Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before deploying and using the appliance, please review the readme files, release notes and the latest version of the Deployment Guide and Administrator’s 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, 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: MSEM73166/70423

Release Date: December 2007

Patents Pending
The Deployment Guide for Trend Micro InterScan Messaging Security Appliance 5000 is intended to introduce the main features of the device and deployment instructions for your production environment. You should read through it prior to deploying or using the device.

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
Chapter 3: Planning for Deployment

Deployment Checklist ................................................................. 3-2
Considering Email and Network Topology ............................ 3-5
  Deploying at the Gateway or Behind the Gateway ............. 3-6
  Deploying without a Firewall .............................................. 3-9
  Deploying in Front of a Firewall .............................. 3-10
    Incoming Traffic .................................................. 3-10
    Outgoing Traffic ................................................ 3-10
  Deploying Behind a Firewall ....................................... 3-11
    Incoming Traffic ................................................ 3-11
    Outgoing Traffic ................................................ 3-11
  Deploying on a Former SMTP Gateway ......................... 3-12
    Incoming Traffic ............................................. 3-12
    Outgoing Traffic ............................................. 3-12
  Deploying in the De-Militarized Zone ....................... 3-12
    Incoming Traffic ............................................. 3-12
    Outgoing Traffic ............................................. 3-13
Chapter 4: Upgrading From Previous Versions

Upgrading From an Evaluation Version ............................................ 4-2
Import/Export Notes ................................................................. 4-4
Upgrading From IMSA 1.0 To IMSA 7.0 ....................................... 4-6
  Exporting IMSA 1.0 Configuration Files .................................. 4-6
  Upgrading From IMSA 1.0 Environment .................................... 4-7
    Upgrading Through The Web Console .................................. 4-7
    Upgrading Through The CLI ................................................ 4-7
  Performing Post-Upgrade Procedures .................................... 4-9
Importing Settings .................................................................. 4-9
  Settings That Cannot Be Migrated From IMSA 1.0 ................. 4-10
Migrating From IMSS 5.7 To IMSA 7.0 ....................................... 4-12
  Exporting From IMSS 5.7 Linux ............................................ 4-12
  Exporting From IMSS 5.7 Solaris: ......................................... 4-12
  Exporting From IMSS 5.7 Windows ...................................... 4-13
### Chapter 5: Troubleshooting, FAQ and Support

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting</td>
<td>5-2</td>
</tr>
<tr>
<td>Troubleshooting Utilities</td>
<td>5-2</td>
</tr>
<tr>
<td>Troubleshooting Issues</td>
<td>5-2</td>
</tr>
<tr>
<td>Frequently Asked Questions (FAQ)</td>
<td>5-5</td>
</tr>
<tr>
<td>Importing and Exporting</td>
<td>5-5</td>
</tr>
<tr>
<td>Using the Knowledge Base</td>
<td>5-7</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>5-8</td>
</tr>
</tbody>
</table>

### Appendix A: Glossary of Terms

### Index
Preface

Welcome to the Trend Micro™ InterScan™ Messaging Security Appliance 5000 Deployment Guide. This manual contains information about device deployment, basic device configuration, and IP Filtering (IPProfiler and Network Reputation Services) activation.

This preface discusses the following topics:

• *InterScan Messaging Security Appliance 5000 7.0 Documentation* on page vi
• *Audience* on page vii
• *Document Conventions* on page viii
InterScan Messaging Security Appliance 5000 7.0 Documentation

The InterScan Messaging Security Appliance (IMSA) 5000 7.0 documentation consists of the following:

- **Quick Start Guide**—Helps you set up IMSA and connect it to your network.
- **Deployment Guide**—Contains information about IMSA features and system requirements, and describes how to deploy and upgrade IMSA in various network environments.
- **Administrator's Guide**—Helps you get IMSA up and running with post-deployment instructions on how to configure and administer IMSA.
- **Online Help**—Provides detailed information about each field on the Web management console and instructions on how to configure all features through the user interface. To access the online help, open the Web management console and then click the help icon ( ).
- **Readme File**—Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, deployment tips, known issues, and product release history.
- **Hardware Maintenance Sheet**—Shows you how to change fans, hard disks, and power supplies.
- **Third-party License Agreements**—Contains a list of license agreements from third party companies whose products IMSA uses.

Audience

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

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

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

To help you locate and interpret information easily, the IMSA 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><strong>Bold</strong></td>
<td>Menus and menu commands, command buttons, tabs, options, and other user interface items</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>References to other documentation</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Examples, sample command lines, program code, Web URL, file name, and program output</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Configuration notes</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Recommendations</td>
</tr>
<tr>
<td><strong>WARNING!</strong></td>
<td>Reminders on actions or configurations that must be avoided</td>
</tr>
</tbody>
</table>
Introducing InterScan™ Messaging Security Appliance 5000 Version 7.0

This chapter introduces InterScan Messaging Security Appliance (IMSA) features, capabilities, and technology, and provides basic information on IP Filtering, which includes IP Profiler and Network Reputation Services (NRS).

Topics include:
- About IMSA 5000 Version 7.0 on page 1-2
- IMSA Features and Benefits on page 1-3
- About Spam Prevention Solution on page 1-11
- About IP Filtering on page 1-12
- About End-user Quarantine (EUQ) on page 1-17
- About Centralized Reporting on page 1-17
- About Control Manager on page 1-17
About IMSA 5000 Version 7.0

InterScan Messaging Security Appliance (IMSA) integrates multi-tiered spam prevention and anti-phishing with award-winning antivirus and anti-spyware. Content filtering enforces compliance and prevents data leakage. This easy-to-deploy appliance is delivered on a highly scalable platform with centralized management, providing easy administration. Optimized for high performance and continuous security, the appliance provides comprehensive gateway email security.

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>Data port redundancy</td>
<td>A second data port to connect to your network if a problem arises with the main data port. The second data port has the same IP address as the main data port, but a different MAC address.</td>
</tr>
<tr>
<td>New hard disks</td>
<td>Two 250GB raid hard disks. See <em>About the RAID Hard Disks</em> on page 2-6.</td>
</tr>
<tr>
<td>Multiple antivirus and malware policies</td>
<td>Multiple IMSA 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. With centralized logging, administrators can quickly audit message-related activities.</td>
</tr>
<tr>
<td>Centralized archive and quarantine management</td>
<td>An easy way to search multiple IMSA 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 were detected as spam. Together with EUQ notification, IMSA will help lower the cost of helpdesk administrative tasks.</td>
</tr>
</tbody>
</table>
## IMSA Features and Benefits

IMSA protects your network from virus infection through the SMTP gateway. In addition, antivirus and content filtering provide intelligent message content management to ensure the integrity of your messaging system.

### New Feature Description

<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, using smart profiles, helps protect the mail server from attacks.</td>
</tr>
<tr>
<td></td>
<td>Trend Micro spam prevention engine accurately detects and removes unwanted email messages.</td>
</tr>
<tr>
<td>Delegated administration</td>
<td>LDAP-integrated account management, which allows users to assign administrative rights for different configuration tasks.</td>
</tr>
<tr>
<td>Easy deployment with</td>
<td>An easy-to-use configuration wizard to get IMSA up and running right out of the box.</td>
</tr>
<tr>
<td>Configuration Wizard</td>
<td></td>
</tr>
<tr>
<td>Advance MTA functions</td>
<td>TLS and other MTA functions help IMSA handle email efficiently and securely.</td>
</tr>
<tr>
<td>Migration</td>
<td>Easy migration process ensures that settings are transferred with 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 issues.</td>
</tr>
<tr>
<td>Integration with Trend Micro</td>
<td>Perform log queries from Control Manager, in addition to other supported features.</td>
</tr>
<tr>
<td>Control Manager™</td>
<td></td>
</tr>
<tr>
<td>Supports 8 bit to 7 bit-MIME</td>
<td>IMSA 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, IMSA will convert the message from 8 bit MIME to 7 bit MIME.</td>
</tr>
<tr>
<td>transformation</td>
<td></td>
</tr>
</tbody>
</table>
### Feature Descriptions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data and hardware redundancy</td>
<td>IMSA provides a second data port for data redundancy and hot swappable hardware components, such as fans, hard disks, and power supplies.</td>
<td>This feature enables IMSA to run uninterrupted, even during times of hardware failure.</td>
</tr>
<tr>
<td>Real-time Statistics and Monitor</td>
<td>Administrators can monitor the scan performance and IP filtering performance of all IMSA devices (within a group) on the Web management console.</td>
<td>IMSA provides administrators with an overview of the system that keeps administrators informed on the first sign of mail processing issues. Detailed logging helps administrators proactively manage issues before they become a problem.</td>
</tr>
<tr>
<td>Antivirus protection</td>
<td>IMSA 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. In addition, IMSA uses Trend Micro MacroTrap™ to scan Microsoft® Office® files. MacroTrap analyzes the macro code in Microsoft Office files to help the scan engine detect macro viruses.</td>
<td>The IMSA enhanced virus/content scanner helps to ensure that your messaging system performs optimally.</td>
</tr>
</tbody>
</table>
Introducing InterScan™ Messaging Security Appliance 5000 Version 7.0

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<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. 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>Helps reduce the risk that a virus compressed using different file compression schemes will enter your network via email.</td>
</tr>
<tr>
<td>Content management</td>
<td>IMSA analyzes the content of email messages and their attachments, and blocks messages or strips attachments if the content violates your policies.</td>
<td>IMSA can block or defer personal communication, large attachments, and other types of content that you deem inappropriate.</td>
</tr>
<tr>
<td>Protection against other email threats</td>
<td></td>
<td></td>
</tr>
<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>IMSA 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>IMSA allows you to configure the types of messages that are allowed to pass through the SMTP gateway.</td>
</tr>
</tbody>
</table>
Degradation of services
Non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours.

Most companies have acceptable usage policies for their messaging system—IMSA provides tools to enforce and ensure compliance with existing policies.

Legal liability and business integrity
Improper use of email can also put a company at risk of legal liability. Employees may engage in sexual or racial harassment, or other illegal activity. Dishonest employees can use a company messaging system to leak confidential information. Inappropriate messages that originate from a company’s mail server damage the company’s reputation, even if the opinions expressed in the message are not those of the company.

IMSA provides tools for monitoring and blocking content to help reduce the risk that messages containing inappropriate or confidential material will be allowed through your gateway.

