TREND MICRO™

# InterScan™ Messaging Security Virtual Appliance 7

Comprehensive Email Protection at the Gateway

## Installation Guide

Messaging Security

Document Part No. MSEM73779/80804

Release Date: September 2008

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

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

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

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

# Contents

## Chapter 4: Installing and Upgrading



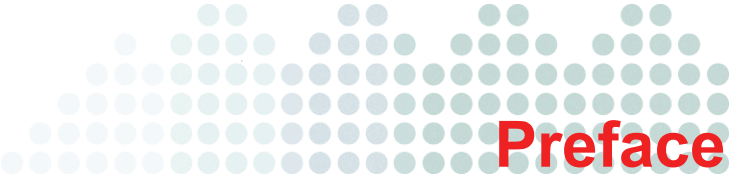
## Chapter 5: Troubleshooting, FAQ, and Support



## Appendix A: Creating a New Virtual Machine Under VMware ESX for IMSVA



## Index




# Preface

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

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

This preface discusses the following topics:

# InterScan™ Messaging Security Virtual Appliance Documentation

The InterScan Messaging Security Virtual Appliance (IMSVA) documentation consists of the following:

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

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

# Audience

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

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

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

# Document Conventions

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

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

# Chapter 1

# Introducing InterScan Messaging Security Virtual Appliance

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

Topics include:

# About IMSVA 7.0

InterScan Messaging Security Virtual Appliance (IMSVA) 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 this release:

| NEW FEATURE | DESCRIPTION |
|---|---|
| Self-contained Installation | IMSVA provides a self-contained installation that provides a purpose-built, hardened, and performance tuned CentOS Linux operating system. This dedicated operating system installs with IMSVA to provide a turnkey solution. A separate operating system, such as Linux, Windows, or Solaris, is not required. |
| Bare Metal and VMware ESX Support | IMSVA can be installed on bare metal server platforms (servers without an operating system) or on VMware virtual platforms. IMSVA is fully supported when running on VMware ESX Server 3.5. |
| Command Line Interface | IMSVA provides a native Command Line Interface (CLI) to perform system monitoring, system administration, debugging, troubleshooting functions, through a secure shell or direct console access. IMSVA's new CLI interface offers stronger console security by preventing unauthorized access to the OS shell. The IMSVA CLI is modeled after industry standard CLI syntax and navigation formats to greatly reduce the learning time. |
| Multiple Network Interfaces Support<br>Route Configuration | IMSVA supports multiple network interfaces, and provides a user interface to configure the route for users to deploy IMSVA more conveniently. |

**TABLE 1-1. New Features**

| NEW FEATURE | DESCRIPTION |
|---|---|
| Multiple Antivirus and Malware Policies | Multiple IMSVA policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria. |
| Centralized Logging and Reporting | A consolidated, detailed report provides top usage statistics and key mail usage data.<br>Centralized logging allows administrators to quickly audit message-related activities. |
| Centralized Archive and Quarantine Management | An easy way to search multiple IMSVA quarantine and archive areas for messages. |
| Scalable Web End-User Quarantine (Web EUQ) | Multiple Web EUQ services offer your users the ability to view quarantined email messages that IMSVA detected as spam.<br>Together with EUQ notification, IMSVA will help lower the cost of helpdesk administrative tasks. |
| Multiple Spam Prevention Technologies | Three layers of spam protection:<br>• Network Reputation Services filters spam senders at the connection layer.<br>• IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS).<br>• Trend Micro Anti-spam engine accurately detects and takes action on spam. |
| Delegated Administration | LDAP-integrated account management which users to assign administrative rights for different configuration tasks. |
| Easy Deployment with Configuration Wizard | An easy-to-use configuration wizard to get IMSVA up and running right out of the box. |
| Advance MTA Functions | Opportunistic TLS, domain based delivery, and other MTA functions help IMSVA handle email efficiently and securely. |
| Migration | Easy upgrade process ensures that settings will be transferred with minimum effort during setup. |

**TABLE 1-1. New Features**

| NEW FEATURE | DESCRIPTION |
|---|---|
| Mail Auditing and Tracking | Detailed logging for all messages to track and identify message flow related issues. |
| Integration with Trend Micro Control Manager™ | Perform log queries on Network Reputation Services from Control Manager, in addition to other supported features. |

