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

www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software usually includes the right to minor product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

Trend Micro, the Trend Micro logo, InterScan Messaging Security Suite, and Control Manager are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2007 Trend Micro Incorporated. All rights reserved.

Document Part Number: MSEM73446/71107

Release Date: November 2007

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

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

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

Preface
InterScan Messaging Security Suite 7.0 Documentation ..................... vi
Audience ........................................................................................................ vi
Document Conventions ............................................................................... vii

Chapter 1: Introducing InterScan™ Messaging Security Suite
About IMSS 7.0 ............................................................................................. 1-2
What’s New .................................................................................................. 1-2
IMSS Main Features and Benefits ............................................................... 1-4
About Spyware and Other Types of Grayware ........................................... 1-9
About Trend Micro Control Manager ....................................................... 1-11
Integrating with Control Manager ............................................................. 1-12

Chapter 2: System Requirements and Component Descriptions
System Requirements .................................................................................. 2-2
About IMSS Components ........................................................................... 2-4
The IMSS Admin Database .......................................................................... 2-4
Central Controller ....................................................................................... 2-4
Scanner Services ......................................................................................... 2-5
Policy Services ............................................................................................ 2-5
Policy Synchronization ................................................................................. 2-6
End-User Quarantine Service ..................................................................... 2-6
Primary and Secondary End-User Quarantine Services ......................... 2-6
End-User Quarantine Server Components ............................................... 2-6
Apache and mod_jk .................................................................................... 2-7
Tomcat .......................................................................................................... 2-7
Struts Framework ......................................................................................... 2-8
End-User Quarantine Application .............................................................. 2-8
The End-User Quarantine Database .......................................................... 2-9
IP Filtering .................................................................................................... 2-9
Network Reputation Services ...................................................................... 2-10
Types of Network Reputation Services .................................................... 2-10
How IP Profiler Works ................................................................................ 2-10
How Network Reputation Service Works ........................................ 2-11

Chapter 3: Planning for Deployment

Deployment Checklist ................................................................. 3-2
Component and Sub-module Installation ..................................... 3-6
IMSS Ports .................................................................................. 3-8
Considering Network Topology .................................................. 3-11
    Installing Without a Firewall .................................................. 3-11
    Installing In Front of a Firewall .............................................. 3-12
        Incoming Traffic ............................................................... 3-12
        Outgoing Traffic ............................................................ 3-12
    Installing Behind a Firewall .................................................. 3-12
        Incoming Traffic ............................................................... 3-13
        Outgoing Traffic ............................................................ 3-13
    Installing on a Former SMTP Gateway ................................... 3-14
        Incoming Traffic ............................................................... 3-14
        Outgoing Traffic ............................................................ 3-15
    Installing in the De-Militarized Zone ..................................... 3-15
        Incoming Traffic ............................................................... 3-15
        Outgoing Traffic ............................................................ 3-16
Understanding Installation Scenarios ........................................ 3-16
    Single-Server Installation ..................................................... 3-16
    Multiple Scanner Service Installation .................................... 3-18
        Installing Multiple Scanner Services and Policy Services ... 3-18
    Multiple End-User Quarantine Service Installation ................ 3-20
        Other Considerations When Deploying End-User Quarantine 3-22
    Communication Between Servers ......................................... 3-22
    Complex Distributed Installation ......................................... 3-23
    Wide-Area Network Installation .......................................... 3-25
        Trend Micro Control Manager ......................................... 3-25
        Fault Tolerance and Failover in a WAN Scenario ............... 3-26
    IP Filtering ........................................................................ 3-28
        Deploying IMSS with IP Filtering ................................... 3-28
        About Failover .............................................................. 3-29

Chapter 4: Installing and Upgrading

Installing and Upgrading ................................................................ 4-2
    Single-Server Installation ..................................................... 4-2
Multiple Scanner and EUQ Service/Database Installation .......... 4-14
Appending Components When No Previously Installed Components Exist ................................................................. 4-14
Appending Components When Previously Installed Components Exist ........................................................................... 4-22
Complex Distributed Installation ................................................. 4-24
Silent Installation .......................................................................... 4-25
Recording the Installation Steps .............................................. 4-25
Running the Silent Installation Script ....................................... 4-26
Upgrading From IMSS 5.7 ............................................................... 4-28
Backing Up Before Upgrading .................................................. 4-28
Backing Up IMSS 5.7 Data for a Single-Server Deployment .... 4-28
Backing Up IMSS 5.7 Data for a Distributed Deployment ...... 4-31
Performing an Upgrade ............................................................... 4-32
Rolling Back After Upgrading ..................................................... 4-38
Rolling Back From a Single Server Deployment ...................... 4-38
Rolling Back From a Distributed Deployment ......................... 4-39
Performing Uninstallation ........................................................... 4-40
Silent Uninstallation ................................................................. 4-44
Upgrading MSDE to SQL Server 2005 Express ......................... 4-45
Prerequisites to Installing SQL Server 2005 Express ................. 4-45
Upgrading MSDE to SQL Server 2005 Express for Previously Installed IMSS 7.0 ............................................................ 4-45
Step 1: Stopping all IMSS services ......................................... 4-45
Step 2: Back Up IMSS Databases ........................................... 4-46
Step 3: Installing SQL Server 2005 Express ......................... 4-46
Step 4: Resetting the Database Administrator’s Password ..... 4-47
Integrating SQL Server 2005 Express With Fresh IMSS 7.0
Installation ................................................................................. 4-49
Step 1: Installing SQL Server 2005 Express ......................... 4-49
Step 2: Enabling Network Access ............................................ 4-49
Step 3: Automating the Startup for SQL Server Browser
Service ..................................................................................... 4-50
Step 4: Installing IMSS 7.0 ..................................................... 4-50

Chapter 5: Troubleshooting, FAQ, and Support
Troubleshooting .......................................................................... 5-2
Welcome to the Trend Micro™ InterScan™ Messaging Security Suite 7.0 Installation Guide. This manual contains information on InterScan Messaging Security Suite (IMSS) features, system requirements, as well as instructions on installation and upgrade.

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

This preface discusses the following topics:

- InterScan Messaging Security Suite 7.0 Documentation on page vi
- Audience on page vi
- Document Conventions on page vii
InterScan Messaging Security Suite 7.0 Documentation

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

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


**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 Microsoft Exchange
- LDAP
- Database management

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

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

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL CAPITALS</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td>Bold</td>
<td>Menus and menu commands, command buttons, tabs, options, and other user interface items</td>
</tr>
<tr>
<td>Italics</td>
<td>References to other documentation</td>
</tr>
<tr>
<td>Monospace</td>
<td>Examples, sample command lines, program code, Web URL, file name, and program output</td>
</tr>
<tr>
<td>Note:</td>
<td>Configuration notes</td>
</tr>
<tr>
<td>Tip:</td>
<td>Recommendations</td>
</tr>
<tr>
<td>WARNING!</td>
<td>Reminders on actions or configurations that must be avoided</td>
</tr>
</tbody>
</table>
Introducing InterScan™ Messaging Security Suite

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

Topics include:
• About IMSS 7.0 on page 1-2
• What's New on page 1-2
• IMSS Main Features and Benefits on page 1-4
• About Spyware and Other Types of Grayware on page 1-9
• About Trend Micro Control Manager on page 1-11
About IMSS 7.0

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

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

What’s New

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

<table>
<thead>
<tr>
<th>New Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple antivirus and malware policies</td>
<td>Multiple IMSS policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria.</td>
</tr>
<tr>
<td>Centralized logging and reporting</td>
<td>A consolidated, detailed report provides top usage statistics and key mail usage data.</td>
</tr>
<tr>
<td></td>
<td>Centralized logging allows administrators to quickly audit message-related activities.</td>
</tr>
<tr>
<td>Centralized archive and quarantine management</td>
<td>An easy way to search multiple IMSS quarantine and archive areas for messages.</td>
</tr>
<tr>
<td>Scalable Web End-User Quarantine (Web EUQ)</td>
<td>Multiple Web EUQ services offer your users the ability to view quarantined email messages that IMSS detected as spam.</td>
</tr>
<tr>
<td></td>
<td>Together with EUQ notification, IMSS will help lower the cost of helpdesk administrative tasks.</td>
</tr>
</tbody>
</table>

**TABLE 1-1. New Features**
## Introducing InterScan™ Messaging Security Suite

### Multiple spam prevention technologies
- Network Reputation Services filters spam senders at the connection layer.
- IP Profiler helps protect the mail server from attacks with smart profiles (SMTP Intrusion Detection Service (IDS)).
- Trend Micro Anti-spam engine accurately detects and takes action on spam.

### IntelliTrap
IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods will enter your network through email.

### Delegated administration
LDAP-integrated account management which allows users to assign administrative rights for different configuration tasks.

### Easy deployment with Configuration Wizard
An easy-to-use configuration wizard to get IMSS up and running right out of the box.

### Advance MTA functions
- Opportunistic TLS, domain based delivery, and other MTA functions help IMSS handle email efficiently and securely.

### Migration
Easy upgrade process ensures that settings will be transferred with minimum effort during setup.

### Mail auditing and tracking
Detailed logging for all messages to track and identify message flow related issues.

### Integration with Trend Micro Control Manager™
Perform log queries from Control Manager, in addition to other supported features. See Integrating with Control Manager on page 1-12.