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

When IMSA 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 IMSA 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 IMSA 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 TrendLabsSM ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees, and eliminate post-outbreak cleanup work by enabling automatic deletion for these types of viruses and their email containers.
Introducing InterScan™ Messaging Security Appliance 5000 Version 7.0

<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<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 1-9</td>
<td>IMSA helps to protect your environment against multiple threat types, thus reducing the security, confidentiality, and legal risks to your organization.</td>
</tr>
<tr>
<td>Integrated spam</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. Note: Please activate SPS before you configure IP Profiler and NRS.</td>
<td>The detection technology used by the Spam Prevention Solution (SPS) is based on advanced content processing technology 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>
<tr>
<td>Spam Filtering with IP Profiler and NRS</td>
<td>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, refer to the IMSA Administrator’s Guide.</td>
<td>With the integration of IP Filtering, which includes IP Profiler and Network Reputation Services (NRS), IMSA can block spammers at the IP level.</td>
</tr>
<tr>
<td>Others</td>
<td>You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™, Microsoft™ Active Directory™ or Sun iPlanet Directory™ for user-group definition and administrator privileges. Note that you have to enable LDAP in order to use End-User Quarantine.</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>
</tbody>
</table>

1-7
<table>
<thead>
<tr>
<th>Feature</th>
<th>Descriptions</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-based management console</td>
<td>Web-based management console allows you to conveniently configure IMSA policies and settings on the Web.</td>
<td>The Web-based console also provides greater security as it is SSL-compatible.</td>
</tr>
<tr>
<td>End-User Quarantine (EUQ)</td>
<td>IMSA 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.</td>
<td>With the Web-based EUQ console, end-users can manage messages that IMSA quarantines.</td>
</tr>
<tr>
<td>Delegated administration</td>
<td>IMSA 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.</td>
<td>By delegating administrative roles to different employees, you can create backups of human resources and promote the sharing of administrative duties.</td>
</tr>
<tr>
<td>Centralized reporting</td>
<td>Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports.</td>
<td>Helps you analyze how IMSA is performing. One time (on demand) reports allow you to specify the type of report content as and when required. Alternatively, you can configure IMSA to automatically generate reports daily, weekly, and monthly.</td>
</tr>
<tr>
<td>System availability monitor</td>
<td>A built-in agent monitors the health of your IMSA server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow.</td>
<td>Email notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.</td>
</tr>
<tr>
<td>POP3 scanning</td>
<td>You can choose to enable or disable POP3 scanning from the Web management console.</td>
<td>In addition to SMTP traffic, IMSA can also scan POP3 messages at the gateway as messaging clients in your network retrieve them.</td>
</tr>
</tbody>
</table>
About Spyware and Other Types of Grayware

Your clients are at risk from potential 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.

Types of Grayware

<table>
<thead>
<tr>
<th>Types of Grayware</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware</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>
<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>
</tbody>
</table>
TABLE 1-2. Types of grayware

How Spyware/Grayware Gets into your Network

Spyware/grayware often gets into a corporate network when users download legitimate software that has grayware applications included in the installation package. Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

<table>
<thead>
<tr>
<th>Types of Grayware</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Others</td>
<td>Other types not covered above.</td>
</tr>
</tbody>
</table>
Potential Risks and Threats

The existence of spyware and other types of grayware on your network have the potential to introduce the following:

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

**TABLE 1-3. Potential risks and threats**

About Spam Prevention Solution

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.
Spam Prevention Solution Technology

SPS uses detection technology 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 spammers change their techniques.

Using Spam Prevention Solution

SPS works through a built-in spam filter that automatically becomes active when you register and activate the SPS license.

About IP Filtering

IMSA 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 the four potential Internet threats:
  - **Spam**—Email with unwanted advertising content.
  - **Viruses**—Various virus threats, including Trojan programs.
  - **Directory Harvest Attack (DHA)**—Programs that could add your user’s email addresses to 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. The email messages are sent to fictitious addresses and when they are returned, they flood the target mail server.
  - **Network Reputation Services™ (NRS)**—Block email from known spam senders at the IP-level.

About Network Reputation Services

Trend Micro Network Reputation Services identify and block spam before spam 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.

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, IMSA can reject the connection and block spam from the sender.

- **Network Spam Prevention Service**—a dynamic real-time solution that identifies and stops sources of spam while they are in the process of sending messages. Network Spam Prevention Service is a DNS query-based service like RBL+ Service. At the core of this service is the RBL+ database, along with the Quick IP Lookup (QIL) database, a dynamic real-time database. These two databases have distinct entries and there is no overlap of the IP addresses, allowing IMSA 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 email containing the potential threats mentioned in the previous section. You can customize several criteria that determine when IMSA 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 IMSA monitors the IP address and a threshold.

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

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

1. Foxproxy queries the IP Profiler’s DNS server to see if the IP address is on the blocked list.
2. If the IP address is on the blocked list, it denies the connection request. If the IP address is not on the blocked list, IMSA analyzes the email traffic according to the threshold criteria you specify for IP Profiler.

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

How Network Reputation Services Work

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

1. IMSA records the IP address of the computer requesting the connection.

2. IMSA 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 IMSA to block the connection request (permanently or temporarily). The decision to block the request depends on the type of spam source, its history, current activity level, and other observed parameters.

Figure 1-1 illustrates how NRS works.
For more information on the operation of Trend Micro Network Reputation Services, visit http://www.trendmicro.com/en/products/nrs/overview.htm

Using the SPS Activation Code

If you purchase the full service of Spam Prevention Solution (SPS), you will receive a registration key that will allow you to create a customer account with Trend Micro and upon completion of the registration process, you will receive your Activation Code. The Activation Code will only allow you access to the level of service to which you are registered.
Using the Network Reputation Services Administration Console

To access global spam information, view reports, create or manage Approved Sender IP and Blocked Sender IP lists, and perform administrative tasks, log on to the Network Reputation Services (NRS) administration console.

This section includes basic instructions on the NRS console. For detailed instructions on configuring each screen, see the NRS console online help. Click the help icon in the upper right corner of any help screen to access the online help.

To use the NRS Administration Console

1. Open a browser and access the following address:
   https://nrs.nssg.trendmicro.com/

2. Select Global Spam Update from the menu

3. Click the following tabs:
   - Spam Alert—Provides a brief overview and discussion of current spamming tactics and their implication for organizations. It also describes how new tactics are being deployed and how they have been designed to get through Trend Micro systems, as well as how Trend Micro is responding to these new threats.
   - ISP.Spam.x—The total spam volume from the top 100 ISPs for a specific week. The networks that are producing the most spam are ranked at the top. The ranking of the ISPs will change on a daily basis.

4. To view reports that summarize the query activity between your MTA and the Network Reputation Services data servers, do the following:
   a. Select Report from the menu.
   b. Click Percentage queries, Queries per hour or Queries per day.

5. To create or manage Approved Sender IP and Blocked Sender IP lists, choose Policy from menu. You can define your Approved Senders by individual IP address and CIDR by country, or by ISP.

6. To add an ISP to the list, choose New ISP from the menu.

7. To change your password or Activation Code, choose Administration from the menu.
About End-user Quarantine (EUQ)

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

About Centralized Reporting

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

About 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 is installed. The Web-based Control Manager management console is generated on this server.

- **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 is included in the IMSA device.

- **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. IMSA can be an entity on the Control Manager management console.

The Control Manager agent is already included in the IMSA device. After the agent is enabled, each scanner will register to the Control Manager server and appear as separate entities.

**Note:** The latest version of Control Manager server version 3.5 Patch 2 is required for use with IMSA. For more information on the latest version and the most recent patches and updates, see the Trend Micro Update Center: [http://www.trendmicro.com/download/product.asp?productid=7](http://www.trendmicro.com/download/product.asp?productid=7)

### Integrating With Control Manager

Table 1-4 shows a list of Control Manager features that IMSA 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 IMSA or Control Manager may initiate the communication process.</td>
<td>No. Only IMSA 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 IMSA should take in order to reduce the likelihood of the IMSA server or its clients from becoming infected. Trend Micro ActiveUpdate Server then deploys this policy to IMSA via Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Log Upload for Query</td>
<td>Uploads IMSA virus logs, Content Security logs, and NRS logs to Control Manager for query purposes.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**TABLE 1-4. Supported Control Manager features**
<table>
<thead>
<tr>
<th>Features</th>
<th>Descriptions</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign On</td>
<td>Manage IMSA from Control Manager directly without first logging on to the IMSA Web management console.</td>
<td>No. You need to first log on to the IMSA Web management console before you can manage IMSA from Control Manager.</td>
</tr>
<tr>
<td>Configuration Replication</td>
<td>Replicate configuration settings from an existing IMSA server to a new IMSA 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>
<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 IMSA 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 IMSA via the IMSA Web management console accessible from Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Renew Product Registration</td>
<td>Renew IMSA product license from Control Manager.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Mail-related Report on Control Manager | Generate the following IMSA mail-related reports from Control Manager:  
• Top 10 Virus Detection Points  
• All Entities Virus Infection List  
• Top 10 Infected Email Sender Report  
• Top 10 Security Violations Reports  
• Virus Infection Channel-Product Relationship Report  
• Filter Events by Frequency  
• Filter Events by Policy  
• Gateway Messaging Spam Summary Report  
• Gateway Messaging Spam Summary Report (for Domains) | Yes        |

**TABLE 1-4.** Supported Control Manager features
Control Manager Agent Installation /Un-installation  
Install / uninstall IMSA Control Manager Agent from Control Manager.

No. IMSA Control Manager agent is included in the IMSA device. To enable/disable the agent, do the following from the IMSA Web management console:
1. Choose Administration > Connections from the menu.
2. Click the TMCM Server tab.
3. To enable/disable the agent, select/deselect the check box next to Enable TMCM Agent respectively.

Event Notification  
Send IMSA event notification from Control Manager.
Yes

Command Tracking for All Commands  
Track the status of commands that the Control Manager issues to IMSA.
Yes

<table>
<thead>
<tr>
<th>Features</th>
<th>Descriptions</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Manager Agent Installation /Un-installation</td>
<td>Install / uninstall IMSA Control Manager Agent from Control Manager.</td>
<td>No. IMSA Control Manager agent is included in the IMSA device. To enable/disable the agent, do the following from the IMSA 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 IMSA event notification from Control Manager.</td>
<td>Yes</td>
</tr>
<tr>
<td>Command Tracking for All Commands</td>
<td>Track the status of commands that the Control Manager issues to IMSA.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

TABLE 1-4. Supported Control Manager features
Requirements and Device Details

This chapter explains what requirements are necessary to manage IMSA, describes hardware and software details, and shows you how to physically mount the device on a rack.

