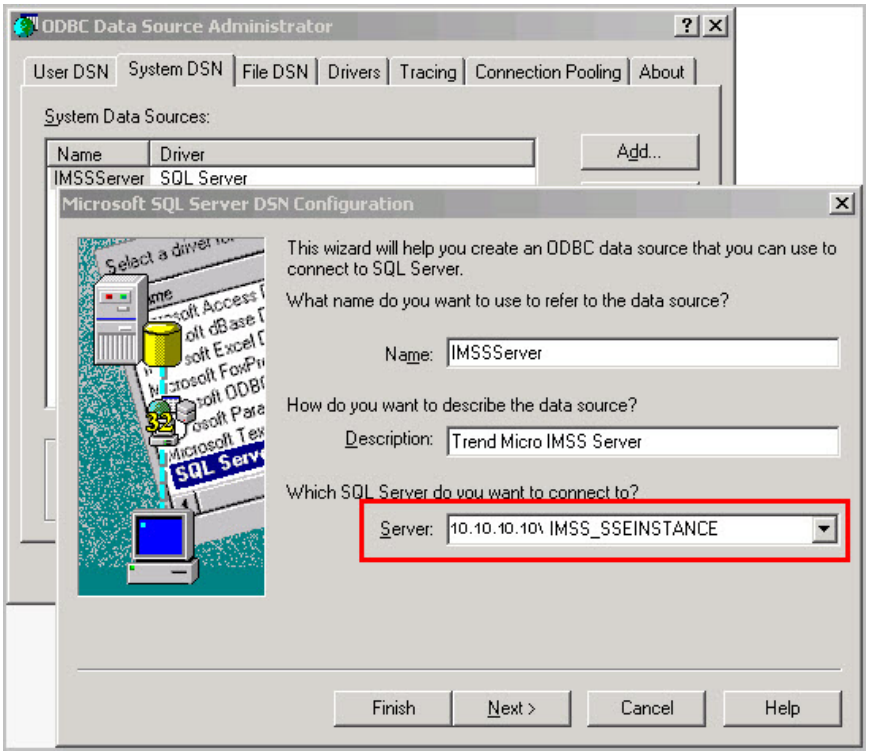
4. Restart the SMTP service on each scanner to use the new IP Profiler DNS server IP address.
5. Change the IP address, for web management console access, to the new IP address in the `adminui` file. The file is located in the IMSS installation directory.

### Changing the IP address of the admin database

**Procedure**

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.

---

### Changing the IP address of primary EUQ servers

---

**Procedure**

1. Change the "ServerName" to the new IP address in the `EUQ.conf` file, located at `<IMSS Install Path>\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 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.

---

### Changing the IP address of secondary EUQ servers

**Procedure**

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 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 on the primary EUQ server to update the `worker.properties` configuration file.

### Removing or adding 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 Apache. 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 in / from the pool of EUQ servers used by Apache to distribute the End User requests.

#### Adding 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.

#### Removing an EUQ database

**Procedure**

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.

**Changing the EUQ database IP address**

**Procedure**

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 informs 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.

## Upgrading

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

During a migration, all IMSS 7.1 settings can be exported, except the data generated, such as reports and logs. During an upgrade, all IMSS 7.1 settings, including the data generated, can be retained.

### How do I upgrade IMSS 7.1 scanners?

To upgrade from multiple IMSS 7.1 scanners:

- Upgrade from the scanner with the most desired settings for the migration.

- Uninstall the remaining scanners.
- Append the multiple scanners.

### Can I upgrade the administrator database and EUQ database from the same IMSS 7.1 database server?

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

### Is rollback to IMSS 7.1 possible after upgrading?

Yes. For details instructions, see *Rolling Back the Upgrade on page 5-16*.

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

Yes. Upgrade can be performed from a computer with any IMSS component installed.

### How do I simplify SPS rules after an upgrade?

To keep all SPS filter settings for all policies of IMSS 7.1, IMSS 7.5 migrates each SPS filter to one or multiple SPS rule(s) in IMSS 7.5. To reduce the number of SPS rules after upgrading, perform the following:

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

## Support Information

### Using the Support Portal

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

**Procedure**

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

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

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

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

## Contacting Technical Support

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

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

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

| | |
|---|---|
| Address | Trend Micro, Inc. 10101 North De Anza Blvd., Cupertino, CA 95014 |
| Phone | Toll free: +1 (800) 228-5651 (sales)<br>Voice: +1 (408) 257-1500 (main) |
| Fax | +1 (408) 257-2003 |

| | |
|---|---|
| Website | http://www.trendmicro.com |
| Email address | support@trendmicro.com |

### Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

## TrendLabs

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

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

Learn more about TrendLabs at:

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

## Security Intelligence

Comprehensive security information is available at the Trend Micro website.

http://www.trendmicro.com/vinfo

Security information includes:

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

## Download Center

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

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

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

## Sending Suspicious Content to Trend Micro

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

## Email Reputation Services

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

https://ers.trendmicro.com/

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

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

## File Reputation Services

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

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

Record the case number for tracking purposes.

## Web Reputation Services

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

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

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

# Index


**TREND MICRO INCORPORATED**

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: MSEM76207/131030