### 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.

<table>
<thead>
<tr>
<th>New Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple spam prevention</td>
<td>Three layers of spam protection:</td>
</tr>
<tr>
<td>technologies</td>
<td>- Network Reputation Services filters spam senders at the connection layer.</td>
</tr>
<tr>
<td></td>
<td>- IP Profiler helps protect the mail server from attacks with smart profiles</td>
</tr>
<tr>
<td></td>
<td>- Trend Micro Anti-spam engine accurately detects and takes action on spam.</td>
</tr>
<tr>
<td>IntelliTrap</td>
<td>IntelliTrap provides heuristic evaluation of compressed files that helps</td>
</tr>
<tr>
<td></td>
<td>reduce the risk that a virus compressed using these methods will enter your</td>
</tr>
<tr>
<td></td>
<td>network through email.</td>
</tr>
<tr>
<td>Delegated administration</td>
<td>LDAP-integrated account management which allows users to assign</td>
</tr>
<tr>
<td></td>
<td>administrative rights for different configuration tasks.</td>
</tr>
<tr>
<td>Easy deployment with</td>
<td>An easy-to-use configuration wizard to get IMSS up and running right out</td>
</tr>
<tr>
<td>Configuration Wizard</td>
<td>of the box.</td>
</tr>
<tr>
<td>Advance MTA functions</td>
<td>Opportunistic TLS, domain based delivery, and other MTA functions help</td>
</tr>
<tr>
<td></td>
<td>IMSS handle email efficiently and securely.</td>
</tr>
<tr>
<td>Migration</td>
<td>Easy upgrade process ensures that settings will be transferred with</td>
</tr>
<tr>
<td></td>
<td>minimum effort during setup.</td>
</tr>
<tr>
<td>Mail auditing and tracking</td>
<td>Detailed logging for all messages to track and identify message flow related</td>
</tr>
<tr>
<td></td>
<td>issues.</td>
</tr>
<tr>
<td>Integration with Trend Micro</td>
<td>Perform log queries from Control Manager, in addition to other supported</td>
</tr>
<tr>
<td>Control Manager™</td>
<td>features. See Integrating with Control Manager on page 1-12.</td>
</tr>
<tr>
<td>Supports 8 bit to 7 bit-MIME</td>
<td>IMSS 7.0 Service Pack 1 supports the transformation of 8 bit to 7 bit-MIME</td>
</tr>
<tr>
<td>transformation</td>
<td>according to the standard defined in RFC 1652 SMTP Service Extension for</td>
</tr>
<tr>
<td></td>
<td>8bit-MIME transport. In the event that the next hop of the SMTP server does</td>
</tr>
<tr>
<td></td>
<td>not support 8 bit MIME, IMSS will convert the message from 8 bit MIME to</td>
</tr>
<tr>
<td></td>
<td>7 bit MIME.</td>
</tr>
</tbody>
</table>

**TABLE 1-1. New Features**
## IMSS Main Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus protection</td>
<td>IMSS performs virus detection using Trend Micro scan engine and a technology called pattern matching. The scan engine compares code in files traveling through your gateway with binary patterns of known viruses that reside in the pattern file. If the scan engine detects a match, it attempts to clean the file by removing the virus code, quarantining the message or taking other actions as configured in the policy rules.</td>
<td>IMSS’s enhanced virus/content scanner keeps your messaging system working at top efficiency.</td>
</tr>
<tr>
<td>IntelliTrap</td>
<td>Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files.</td>
<td>Helps reduce the risk that a virus compressed using different file compression schemes will enter your network via email.</td>
</tr>
<tr>
<td></td>
<td>Because there is the possibility that IntelliTrap may incorrectly identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when the IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature. By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be incorrectly classified as security risks.</td>
<td></td>
</tr>
<tr>
<td>Content management</td>
<td>IMSS analyzes email messages and their attachments, traveling to and from your network, for appropriate content.</td>
<td>Content that you deem inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using IMSS.</td>
</tr>
</tbody>
</table>

**TABLE 1-2. Main features and benefits**
Introducing InterScan™ Messaging Security Suite

Protection against other email threats

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS attacks</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Malicious email content</td>
<td>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.</td>
<td>IMSS allows you to configure the types of messages that are allowed to pass through the SMTP gateway.</td>
</tr>
<tr>
<td>Degradation of services</td>
<td>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.</td>
<td>Most companies have acceptable usage policies for their messaging system—IMSS provides tools to enforce and ensure compliance with existing policies.</td>
</tr>
<tr>
<td>Legal liability and business integrity</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Table 1-2. Main features and benefits**
Mass mailing virus containment

Email-borne viruses that may automatically spread bogus messages through a company’s messaging system can be expensive to clean up and cause panic among users.

When IMSS detects a mass-mailing virus, the action taken against this virus can be different from the actions against other types of viruses. For example, if IMSS detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if IMSS detects a mass-mailing virus, the program can automatically delete the entire message.

By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value.

The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs\textsuperscript{SM} ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.

**TABLE 1-2. Main features and benefits**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass mailing virus containment</td>
<td>Email-borne viruses that may automatically spread bogus messages through a company’s messaging system can be expensive to clean up and cause panic among users. When IMSS detects a mass-mailing virus, the action taken against this virus can be different from the actions against other types of viruses. For example, if IMSS detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if IMSS detects a mass-mailing virus, the program can automatically delete the entire message.</td>
<td>By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value. The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs\textsuperscript{SM} ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.</td>
</tr>
<tr>
<td>Spyware and other types of grayware</td>
<td>Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see About Spyware and Other Types of Grayware on page 1-8</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Integrated spam

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Prevention Solution (SPS)</td>
<td>Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam-detection services to other Trend Micro products. To use SPS, you must pay for and obtain an SPS Activation Code. For more information, refer to your sales representative. SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license. <strong>Note:</strong> Please activate SPS before you configure IP Profiler and NRS.</td>
<td>The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real-time detection that is highly adaptable, even as spam originators change their techniques.</td>
</tr>
</tbody>
</table>

## Spam Filtering with IP Profiler and NRS

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| IP Profiler                          | IP Profiler is a self-learning, fully configurable feature that proactively blocks IP addresses of computers that send spam and other types of potential threats. NRS blocks IP addresses of known spam senders that Trend Micro maintains in a central database. For details, see the following:  
  • IP Filtering on page 2-9  
  • Network Reputation Services on page 2-10  
  • How IP Profiler Works on page 2-10  
  • How Network Reputation Service Works on page 2-11 | With the integration of IP Filtering, which includes IP Profiler and Network Reputation Services (NRS), IMSS can block spammers at the IP level.                                                                 |

## Others

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP &amp; domain-based policies</td>
<td>You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™ or Microsoft™ Active Directory™ for user-group definition and administrator privileges. Note that you have to enable LDAP in order to use web quarantine tool.</td>
<td>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.</td>
</tr>
<tr>
<td>Web-based management console</td>
<td>Web-based management console allows you to conveniently configure IMSS policies and settings on the Web.</td>
<td>The Web-based console also provides greater security as it is SSL-compatible.</td>
</tr>
</tbody>
</table>

**Table 1-2.** Main features and benefits
IMSS provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Spam Prevention Solution (SPS) quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete or approve for delivery.

With the Web-based EUQ console, end-users can manage messages that IMSS quarantines.

IMSS offers the ability to create different access rights to the Web management console. You can choose which sections of the console are accessible for different administrator logon account.

By delegating administrative roles to different employees, you can create backups of human resources and promote the sharing of administrative duties.

Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports. Helps you analyze how IMSS is performing. One time (on demand) reports allow you to specify the type of report content as and when required. Alternatively, you can configure IMSS to automatically generate reports daily, weekly, and monthly.

A built-in agent monitors the health of your IMSS server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow. Email notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.

You can choose to enable or disable POP3 scanning from the Web management console. In addition to SMTP traffic, IMSS can also scan POP3 messages at the gateway as messaging clients in your network retrieve them.

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.
Introducing InterScan™ Messaging Security Suite

About Spyware and Other Types of Grayware

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

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

TABLE 1-3. Types of spyware/grayware
### Types of Spyware/Grayware

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

**TABLE 1-3. Types of spyware/grayware**
About Trend Micro Control Manager

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

Control Manager consists of the following components:

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

  **Note:** You must install Control Manager Server 3.5 Patch 2 or later for it to work with IMSS 7.0 Windows.

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

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

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

  When you install a scanner, the Control Manager agent is also installed automatically. After the agent is enabled, each scanner will register to the Control Manager server and appear as separate entities.
Note: Use Control Manager server version 3.5 or later when using Control Manager to manage IMSS. For more information on the latest version and the most recent patches and updates, see the Trend Micro Update Center:

Integrating with Control Manager

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

<table>
<thead>
<tr>
<th>Features</th>
<th>Descriptions</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-way communication</td>
<td>In a 2-way communication, either IMSS or Control Manager may initiate the communication process.</td>
<td>No. Only IMSS can initiate a communication process with Control Manager.</td>
</tr>
<tr>
<td>Outbreak Prevention Policy</td>
<td>The Outbreak Prevention Policy (OPP) is a quick response to an outbreak developed by TrendLabs that contains a list of actions IMSS should take in order to reduce the likelihood of the IMSS server or its clients from becoming infected. Trend Micro ActiveUpdate Server then deploys this policy to IMSS via Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Log Upload for Query</td>
<td>Uploads IMSS virus logs, Content Security logs, and NRS logs to Control Manager for query purposes.</td>
<td>Yes</td>
</tr>
<tr>
<td>Single Sign On</td>
<td>Manage IMSS from Control Manager directly without first logging on to the IMSS Web management console.</td>
<td>No. You need to first log on to the IMSS Web management console before you can manage IMSS from Control Manager.</td>
</tr>
<tr>
<td>Configuration Replication</td>
<td>Replicate configuration settings from an existing IMSS server to a new IMSS server from Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Pattern Update</td>
<td>Update virus/malware pattern files from Control Manager.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

TABLE 1-4. Supported Control Manager features
**Introducing InterScan™ Messaging Security Suite**