Topics include:

- System Requirements on page 2-2
- Device and Application Details on page 2-3
- Mounting the Device on a Rack on page 2-11
- Using the Liquid Crystal Display Module (LCM) on page 2-21
System Requirements

To deploy and configure IMSA, the following are required:

Additional hardware requirements and tools:
- Configuration computer
- Crossover cable
- Serial cable

Application requirements:
- SSH communications application
- Serial communications application
- Internet Explorer® 6.0 or later or Firefox® 2.0 or later
- Microsoft Virtual Machine® (JVM) 5.0 or SUN JRE 1.4+
- Trend Micro™ Control Manager (TMCM) version 3.5 patch 2

Additional Hardware Requirements and Tools

<table>
<thead>
<tr>
<th>Hardware</th>
<th>System Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration computer</td>
<td>Any desktop or notebook computer with an Ethernet port and a console port.</td>
<td>To rescue the operating system, the computer must have an IP address in the same subnet as the IMSA MANAGED port. By default, the MANAGED port IP address is 192.168.252.1 and the default subnet mask is 255.255.255.0.</td>
</tr>
<tr>
<td>Crossover cable</td>
<td>Standard CAT5 Ethernet crossover cable (included in the IMSA carton).</td>
<td>To connect the configuration computer to the IMSA MANAGED port, use a crossover cable. From the MANAGED port, you can perform initial configuration or reinstall the application files.</td>
</tr>
<tr>
<td>Serial cable</td>
<td>Standard RS232 serial cable (included in the IMSA carton).</td>
<td>To connect the configuration computer to the IMSA Console port, use a serial cable. From the console port you can monitor the status of an operating system rescue.</td>
</tr>
</tbody>
</table>
Application Requirements

Table 2-2 lists the minimum application requirements to access the CLI and Web console interfaces and to manage IMSA with Control Manager.

<table>
<thead>
<tr>
<th>Application</th>
<th>System Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH communications application</td>
<td>SSH protocol version 2</td>
<td>To connect to the <strong>MANAGED</strong> port, use an SSH communications application. To adequately view the IMSA CLI through an SSH connection, set the terminal window size to 80 columns and 24 rows.</td>
</tr>
<tr>
<td>Serial communications application</td>
<td>—</td>
<td>To perform basic device configuration, use a serial communications application, such as HyperTerminal, when you connect to the <strong>Console</strong> port.</td>
</tr>
<tr>
<td>Internet Explorer®</td>
<td>Version 6.0</td>
<td>To access the Web console, which allows you to configure all IMSA settings, use Internet Explorer 6.0 or above or Firefox 2.0 or above. Using the data port IP address you set during initial configuration, enter the following URL: https://[IP Address]:8445</td>
</tr>
<tr>
<td>Mozilla Firefox®</td>
<td>Version 2.0</td>
<td></td>
</tr>
<tr>
<td>Java Virtual Machine</td>
<td>Version 5.0 or later or SUN JRE 1.4+</td>
<td>To view certain items in the Web console, the computer must have JVM.</td>
</tr>
<tr>
<td>Trend Micro Control Manager</td>
<td>Version 3.5 patch 2</td>
<td>If you want to use Trend Micro Control Manager 3.5 to manage IMSA, update the Control Manager server to version 3.5 patch 2. The patch file is located on the Solutions CD for IMSA 5000. After applying the patch, register IMSA with your TMCM server.</td>
</tr>
</tbody>
</table>

**Table 2-2. Minimum software requirements**

Device and Application Details

This section provides information on the IMSA device and the instructions to change hardware components. For a summary of the items on the device front and back panels, see the *Quick Start Guide.*
Hardware Specifications

Table 2-3 provides a list of the IMSA hardware specifications.

<table>
<thead>
<tr>
<th>Power</th>
<th>Watt</th>
<th>500 W or 400 W ATX (1+1 redundant 400 W/each)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>AC 100 ~ 240 V @ 50 ~ 60 Hz, full range</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Environment</th>
<th>Operating</th>
<th>Non-Operating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>0 ~ 40 °C (32 ~ 104 °F)</td>
<td>-20 ~ 75 °C (-4 ~ 167 °F)</td>
</tr>
<tr>
<td>Humidity</td>
<td>5 ~ 85% @ 40 °C (104 °F)</td>
<td>5 ~ 95%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Characteristics</th>
<th>Dimensions (W x H x D)</th>
<th>426 x 88 x 485 mm (16.8” x 3.46” x 19.1”)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weight</td>
<td>18 Kg (40 lb)</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 2-3.** IMSA hardware specifications

IMSA Ports

Table 2-4 lists the ports that IMSA uses.

<table>
<thead>
<tr>
<th>Port</th>
<th>Services Using the Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5060</td>
<td>Policy service</td>
<td></td>
</tr>
<tr>
<td>15505</td>
<td>IMSA control service</td>
<td>The IMSA Manager.</td>
</tr>
<tr>
<td>53</td>
<td>UDP/TCP IP Profiler</td>
<td>IP Profiler uses this port to check whether an IP address should be blocked.</td>
</tr>
<tr>
<td>5432</td>
<td>Database service</td>
<td></td>
</tr>
<tr>
<td>8009</td>
<td>EUQ Internal service</td>
<td></td>
</tr>
<tr>
<td>10024</td>
<td>Scan daemon</td>
<td>Used internally by the scan daemon.</td>
</tr>
<tr>
<td>10025</td>
<td>Scan daemon</td>
<td>Receives mail from MTA.</td>
</tr>
<tr>
<td>10026</td>
<td>MTA</td>
<td>Receives scanned mail from daemon.</td>
</tr>
</tbody>
</table>

Ports for services that require outside access to the device

<table>
<thead>
<tr>
<th>Port</th>
<th>Services Using the Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8445</td>
<td>HTTPS</td>
<td>Web console remote access.</td>
</tr>
<tr>
<td>8446, 8447</td>
<td>EUQ</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 2-4.** IMSA Ports
## Requirements and Device Details

### Table 2-4. IMSA Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Services Using the Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>SSHD</td>
<td>Secure shell remote access.</td>
</tr>
<tr>
<td></td>
<td><strong>Ports for services that depend on IMSA</strong></td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>NTPD</td>
<td>If network time is enabled, this port must be accessible.</td>
</tr>
<tr>
<td>389</td>
<td>LDAP</td>
<td>If IP Profiler is enabled, access must be available on all devices. Otherwise, only devices running LDAP require access on this port.</td>
</tr>
<tr>
<td>User defined</td>
<td>Web proxy</td>
<td>Only the parent device uses this port to access the Trend Micro ActiveUpdate server (for component updates) and the product registration server.</td>
</tr>
<tr>
<td>User defined</td>
<td>TMCM console</td>
<td>Access required if TMCM agent is enabled.</td>
</tr>
</tbody>
</table>
About the RAID Hard Disks

IMSA has two hot-swappable RAID hard disks that work as RAID 1 to perform all system and application functions. For specifications that apply to both hard disks, see Table 2-5.

<table>
<thead>
<tr>
<th>Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>WD2500YS-01SHB0 Serial ATA RAID Hard Disk</td>
</tr>
<tr>
<td>Disk size</td>
<td>250GB. Comprised of the following:</td>
</tr>
<tr>
<td></td>
<td>• MTA Queue Partition size 20GB</td>
</tr>
<tr>
<td></td>
<td>• Data Partition size 190GB</td>
</tr>
<tr>
<td>Hot-swappable support</td>
<td>Swap a damaged or under-performing hard disk for a new disk. IMSA</td>
</tr>
<tr>
<td></td>
<td>automatically synchronizes data between disks.</td>
</tr>
<tr>
<td>Monitoring support</td>
<td>The InterScan hardware monitor can monitor hard drive status and send</td>
</tr>
<tr>
<td></td>
<td>a notification to an email address that you set and send an SNMP trap</td>
</tr>
<tr>
<td></td>
<td>notification to an SNMP server.</td>
</tr>
</tbody>
</table>

TABLE 2-5. RAID hard disk specifications

Swapping Hard Disks

If one hard disk fails, you can swap it out for a new disk without turning off the device.

**To swap hard disks:**

1. Slide the safety clip on the front of the hard drive to the open position.
2. Pull the release lever.
   The hard disk detaches.
3. Pull out the hard disk.
4. Insert the new hard disk.
5. Press the hard disk completely in the slot until the release lever closes.
6. Slide the safety clip to the closed position.
   The device starts to build the new hard disk. The build time depends heavily on the amount of traffic and the functions that the IMSA CPUs are processing.
WARNING! Do not add or remove any disks during the build process.

7. If you want to monitor the status of the build process, enter the CLI and view **Device Information and Status** (see *Using the Command Line Interface section of the Administrator’s Guide*).

**Note:** Both IMSA CPUs are designed to operate at about 50% usage under normal circumstances with both hard disks in operation. When you swap in a new hard disk, the CPUs will have enough resources to build the new hard disk and continue processing operations.

---

**About the Power Supplies**

IMSA provides two power supplies, one for primary use and one for backup. For specifications that apply to the power supplies, see the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>RR2Z-6400P-R (ROHS)</td>
</tr>
<tr>
<td>Size</td>
<td>265.00x101.00x84.00 (MM)</td>
</tr>
<tr>
<td>AC INPUT</td>
<td>100-240V 60-50Hz 8-5A</td>
</tr>
<tr>
<td>DC OUTPUT</td>
<td>400W (MAX)</td>
</tr>
</tbody>
</table>

**TABLE 2-6. Power supply specifications**
## Powering Off

For a summary of different methods of powering off IMSA, see Table 2-7.

<table>
<thead>
<tr>
<th>Action</th>
<th>When Device is Turned On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressing the power button (briefly)</td>
<td>Shuts all IMSA applications down and powers the device off slowly. This method takes about 3 minutes.</td>
</tr>
<tr>
<td>Pressing and holding the power button (4 seconds or longer)</td>
<td>Forces IMSA to shut down immediately.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!  This method might cause RAID disk initialization and data could be lost.</strong></td>
</tr>
<tr>
<td>Pressing the Reset button</td>
<td>Forces IMSA to shut down immediately.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!  This method might cause RAID disk initialization and data could be lost.</strong></td>
</tr>
<tr>
<td>On the CLI, selecting 5) Shutdown &gt; 2) Power off</td>
<td>The safest way to power off the device. Trend Micro recommends using this method.</td>
</tr>
</tbody>
</table>

### TABLE 2-7. Powering the device off

## Power Supply Failure

If a power supply fails:

- The power supply will continue beeping.
- The green LED on the power supply does not illuminate.
- The other power supply can still provide all necessary power requirements.
- IMSA sends a hardware notification.
- The LCD will display the following:

```
Power Supply
One Unit Failed
```
Changing Power Supplies

If a power supply fails, you can easily replace it with a power supply that meets the specifications in Table 2-6.

To change a power supply:
1. Unplug the power cables.
2. Loosen the holding screw.
3. Pull the power supply out of the device.
4. Insert the new power supply.
5. Press the power supply completely in the slot until you hear a click.
6. Tighten the holding screw.
7. Plug in the power cable.

About the Processor System

IMSA uses two CPUs with the specifications listed in Table 2-8.