**TABLE 1-1. New Features**

# IMSVA Main Features and Benefits

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Real-time Statistics and Monitor | Administrators can monitor the scan performance and IP filtering performance of all IMSVA devices (within a group) on the Web management console. | IMSVA 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. |
| Antivirus protection | IMSVA 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. | IMSVA's enhanced virus/content scanner keeps your messaging system working at top efficiency. |

**TABLE 1-2. Main Features and Benefits**

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Intellitrap | Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files.<br>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 IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature.<br>By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be incorrectly classified as security risks. | Helps reduce the risk that a virus compressed using different file compression schemes will enter your network through email. |
| Content management | IMSVA analyzes email messages and their attachments, traveling to and from your network, for appropriate content. | Content that you deem inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using IMSVA. |
| Protection against other email threats | | |
| DoS attacks | By flooding a mail server with large attachments, or sending messages that contain multiple viruses or recursively compressed files, individuals with malicious intent can disrupt mail processing. | IMSVA 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. |

**TABLE 1-2. Main Features and Benefits**

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Malicious email content | Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions. | IMSVA allows you to configure the types of messages that are allowed to pass through the SMTP gateway. |
| Degradation of services | Non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours. | Most companies have acceptable usage policies for their messaging system—IMSVA 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. | IMSVA provides tools for monitoring and blocking content to help reduce the risk that messages containing inappropriate or confidential material will be allowed through your gateway. |

**TABLE 1-2. Main Features and Benefits**

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Mass mailing virus containment | Email-borne viruses that may automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users.<br>When IMSVA detects a mass-mailing virus, the action taken against this virus can be different from the actions against other types of viruses.<br>For example, if IMSVA 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 IMSVA detects a mass-mailing virus, the program can automatically delete the entire message. | By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value.<br>The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs$^{SM}$ ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers. |
| Spyware and other types of grayware | | |
| Spyware and other types of grayware | Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see About Spyware and Other Types of Grayware on page 1-10 | IMSVA's ability to protect your environment against spyware and other types of grayware enables you to significantly reduce security, confidentiality, and legal risks to your organization. |

**TABLE 1-2. Main Features and Benefits**

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Integrated spam | | |
| Spam Prevention Solution (SPS) | Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam-detection services to other Trend Micro products. To use SPS, you must pay for and obtain an SPS Activation Code. For more information, refer to your sales representative.<br>SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license.<br>**Note:** Activate SPS before you configure IP Profiler and NRS. | The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real time detection that is highly adaptable, even as spam originators change their techniques. |
| Spam Filtering with IP Profiler and NRS | IP Profiler is a self-learning, fully configurable feature that proactively blocks IP addresses of computers that send spam and other types of potential threats. NRS blocks IP addresses of known spam senders that Trend Micro maintains in a central database. | With the integration of IP Filtering, which includes IP Profiler and Network Reputation Services (NRS), IMSVA can block spammers at the IP level. |
| Others | | |
| LDAP & domain-based policies | You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™ or Microsoft™ Active Directory™ for user-group definition and administrator privileges.<br>**Note:** You must have LDAP in order to use End-User Quarantine. | Using LDAP, you can define multiple rules to enforce your company's email usage guidelines. You can define rules for individuals or groups, based on the sender and recipient addresses. |

**TABLE 1-2. Main Features and Benefits**

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| Web-based management console | Web-based management console allows you to conveniently configure IMSVA policies and settings on the Web. | The Web-based console also provides greater security as it is SSL-compatible. |
| End-User Quarantine (EUQ) | IMSVA provides Web-based EUQ to improve spam management. The Web-based EUQ service allows end-users to manage their own spam quarantine. Spam Prevention Solution (SPS) quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete or approve for delivery. | With the Web-based EUQ console, end-users can manage messages that IMSS quarantines. |
| Delegated administration | IMSVA offers the ability to create different access rights to the Web management console. You can choose which sections of the console are accessible for different administrator logon account. | By delegating administrative roles to different employees, you can create backups of human resources and promote the sharing of administrative duties. |
| Centralized reporting | Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports. | Helps you analyze how IMSVA is performing.<br>One time (on demand) reports allow you to specify the type of report content as and when required. Alternatively, you can configure IMSVA to automatically generate reports daily, weekly, and monthly. |
| System availability monitor | A built-in agent monitors the health of your IMSVA server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow. | Email notification on detection of system failure allows you to take immediate corrective actions and minimize downtime. |