<table>
<thead>
<tr>
<th>Features</th>
<th>Descriptions</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engine Update</td>
<td>Update Scan Engine from Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Product Component Update</td>
<td>Update IMSS product components such as patches and hot fixes from Control Manager.</td>
<td>No, refer to the specific patch or hot fix readme file for instructions on how to update the product components.</td>
</tr>
<tr>
<td>Configuration By User Interface Redirect</td>
<td>Configure IMSS via the IMSS Web management console accessible from Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Renew Product Registration</td>
<td>Renew IMSS product license from Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Mail-related Report on Control Manager</td>
<td>Generate the following IMSS mail-related reports from Control Manager: • Top 10 Virus Detection Points • All Entities Virus Infection List • Top 10 Infected Email Sender Report • Top 10 Security Violations Reports • Virus Infection Channel-Product Relationship Report • Filter Events by Frequency • Filter Events by Policy • Gateway Messaging Spam Summary Report • Gateway Messaging Spam Summary Report (for Domains)</td>
<td>Yes</td>
</tr>
<tr>
<td>Control Manager Agent Installation /Un-installation</td>
<td>Install / uninstall IMSS Control Manager Agent from Control Manager.</td>
<td>No, IMSS Control Manager agent is automatically installed when you install IMSS. To enable/disable the agent, do the following from the IMSS Web management console: 1. Choose Administration &gt; Connections from the menu. 2. Click the TMCM Server tab. 3. To enable/disable the agent, select/deselect the check box next to Enable TMCM Agent respectively.</td>
</tr>
<tr>
<td>Event Notification</td>
<td>Send IMSS event notification from Control Manager.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**TABLE 1-4. Supported Control Manager features**
Command Tracking for All Commands  
Track the status of commands that the Control Manager issues to IMSS.

<table>
<thead>
<tr>
<th>Features</th>
<th>Descriptions</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Tracking for All Commands</td>
<td>Track the status of commands that the Control Manager issues to IMSS.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**TABLE 1-4.** Supported Control Manager features
System Requirements and Component Descriptions

This chapter explains what requirements are necessary to manage InterScan Messaging Security Suite (IMSS) and explains the various software components it needs to function.

Topics include:

• System Requirements on page 2-2
• About IMSS Components on page 2-4
System Requirements

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

| Operating System | • Microsoft™ Windows™ Server 2003 SP1, SP2 Editions  
|                  | • Microsoft Windows Server 2003 R2, SP2 Editions  
|                  | • Microsoft Windows Server 2003 x64 SP2 Editions  
|                  | • Microsoft Windows Server 2003 x64 R2, SP2 Editions  
|                  | • Microsoft Windows 2000 Advanced Server SP4  
| Note:            | Microsoft Windows 2000 SP4 requires Microsoft MDAC 2.8  
|                  | SP1 or above for IMSS database connection. Download  
|                  | the latest MDAC version from the Microsoft site:  

| Recommended CPU  | Intel™ Dual Pentium™ IV 3GHz or above  
| Minimum CPU      | Intel Pentium IV 2.4GHz  
| Recommended Memory | 2GB RAM  
| Minimum Memory   | 1GB RAM  
| Recommended Disk Space | • 10GB for mail storage  
|                    | • 50GB or more for the Admin database  
|                    | • 20GB or more for the EUQ database  
|                    | • 40GB or more for the working quarantine folder  
| Note:             | These recommendations are based on 500,000 email  
|                   | messages/day, a 50% quarantine rate, and logs preserved for a  
|                   | month.  

TABLE 2-1. System Requirements
### Minimum Disk Space
- 10GB for mail storage
- 20GB for the Admin database
- 10GB for the EUQ database
- 1GB for the working quarantine folder.

### Recommended Swap Space
Trend Micro recommends a swap space between 4GB and 4 times the physical memory size.

**Note:** Each IMSS child process consumes 120MB of memory. Therefore, for better performance, enough physical and virtual memory should be allocated to handle peak traffic. For example, a computer with 2GB of physical memory and 8GB of swap space might be able to allow 75 child processes to be created. The required swap space also depends on the other application's memory usage. IMSS can then simultaneously handle 75 incoming connections from upstream MTA.

### Browser
- Internet Explorer 6 SP1 or Internet Explorer 7
- Firefox 1.5

### Microsoft SQL Server
- Microsoft SQL Server Desktop Edition (MSDE) SP4
- Microsoft SQL Server 2005 SP1, SP2
- Microsoft SQL Server 2000 SP4
- Microsoft SQL Server 2005 Express SP1, SP2

**Note:** MSDE 2000 has the following limitations:
- 2GB data
- 5 concurrent user connections or workloads

Trend Micro recommends not using MSDE, if the daily mail traffic is more than 30,000 or if you are using IMSS EUQ, to ensure adequate storage space for reports and log query results.

Mainstream support for MSDE will also expire on April 8th, 2008. Trend Micro recommends that you upgrade MSDE to SQL Server 2005 Express, which can handle up to 4GB data. See [Upgrading MSDE to SQL Server 2005 Express](#) on page 4-45.

### Microsoft Data Access Components
Microsoft Data Access Components (MDAC) 2.8 SP1 or above

### LDAP server
- Microsoft Active Directory 2000 or 2003
- IBM Lotus<sup>®</sup> Domino™ 6.0 or above
- Sun™ One LDAP 5.2 or above

<table>
<thead>
<tr>
<th>TABLE 2-1. System Requirements</th>
<th></th>
</tr>
</thead>
</table>
Note: The default location for the IMSS Admin DB and EUQ DB is \C:\Program Files\Trend Micro\MSDE\ if you have installed these databases using MSDE. If you are using SQL server, the Admin DB and EUQ DB will be located at the SQL server’s data folder. The default IMSS Quarantine working folder is \C:\Program Files\Trend Micro\IMSS\queue\.

About IMSS Components

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

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

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 the bundled Microsoft SQL Server Desktop Engine (MSDE) database or use existing Microsoft SQL servers.

Central Controller

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

Servers configured as scanner services do the following:

- Accept SMTP and POP3 messaging traffic
- Request policy from a policy service
- Evaluate the message based on the applicable policies
- Take the appropriate action on the message based on the evaluation outcome
- Store quarantined and archived messages locally
- Logs policy and system activity locally, and automatically updates the log portion of the IMSS database at scheduled intervals, allowing users to search through quarantined items and logs

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

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

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

Policy Services

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

**Policy Synchronization**

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

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

**End-User Quarantine Service**

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

**Primary and Secondary End-User Quarantine Services**

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

**End-User Quarantine Server Components**

The EUQ Server includes the following software components:

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

The Tomcat and Apache software are installed in the `{IMSS}\UI` directory. The other components are installed in the `{IMSS}\UI\euqUI` directory. Both Apache and Tomcat are controlled by Windows services management console (`services.msc`) in Administrative Tools menu.

**Apache and mod_jk**


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

**Tomcat**

The EUQ Server uses Tomcat Application server to handle the requests from end-users. The Tomcat Application Server installed in the Primary EUQ Server also accepts requests from the Apache HTTP Server and balances the load across all installed EUQ Servers using the Apache JServ Protocol version 1.3 protocol AJP13 (see [http://tomcat.apache.org/tomcat-3.3-doc/AJPv13.html](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\1.keystore`).

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

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

**Struts Framework**

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

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

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

**End-User Quarantine Application**

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

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

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

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

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 server to install the EUQ database.

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

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

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

IP Filtering

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

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

  IP profiler detects any of these four potential Internet threats:

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

• **Network Reputation Services™ (NRS)**—Blocks email from known spam senders at the IP-level.

### Network Reputation Services

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

### Types of Network Reputation Services

NRS provides two types of services:

• **Real-time Blackhole List (RBL+)™ Service**—Blocks spam at its source by validating IP addresses against the industry’s most comprehensive and reliable reputation database. Your designated mail server makes a DNS query to the RBL+ database server whenever an incoming mail message is received from an unknown host. If the host is listed in the RBL+ database, IMSS can reject the connection and block spam from the sender.

• **Network Anti-Spam™ Service**—A dynamic real-time solution that identifies and stops sources of spam while they are in the process of sending messages in bulk. Network Anti-Spam Service is a DNS query-based service like RBL+ Service. At the core of this service is the RBL+ database, along with the QIL database, a dynamic real-time database. These two databases have distinct entries and there is no overlap of the IP addresses, allowing us to maintain a highly efficient and effective database that can quickly respond to zombies, BGP attacks and other highly dynamic sources of spam.

### How IP Profiler Works

IP Profiler proactively learns IP addresses of computers that send emails containing potential threats. You can customize several criteria that determine when IMSS will start taking a specified action on an IP address. The criteria differ depending on the
potential threat, but commonly include a duration during which IMSS monitors the IP address and a threshold.

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

1. MTA queries the IP Profiler’s DNS server to see if the IP address is on the blocked list.
2. If the IP address is on the blocked list, it denies the connection request. If the IP address does not appear on the blocked list, IMSS analyzes the email traffic according to the threshold criteria you specify for IP Profiler.
3. If the email traffic violates the criteria, IMSS adds the sender IP address to the blocked list.

How Network Reputation Service Works

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

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

**FIGURE 2-1. How NRS works**

Planning for Deployment

This chapter explains how to plan for InterScan Messaging Security Suite (IMSS) deployment.