<table>
<thead>
<tr>
<th>Item</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td></td>
</tr>
<tr>
<td>Brand</td>
<td>INTEL™</td>
</tr>
<tr>
<td>Model</td>
<td>XEON EMT64 with hyperthreading</td>
</tr>
<tr>
<td>Speed</td>
<td>2.8 GHz or above</td>
</tr>
<tr>
<td>Chipset</td>
<td>Intel 7520 (Lindenhurst) + 6300ESB (Hance Rapids)</td>
</tr>
<tr>
<td>Front side bus</td>
<td>800MHz</td>
</tr>
<tr>
<td>BIOS</td>
<td>Award 4MB Flash</td>
</tr>
</tbody>
</table>

**TABLE 2-8. CPU specifications**

About the Operating System

IMSA is shipped with Linux-like operating system.
About the Hardware Monitor and Watchdog

IMSA includes a built-in hardware monitor that can send notification messages to you when critical hardware events occur, such as low fan speed and power failure.

IMSA also includes a built-in watchdog service that automatically reboots if the IMSA operating system panics (when the kernel detects an unrecoverable system error). The watchdog service cannot be disabled.
Mounting the Device on a Rack

Use one of the following methods to mount the device in a 19-inch standard cabinet rack:

- Sliding mount—Allows you to slide the device in and out of the rack cabinet (see Figure 2-7 for illustration).
- Fixed mount—Secures the device in a fixed position (see Figure 2-9 for illustration).

To mount IMSA, see the following sections:

Step 1: Preparing the Device on page 2-12
Step 2: Installing the Slide Sets on page 2-13
Step 3: Mounting the Device on the Rack on page 2-16

**WARNING!** Do not install rack kit components designed for another system. Use only the rack kit for your device. Using the rack kit for another system may damage the device and cause injury.
Step 1: Preparing the Device

To prepare the device:

1. Use a minimum of two (2) ear screws to attach each ear to the device side panels.
2. Hold the rails and slide sets horizontally with the slide’s back facing you.
3. To detach a rail from a slide, pull the rail lock to the right.

4. Use four (4) slide screws to attach each rail to the device side panels.
Step 2: Installing the Slide Sets

This task involves installation of the slide sets to a four-post rack.

To install the slide sets:

1. If the rack doors are still covering the rack slots where you want to mount the device, remove the rack doors.

   **Tip:** Refer to documentation provided with the rack cabinet for details on how to remove the rack doors.

2. Use masking tape or felt-tip pen to place a mark on the rack’s front vertical rails where you want to position the bottom of the device. Figure 2-3 illustrates this step.

![Graphical representation of the device position in the rack and slide set guides (rack markings)](image)

3. Place a mark 1.70 inches (4.32 centimeters) above the original mark you made (or count up two holes) and mark the rack’s front vertical rails to indicate placement of the device’s upper edge on the vertical rails.
Tip: An IMSA device occupies 2 RU (3.40 inches or 8.64 centimeters, six rack holes) of vertical space in the rack.

4. Install one pair of cage nuts to occupy holes between the marks you made on the front vertical rail.

FIGURE 2-4  Cage nuts for a sliding mount
5. Remove the inside screw and nut from the slide.
6. Loosen the outside screw and nut.

**FIGURE 2-5** Removing and loosening the side nuts

7. Starting with the front vertical rail, hold and position the slide set tip to align with the holes of the cage nuts.
8. At the back of the cabinet, pull back the slide set until the mounting holes align with their respective cage nut holes on the back vertical rail.
9. With the slide at the correct length, remove the slide from the rack and reinsert the inside screw and nut.
10. Tighten the outside screw and nut.
11. To secure the slide set to the front vertical rail, place the slide back in the rack and install two cage screws over the slide set and the top and bottom holes of the cage nuts.

**FIGURE 2-6** Installing the cage screws in the top and bottom holes of the slide set (front vertical rail view)
12. Repeat the above steps for the other slide set.
13. Ensure that the slide sets are installed at the same position on the vertical rails on each side of the rack.

![Mounted slide sets](image)

**FIGURE 2-7 Mounted slide sets**

14. On each side of the rack, install another pair of cage nuts, one above and one below the mounted slide sets.

### Step 3: Mounting the Device on the Rack

**WARNING!** Do not attempt to mount the device on the rack by yourself; perform the task with another person. Attempting to mount the device alone could cause physical harm or injury.

**To mount the device on the rack:**

1. Pull the two slides out of the rack until the release latches lock in a fully extended position.
2. Lift the device into position in front of the extended slides.
3. Holding the top and bottom panels, align and fit the side panel rails on the left and right slide sets (see Figure 2-7).
4. Gently push the device into the rack until the slide sets into locked position.
5. Pull back on the slide locks, on either side of the IMSA device, and finish sliding the device into the rack.

FIGURE 2-8 Mounted device (sliding mount)
6. Install the mounting screws to prevent the device from sliding in or out.

FIGURE 2-9 Mounted IMSA device (fixed mount)
Removing an IMSA Device From a Rack

To help ensure safety, do not attempt to remove an IMSA device from a rack by yourself.

To remove the device from a rack:

1. Remove the mounting screws from the front panel of the device.
2. Gently slide the device out of the rack, until the device reaches the locking position.

FIGURE 2-10   Removing the device from a rack
3. Slide the rail locks on either side of the device toward you, and slide the device completely free of the rack.

**FIGURE 2-11** Pulling the rail locks
Using the Liquid Crystal Display Module (LCM)

A liquid crystal display module (LCM) is located on the front of the IMSA device. It includes the following components:

- Liquid crystal display (LCD)—Displays a series of messages related to system status.
- Enter button —Used to enter rescue mode (see *Using the Command Line Interface* section in the Administrator’s Guide). The other buttons are not used.

Reading the LCD

The LCD shows the messages in Table 2-9.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot up messages</td>
<td>Several boot up messages display during startup, when IMSA performs a memory test, hard disk detection, and PCI scan.</td>
</tr>
<tr>
<td>Rescue Mode? () sec. left</td>
<td>Displays after boot up for 5 seconds. The number of seconds indicates the time remaining to enter rescue mode, from which you can rescue the operating system (see the IMSA Administrator’s Guide).</td>
</tr>
<tr>
<td>Image Corrupt</td>
<td>The operating system rescue failed.</td>
</tr>
<tr>
<td>Trend Micro Inc. IMSA 5000</td>
<td>The device is operating normally.</td>
</tr>
<tr>
<td>CPU Temperature High Warning</td>
<td>The CPU temperature is over the maximum allowed. Make sure that the fan vents have adequate ventilation.</td>
</tr>
<tr>
<td>Appliance Fan Low Warning</td>
<td>The fan is spinning too slowly and the device is in danger of overheating. Replace the fan.</td>
</tr>
<tr>
<td>Power Supply One Unit Failed</td>
<td>A problem exists with the power supply. Replace the power supply.</td>
</tr>
<tr>
<td>RAID Error HDD 1 (or 2) Not Ready</td>
<td>The hard disk is not ready or a problem exists with the hard disk. Wait for the hard disk to enter a ready state. If the message persists, replace the hard disk.</td>
</tr>
<tr>
<td>RAID Error RAID Card Failed</td>
<td>A problem exists with the RAID card. Replace the RAID card.</td>
</tr>
</tbody>
</table>

**TABLE 2-9. LCD messages**
Planning for Deployment

This chapter explains how to plan for IMSA deployment. For instructions on performing initial configuration, see the Quick Start Guide in the carton or the PDF version on the included Solutions CD for IMSA 5000.

Topics include:

• Deployment Checklist on page 3-2
• About Device Services on page 3-13
• Considering Email and Network Topology on page 3-5
• Understanding POP3 Scanning on page 3-15
## Deployment Checklist

<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 IMSA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose one of the following locations on your network where you would like to deploy IMSA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• At the gateway</td>
<td></td>
<td>Deploying at the Gateway or Behind the Gateway on page 3-6</td>
</tr>
<tr>
<td></td>
<td>• Behind the gateway</td>
<td></td>
<td>Deploying at the Gateway or Behind the Gateway on page 3-6</td>
</tr>
<tr>
<td></td>
<td>• Without a firewall</td>
<td></td>
<td>Deploying without a Firewall on page 3-9</td>
</tr>
<tr>
<td></td>
<td>• In front of a firewall</td>
<td></td>
<td>Deploying in Front of a Firewall on page 3-10</td>
</tr>
<tr>
<td></td>
<td>• Behind a firewall</td>
<td></td>
<td>Deploying Behind a Firewall on page 3-11</td>
</tr>
<tr>
<td></td>
<td>• On a former SMTP gateway</td>
<td></td>
<td>Deploying on a Former SMTP Gateway on page 3-12</td>
</tr>
<tr>
<td></td>
<td>• In the De-Militarized Zone</td>
<td></td>
<td>Deploying in the De-Militarized Zone on page 3-12</td>
</tr>
</tbody>
</table>

| Step 2 - Plan the scope | | | |
|-------------------------| | | |
### 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>Decide whether you would like to deploy a single IMSA device or multiple devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Single IMSA device</td>
<td></td>
<td>About Device Roles on page 3-13</td>
</tr>
<tr>
<td></td>
<td>• Multiple IMSA devices</td>
<td></td>
<td>About Device Roles on page 3-13</td>
</tr>
<tr>
<td></td>
<td><strong>Step 3 - Deploy or Upgrade</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deploy a new IMSA device or upgrade from a previous version.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mount the device</td>
<td></td>
<td>Mounting the Device on a Rack on page 2-11</td>
</tr>
<tr>
<td></td>
<td>• Boot up the device</td>
<td></td>
<td>IMSA Quick Start Guide.</td>
</tr>
<tr>
<td></td>
<td>• Decide on the device role</td>
<td></td>
<td>About Device Roles on page 3-13</td>
</tr>
<tr>
<td></td>
<td>• Configure the device</td>
<td></td>
<td>Setting Up a Single Parent Device on page 3-17</td>
</tr>
<tr>
<td></td>
<td>• Upgrade the device</td>
<td></td>
<td>Setting Up a Child Device on page 3-29.</td>
</tr>
<tr>
<td></td>
<td>• Verify that deployment is successful</td>
<td></td>
<td>Upgrading From Previous Versions on page 4-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Verifying Successful Deployment on page 3-31</td>
</tr>
</tbody>
</table>

3-3
### Step 4- Start services

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Optional</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scanner</strong></td>
<td></td>
<td>IMSA Services section of the Administrator’s Guide.</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EUQ</strong></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5- Configure other IMSA settings

Configure various IMSA settings to get IMSA up and running.