**TABLE 1-2. Main Features and Benefits**

| FEATURE | DESCRIPTIONS | BENEFITS |
|---|---|---|
| POP3 scanning | You can choose to enable or disable POP3 scanning from the Web management console. | In addition to SMTP traffic, IMSVA can also scan POP3 messages at the gateway as messaging clients in your network retrieve them. |
| Integration with Trend Micro Control Manager™ | Trend Micro Control Manager™ (TMCM) is a software management solution that gives you the ability to control antivirus and content security programs from a central location regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus and content security policy.<br>For details, see About Trend Micro Control Manager on page 1-12. | Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in IMSVA to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available. |

**TABLE 1-2. Main Features and Benefits**

# About Spyware and Other Types of Grayware

Your clients are at risk from threats other than viruses. Grayware can negatively affect the performance of the computers on your network and introduce significant security,

confidentiality, and legal risks to your organization (see Table 1-3).

| TYPES OF SPYWARE/GRAYWARE | DESCRIPTIONS |
|---|---|
| Spyware/Grayware | Gathers data, such as account user names and passwords, and transmits them to third parties. |
| Adware | Displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser. |
| Dialers | Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem. |
| Joke Program | Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes. |
| Hacking Tools | Helps hackers enter computers. |
| Remote Access Tools | Helps hackers remotely access and control computers. |
| Password Cracking Applications | Helps hackers decipher account user names and passwords. |
| Others | Other types not covered above. |

**TABLE 1-3. Types of spyware/grayware**

# About Trend Micro Control Manager

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

Control Manager consists of the following components:

- **Control Manager server**—The Control Manager server is the computer upon which the Control Manager application installs. The Web-based Control Manager management console generates from 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. The agent automatically installs when you install IMSVA.

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

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

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

## Integrating with Control Manager

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

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

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

| FEATURES | DESCRIPTIONS | SUPPORTED? |
|---|---|---|
| Engine Update | Update Scan Engine from Control Manager. | Yes |
| Product Component Update | Update IMSVA product components such as patches and hot fixes from Control Manager. | No.<br>Refer to the specific patch or hot fix readme file for instructions on how to update the product components. |
| Configuration By User Interface Redirect | Configure IMSVA through the IMSVA Web management console accessible from Control Manager. | Yes |
| Renew Product Registration | Renew IMSVA product license from Control Manager. | Yes |
| Mail-related Report on Control Manager | Generate the following IMSVA mail-related reports from Control Manager:<br>• Top 10 Virus Detection Points<br>• All Entities Virus Infection List<br>• Top 10 Infected Email Sender Report<br>• Top 10 Security Violations Reports<br>• Virus Infection Channel-Product Relationship Report<br>• Filter Events by Frequency<br>• Filter Events by Policy<br>• Gateway Messaging Spam Summary Report<br>• Gateway Messaging Spam Summary Report (for Domains) | Yes |

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

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

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

# Chapter 2

# System Requirements and Component Descriptions

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

Topics include:

# System Requirements

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

**TABLE 2-1. System Requirements**

| HARDWARE/SOFTWARE | DESCRIPTION |
|---|---|
| Operating System | IMSVA provides a self-contained installation that provides a purpose-built, hardened, and performance tuned CentOS Linux operating system. This dedicated operating system installs with IMSVA to provide a turnkey solution. A separate operating system, such as Linux, Windows, or Solaris, is not required. |
| Recommended CPU | Dual 2.4GHz Intel™ Core2Duo™ processors |
| Minimum CPU | Dual 2.0 GHz Intel™ Pentium™ Xeon processors |
| Recommended Memory | 4GB RAM |
| Minimum Memory | 2GB RAM |
| Recommended Disk Space | 250GB<br>IMSVA automatically partitions the detected disk space as per recommended Linux practices |
| Minimum Disk Space | 80GB<br>IMSVA automatically partitions the detected disk space as per recommended Linux practices |
| Monitor | Monitor that supports 800 x 600 resolution with 256 colors or higher |

**TABLE 2-1. System Requirements**

| HARDWARE/SOFTWARE | DESCRIPTION |
|---|---|
| Server Platform Compatibility | IMSVA should install and operate without issues on many brands of “off-the-shelf ” server platforms. However, Trend Micro cannot guarantee 100% compatibility with all brands and models of server platforms.<br>To obtain a list of Trend Micro certified servers that are guaranteed compatible with IMSVA, access the following URL:<br>http://www.trendmicro.com/go/certified<br>To obtain a general list of available platforms that should operate with IMSVA, access the following URL:<br>http://wiki.centos.org/HardwareList<br>Trend Micro cannot guarantee full compatibility with the hardware components from this general list. |