Topics include:

- Deployment Checklist on page 3-2
- Component and Sub-module Installation on page 3-6
- IMSS Ports on page 3-8
- Considering Network Topology on page 3-11
- Understanding Installation Scenarios on page 3-16
- IP Filtering on page 3-28
- About Failover on page 3-29
Deployment Checklist

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

<table>
<thead>
<tr>
<th>Tick when completed</th>
<th>Tasks</th>
<th>Optional</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 - Identify the location of IMSS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Choose one of the following locations on your network where you would like to install IMSS.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Without a firewall</td>
<td></td>
<td>Installing Without a Firewall on page 3-11</td>
<td></td>
</tr>
<tr>
<td>• In front of a firewall</td>
<td></td>
<td>Installing In Front of a Firewall on page 3-12</td>
<td></td>
</tr>
<tr>
<td>• Behind a firewall</td>
<td></td>
<td>Installing Behind a Firewall on page 3-12</td>
<td></td>
</tr>
<tr>
<td>• On a former SMTP gateway</td>
<td></td>
<td>Installing on a Former SMTP Gateway on page 3-14</td>
<td></td>
</tr>
<tr>
<td>• In the De-Militarized Zone</td>
<td></td>
<td>Installing in the De-Militarized Zone on page 3-15</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 - Plan the scope</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decide whether you would like to install IMSS on a single server or multiple servers.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Single-server installation</td>
<td></td>
<td>Single-Server Installation on page 3-16</td>
<td></td>
</tr>
</tbody>
</table>
### Planning for Deployment

<table>
<thead>
<tr>
<th>Tick when completed</th>
<th>Tasks</th>
<th>Optional</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Multiple scanner service</td>
<td></td>
<td><a href="#">Multiple Scanner Service Installation</a> on page 3-18</td>
</tr>
<tr>
<td></td>
<td>• Multiple EUP service</td>
<td></td>
<td><a href="#">Multiple End-User Quarantine Service Installation</a> on page 3-20</td>
</tr>
<tr>
<td></td>
<td>• Complex distributed</td>
<td></td>
<td><a href="#">Complex Distributed Installation</a> on page 3-23</td>
</tr>
<tr>
<td></td>
<td>• Wide area network</td>
<td></td>
<td><a href="#">Wide-Area Network Installation</a> on page 3-25</td>
</tr>
<tr>
<td>Note:</td>
<td>Trend Micro recommends that you consider the failover plan before deciding on the scope.</td>
<td></td>
<td><a href="#">About Failover</a> on page 3-29</td>
</tr>
</tbody>
</table>

#### Step 3 - Install or Upgrade

Perform either a fresh installation of IMSS or upgrade from a previous version.

<table>
<thead>
<tr>
<th></th>
<th>Tasks</th>
<th>Optional</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Install IMSS components</td>
<td></td>
<td><a href="#">Single-Server Installation</a> on page 4-2</td>
</tr>
<tr>
<td></td>
<td>• Upgrade from a previous version</td>
<td></td>
<td><a href="#">Upgrading From IMSS 5.7</a> on page 4-28</td>
</tr>
</tbody>
</table>

#### Step 4 - Configure basic IMSS settings

Go through the 8 steps of configuring the Central Controller via the Configuration Wizard.
### Step 5 - Start services

Activate IMSS services to start protecting your network against various threats.

- **Scanner**
- **Policy**
- **EUQ**

### Optional Reference

- **Scanner** — IMSS Services section of the Administrator’s Guide.
- **Policy**
- **EUQ** — Yes

### Step 6 - Configure other IMSS settings

Configure various IMSS settings to get IMSS up and running.

- **IP Filtering Rules**
- **SMTP Routing**
- **POP3 Settings**
- **Policy and scanning exceptions**

### Optional Reference

- **IP Filtering Rules** — Yes
- **SMTP Routing** — Scanning SMTP Messages section of the Administrator’s Guide.
- **POP3 Settings** — Yes
- **Policy and scanning exceptions** — Managing Policies section of the Administrator’s Guide.
### Planning for Deployment

- **Perform a manual update of components and configure scheduled updates**
  - Reference: Updating Scan Engine and Pattern Files section of the Administrator’s Guide.

- **Log settings**
  - Reference: Configuring Log Settings section of the Administrator’s Guide.

#### Step 7 - Back up IMSS

- **Back up the IMSS admin database as a precaution against system failure**
  - Task: Back up IMSS admin database
  - Reference: Backing Up IMSS section of the Administrator’s Guide.
Component and Sub-module Installation

When you install an IMSS component, additional sub-modules are also installed automatically. Table 3-1 lists each component sub-module.

<table>
<thead>
<tr>
<th>Main Component</th>
<th>Installed Sub-module</th>
<th>Sub-module Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSS Admin Database</td>
<td>Administrator Database</td>
<td>The main IMSS admin database that stores all global settings.</td>
</tr>
<tr>
<td></td>
<td>Database Server</td>
<td>The server on which the IMSS admin database runs.</td>
</tr>
<tr>
<td>Central Controller</td>
<td>Apache® Tomcat®</td>
<td>The Web server for the IMSS Web management console, through which you configure settings.</td>
</tr>
<tr>
<td></td>
<td>Named Server*</td>
<td>The DNS server for IP Profiler.</td>
</tr>
<tr>
<td></td>
<td>FoxDNS</td>
<td>Contains the list of blocked and white IP addresses for IP Profiler and writes the list to the named server.</td>
</tr>
<tr>
<td></td>
<td>IMSSMGR</td>
<td>A module to manage IMSS-related processes.</td>
</tr>
<tr>
<td>Scanner Service</td>
<td>Scanning Services</td>
<td>Performs all email-scanning actions.</td>
</tr>
<tr>
<td></td>
<td>Policy Services</td>
<td>A remote store of rules for the scanner services, caching rules that would otherwise require a database look-up</td>
</tr>
<tr>
<td></td>
<td>Control Manager Agent</td>
<td>The software component required for Control Manager to manage IMSS.</td>
</tr>
<tr>
<td></td>
<td>IMSSMGR</td>
<td>A module to manage scanner processes.</td>
</tr>
<tr>
<td></td>
<td>SMTP Service</td>
<td>Trend Micro MTA/MDA</td>
</tr>
<tr>
<td></td>
<td>IP Profiler</td>
<td>Part of Trend Micro MTA</td>
</tr>
<tr>
<td></td>
<td>NRS</td>
<td>Part of Trend Micro MTA</td>
</tr>
</tbody>
</table>

TABLE 3-1. Component and sub-module installation
### EUQ Service

- **Apache Tomcat**: The Web server for the EUQ Web console, through which your users can access the email messages that IMSS quarantined as spam.
- **Apache Service**: You install this module with the primary EUQ services for load balancing purposes when you choose to install multiple EUQ services.
- **IMSSMGR**: A module to manage EUQ processes.

### 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.

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

---

**TABLE 3-1. Component and sub-module installation**
### IMSS Ports

See Table 3-2 for the ports IMSS uses.

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>The MTA service port. The mail server will listen at this port to accept messages. This port must be opened at the firewall, or the server is not able to accept mails.</td>
<td>From the Web management console, click Administration &gt; IMSS Configuration &gt; SMTP Routing &gt; Connections on the menu.</td>
</tr>
<tr>
<td>110</td>
<td>IMSS scanner generic POP3 port. The scanner uses this port to accept POP3 request and scan POP3 mails for all POP3 servers.</td>
<td>From the Web management console, click Administration &gt; IMSS Configuration &gt; Connections &gt; POP3 on the menu.</td>
</tr>
<tr>
<td>5060</td>
<td>Policy Server listening port. The scanner will connect to this port to query matched rules for every message.</td>
<td>From the Web management console, click Administration &gt; IMSS Configuration &gt; Connections &gt; Components on the menu.</td>
</tr>
<tr>
<td>8005</td>
<td>Admin UI Web Server (Tomcat) management port that can handle Tomcat management command.</td>
<td>{IMSS}\UI\adminUI\conf\server.xml : Server\port</td>
</tr>
<tr>
<td>8009</td>
<td>EUQ Console Tomcat AJP port. This port is used to perform load balancing between several Tomcat servers and the Apache HTTP server.</td>
<td>{IMSS}\UI\euqUI\conf\server.xml: Server\Service\Connector (protocol=AJP\1.3)\port</td>
</tr>
<tr>
<td>8015</td>
<td>Tomcat management port that can handle Tomcat management command.</td>
<td>{IMSS}\UI\euqUI\conf\server.xml: Server\port</td>
</tr>
</tbody>
</table>

**TABLE 3-2. IMSS Ports**

3-8
You need to open this port to log on to the Web management console using a Web browser.

You need to open this port to log on to the Web management console using a Web browser.

Tomcat listen port:
{IMSS}\UI\adminUI\conf\server.xml:
Server\Service\Connector\port

EUQ service listening port.
{IMSS}\UI\euqUI\conf\server.xml:
Server\Service\Connector\port

EUQ service listening port with load balance.
{IMSS}\UI\euqUI\conf\EUQ.conf:
Listen\VirtualHost\ServerName

IMSS scanner reprocessing port. Messages released from the central quarantine area in the admin database and from the EUQ database will be sent to this port for reprocessing.
imss.ini\[Socket_3\]proxy_port

The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSS.) All messages sent to this port will not be scanned by IMSS. Due to security considerations, the port is only bound at IMSS server's loopback interface (127.0.0.1). It is therefore not accessible from other computers. You are not required to open this port at the firewall.
tsmtpd.ini

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
</table>
| 8445        | Admin UI listening port. You need to open this port to log on to the Web management console using a Web browser. | Tomcat listen port:
{IMSS}\UI\adminUI\conf\server.xml:
Server\Service\Connector\port |
| 8446        | EUQ service listening port. | {IMSS}\UI\euqUI\conf\server.xml:
Server\Service\Connector\port |
| 8447        | EUQ service listening port with load balance. | {IMSS}\UI\euqUI\conf\EUQ.conf:
Listen\VirtualHost\ServerName |
| 10024       | IMSS scanner reprocessing port. Messages released from the central quarantine area in the admin database and from the EUQ database will be sent to this port for reprocessing. | imss.ini\[Socket_3\]proxy_port |
| 10026       | The IMSS "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSS.) All messages sent to this port will not be scanned by IMSS. Due to security considerations, the port is only bound at IMSS server's loopback interface (127.0.0.1). It is therefore not accessible from other computers. You are not required to open this port at the firewall. | tsmtpd.ini |