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Optional</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Filtering Rules</strong></td>
<td>Yes</td>
<td>IP Filtering Service section of the Administrator’s Guide.</td>
</tr>
<tr>
<td><strong>SMTP Routing</strong></td>
<td></td>
<td>Scanning SMTP Messages section of the Administrator’s Guide.</td>
</tr>
<tr>
<td><strong>POP3 Settings</strong></td>
<td>Yes</td>
<td>Scanning POP3 Messages section of the Administrator’s Guide.</td>
</tr>
<tr>
<td><strong>Policy and scanning exceptions</strong></td>
<td></td>
<td>Managing Policies section of the Administrator’s Guide.</td>
</tr>
</tbody>
</table>
### Considering Email and Network Topology

Decide how you want to use IMSA in your existing email and network topology. The following are common scenarios for handling SMTP traffic:

<table>
<thead>
<tr>
<th>Tick when completed</th>
<th>Tasks</th>
<th>Optional</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Perform a manual update of components and configure scheduled updates</td>
<td></td>
<td>Updating Scan Engine and Pattern Files section of the Administrator’s Guide.</td>
</tr>
<tr>
<td></td>
<td>• Log settings</td>
<td></td>
<td>Configuring Log Settings section of the Administrator’s Guide.</td>
</tr>
</tbody>
</table>

---

**Step 7 - Back up IMSA**

Perform a backup of IMSA as a precaution against system failure

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Export IMSA settings</td>
<td></td>
<td></td>
<td>Backing Up IMSA Settings section of the Administrator’s Guide</td>
</tr>
</tbody>
</table>
Deploying at the Gateway or Behind the Gateway

<table>
<thead>
<tr>
<th></th>
<th>Single Device</th>
<th>Multiple Devices</th>
</tr>
</thead>
</table>
| **At the Gateway**  | The only setup if you plan to use IP Filtering with the device. IMSA is deployed at the gateway to provide antivirus, content filtering, spam prevention and IP Filtering services, which include Network Reputation Services and IP Profiler. See Figure 3-1. | The only setup if you plan to use IP Filtering with at least one of the devices. You can enable or disable services on different devices. See the following:  
  • Figure 3-3.  
  • Choosing Services on page 3-14. |
| **Behind the Gateway** | The most common setup. IMSA is deployed between upstream and downstream MTAs to provide antivirus, content filtering and spam prevention services. See Figure 3-2.                                                  | The most common group setup. IMSA devices are deployed between upstream and downstream MTAs to provide antivirus, content filtering and spam prevention services. You can enable or disable services on different devices. See the following:  
  • Figure 3-4.  
  • Choosing Services on page 3-14. |

**Trend Micro Control Manager scenario**

If you have multiple groups, you can use Trend Micro Control Manager (TMCM) to manage the devices.

### TABLE 3-1. Common scenarios for handling SMTP traffic
Planning for Deployment

FIGURE 3-1. Single IMSA device at the gateway

FIGURE 3-2. Single IMSA device behind the gateway
FIGURE 3-3. IMSA group at the gateway

FIGURE 3-4. IMSA group behind the gateway
Deploying without a Firewall

Figure 3-5 illustrates how to deploy IMSA and Postfix when your network does not have a firewall:

**FIGURE 3-5  Deployment topology: no firewall**
Deploying in Front of a Firewall

Figure 3-6 illustrates the deployment topology when you deploy IMSA in front of your firewall:

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

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

**Tip:** For more information, see Configuring SMTP Routing section of the Administrator’s Guide.
Deploying Behind a Firewall

Figure 3-7 illustrates how to deploy IMSA and Postfix behind your firewall:

**FIGURE 3-7 Deployment scenario: behind a firewall**

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

**Outgoing Traffic**
- Configure all internal SMTP gateways to send outgoing mail to Postfix and then to IMSA.
- If you are replacing your SMTP gateway with IMSA, configure your internal mail server to send outgoing email through Postfix and then to IMSA.
- Configure Postfix and IMSA to route all outgoing email (to domains other than local), to the firewall or deliver the messages.
- Configure IMSA to allow internal SMTP gateways to relay to any domain using IMSA.
Tip:
For more information, see Configuring SMTP Routing section of the Administrator’s Guide.

Deploying on a Former SMTP Gateway

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

On the SMTP gateway:

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

Note: The existing SMTP gateway binds to port 25.

Incoming Traffic

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

Outgoing Traffic

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

Deploying in the De-Militarized Zone

You can also deploy IMSA and Postfix in the De-Militarized Zone (DMZ):

Incoming Traffic

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

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

**Outgoing Traffic**
- Configure Postfix to route all outgoing email (destined to domains other than the local domain) to the firewall or deliver using IMSA.
- Configure all internal SMTP gateways to forward outgoing mail to Postfix and then to IMSA.
- Configure IMSA to allow internal SMTP gateways to relay, through Postfix and IMSA, to any domain.

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

---

**About Device Roles**

IMSA can act as a *parent* or *child* device. Parent and child devices compose a *group*, where the parent provides central management services to the child devices registered to it.

- **Parent**—Manages child devices. If you are deploying a single IMSA device, select parent mode during setup so that all IMSA components are deployed.
- **Child**—Is managed by a single parent device and will use all global settings that you configure through the parent device’s Web console.

A *group* refers to a parent device with at least one child device registered to it.

---

**About Device Services**

You can enable different kinds of services on IMSA devices.

Parent-only services:
- **Admin user interface service (Web console)**—Manages global settings.

Parent and child services:
• **Policy service**—Manages the rules that you configure.
• **Scanner service**—Scans email traffic.
• **EUQ service**—Manages End-User Quarantine, which allows your users to view their email messages that IMSA determined were spam.
• **Command Line Interface (CLI) service**—Provides access to CLI features.

A child device is functional only when it is registered to a parent.

### Choosing Services

You can enable different types of services on parent and child devices. For example, to increase throughput, you can just enable the administrative services on the parent device, and allow the child devices to scan traffic and provide EUQ services.

You can deploy IMSA devices in a parent/child group in either deployment scenario. However, if you enable the scanner service on parent and child devices, you must use the same type of deployment for all devices in a single group. You cannot deploy some child devices at the gateway and others behind the gateway.

In addition to the above SMTP-scanning scenarios, you might want IMSA to scan POP3 traffic. See *Understanding POP3 Scanning* on page 3-15 for more information.

### Deploying IMSA with IP Filtering

The Trend Micro IP Filtering, which includes IP Profiler and Network Reputation Services (NRS) blocks connections at the IP level.

To use IP Filtering, any firewall between IMSA and the edge of your network must not modify the connecting IP address as IP Filtering is not compatible with networks using Network Address Translation (NAT). If IMSA accepts SMTP connections from the same source IP address, for instance, IP Filtering will not work, as this address would be the same for every received message and the IP filtering software would be unable to determine whether the original initiator of the SMTP session was a known sender of spam.
Understanding POP3 Scanning

In addition to SMTP traffic, IMSA can scan POP3 messages at the gateway as your clients retrieve them. Even if your company does not use POP3 email, your employees might access personal, Web-based POP3 email accounts, which can create points of vulnerability on your network if the messages from those accounts are not scanned.

The most common email scanning deployments will use IMSA to scan SMTP traffic, which it does by default. However, to scan POP3 traffic that your organization might receive from a POP3 server over the Internet, enable POP3 scanning.

With POP3 scanning enabled, IMSA acts as a proxy, positioned between mail clients and POP3 servers, to scan messages as the clients retrieve them.

To scan POP3 traffic, configure your email clients to connect to the IMSA server POP3 proxy, which connects to POP3 servers to retrieve and scan messages.

Requirements for POP3 Scanning

For IMSA to scan POP3 traffic, a firewall must be installed on the network and configured to block POP3 requests from all computers except IMSA. This configuration ensures that all POP3 traffic passes through the firewall to IMSA and that IMSA only scans the POP3 traffic.

Note: If you disable POP3 scanning, your clients cannot receive POP3 mail.

Configuring a POP3 Client that Receives Email Through IMSA

To configure a POP3 client using a generic POP3 connection, configure the following:

- **IP address/Domain name**—The IMSA IP address or domain name.
- **Port**—IMSA Generic POP3 port.
- **Account**—account_name#POP3_Server_Domain-name

for example: user#10.18.125.168
To configure a POP3 client using dedicated POP3 connections, configure the following:

- **IP address**—The IMSA IP address.
- **Port**—The IMSA dedicated POP3 port.
- **Account**—account_name@POP3_Server_Domain-name
  
  for example: user@domain.com
Opening the IMSA Web Console

You can view the IMSA management console with a Web browser from the server where you deployed the program, or remotely across the network.

To view the console in a browser, go to the following URL:

\[
\text{https://}\{\text{imsa}\}:8445
\]

where \{imsa\} refers to the IP address or Fully Qualified Domain Name. For example: \text{https://196.168.10.1:8445} or \text{https://imsa1:8445}

An alternative to using the IP address is to use the target server’s fully qualified domain name (FQDN). To view the management console using SSL, type “https://” before the domain name and append the port number after it.

The default login credentials are as follows:

- Administrator user name: \text{admin}
- Password: \text{imsa7.0}

Type the logon credentials the first time you open the console and click the Log on button. To prevent unauthorized changes to your policies, Trend Micro recommends that you set a new logon password immediately following deployment.

\[\text{Note:}\] If you are using Internet Explorer (IE) 7.0 to access the Web console, IE will block the access and display a popup dialog box indicating that the certificate was issued from a different web address. Simply ignore this message and click Continue to this Web site to proceed.

\[\text{Tip:}\] To prevent unauthorized changes to your policies, Trend Micro recommends changing the password regularly.

Setting Up a Single Parent Device

IMSA provides a configuration wizard to help you configure all the settings you need to get IMSA up and running.
To set up a single parent device:

1. Connect your management computer to the Managed port with the included Crossover cable. The IP address of the Managed port is 192.168.252.1, so your computer’s IP address must be in network segment 192.168.252.0/24 (such as 192.168.252.2) and have the subnet mask 255.255.255.0.

2. On the management computer, open Internet Explorer (version 6.0 or later) or Firefox (version 2.0 or later).

3. Enter the following URL (accept the security certificate if necessary):
   
   https://192.168.252.1:8445
   
   The login screen appears.

4. Select the “Open Configuration Wizard” check box.

5. Type the following default user name and password:
   - User name: admin
   - Password: imsa7.0

   The Configuration Wizard screen appears.

6. Progress through the Wizard screens to configure the settings.

Step 1: Configuring the System Settings

1. After you read the welcome screen, click Next. The Local System Settings screen appears.
2. Modify the device host name, IP address, and netmask if necessary. Also, configure your network settings and set the device system time.

**Note:** The local system settings take effect immediately when you click the Next button. If the IP address or time settings are changed, IMSA will restart. Wait until IMSA is online and then log on again.
Step 2: Configuring the Deployment Settings

1. Click Next. The Deployment Settings screen appears.

   ![Deployment Settings Screen]

   You can deploy two or more IMSA devices in a group. One device acts as the parent device, which controls the child devices.