## Additional Requirements and Tools

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

**TABLE 2-2. Minimum Software Requirements**

| APPLICATION | SYSTEM REQUIREMENT | DETAILS |
|---|---|---|
| SSH communications application | SSH protocol version 2 | To adequately view the IMSVA CLI through an SSH connection, set the terminal window size to 80 columns and 24 rows. |
| VMware™ ESX server | Version 3.5 | If you want to install IMSVA as virtual machine, install IMSVA on a VMware ESX server 3.5. |

**TABLE 2-2. Minimum Software Requirements**

| APPLICATION | SYSTEM REQUIREMENT | DETAILS |
|---|---|---|
| Internet Explorer© | Version 6.0 | To access the Web console, which allows you to configure all IMSVA 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 |
| Mozilla Firefox© | Version 2.0 | |
| Java™ Virtual Machine | Version 5.0 or later or SUN JRE 1.4+ | To view certain items in the Web console, the computer must have JVM. |
| Trend Micro Control Manager | Version 3.5 patch 5 hot fix 1553 | If you want to use Trend Micro Control Manager 3.5 to manage IMSVA, update the Control Manager server to version 3.5 patch 5 hot fix 1553. |

# About IMSVA Components

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

## 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, contact 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.

## IP Filtering

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

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

  IP profiler detects any of these four potential Internet threats:

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

## Network Reputation Services

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

### Types of Network Reputation Services

NRS provides two types of services:

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

## How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email containing threats mentioned in the section IP Filtering on page 2-5. You can customize several criteria that determine when IMSVA 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 IMSVA monitors the IP address and a threshold.

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

The following process takes place after IMSVA 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, IMSVA denies the connection request.

   If the IP address is not on the blocked list, IMSVA analyzes the email traffic according to the threshold criteria you specify for IP Profiler.

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

## How Network Reputation Service Works

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

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

Figure 2-1 illustrates how NRS works.

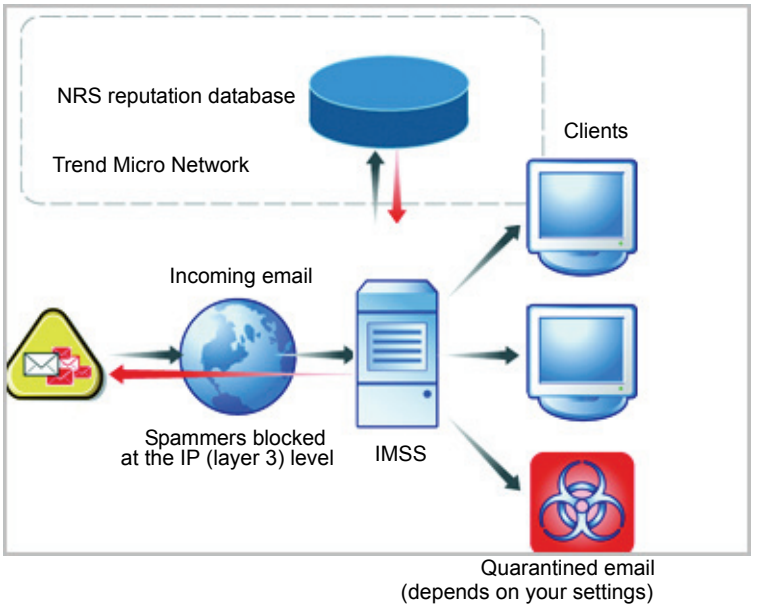



**FIGURE 2-1 How NRS works**

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

## Using the NRS Management Console

Log on to the Network Reputation Services management console to access global spam information, view reports, create or manage Approved Sender IP and Blocked Sender IP lists, and perform administrative tasks.

This section includes basic instructions for using the NRS console. For detailed instructions on configuring the settings for 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 Management Console:**

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

   `https://nrs.nssg.trendmicro.com/`

2. Select **Global Spam Update** from the menu.
3. Click any of the following tabs:
   - **Spam Alert:** Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.
   - **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 ISP's will change on a daily basis.
4. To view reports that summarize the query activity between your MTA and the Network Reputation Services database 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 the 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.

   To change your password or Activation Code, choose **Administration** from the menu.

# About End-User Quarantine (EUQ)

IMSVA 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 IMSVA) 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 InterScan Messaging Security Virtual Appliance is performing, use the centralized reporting feature. You can configure one time (on demand) reports or automatically generate reports (daily, weekly, and monthly).