**TABLE 3-2. IMSS Ports**
Trend Micro™ InterScan™ Messaging Security Suite 7.0 Installation Guide

15505 | IMSS Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the Web management console. The manager also provides quarantine/archive query results to the Web management console and the EUQ Web console through this port. | From the Web management console, click Administration > IMSS Configuration > Connections > Components on the menu. |

IMSS uses the following ports when you enable related service:

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>389</td>
<td>LDAP server listening port. You would need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.</td>
<td>From the Web management console, click Administration &gt; IMSS Configuration &gt; Connections &gt; LDAP on the menu.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>Microsoft IIS http listening port.</td>
<td>From the Web management console, click Administration &gt; IMSS Configuration &gt; Connections &gt; TMCM Server on the menu.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Microsoft IIS https listening port. You would need this port if you are using Control Manager to manage IMSS, as the Control Manager Server depends on Microsoft IIS.</td>
<td>From the Web management console, click Administration &gt; IMSS Configuration &gt; Connections &gt; TMCM Server on the menu.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>KDC port for Kerberos realm.</td>
<td>Not configurable on the IMSS server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Component and Role</th>
<th>Configuration Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>The Bind service listening port. Please do not change the port.</td>
<td>Not configurable on the IMSS server.</td>
</tr>
</tbody>
</table>

**TABLE 3-2. IMSS Ports**
Considering Network Topology

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

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

Installing Without a Firewall

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

![Figure 3-1 Installation topology: no firewall](image)

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

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

![Installation topology: in front of the firewall](image)

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

**Incoming Traffic**
- IMSS should be the first server to receive incoming email. Configure the MX records on the DNS servers that currently reference your SMTP gateway or firewall to reference the address of the IMSS server, or the switch that performs load balancing between scanners.
- Configure the relay control settings to allow relay for local domains only.

**Outgoing Traffic**
- If there is no firewall, configure the SMTP gateways to route all outgoing emails to IMSS. If there is a firewall, configure the firewall (proxy-based) to route all outbound emails to IMSS so that:
  - Outgoing SMTP emails can only go to the IMSS server(s).
  - Incoming SMTP emails can only come from the IMSS server(s).
- Configure IMSS to allow internal SMTP gateways to relay to any domain through IMSS.

Installing Behind a Firewall

Figure 3-3 illustrates how to deploy IMSS behind the firewall:
Planning for Deployment

FIGURE 3-3   Installation topology: behind a firewall

Incoming Traffic
- If you have a proxy-based firewall, configure it so:
  - Outgoing SMTP emails can only go to the IMSS server or the switch performing load balancing between scanners.
  - Incoming SMTP emails can only come from the IMSS server(s).
- If you have a packet-based firewall:
  - 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 emails destined to your local domain(s) to the SMTP gateway or your internal mail server (Exchange IMS).
  - Configure relay restriction to relay only for local domain(s).

Outgoing Traffic
- Configure all internal SMTP gateways to forward outgoing emails to the IMSS server.
- If you are replacing your SMTP gateway with IMSS, configure your internal mail server (for example, Exchange IMS) to forward outgoing emails to the IMSS server.
- Configure IMSS to route all outgoing emails (to domains other than the local domains) to the firewall, or deliver this email by using an external DNS server.
- Configure IMSS to allow internal SMTP gateways to relay, by using IMSS, to any domain.
Installing on a Former SMTP Gateway

Figure 3-4 shows a single-server installation of IMSS placed on the same server that previously hosted the SMTP gateway.

![Diagram of installation topology: On a former SMTP gateway](image)

**Figure 3-4  Installation topology: On a former SMTP gateway**

On the SMTP gateway:
- Allocate a new TCP/IP port to route SMTP emails in the gateway. It must be a port unused 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 emails to the SMTP gateway and the newly allocated port.
Outgoing Traffic

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

Installing in the De-Militarized Zone

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

Incoming Traffic

- If you have a proxy-based firewall, configure it so that incoming and outgoing SMTP emails can only go from the DMZ to the internal email servers.
- If you have a packet-based firewall, reconfigure it so that the mail exchange (MX) records on the DNS server that currently reference your SMTP gateway reference the address of the server hosting IMSS or the switch performing load balancing between scanners.
- Configure IMSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server (that is, Exchange IMS).
Outgoing Traffic

- Configure IMSS to route all outgoing emails (destined to domains other than the local domains) to the firewall or deliver by using an external DNS server.
- Configure all internal SMTP gateways to forward outgoing emails to the IMSS server.

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

Understanding Installation Scenarios

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

Single-Server Installation

For a single-server installation, you will need to have a server that meets the single-server installation requirements. If you install IMSS as a single-server installation and need to add capacity later, you can easily add additional scanner services, creating a multiple scanner service installation.

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

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

Note: To use IP filtering services, you must deploy IMSS as the Edge MTA.
Figure 3-6 shows how a single-server installation of IMSS fits into a standard messaging network topology.

**FIGURE 3-6 Single server deployment**

To perform a single-server installation:
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 database and Policy Service installed on the first server. This installation scenario provides a high level of message throughput. You can also choose to install the end-user console to enable End-User Quarantine (EUQ) management of spam-quarantined items.

Installing Multiple Scanner Services and Policy Services

To increase performance, add additional scanner services or policy service/scanner service pairs to your installation.

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

You can place a layer 4 switch between the edge MTA and the IMSS scanner services for load balancing purposes.

Note: To use IP filtering services, you must deploy IMSS as the Edge MTA.
FIGURE 3-7  Multiple scanner service and policy service deployment

To perform a multiple scanner service installation:

1. On one computer, install IMSS and End-User Quarantine.
2. On other computers, install the necessary scanner services and policy services.

   **Note:** Always install the policy service on the same computer with scanner service installed. You can choose to start-up any number of policy services as required.

3. After you open the IMSS Web management console and perform initial configuration, go to the System Summary screen.

4. Click Start for the scanner or policy services you want to enable.

**Multiple End-User Quarantine Service Installation**

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

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

Figure 3-8 shows how a single-server installation of IMSS with a separate primary EUQ server and additional secondary EUQ servers (with Apache services for load balancing) and distributed EUQ databases fit into a standard messaging network topology.

   **Note:** To use IP filtering services, you must deploy IMSS as the Edge MTA.
FIGURE 3-8  Multiple EUQ service deployment
To perform a multiple EUQ service installation:

1. On one computer, install IMSS.
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 and install the EUQ database on the same computer where EUQ services will run, or on different computers.

Note: Only the Apache service with the primary EUQ service is running for load balancing after installation.

4. After you open the IMSS Web management console and perform initial configuration, go to the System Summary screen.
5. Click Start for the EUQ services you want to enable.

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 be of a type that does 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.

Communication Between Servers

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

**Complex Distributed Installation**

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

You can also choose to install multiple instances of the end-user console to enable users to manage spam-quarantined items. Likewise, you can install multiple EUQ databases to enhance EUQ performance. You can always install additional instances of scanner services and EUQ services.

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

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 each IMSS deployment.

Figure 3-9 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:** Only the Apache service with the primary EUQ service is running for load balancing after installation.

You should always install the policy service on the same computer with the scanner service. You can choose to start any number of policy services as required.
Note: To use IP filtering services, you must deploy IMSS as the Edge MTA.

FIGURE 3-9 Complex architecture deployment
Wide-Area Network Installation

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

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

Trend Micro Control Manager

To easily manage all IMSS servers (with Central Controllers installed), Trend Micro recommends installing a Trend Micro Control Manager server. This scenario includes two Control Manager servers, which manage all sites and communicate with each other to replicate database information.

Figure 3-10 shows a multi-site WAN deployment.
The following describes how each site differs in this scenario:

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

**Fault Tolerance and Failover in a WAN Scenario**

Three out of the four sites in this scenario use multiple scanner services with policy services installed. Policy services can access cached IMSS settings from the IMSS...
admin database. Any scanner service that goes down can use another active policy service. Therefore, if one policy service stops or if an interruption to the communication with the central database occurs, both scanner services remain operational and continue processing emails by using the active policy service that has a connection to the IMSS server. See Figure 3-11.

Each site has its own Central Controller and database server, all of which report back to two Control Manager servers. Control Manager servers can replicate the IMSS configurations in the IMSS admin databases between all IMSS deployments registered to the same Control Manager server. If one of the IMSS admin databases become corrupt or unoperational, you can use the replica for restoration.

**FIGURE 3-11 Failover**
IP Filtering

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

Deploying IMSS with IP Filtering

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

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

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

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

Table 3-3 shows what happens when certain IMSS components malfunction, and how you can plan for failover to keep your IMSS protection up and running. For more information about failover in a WAN deployment scenario, see *Fault Tolerance and Failover in a WAN Scenario* on page 3-26.