   - **Parent Device**
     - Import Settings...
     - Gateway deployment (To use IP filtering, you must deploy IMSA at the gateway.)
     - Enable End-User Quarantine (Quarantine all spam and allow users to access their spam through a Web console.)
     - Automatically synchronize system time with NTP servers

   - **Child Device**
     - Register to parent device IP address

2. Select **Parent Device** or **Child Device**. If this is the first device you are setting up, you must select **Parent Device**. You can configure additional child devices at a later time.

   To deploy the device between upstream and downstream MTAs, clear the gateway deployment check box.

   Also, decide if you want to use EUQ or NTP services.
Step 3: Configuring the SMTP Routing Settings

1. Click Next. The SMTP Routing Settings screen appears.

2. Add all SMTP server domains and their corresponding SMTP server names to the relay domain list. IMSA needs this information to pass email to SMTP servers for delivery.
Step 4: Configuring the Notification Settings

1. Click Next. The Notification Settings screen appears.

2. If you want to receive notifications for system and policy events, configure the Email or SNMP trap notification settings.
Step 5: Configuring the Update Source

1. Click Next. The Update Source screen appears.

2. Configure the following update settings, which will determine from where IMSA will receive its component updates and through which proxy (if any) IMSA needs to connect to access the Internet:

   • **Source**—Click Trend Micro ActiveUpdate (AU) server to receive updates directly from Trend Micro. Alternatively, click Other Internet source and type the URL of the update source that will check the Trend Micro AU server for updates. You can specify an update source of your choice or type the URL of your Control Manager server, if applicable.

   • **Proxy Settings**—Select the Use proxy server check box and configure the proxy type, server name, port, user name, and password.
Step 6: Configuring the LDAP Settings

1. Click Next. The LDAP Settings screen appears.

![Configuration Wizard]

**LDAP Settings**

Enter LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or web quarantine authentication. You must enable LDAP to use the web quarantine tool.

<table>
<thead>
<tr>
<th><strong>LDAP server type</strong></th>
<th>Microsoft Active Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAPI</td>
<td></td>
</tr>
<tr>
<td>LDAPI server</td>
<td>Example: example.com or 123.123.123.123</td>
</tr>
<tr>
<td>Listening port number</td>
<td>369</td>
</tr>
<tr>
<td>Enable LDAP2</td>
<td></td>
</tr>
<tr>
<td>LDAP server</td>
<td>Example: example.com or 123.123.123.123</td>
</tr>
<tr>
<td>Listening port number</td>
<td>369</td>
</tr>
</tbody>
</table>

**LDAP cache expiration for policy services and EUQ services**

Time to Live in minutes: 1440

**LDAP admin**

<table>
<thead>
<tr>
<th><strong>LDAP admin account</strong></th>
<th>Example: DomainNameAccount_AName or Account_AName@DomainName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>**********</td>
</tr>
<tr>
<td>Base distinguished name</td>
<td>Example: DC=foo, DC=monnet, DC=morg</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Simple</td>
</tr>
<tr>
<td></td>
<td>Advanced, using Kerberos authentication for Active Directory</td>
</tr>
<tr>
<td></td>
<td>Kerberos authentication default realm:</td>
</tr>
<tr>
<td></td>
<td>Default domain:</td>
</tr>
<tr>
<td></td>
<td>KDC and admin server:</td>
</tr>
<tr>
<td></td>
<td>KDC port number:</td>
</tr>
</tbody>
</table>
2. Configure LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication.

a. For **LDAP server type**, select one of the following:
   - Microsoft Active Directory
   - Domino
   - Sun iPlanet Directory

b. To enable one or both LDAP servers, select the check boxes next to **Enable LDAP 1** or **Enable LDAP 2**.

c. Type the names of the LDAP servers and the port numbers they listen on.

d. Under **LDAP Cache Expiration for Policy Services and EUQ services**, type a number that represents the time to live next to the **Time To Live in minutes** field.

e. Under **LDAP Admin**, type the administrator account, its corresponding password, and the base-distinguished name. See Table 3-2 for a guide on what to specify for the LDAP admin settings.

```
<table>
<thead>
<tr>
<th>LDAP Server</th>
<th>LDAP Admin Account (examples)</th>
<th>Base Distinguished Name (examples)</th>
<th>Authentication Method</th>
</tr>
</thead>
</table>
| Active Directory           | • Without Kerberos: user1@domain.com (UPN) or domain\user1  
                            | • With Kerberos: user1@domain.com |
|                            | dc=domain, dc=com            |                                    | • Simple                         |
|                            |                              |                                    | • Advanced (with Kerberos)      |
| Domino                    | user1\domain                 | Not applicable                     | Simple                           |
| Sun iPlanet Directory      | uid=user1, ou=people, dc=domain, dc=com | dc=domain, dc=com | Simple                           |
```

**TABLE 3-2. LDAP admin settings**

f. For **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos authentication default realm, Default domain, KDC and admin server, and KDC port number.
Note: Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication. You must enable LDAP to use End-User Quarantine.

Step 7: Configuring the Internal Addresses

1. Click Next. The Internal Addresses screen appears.

2. IMSA uses the internal addresses to determine whether a policy or an event is inbound or outbound.
   - If you are configuring a rule for outgoing messages, the internal address list applies to the senders.
   - If you are configuring a rule for incoming messages, the internal address list applies to the recipients.

To define internal domains and user groups, do one of the following:
• Select **Enter domain** from the drop-down list, type the domain in the text box, and then click `>>`.

• Select **Search for LDAP groups** from the drop-down list. A screen for selecting the LDAP groups appears. Type an LDAP group name for which you want to search in the text box and click **Search**. The search result appears in the list box. To add it to the **Selected** list, click `>>`.

### Step 8: Configuring TMCM Server Settings

1. Click Next. The TMCM Server Settings screen appears.

2. If you will use Control Manager to manage IMSA, do the following:
   a. Select **Enable TMCM Agent** (included with IMSA by default).
   b. Next to **Server**, type the TMCM IP address or FQDN.
c. Next to **Communication protocol**, select **HTTP** or **HTTPS** and type the corresponding port number. The default port number for HTTP access is 80, and the default port number for HTTPS is 443.

d. Under **Web server authentication**, type the user name and password for the Web server if it requires authentication.

e. If a proxy server is between IMSA and TMCM, select **Enable proxy**.

f. Type the proxy server port number, user name, and password.

### Step 9: Activating the Product

1. Click **Next**. The Product Activation screen appears. You must activate the Antivirus and Content Filter to enable scanning and security updates. If you want to scan email traffic for spam or use IP Filtering (NRS and IP Profiler), enter the SPS Activation Code.

2. Type the Activation Codes for the products you want to activate. If you do not have an Activation Code, click **Register Online** and follow the directions at the Trend Micro Registration Web site.
Step 10: Reviewing the Settings

1. Click Next. The Review Settings screen appears.

2. If your settings are correct, click Finish.
   To modify any of your settings, click Back and keep moving through the screens
   until your settings are complete. IMSA will be operational after you click Finish
   and exit the Wizard.

Setting Up a Child Device

This section explains how to set up a child device and register it to the parent device.

To set up a child device:

1. Determine the IP address of the child device.
2. On the parent device, do the following:
   a. After you set up a parent device (see Setting Up a Single Parent Device on
      page 3-17), make sure the parent device is operational.
b. Log on to the Web console. Make sure that you are logging on the parent device Web console.

c. Choose Administration > IMSA Configuration > Connections > Child IP.

d. Under Add IP Address, add the IP address of the child device.

3. On the child device, do the following:

a. Just as you did for the parent device, connect a management computer to the child device and log on to the Web console. All IMSA devices have the same default IP addresses and Web console login credentials.

b. In the Setup Wizard, configure the local system settings and then click Next>.

c. On the Deployment Settings screen, select Child Server and add the Parent device IP address.

d. Click Finish.

4. On the parent device, do the following:

a. Choose Summary > System from the menu.

b. Verify that the child device appears under Managed Services and that a green check box appears under Connection. You can start or stop Scanner, Policy, or EUQ services.

   Note: If you enabled EUQ on the parent, it will also be enabled on the child.

5. If you want to use EUQ on the child device, redistribute the data across the EUQ databases:

a. On the parent device, choose Administration > End-User Quarantine. The EUQ Management tab appears by default.

b. Choose Redistribute all or Only redistribute approved senders. Trend Micro recommends choosing Redistribute all.
c. Click **Redistribute**.

**Note:** If you registered an EUQ-enabled child device to its parent device, add senders to the approved senders list, and then re-distribute EUQ data, some of the newly added approved senders might not appear.

Trend Micro recommends the following:
- After redistributing EUQ, the administrator informs all end users to verify that the newly added approved senders are still available.
- That the administrator notifies all end users not to add EUQ approved senders list when the administrator is adding a child device and redistributing EUQ.

---

**Verifying Successful Deployment**

After you have set up the IMSA devices, the services should be started automatically.

**To verify that IMSA services are active:**

1. Click **Summary** from the menu. The Real-time Statistics tab appears by default.
2. Click the **System** tab.
3. Under **Managed Services**, ensure that the scanner and policy services are active. Otherwise, click the **Start** button to activate them.

**Note:** You can choose to enable or disable the EUQ services.
Upgrading From Previous Versions

This chapter provides detailed instructions on how you can upgrade to IMSA 7.0 from the evaluation version of IMSA 7.0, from IMSA 1.0 or IMSS 5.7.

Topics include:

- *Upgrading From an Evaluation Version* on page 4-2
- *Import/Export Notes* on page 4-4
- *Upgrading From IMSA 1.0 To IMSA 7.0* on page 4-6
- *Migrating From IMSS 5.7 To IMSA 7.0* on page 4-12
- *Settings That Can Be Migrated From IMSS 5.7* on page 4-14
Upgrading From an Evaluation Version

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

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

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

To upgrade from the evaluation period:

1. Choose Administration > Product Licenses from the menu.
2. Click the **Enter a new code** hyperlink under the Trend Micro Antivirus and Content Filter or Spam Prevention Solution (SPS) sections accordingly.

3. Type the new Activation Code in the box provided.
4. Click *Activate*.

**Import/Export Notes**

To re-use settings from IMSA 1.0 or IMSS 5.7 in IMSA 7.0, you need to export the original settings from the previous versions before performing the upgrade, then importing these settings after the upgrade.

Note the following when importing and exporting settings:

- You cannot import or export the component list and child device registration information.
- When exporting/importing your settings, the database will be locked. Therefore, all IMSA actions that depend on database access, such as performing a mail trace, will not function.
- SMTP Routing Settings will be overwritten instead of appended, after importing configuration that was exported from IMSA 1.0 or IMSA 7.0.