# Chapter 3

# Planning for Deployment

This chapter explains how to plan for IMSVA deployment. For instructions on performing initial configuration, see the *Administrator's Guide*.

Topics include:

# Deployment Checklist

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

**TABLE 3-1. Deployment Checklist**

| TICK  WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | Step1 - Identify the location of IMSVA | | |
| | Choose one of the following locations on your network where you would like to install IMSVA. | | |
| | • At the gateway | | Deploying at the Gateway or Behind the Gateway on page 3-5 |
| | • Behind the gateway | | Deploying at the Gateway or Behind the Gateway on page 3-5 |
| | • Without a firewall | | Installing without a Firewall on page 3-8 |
| | • In front of a firewall | | Installing in Front of a Firewall on page 3-8 |
| | • Behind a firewall | | Installing Behind a Firewall on page 3-9 |
| | • On a former SMTP gateway | | Deploying on a Former SMTP Gateway on page 3-10 |

**TABLE 3-1. Deployment Checklist**

| TICK  WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | • In the De-Militarized Zone | | Installing in the De-Militarized Zone on page 3-11 |
| | Step 2 - Plan the scope | | |
| | Decide whether you would like to install a single IMSVA device or multiple devices. | | |
| | • Single device installation | | About Device Roles on page 3-12 |
| | • Multiple IMSVA devices | | About Device Roles on page 3-12 |
| | Step 3 - Deploy or Upgrade | | |
| | Deploy a new IMSVA device or upgrade from a previous version. | | |
| | • Upgrade from a previous version | | Importing Settings on page 4-19 |
| | Step 4 - Start services | | |
| | Activate IMSVA services to start protecting your network against various threats. | | |
| | • Scanner | | IMSVA Services section of the *Administrator's Guide*. |
| | • Policy | | |
| | • EUQ | Yes | |
| | Step 5 - Configure other IMSVA settings | | |
| | Configure various IMSVA settings to get IMSVA up and running. | | |

**TABLE 3-1. Deployment Checklist**

| TICK ✓ WHEN COMPLETED | TASKS | OPTIONAL | REFERENCE |
|---|---|---|---|
| | • IP Filtering Rules | Yes | IP Filtering Service section of the *Administrator's Guide*. |
| | • SMTP Routing | | Scanning SMTP Messages section of the *Administrator's Guide*. |
| | • POP3 Settings | Yes | Scanning POP3 Messages section of the *Administrator's Guide*. |
| | • Policy and scanning exceptions | | Managing Policies section of the *Administrator's Guide*. |
| | • Perform a manual update of components and configure scheduled updates | | Updating Scan Engine and Pattern Files section of the *Administrator's Guide*. |
| | • Log settings | | Configuring Log Settings section of the *Administrator's Guide*. |
| | Step 6 - Back up IMSVA | | |
| | Perform a backup of IMSVA as a precaution against system failure | | |
| | Back up IMSVA settings | | Backing Up IMSVA section of the *Administrator's Guide*. |

# Considering Network Topology

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

## Deploying at the Gateway or Behind the Gateway

**TABLE 3-2. Common scenarios for handling SMTP traffic**

| | SINGLE DEVICE | MULTIPLE DEVICES |
|---|---|---|
| At the Gateway | The only setup if you plan to use IP Filtering with the device. IMSVA 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:<br>• Figure 3-3<br>• Choosing Services on page 3-12. |
| Behind the Gateway | The most common setup. IMSVA 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. IMSVA 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<br>• Figure 3-4<br>• Choosing Services on page 3-12. |
| **TREND MICRO CONTROL MANAGER SCENARIO** | | |
| If you have multiple groups, you can use **Trend Micro Control Manager** (TMCM) to manage the devices. | | |