<table>
<thead>
<tr>
<th>Component that Malfunctions</th>
<th>Expected Result</th>
<th>Recommended Failover Plan</th>
</tr>
</thead>
</table>
| Scanner service is not running or becomes disconnected | 1. IMSS tries to restart the scanner service  
2. IMSS sends an event notification if the service cannot be started within the time you specify for notifications. | Install multiple scanners for load balancing and failover. For details, see *Multiple Scanner and EUQ Service/Database Installation* on page 4-14. |
| Policy service is not running or a communication problem occurs with the IMSS server | 1. Scanner services using the stopped policy service switch to an active policy service (if available).  
2. IMSS tries to restart the policy service.  
3. IMSS sends an event notification if the service cannot be started or reconnected within the time you specify for notifications. | Install multiple scanners for load balancing and failover. For details, see *Multiple Scanner and EUQ Service/Database Installation* on page 4-14. |
| IMSS admin database is not running | 1. The IMSS server will continue to operate.  
2. IMSS sends an event notification if it is unable to start the service within the time you specify for notifications. | Back up the admin database periodically. For more information on backup and restore, visit www.microsoft.com. |
| EUQ service database is not running | 1. An error message appears on the EUQ Web console.  
2. IMSS sends an event notification if it is unable to start the service within the time you specify for notifications. | Back up the EUQ Database periodically. For more information on backup and restore, visit www.microsoft.com. |
### TABLE 3-3. Failover Scenarios

<table>
<thead>
<tr>
<th>Component that Malfunctions</th>
<th>Expected Result</th>
<th>Recommended Failover Plan</th>
</tr>
</thead>
</table>
| LDAP server is not running  | 1. An error message appears on the EUQ Web console during EUQ login.  
2. IP Profiler will not use the LDAP settings.  
3. If LDAP is disconnected and you have specified LDAP groups in the policy route, IMSS will continue to run normally using the cached LDAP entities (if available) when performing a policy match. IMSS will also automatically send an event notification regarding the disconnection to the addressees specified in Administration > Notifications > Delivery Settings. | Enable a secondary LDAP server as follows:  
1. Choose Administration > Connections.  
2. Click the LDAP tab.  
3. Select the check box next to Enable LDAP2 and provide the required information. Trend Micro also recommends that you enable the fault tolerance feature on the LDAP server. |

**Note:** IMSS automatically sends the LDAP disconnection notification in the backend and you cannot configure the notification settings from the Web management console.
Installing and Upgrading

This chapter explains how to install and uninstall InterScan Messaging Security Suite (IMSS) under various scenarios, as well as provides instructions on how to back up, restore and upgrade IMSS.

- Single-Server Installation on page 4-2
- Multiple Scanner and EUQ Service/Database Installation on page 4-14
- Complex Distributed Installation on page 4-24
- Silent Installation on page 4-25
- Upgrading From IMSS 5.7 on page 4-28
- Rolling Back After Upgrading on page 4-38
- Performing Uninstallation on page 4-40
Single-Server Installation

To perform a basic installation:

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

![Setup Type Screen]

3. Select Install a new IMSS server.
4. Click Next. The License Agreement screen appears.

![License Agreement Screen]
5. Please read the license agreement carefully before selecting **I accept the terms of the license agreement**.

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

![Administration Database Settings](image)

To use an existing database server:

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

b. Click **Next**. Type the required information for the existing database server.
Note: If you have multiple database servers on the target computer, then type the IP address or hostname.

To install the Microsoft SQL Server Desktop Engine (MSDE) database on this server:

a. Select Install MSDE.

b. Type a Database name and Password for the MSDE “sa” user account.
Tip: MSDE 2000 has the following limitations:
- 2GB data
- 5 concurrent user connections or workloads
Trend Micro recommends not using MSDE, if the daily mail traffic is more than 30,000 or if you are using IMSS EUQ. This is to ensure adequate storage space for reports and log query results.

Note: Enable the database service TCP/IP protocol to avoid the following issues:
1. Installation cannot connect to the existing database using an IP address.
2. Central controller management console is unable to open.

7. Click Next. The Choose Destination Location screen appears.
8. To change the destination directory, click **Browse** and locate the desired directory.

**Note:** IMSS 7.0 cannot install on Windows 2003 x64 platforms in the directory 
C:\program Files\Trend Micro\imss. Only x64 programs can deploy to that directory on Windows 2003 x64 platforms.

To install IMSS in the following directory on x64 platforms use 
C:\program Files (x86)\Trend Micro\imss.
9. Click Next. The IMSS Components screen appears.

![IMSS Components screen](image)

10. Select the required components:

- **IMSS Central Controller**: The central controller contains a working Web server component that serves Web console interface screens to browsers. The Web management console allows administrators to configure and control IMSS.

- **IMSS Scanner Service**: Scanners accept SMTP and POP3 messaging traffic, request policy from a policy server, evaluate the message based on the applicable policies, and take the appropriate action on the message based on the evaluation outcome.

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

- **IMSS End-User Quarantine Database**: The EUQ database stores quarantined spam email information and the end-user approved sender list. If you install EUQ, you must also install the EUQ database (or multiple databases for scalability).

11. Select Next. The End-user Quarantine (EUQ) Database Settings screen appears if you have selected the IMSS End-user Quarantine Database option.
To use an existing database server:

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

b. Click **Next**. Type the information for the existing database server.
To install an MSDE database on this server:

a. Select Install MSDE.

b. Type the EUQ database name and a Password for the MSDE "sa" user account.

12. Click Next. The Settings Summary screen appears.
13. Verify the selected components and the defined settings. Click Next. The Setup Status screen appears and installation begins.
14. Click Next. The InstallShield Wizard Complete screen appears.
15. Select Yes, I want to restart my computer now.
16. Click Finish.
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.

Appending Components When No Previously Installed Components Exist

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

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

3. Select 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.
6. Click Next. The Choose Destination Location screen appears.

7. Specify the destination path.
8. Click **Next**. The IMSS components screen appears.

To install additional IMSS Scanner Service:

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

b. Click **Next**. The Settings Summary screen appears.
c. Verify the settings and click Next. The Setup Status screen appears.

d. Click Next. The files install.
To install additional EUQ Service and/or EUQ Database:

- Select **IMSS End-user Quarantine Service** and/or **IMSS End-user Quarantine Database**.
- 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 MSDE database on this server:

i. Select **Install MSDE**.

ii. Type the **EUQ database name** and a **Password** for the MSDE “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.
9. Click **Next**. The InstallShield Wizard Complete screen appears.

10. Select **Yes, I want to restart my computer now**. 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 redistribute data from the original EUQ databases to all databases.

Appending Components When Previously Installed Components Exist

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

1. Double-click Setup.exe. The Preparing to Install... screen appears, followed by the Welcome screen.
2. Click Next. The Setup Type screen appears.
3. Select Add or remove components for an existing IMSS Server.
4. Click Next. The Select Features screen appears.
5. Choose the component to add.
6. Click **Next**. The Settings Summary screen appears. If you have chosen to install additional EUQ Service or Database, you will be prompted to provide the EUQ database information before you see the Settings Summary screen.
7. Click **Next**. The Setup Status screen appears.
8. After installation, the Maintenance Complete screen appears.

9. Select **Yes, I want to restart my computer now**.
10. Click **Finish**.

**Complex Distributed Installation**

To deploy a complex distributed scenario, do the following:

1. Install IMSS on a single server (see *Single-Server Installation* on page 4-2).
2. Append additional IMSS scanner services, EUQ services or EUQ databases (see *Multiple Scanner and EUQ Service/Database Installation* on page 4-14).

**Tip:** MSDE 2000 has the following limitations:
- 2GB data
- 5 concurrent user connections or workloads
Trend Micro recommends not using MSDE, if the daily mail traffic is more than 30,000 or if you are using IMSS EUQ. This is to ensure adequate storage space for reports and log query results.
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 everytime you run setup.exe on other computers.

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

Silent installation includes two main steps:

**Step 1:** Recording the installation steps.
**Step 2:** Running the script to install additional components.

Recording the Installation Steps

To record the installation steps:

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 `InstRecord.bat` file to record the installation steps in the specified script. For example:

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

4. Type `setup.exe` to run the installation program. See *Single-Server Installation* on page 4-2.

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

---

### Running the Silent Installation Script

To install additional components using the silent installation script:

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

2. Change to a sub folder called `utility`.

---

![Command window output]

---

4-26
3. Run the `InstSilent.bat` file to install components using the silent installation script created earlier. See *Recording the Installation Steps* on page 4-25. For example:

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

4. The installation proceeds silently in the background without pop-up installation pages.

**Note:** To verify that installation has been completed successfully, click **Summary > System** tab on the Web management console and check the **Managed Server Settings**.
Upgrading From IMSS 5.7

The IMSS 7.0 installation program can automatically upgrade from IMSS version 5.7. When the installation program detects IMSS 5.7, it can perform the following:

• Uninstall the previous version of IMSS
• Install IMSS
• Migrate all existing settings

**Tip:** If you choose not to migrate your old IMSS settings, Trend Micro recommends completely uninstalling IMSS and then performing a fresh install, rather than installing IMSS 7.0 over an existing installation.

Backing Up Before Upgrading

If there are problems with upgrading, you will need to roll back to your previous settings. In order to roll back smoothly, retain as much data from IMSS 5.7 as possible.

**Tip:** Before performing an upgrade, Trend Micro recommends backing up data according to the following steps.

Backing Up IMSS 5.7 Data for a Single-Server Deployment

To back up IMSS 5.7 data before upgrading:

1. Stop all IMSS 5.7 services from the System Service Manager.
2. Back up IMSS on the database server using the Microsoft SQL management tool.
3. Stop the database service from the System Service Manager.
4. Stop IIS services from the System Service Manager.
5. Back up the installation folder of IMSS 5.7.
6. Export the policy settings from the registry:

HKEY_LOCAL_MACHINE>SOFTWARE>TrendMicro
Backing Up IMSS 5.7 Data for a Distributed Deployment

If you deployed IMSS 5.7 in a distributed environment, then each component can appear on a dedicated server as follows:

- Server 1: IMSS 5.7 scanner
- Server 2: IMSS 5.7 database
- Server 3: IMSS 5.7 Central Report and EUQ

Under such conditions, the steps for rolling back may be slightly different from those in a single server deployment.