Trend Micro strongly suggests that you:

- Adjust the component list and child device registration information after import if necessary.
- Backup a copy of current configuration before each import operation, in order to recover from mistaken import processes.
- Perform import/export when IMSA is idle because importing and exporting affects IMSA performance.
Upgrading From IMSA 1.0 To IMSA 7.0

Obtain the IMSA 5000 Solutions CD, which has the files you need to perform the upgrade. If you do not have the CD, you can download the files from Trend Micro at:
www.trendmicro.com/download

To prepare for upgrade:

1. Stop email traffic flow to IMSA 1.0.
2. Enter the IMSA 1.0 CLI and select 6) Utility > 1) Enter shell environment.
3. To verify whether or not all email messages have been delivered, type the following command:
   
   `postqueue -p`

4. Backup your IMSA 1.0 settings (see Exporting IMSA 1.0 Configuration Files on page 4-6 or your IMSA 1.0 documentation).

Before you upgrade, verify that you have the correct hard disks (see Additional Hardware Requirements and Tools on page 2-2). If you need to replace the hard disks, you must upgrade through the CLI.

Exporting IMSA 1.0 Configuration Files

To export from IMSA 1.0:

1. On the Web console, choose Configuration > Import/Export.
2. Click Export. IMSA generates a .dat file for configuration files.
3. Click Save.

   **WARNING!** To prevent accidental modification of the configuration data file, do not click Open to export the settings.

4. Choose a location to save the files.
5. Click Save.
Upgrading From IMSA 1.0 Environment

There are two ways to upgrade IMSA 1.0 to IMSA 7.0:

- **Web console**—Use the Web console for easy upload if you will keep the same hard disk.
- **Command Line Interface (CLI)**—Use the CLI if you upgrade the hard disk from 80GB to 250GB.

**Note:** The root password will not be changed after upgrading from IMSA 1.0.

Upgrading Through The Web Console

**To upgrade through the Web console:**

1. Log on to the IMSA 1.0 Web console.
2. Choose **Configuration > Update > IMSA Product Patch** from the menu.
3. Click **Browse** and select the IMSA 7.0 tar.gz file.
4. Click **Submit**.
5. Agree to the license agreement. The IMSA device will reboot automatically after the update finishes.
6. To verify that the upgrade was successful, log on to the Web console. If the new console opens, the upgrade is complete.

Upgrading Through The CLI

**To upgrade through the CLI:**

1. Enter the IMSA 1.0 CLI through a serial connection to the Console port and select 8) **Shutdown > 2) Power off.**
2. If you want to replace the hard disk, do the following:
   a. Slide the safety clip on the front of the hard drive to the open position.
   b. Pull the release lever. The hard disk detaches.
   c. Pull out the hard disk.
   d. Insert the new hard disk.
   e. Press the hard disk completely into the slot until the release lever closes.
f. Slide the safety clip to the closed position.

3. Connect your management computer to the **MANAGED** port (default IP address: 192.168.252.1) with the crossover cable.

4. Change your computer’s IP address to 192.168.252.2.

**Note:** You must be connected to the **MANAGED** port to upload the new files. You can also connect the computer to the Console port, but you cannot upload files from the Console port.

5. Turn on the device and enter rescue mode using one of the following methods:
   - If you are connected to the Console port, select “r” to enter Rescue mode when prompted on the CLI.
   - Press the Enter button on the device.

6. Run the **IMSA_Upload_Utility.EXE** tool on the IMSA Solutions CD.

7. When prompted, select the operating system upgrade file with the .G extension under \Packages\Upgrade\FromCLI.

8. The hard disk reformat process and operating system upgrade will begin, and IMSA will automatically reboot.

9. Repeat steps 5 through 7, but select the new application upgrade file with the .A extension \Packages\Rescue\Application.

The following System Settings will be preserved after upgrade:

- Network Settings
- Timezone
- Date and Time
- SSH enable/disable status
- CLI logon account

The Web console is always enabled and upgraded to the new version.
Performing Post-Upgrade Procedures

To perform post-upgrade procedures:
1. Log on to the IMSA 7.0 Web console. If the Web console does not load, repeat the upgrade process.
2. Choose Administration > Import/Export from the menu.
3. Import your original IMSA 1.0 settings. (see Importing Settings on page 4-9)
4. Modify the settings for your network environment if necessary.
5. Restore email traffic flow to IMSA.

Importing Settings

To re-use the original configuration settings from IMSA 1.0 or IMSS 5.7 after upgrading to IMSA 7.0, import the configuration files that you have backed up previously.

To import device configuration files:
1. Log on to the IMSA 7.0 Web console.
2. Choose Summary from the menu. The Real-time Statistics tab appears by default.
3. Click the System tab.
4. Verify that no services are starting or stopping. If services are starting or stopping, wait until they are stable.
5. Choose Administration > Import/Export from the menu.
6. Under Import Configuration Files, click Browse... and locate the file.
7. Click Import. The original IMSA 7.0 settings and rules, such as domain-based delivery settings, will be deleted and replaced by the imported settings and rules. All services on each device in the group will be restarted to apply the imported settings and rules. Wait until all services are restarted.
8. If the import is successful, you may click Download the log file to view details of the import.
During import, do not:
• Access other Web console screens or modify any settings.
• Perform any database operations.
• Start/stop any services on the device or in the group to which the device belongs.
• Register/unregister any child devices into/from the group to which the device belongs.
• Launch other export or import tasks.

**Settings That Cannot Be Migrated From IMSA 1.0**

IMSA 7.0 will not migrate the following settings from IMSA 1.0:

**EUQ Settings**
• EUQ approved senders
• EUQ spam mail

**Report Settings**
• Perl reports
• SPS reports

**Configuration Settings**
• Quarantine area and archive folder paths
• Email messages in queue folder
• Log paths
• Limits on notifications for processes per hour
• Web console password
• Database settings in odbc.ini and database.ini
Policy Settings
• Security settings: number of clean attempts, number of viruses reported, and message size criteria
• User-defined virus filters in sub-policies
• Customized actions for “No virus” in the virus filter
• Virus scanning settings for “Extensions to Exclude” for “Specified File Types”
• Global spam scanning mode
• Additional sensitivity for SPS filtering
• Action settings for graymail
• Advanced action settings for spam
• Expression list matching for attachments or file type in the advanced content filter
• Actions for “Archive Original”
• Notifications with original mail attachments
• Forwarding original email message attachments

TMCM Settings
• TMCM server settings
• TMCM Web server authentication settings
• Proxy settings

Update Settings
• ActiveUpdate server settings
• Proxy settings

NRS Settings
All NRS settings cannot be migrated.
Migrating From IMSS 5.7 To IMSA 7.0

If you want to re-use your policy settings from IMSS 5.7 (Linux, Solaris, or Windows), you must first export the settings into a file. Thereafter, you can import the file into IMSA 7.0 (see Importing Settings on page 4-9).

Exporting From IMSS 5.7 Linux

To export from IMSS 5.7 Linux:

1. Upload IMSS_5.7_Linux_GM_Export_tool.tar to your IMSS 5.7 Linux server and save it into a temporary folder (/tmp).
2. Unpack the tarball by typing the following command:
   ```
   tar xvf IMSS_5.7_Linux_GM_Export_tool.tar
   ```
3. Run the export tool by typing the following:
   ```
   ./export.sh
   ```

Use Binary mode to download the export tool and extract it on the IMSS 5.7 Linux server. Otherwise, the tool might not be extracted successfully.

The exported package will be saved in the current working directory with the name `imss.pol.tar.gz`.

Alternatively, you can type the following command to export the package to a designated folder:

```
./export.sh [pathname]
```

If the export fails, view the detailed export log (`export.log`) in the current working directory.

Exporting From IMSS 5.7 Solaris:

To export from IMSS 5.7 Solaris:

1. Upload the IMSS_5.7_Solaris_GM_Export_tool.tar to your IMSS 5.7 Solaris server and save it into a temporary folder (/tmp).
2. Unpack the tarball by typing the following command:
   ```
   tar xvf IMSS_5.7_Solaris_GM_Export_tool.tar
   ```
3. Run the export tool by typing the following:
   ```
   ./export.sh
   ```

   Use Binary mode to download the export tool and extract it on the IMSS 5.7 Solaris server. Otherwise, the tool might not be extracted successfully.

   The exported package will be saved in the current working directory with the name `imss.pol.tar.gz`.

   Alternatively, you can type the following command to export the package to a designated folder:
   ```
   ./export.sh [pathname]
   ```

   If the export fails, view the detailed export log (`export.log`) in the current working directory.

Exporting From IMSS 5.7 Windows

To export from IMSS 5.7 Windows:

1. Upload `IMSS_5.7_Windows_GM_Export_Tool.zip` to your IMSS 5.7 Windows server.
2. Unpack the package.
3. Run the export tool: `export_tool.exe`.

   The exported package will be saved in the current working directory with the name `imss.pol.tar.gz`.

   Alternatively, you can type the following command to export the package to a designated folder:
   ```
   ./export_tool.exe [pathname]
   ```

   If the export fails, view the detailed export log (`export.log`) in the current working directory.

Note: If any of your IMSS 5.7 Windows settings use double-byte characters, make sure the locale of the Windows is also in double-byte characters. Otherwise, the double-byte character settings cannot be migrated correctly.
Settings That Can Be Migrated From IMSS 5.7

IMSA 7.0 will only migrate policy settings from IMSS 5.7. All other settings will not be migrated.

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

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

Topics include:

- Troubleshooting on page 5-2
- Frequently Asked Questions (FAQ) on page 5-5
- Using the Knowledge Base on page 5-7
- Contacting Support on page 5-8
Troubleshooting

This section provides a list of IMSA troubleshooting utilities and solutions to issues you might encounter. If you have additional problems, check the Trend Micro Knowledge Base:

http://esupport.trendmicro.com

Troubleshooting Utilities

Use the following troubleshooting-related utilities and commands with caution. Trend Micro recommends contacting your support provider before modifying any internal IMSA files.