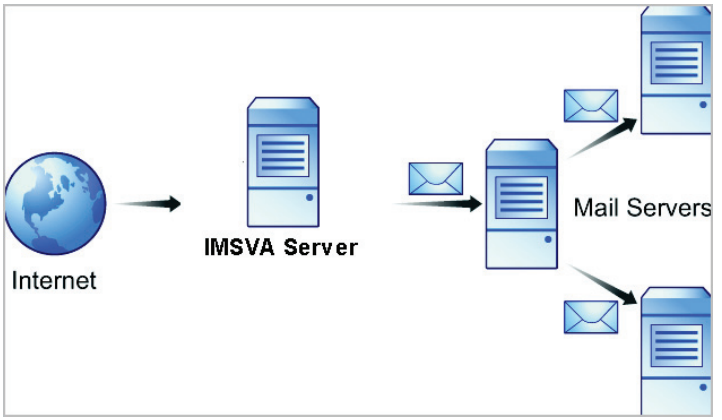



**FIGURE 3-1 Single IMSVA device at the gateway**

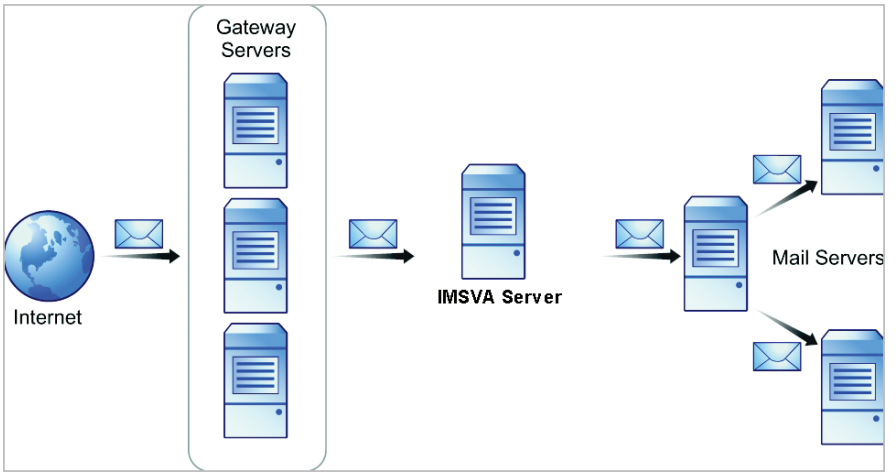



**FIGURE 3-2 Single IMSVA device behind the gateway**

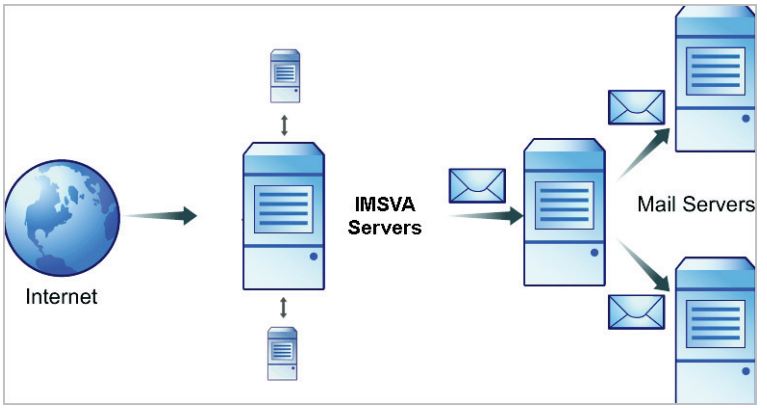



**FIGURE 3-3 IMSVA group at the gateway**

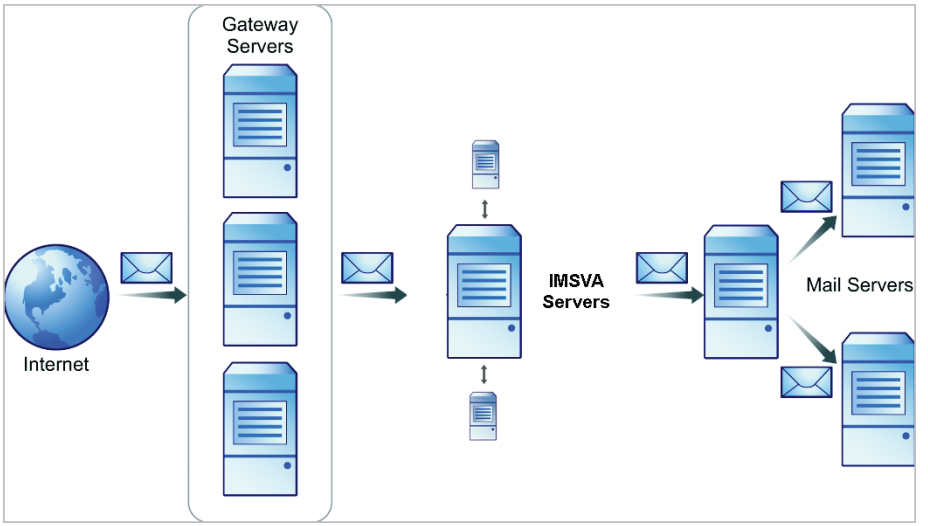



**FIGURE 3-4 IMSVA group behind the gateway**

## Installing without a Firewall

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

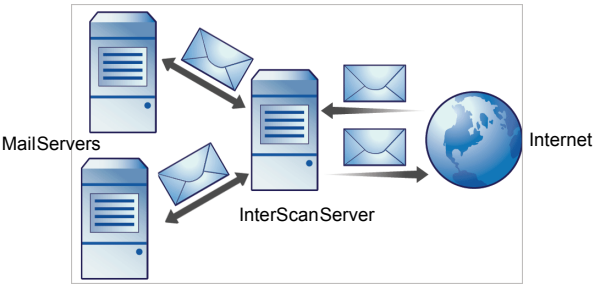



**FIGURE 3-5 Installation topology: no firewall**

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

## Installing in Front of a Firewall

Figure 3-6 illustrates the installation topology when you install IMSVA in front of your firewall:

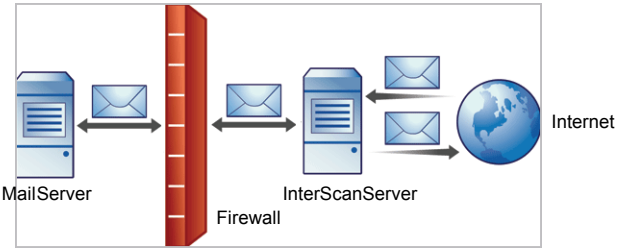



**FIGURE 3-6 Installation topology: in front of the firewall**

### Incoming Traffic

- Postfix should receive incoming messages first, then transfers them to IMSVA. Configure IMSVA to reference your SMTP server(s) or configure the firewall to permit incoming traffic from the IMSVA 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 IMSVA, so that:
  - Outgoing SMTP email goes to Postfix first and then to IMSVA.
  - Incoming SMTP email can only come from Postfix to IMSVA servers.
- Configure IMSVA to allow internal SMTP gateways to relay, through Postfix, to any domain through IMSVA.

---

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

---

## Installing Behind a Firewall

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

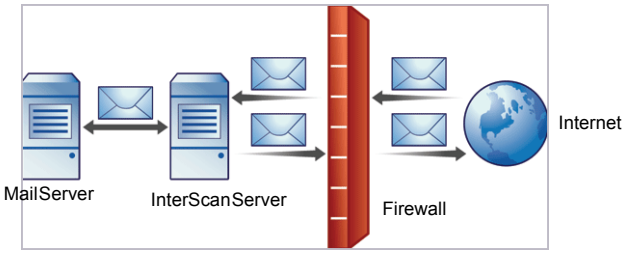



**FIGURE 3-7 Installation scenario: behind a firewall**

### Incoming Traffic

- Configure your proxy-based firewall, so:

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

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

## Deploying on a Former SMTP Gateway

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

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

**Note:** The existing SMTP gateway binds to port 25.

### Incoming Traffic

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

## Installing in the De-Militarized Zone

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

### Incoming Traffic

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

### Outgoing Traffic

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

---

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