To back up IMSS 5.7 data for a distributed deployment:

On Server 1:

1. Stop all IMSS 5.7 services from the System Service Manager.
2. Stop IIS services from the System Service Manager.
3. Back up the home folder of IMSS 5.7.
4. Export IMSS 5.7 policy settings from the registry:
   HKEY_LOCAL_MACHINE>SOFTWARE>TrendMicro
   On Server 2:
   1. Backup the IMSS database on the database server using the Microsoft SQL Management tool.
   2. Stop the database service.
   On Server 3:
   1. Stop all IMSS 5.7 services from the System Service Manager.
   2. Stop the IIS Admin Service from the System Service Manager.
   3. Back up the installation folder of IMSS 5.7.

Performing an Upgrade

To perform an upgrade:

1. Type setup.exe. The Migrate option appears if the installation package detects the existence of IMSS 5.7.

   ![IMSS Installation Window]

   Note: If you select Fresh Install, the setup program uninstalls IMSS 5.7, then installs IMSS 7.0.

2. Select Migrate.
3. Click **Next**. The Migration Information screen appears.

   ![Migration Information Screen](image)

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

4. Click **Next**. The Policy Setting screen appears if you have policies with special routes in IMSS 5.7.
5. Select the policy directions by clicking **Incoming/Outgoing**.

Click **Next**. Migration data backs up and a setup confirmation screen appears.

6. Click **Yes**. IMSS 5.7 uninstalls.
A confirmation screen appears.

7. Click **Yes** to remove all remaining IMSS 5.7 components. Uninstallation continues.
The Migration Status screen appears, showing the IMSS 5.7 uninstallation results.
8. Click Next. Configure and install IMSS 7.0 (as in *Single-Server Installation* on page 4-2). As installation completes, the installation program imports IMSS 5.7 data to IMSS 7.0.

The Migration Results screen appears.
Note: After upgrading, IMSS detects invalid x-filter rules and places the result into C:\Imss7InstLog\migration\installlog\InvalidRule.txt. IMSS 5.7 accepts expressions preceding with an asterisk, such as *aaabbb, but IMSS 7.0 cannot accept such expressions. To eliminate such syntax errors, please replace the asterisks found at the beginning of expressions with "\*" or ".*"

Rolling Back After Upgrading

Currently, the IMSS 7.0 installation program does not support rolling back automatically after an upgrade. Therefore, this section describes manually rolling back from the upgraded IMSS 7.0 to IMSS 5.7.

Rolling Back From a Single Server Deployment

To roll back from a single server deployment:

1. Uninstall all IMSS7.0 components using the uninstallation program.
2. Perform a fresh install for IMSS 5.7.
3. Stop all IMSS 5.7 services from the System Service Manager.
4. Start the database service.
5. Restore the database data for IMSS 5.7 using the Microsoft SQL Management tool.
6. Stop the database service.
7. Stop IIS services from the System Service Manager.
8. Restore the IMSS 5.7 installation folder.
10. Import the old IMSS 5.7 policy settings into the registry.
12. Start the database service.
13. Start all services of IMSS 5.7 in the following sequence:
   a. Start TMI.
   b. Start CCGI.
   c. Start all other IMSS-related services.

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

Rolling Back From a Distributed Deployment

To roll back from a distributed deployment (using the previous distributed deployment example):

1. Uninstall all IMSS 7.0 components using the uninstallation program.
2. Perform a fresh install of IMSS 5.7. Follow the previous IMSS 5.7 deployment.
3. Stop all IMSS 5.7 services:
   a. On Server 1: Stop all IMSS-related services and the IIS service.
   b. On Server 3: Stop all IMSS-related services.
4. Restore IMSS 5.7-related data On Server 1:
   a. Restore the IMSS 5.7 installation folder.
   b. Delete “TrendMicro” from the registry.
   c. Import the old IMSS 5.7 policy settings into the registry.
5. On Server 2: Restore IMSS 5.7 database data using the Microsoft SQL Management tool
6. On Server 3: Restore the IMSS 5.7 installation folder.
7. On Server 2: Restart the database service.
8. On Server 1:
   b. Start all IMSS-related services in the following sequence:
      i. Start TMI.
      ii. Start CCGI.
iii. Start all other IMSS-related services.

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


Performing Uninstallation

This section describes how to remove IMSS components. You can uninstall the Central Controller, Scanner services, and EUQ components separately or concurrently.

To uninstall IMSS:

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

2. Select the components to remove:
   To remove all IMSS components from your 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. Deselect the component to be uninstalled. For example, to uninstall the EUQ database, uncheck the respective option.
d. Click Next. The following message appears if you chose to uninstall the EUQ database.

![Screenshot of uninstallation message]

```
Trend Micro InterScan Messaging Security Suite - InstallShield Wizard

Note: Uninstallation will only unregister the EUQ database in the administrator database. The EUQ database is not deleted.
```

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 is similar to the steps in Silent Installation on page 4-25.

**Note:** Please run the silent uninstallation on the computer that has a similar environment as the computer where you recorded the silent installation script. Close all Service Management screens when you record the silent installation script or execute a silent installation.
Upgrading MSDE to SQL Server 2005 Express

You can install IMSS Admin Database and EUQ Database using Microsoft SQL Server Desktop Engine (MSDE). However, in accordance to the standard Microsoft lifecycle policies, mainstream support for MSDE will end on April 8th, 2008. This section provides instructions on how you can integrate IMSS 7.0 with the next version of MSDE—SQL Server 2005 Express.

Prerequisites to Installing SQL Server 2005 Express

Prior to installing SQL Server 2005 Express, you are required to download and install the following:

- Windows Installer 3.1
- .NET Framework 2.0

For more information, visit http://www.microsoft.com/technet/prodtechnol/sql/2005/msde2sqlexpress.mspx#ESHAC

Upgrading MSDE to SQL Server 2005 Express for Previously Installed IMSS 7.0

If you have previously installed MSDE with IMSS 7.0, do the following to completely upgrade MSDE to SQL Server 2005 Express:

**Step 1:** Stop all IMSS services
**Step 2:** Back up IMSS databases
**Step 3:** Install SQL Server 2005 Express
**Step 4:** Reset the database administrator’s password
**Step 5:** Start IMSS services

**Step 1: Stopping all IMSS services**

**To stop IMSS services:**

1. Logon as the administrator at the computer where you installed IMSS 7.0 components.
2. Open a command prompt and type the following commands to stop IMSS services:
   net stop TmImssManager
   net stop TmImssAdminUI
   net stop TmImssTasks
   net stop TmImssScan
   net stop TmImssMTA
   net stop TmImssPolicy
   net stop TmImssIpprofiler
   net stop TmImssCMAgent
   net stop TmImssEuqUI

Step 2: Back Up IMSS Databases
Trend Micro recommends that you back up the IMSS Admin database and EUQ database before upgrading MSDE. Should any unexpected event occur during upgrade, you can then use the `restore database` command to roll back the databases to the original state.

To back up IMSS databases:

1. Open a command prompt and type the command `osql` to connect to the instance you wish to upgrade.
   To connect to the local, default instance of MSDE using Windows Authentication, type the command `osql -E`.
2. Back up IMSS databases on the MSDE instance by entering the following commands at the `osql` command prompt:
   1> backup database imss to disk='c:\imss.dat'
   2> GO
   1> backup database imssequ to disk='c:\imsssequ.dat'
   2> GO

Step 3: Installing SQL Server 2005 Express

To install SQL Server 2005 Express:

1. Logon as the administrator at the computer where you installed MSDE.
2. Type `sqlexpr.exe` to start the SQL Server 2005 Express setup program.
   For details, visit
#ESHAC

**Note:**
1. Trend Micro recommends that you use the **advanced configuration options** on the Registration Information screen to upgrade MSDE.
2. On the Instance Name screen, select the instance used by IMSS.
3. Choose the **Windows Authentication Mode** when upgrading the database from MSDE to SQL Server 2005 Express.

---

### Step 4: Resetting the Database Administrator’s Password

The Windows Authentication Mode does not require any password when you upgrade from MSDE to SQL Server 2005 Express. However, you are required to reset the database administrator’s password in order to connect to the existing IMSS databases after the upgrade.

**To reset the database administrator’s password:**

1. Open a command prompt.
2. Type `sqlcmd -E` to start the sqlcmd session.
3. Enter the following commands to enable the `sa` account and set the password for `sa`:
   ```
   1> ALTER LOGIN sa ENABLE
   2> GO
   1> ALTER LOGIN sa WITH PASSWORD = '<password>'
   2> GO
   ```

**Note:** You are required to use the old MSDE `sa` password.
Step 5: Start IMSS Services

To start IMSS services:

1. Logon as the administrator at the computer where you installed IMSS services.
2. Type the following commands in sequence at the command prompt:

   net start TmImssManager
   net start TmImssAdminUI
   net start TmImssTasks
   net start TmImssMTA
   net start TmImssScan
   net start TmImssPolicy
   net start TmImssIpprofiler
   net start TmImssCMAgent
   net start TmImssEuqUI
Integrating SQL Server 2005 Express With Fresh IMSS 7.0 Installation

If you are performing a fresh installation of IMSS 7.0, do the following to integrate SQL Server 2005 Express with IMSS 7.0:

**Step 1:** Install SQL Server 2005 Express
**Step 2:** Enable network access
**Step 3:** Automate the startup for SQL Server Browser Service
**Step 4:** Install IMSS 7.0

**Step 1: Installing SQL Server 2005 Express**

To install SQL Server 2005 Express:

1. Logon as the administrator.
2. Type `sqlexpr.exe` to start the SQL Server 2005 Express setup program.
   

**Note:** Choose the **Mixed Mode** (Windows Authentication and SQL Server Authentication) when performing a fresh installation of SQL Server 2005 Express.

**Step 2: Enabling Network Access**

By default, the named pipes and TCP/IP protocols are disabled with the installation of SQL Server 2005 Express. You can enable these protocols using the SQL Server Configuration Manager.