• Firewall setting check:
  
  `iptables -nvxL`

• PostgreSQL command line tool:
  
  `/opt/trend/imss/PostgreSQL/bin/psql -U sa -d imss`

• cdt (password: “trend”)—Collect the following information:
  
  • Configuration information
  • Logs
  • Core dumps

• Other utilities:
  
  • `pstack`—shows the callstack of the process, including all threads
  • `ipcs`—lists all IPCs in the current system
  • `gdb`—the debugger
  • `tcpdump`—sniffs network packages
  • `netstat`—lists current network connection

Troubleshooting Issues

Table 5-1 shows common troubleshooting issues you might encounter with IMSA. Read through the solutions below.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
</table>
| Devices in a group cannot communicate | If several IMSA devices are deployed in a group, they must communicate with each other. Verify that the following ports are accessible on all devices:  
• 5060—Policy service  
• 15505—IMSA control service  
• 53 UDP/TCP—IP Profiler  
• 5432—Database service  
• 8009—EUQ internal service  
Also verify the following:  
• The current firewall settings in “iptables”.  
• The firewall configuration files in /etc/conf/fw.rules.  
• The table “tb_trusted_ip_list” in the database has the IP addresses of the correct devices. The IP address of any other devices trying to access this device must be in this list.  
Also verify that all the necessary port IMSA uses are accessible for the relevant services (see *IMSA Ports* on page 2-4). |
| Child device has trouble registering to a parent | Do the following:  
1. Open the parent device’s Web console and choose Administration > IMSA Configuration > Connections > Child IP.  
2. Verify that the IP address of the child is on the Child IP Address List.  
3. In the Configuration Wizard, verify that Child is selected for the device role.  
4. Verify that the Admin Database is accessible.  
5. Unregister the Control Manager agent (if TMCM agent is enabled).  
6. Verify that no other child device registered to the parent has the same IP address as the device you are trying to register.  
7. Remove all the logs and quarantined messages.  
8. Change the configuration and restart the services.  
The parent device Web console (in the Configuration Wizard) makes the initial request. If you encounter any registration issues, run the following command to get the error message from the console:  
```
/opt/trend/imss/script/cfgtool reg IPADDR sa postgresQL
``` |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Suggested Resolution</th>
</tr>
</thead>
</table>
| Child device has trouble unregistering from the parent | Do the following:  
1. Connect to the child device through the command line interface.  
2. Check whether the Admin Database is accessible. If yes, remove the child device from the Child IP list on the parent Web console and update the trusted child list.  
3. Rescue the device, which will forcibly unregister it from the parent.  
4. Update the patches.  
To verify that a child is unregistered from its parent, try to access the Web console on the child device. If the console is accessible, the device is successfully unregistered.  
You can also run the following command:  
/opt/trend/imss/script/cfgtool.sh dereg |
Frequently Asked Questions (FAQ)

Importing and Exporting

Will all IMSA 1.0 or IMSS 5.7 settings be retained during migration?
No. Due to architectural changes in IMSA 7.0, some settings will not be retained. After migration has completed successfully, a report containing the "Migrated Settings" and "Settings Not Migrated" information will be displayed. All settings that are not retained and policies that are not migrated can be found in the "Settings Not Migrated" section.

What is the mapping relationship between IMSA 1.0 or IMSS 5.7 policies and IMSA 7.0 rules?
After the migration has completed successfully, a report containing the "Migrated Settings" and "Settings Not Migrated" information will be displayed. The mapping relationship is described in the "Migrated Settings" section.

How are filters and policies mapped during migration?
The architectures of IMSA 1.0 or IMSS 5.7 and IMSA 7.0 are very different. Therefore, the migration module maps all IMSA 1.0 or IMSS 5.7 filters to related rules in IMSA 7.0 in the following ways:

- **Virus filter(s)** — There is only one virus rule for both incoming and outgoing traffic 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.
- **SPS filter(s)** — The migration module maps each SPS filter into one SPS rule after migration or several SPS rules depending on the Routes and Filter Actions. There will normally be one SPS rule after migration. The following are exceptions when there will be several SPS rules:
  - If there are multiple routes with different "To" or "From" addresses.
    For example: SPS filter with the routes (a->b; c->d; e->b) will be migrated to two SPS rules with the routes (a,e->b; c->d)
  - **If three filter actions are different.**
For example, SPS filter with the following filter actions will be migrated to two SPS rules named "Spam Filter (SPS) BlackWhiteList And Phish->Global Policy" and "Spam Filter (SPS) Spam->Global Policy"
  • "Tag and Deliver" for "Blocked senders"
  • "Tag and Deliver" for "Phishing emails"
  • "Quarantine" for "Spam"

  • eManager filter
    • There will be several rules for one eManager filter after migration if there are multiple routes with different "To" or "From" addresses. For example: eManager filter with the routes (a->b; c->d; e->b) will be migrated to two eManager rules with the routes (a,e->b; c->d)
    • There will be two rules for one eManager filter after migration if it was "active" in IMSA 1.0 or 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 IMSA 1.0 or IMSS 5.7 for both SMTP and POP3 traffic. The rule direction is for "Both incoming and outgoing directions". You can add the related rule for the POP3 rule direction in IMSA 7.0 if necessary.

What is the source of internal addresses during migration?
To retain IMSA 1.0 or IMSS 5.7 internal domains, IMSA 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 do I upgrade multiple IMSA 1.0 devices into a IMSA7.0 group?
To upgrade from multiple IMSA 1.0 devices:
  • Export settings from the IMSA 1.0 device with the desired settings
  • Upgrade all IMSA 1.0 devices to IMSA7.0
• Import the settings into one of the IMSA 7.0 parent device
• Register all other IMSA 7.0 devices to that parent device

Is a smooth rollback to IMSA 1.0 possible after upgrade?
Yes, you can rollback to IMSA 1.0 after upgrade by doing one of the following:

If you want to replace 250GB hard disks with the original IMSA 1.0 80GB hard disks
• Shutdown the IMSA device and unplug the hard disks from the disk bays
• Rescue IMSA 1.0 .R package
• Rescue IMSA 1.0 .B package
• Shutdown the device and plug the old hard disks into the disk bays
• Enter CLI and configure the system setting

If you want to keep the hard disk, you should store the IMSA 1.0 application GM build in an ftp server
• Rescue IMSA 7.0 .G package
• Rescue IMSA 1.0 .R package
• Rescue IMSA 1.0 .B package
• Enter CLI and configure the system setting
• Enter shell, run the command:
  ```
  mount /dev/sda6 /mnt/backup
  ```
• Download the IMSA 1.0 application build from the ftp server and save it into the directory /mnt/backup, that is, store this application build into /dev/sda6
• Return to CLI, enter the Maintenance menu to rescue IMSA application
• Restore IMSA 1.0 application level configurations into the IMSA device.

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

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

**Contacting Support**

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

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

http://www.trendmicro.com/support

Get the latest Trend Micro product documentation:

http://www.trendmicro.com/download

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

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

This glossary describes special terms as used in this document or the online help.

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Activation Code             | A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4  
**Also see** Registration Key. |
| ActiveUpdate server         | The Trend Micro server with all official, up-to-date product components, including the virus pattern file and scan engine.                |
| Spam prevention engine      | A Trend Micro software component that enables several Trend Micro products to scan for spam.                                             |
| antivirus filter            | A type of IMSA filter that protects your network from viruses, Trojans, spyware and other grayware.                                     |
| console port                | The port through which you can connect a computer to IMSA to access the command line interface (serial connection).                        |
| Control Manager (TMCM)     | 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. |
| data port                   | The port through which IMSA connects to your network.                                                                                   |
**Term** | **Explanation**
--- | ---
End User License Agreement (EULA) | A legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product.

Many users inadvertently agree to the installation of spyware and adware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.

grayware | Any number of software applications that gather data, display advertisements, or help hackers break into a system or crack passwords.

IntelliTrap | A built-in Trend Micro technology that helps IMSA evaluate compressed files that could contain viruses or other Internet threats.

IntelliTrap pattern file | A file that enables several Trend Micro products to identify viruses and other Internet threats that hide in compressed files.

IntelliTrap exception | A list of legitimate applications and files that IntelliTrap will not identify as a virus or other threat.

MacroTrap | Built-in Trend Micro technology that analyzes macro code in Microsoft Office files to help the scan engine detect macro viruses.

management port | The port through which you can connect a computer to IMSA to access the command line interface (SSH connection). This port is labeled MANAGED on the device.

MTA (Mail Transfer Agent) | The program responsible for delivering email messages.

Network Reputation Services (NRS) | A Trend Micro product that helps block email from known spammers. To use NRS, purchase a separate Activation Code.

online help | Documentation that is bundled with the GUI.

Registration Key | A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4X-39HB-MNW8

Also see Activation Code.

Reputation Database | A Trend Micro database of known spammers. NRS queries the Reputation Database to determine if a computer that is sending email to your network is a known spammer.
<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>rescue</td>
<td>Re-installing the operating system or application files.</td>
</tr>
<tr>
<td>route</td>
<td>A specific To and From link between a sender and receiver or a set of senders and receivers.</td>
</tr>
<tr>
<td>scan engine</td>
<td>A component that several Trend Micro products use to scan for viruses, grayware, and other potential threats.</td>
</tr>
<tr>
<td>spyware</td>
<td>Applications that gather data, such as account user names and passwords, and transmit them to third parties. Spyware is a type of Grayware.</td>
</tr>
<tr>
<td>spyware pattern file</td>
<td>A file that several Trend Micro products use to identify spyware and other types of grayware.</td>
</tr>
<tr>
<td>virus pattern file</td>
<td>A file that several Trend Micro products use to identify viruses and other Internet Threats.</td>
</tr>
</tbody>
</table>

**TABLE A-1. Glossary of terms**
Index

A
application requirements 2-3
Audience vii

C
changing power supplies 2-8
CPU 2-9

D
deploying
  before a firewall 3-10
  behind a firewall 3-11
  in the DMZ 3-12
  on SMTP gateway 3-12
device details 2-3
Documentation vi

E
email threats
  spam 1-6
  unproductive messages 1-6

F
features 1-3
filtering, how it works 1-7

G
glossary A-I
grayware 1-9

H
hard disks 2-6
Hardware Maintenance Sheet vi
hardware monitor 2-10
hardware requirements 2-2
Hardware Specifications 2-4

I
Introducing IMSA 1-2
IP Filtering
  about 1-12

L
LCD 2-21
LCM 2-21

M
mass mailing viruses
  pattern 1-6
minimum requirements 2-2
mounting the device 2-11

N
notifications
  hardware monitor 2-10
NRS
  how it works 1-14

O
Online Help vi
operating system
  automatic restart 2-10

P
pattern matching 1-4
POP3
  deployment planning 3-15
power supplies
  about 2-7
  changing 2-8
powering off 2-8
Preface v
processor 2-9

Q
Quick Start Guide vi
R
rack mounting 2-11
RAID hard disks 2-6
Readme File vi
requirements 2-2
restarting
  automatic watchdog service 2-10
S
spyware and grayware 1-9
swapping the hard disks 2-6
system requirements 2-2
T
third-party license agreements vi

Tips
  mounting Network VirusWall 2-14
  rack space 2-14
  removing rack doors 2-13
  required rack cabinet space 2-14
  turning off the device 2-8
U
using
  the LCM 2-21
W
watchdog service 2-10