---

# About Device Roles

IMSVA 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 IMSVA device, select parent mode during setup so that all IMSVA 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 IMSVA 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 IMSVA 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 IMSVA 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 IMSVA to scan POP3 traffic. See Understanding POP3 Scanning on page 3-14 for more information.

## Deploying IMSVA 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 IMSVA 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 IMSVA 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 Internal Communication Port

IMSVA supports multiple network interfaces. This means one IMSVA device may have multiple IP addresses. This introduces challenges when devices try to communicate using a unique IP address. IMSVA incorporates the use of an Internal Communication Port to overcome this challenge.

- Users must specify one network interface card (NIC) as an Internal Communication Port to identify the IMSVA device during installation.
- After installation, users can change the Internal Communication Port on the IMSVA Web console through the Configuration Wizard or the command line interface (CLI).
- In a group scenario, parent devices and child devices must use their Internal Communication Port to communicate with each other. When registering a child device to parent device, the user must specify the IP address of the parent device's Internal Communication Port.

**Tip:** Trend Micro recommends configuring a host route entry on each IMSVA device of the group to ensure that parent-child communication uses the Internal Communication Port.

- IMSVA devices use the Internal Communication Port's IP address to register to Control Manager servers. When users want to configure IMSVA devices from the Control Manager Web console, the Web console service on the Internal Communication Port needs to be enabled. By default, the Web console service is enabled on all ports.

# Understanding POP3 Scanning

In addition to SMTP traffic, IMSVA 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 IMSVA 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, IMSVA 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 IMSVA server POP3 proxy, which connects to POP3 servers to retrieve and scan messages.