Step 3: Automating the Startup for SQL Server Browser Service

The SQL Server Browser service identifies which network ports the SQL Server 2005 Express instance listens on. Use the SQL Server 2005 Surface Area Configuration utility to set the startup type for SQL Server Browser Service to Automatic.

For details, visit http://www.microsoft.com/technet/prodtechnol/sql/2005/msde2sqlexpress.mspx#EV OAE)

Step 4: Installing IMSS 7.0

See Single-Server Installation on page 4-2 for details on how to install IMSS 7.0.

Note the following when integrating IMSS 7.0 with SQL Server 2005 Express during installation:

1. On the Administration Database Settings screen, choose Use existing database server.

2. Click Next.
3. Provide the Administration Database Settings information. Ensure that you append the database instance name at the **Database Server** field. The default instance name of SQL Server 2005 is SQLEXPRESS.
Troubleshooting, FAQ, and Support

This chapter explains how to troubleshoot common InterScan Messaging Security Suite (IMSS) issues, search the Trend Micro Knowledge Base, and contact support.

Topics include:

- Troubleshooting on page 5-2
- Frequently Asked Questions on page 5-3
- Using the Knowledge Base on page 5-8
- Contacting Support on page 5-8
Troubleshooting

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

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

<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The NRS installation does not validate the NRS Activation Code</td>
<td>To validate the Activation Code, the NRS installation script accesses Trend Micro through the Internet. Verify that your DNS server is operating correctly and that the computer on which you are installing NRS has access to the Internet.</td>
</tr>
<tr>
<td>IMSS cannot work normally due to a database access issue, if IMSS is installed on Windows 2000 SP4.</td>
<td>The MDAC version is lower than 2.8 SP1. Please download and install the latest Microsoft MDAC version from the Microsoft Web site: <a href="http://msdn2.microsoft.com/en-us/data/aa937729.aspx">http://msdn2.microsoft.com/en-us/data/aa937729.aspx</a></td>
</tr>
</tbody>
</table>

TABLE 5-1.  Troubleshooting issues
Frequently Asked Questions

Installation

Can the IMSS administrator database be installed separately?
Yes. You can install the IMSS administrator database separately in two ways
• Run the install program and configure the IMSS database only without selecting any other IMSS components.
• Run the install program at the command interface, if you have an existing database server on the target machine:
  • Go to the setup folder.
  • Run the installation program using the following command:
    `setup.exe /zOnlyInstDB`
  • Follow the installation screens to install the IMSS admin database.

Note: After installing the IMSS admin database, run the installation program and install any other components using an account other than "sa" to connect to the IMSS database.

Can I install multiple database instances on the target computer?
No. If you have an existing database on the target computer, use it only for the IMSS database or EUQ database. Alternatively, uninstall the existing database and install a new MSDE database. MSDE is included in the IMSS installation package.

How many scanners can I install?
You can install any number of scanners.

How many EUQ services and EUQ databases can I install?
You can install up to 8 EUQ services and EUQ databases.

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 install program tries to remove the database. Remove all connections to the old database, drop the database, and create a new database.

Must IMSS 7.0 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 can’t the shortcut for the Web management console on the target computer work?
If the target computer is on a Windows 2003 platform, then 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 Web management console service.
• Running: If the Web management console starts up before the database, then restart the Web management console service.

Can IMSS use a domain account to access a database?
No. IMSS 7.0 does not support Windows authentication.

Can the database server be referenced by hostname?
Yes. You can specify the "IP\Instance" or "Hostname\Instance".

Can the server IP address be changed?
Yes.
To change the server IP address:
 a. Stop all IMSS services.
 b. Change the server IP address.
 c. Change the ODBC DSN IP address in the control panel.
d. Change the IP address in ODBC.ini and EUQ.ini in the IMSS configuration folder.

e. Change the database URL and user name/password in

```
%IMSS_HOME%/ui/adminUI/webapps/ROOT/WEB-INF.struts-config-common.xml
```

e. Change the database URL and user name/password in

```
%IMSS_HOME%/ui/adminUI/webapps/ROOT/WEB-INF.struts-config-common.xml
```

f. 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.

g. Modify `tsmtpd.ini` as required for MTA flow.

h. Restart all IMSS services.

Where is the MIB file for SNMP notification?
The file is located at `%IMSS_HOME%/help/IMSS70_win.mib`.

How can I migrate DBCS settings in IMSS 5.7?
Before migration, make sure that the language settings are correct.

a. Install East Asian language files. For Windows 2003, click **Control panel > Regional and Language Options > Languages** and select Install files for East Asian languages.

b. Change the Language for non-Unicode programs setting to Chinese/Japanese as required by the DBCS language used in IMSS 5.7.

c. Perform a migration installation.

**Upgrading**

Are all IMSS 5.7 settings maintained during migration?
No. Due to architectural changes in IMSS 7.0, some settings cannot be retained. The IMSS 7.0 installer will ask for the new values for these settings during migration and the settings can also be found in the general migration report:
What is the mapping relationship between IMSS 5.7 policies and IMSS 7.0 rules?
The mapping relationship is described in the detailed migration report:
C:\Imss7InstLog\migration\installlog\MigrationReport\DetailReport.txt.

How do I migrate multiple IMSS 5.7 scanners?
To migrate multiple IMSS 5.7 scanners:
- Migrate from the scanner with the most desired settings for the migration.
- Uninstall the remaining scanners.
- Append the multiple scanners.

Can I migrate the admin database and EUQ database from the same IMSS 5.7 database server?
Yes. IMSS 5.7 database settings (such as LDAP settings and EUQ settings) are retained.

Is a smooth rollback to IMSS 5.7 possible after migration?
Yes. See Rolling Back After Upgrading on page 4-38 for detailed rollback instructions.

Is it possible to migrate on a computer that has only the EUQ component?
No. Migrate from a computer with an installed IMSS 5.7 scanner.

How do I simplify SPS rules after migration?
In order to retain all SPS filter settings for all policies of IMSS 5.7, IMSS 7.0 migrates each SPS filter to one SPS rule in IMSS 7.0. If you want to reduce the number of SPS rules after migration, perform the following:
- Create a new SPS rule after migration.
- Delete all migrated SPS rules.

What is the source of internal addresses during migration?
To maintain IMSS 5.7 internal domains, IMSS 7.0 extracts all domains from the following fields:
- Domains in the "To" field of incoming policy routes
- Domains in the "From" field of outgoing policy routes

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

**How are filters and policies mapped during migration?**

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

a. Virus filter(s): There is only one virus rule for both directions after migration (regardless of the number of virus filters in IMSS 5.7).
   - The status of virus rules will be "Enable" if one of the virus filters is "active" in IMSS 5.7;
   - Otherwise, the status of the virus rule will be "disable" after migration.

b. SPS filter(s): The migration module maps each SPS filter into one SPS rule after migration.

c. eManager filter:
   - There will be two rules for one eManager filter after migration if it is "active" in IMSS 5.7 for both SMTP and POP3 traffic.
   - There will be only one rule for one eManager filter after migration if it is "inactive" in IMSS 5.7 for both SMTP and POP3 traffic. The rule direction is for "Both Incoming and outgoing directions". You can add the related rule for the POP3 direction in IMSS 7.0 if necessary.
Using the Knowledge Base

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

http://esupport.trendmicro.com

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

Contacting Support

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

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

http://us.trendmicro.com/us/about/contact_us/

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

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

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

A
about IMSS 1-2
admin database 3-6
Apache 3-7
  Tomcat 3-6
append components 4-14
archive 1-2
audience vi
B
browser requirements 2-3
C
CCGI 4-39
central controller 2-5
centralized archive and quarantine 1-2
centralized logging 1-2
centralized policy 1-2
component and sub-module installation 3-6
configuration wizard 1-3
contact
  support 5-8
CPU requirements 2-2
D
database
  on central controller 2-4
database server 3-6
disk space requirements 2-2
Documentation vi
E
email threats
  spam 1-5
  unproductive messages 1-5
EUQ 1-2
F
failover 3-29
filtering, how it works 1-7
Firefox 2-3
I
IMSS 1-2
IMSS components
  admin database 2-4
  central controller 2-4
  EUQ database 2-9
  EUQ primary and secondary services 2-6
  installation 3-6
  policy services 2-5
  policy services synchronization 2-6
  scanner services 2-5
IMSSMGR 3-6
Install 2-1
installation
  clustered 3-23
  IP Filtering, installation
    EUQ 3-28
  scenarios 3-16
installing
  before a firewall 3-12
  behind a firewall 3-12
  multiple scanner and EUQ
    service/database 4-14
  no firewall 3-11–3-12, 3-14
  on SMTP gateway 3-14
  single server 4-2
Internet Explorer 2-3
IP Filtering
about 2-9
IP Profiler 1-3
about 2-9
detects 2-9
how it works 2-10

K
Knowledge Base 5-8

L
logs 1-2

M
mass mailing viruses
pattern 1-6
Memory requirements 2-2
minimum requirements 2-2
MSDE 4-5, 4-10, 4-20
MTA features, opportunistic TLS 1-3

N
named server 3-6
new features 1-2
NRS 1-3
about 2-10
how it works 2-11
services 2-10

O
Online Help vi

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

Q
quarantine 1-2

R
Readme File vi
reports 1-2
requirements 2-2
rollback 4-38

S
scanners 2-6
silent install 4-25
spam prevention 1-3
spyware and grayware 1-9
support 5-8
swap space requirements 2-3
system requirements 2-2

T
TMCM
about, Control Manager
about 1-11
TMCM agent, agent
TMCM 1-11
TMI 4-39
Tomcat 3-6-3-7
Trend Micro Knowledge Base 5-8
troubleshooting 5-2
NRS 5-2

W
Web EUQ 1-2
what’s new 1-2

X
x64 4-7