## Requirements for POP3 Scanning

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

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

- **IP address/Domain name**—The IMSVA IP address or domain name.
- **Port**—IMSVA 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 IMSVA IP address.
- **Port**—The IMSVA dedicated POP3 port.
- **Account**—`account_name@POP3_Server_Domain-name`

  for example: `user@domain.com`

# Opening the IMSVA Web Console

You can view the IMSVA 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:

https://{IMSVA}:8445

where {IMSVA} refers to the IP address or Fully Qualified Domain Name. For example: `https://196.168.10.1:8445` or `https://IMSVA1:8445`

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 logon credentials are as follows:

- Administrator user name: **admin**
- Password: **The password specified during installation**

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.

**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.

**Tip:** To prevent unauthorized changes to your policies, Trend Micro recommends changing the password regularly.

# Setting Up a Single Parent Device

IMSVA provides a configuration wizard to help you configure all the settings you need to get IMSVA up and running.

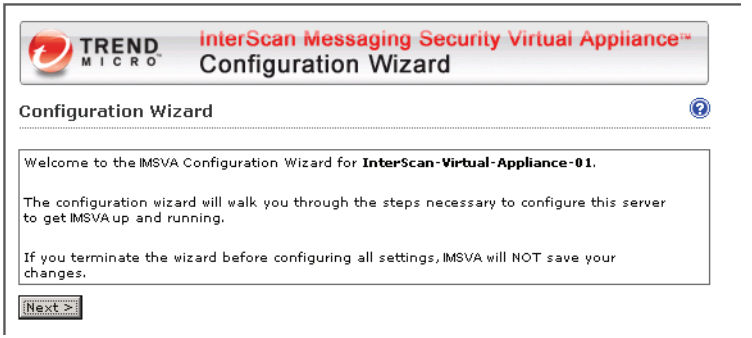
**To set up a single parent device:**

1. Make sure that your management computer can ping IMSVA's IP address that you configured during installation.
2. On the management computer, open Internet Explorer (version 6.0 or later) or Firefox (version 2.0 or later).
3. Type the following URL (accept the security certificate if necessary):

   ```
   https://<IP address>:8445
   ```

   The logon screen appears.
4. Select the **Open Configuration Wizard** check box.
5. Type the following default user name and password:
   - User name: **admin**
   - Password: **The password specified during installation**

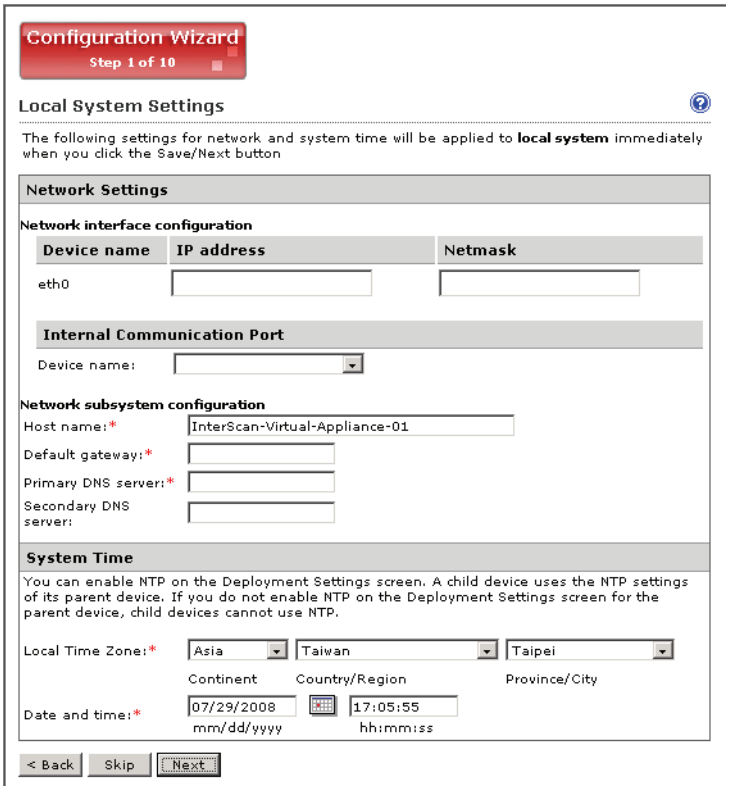
   The Configuration Wizard screen appears.




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

## Step 1: Configuring 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.

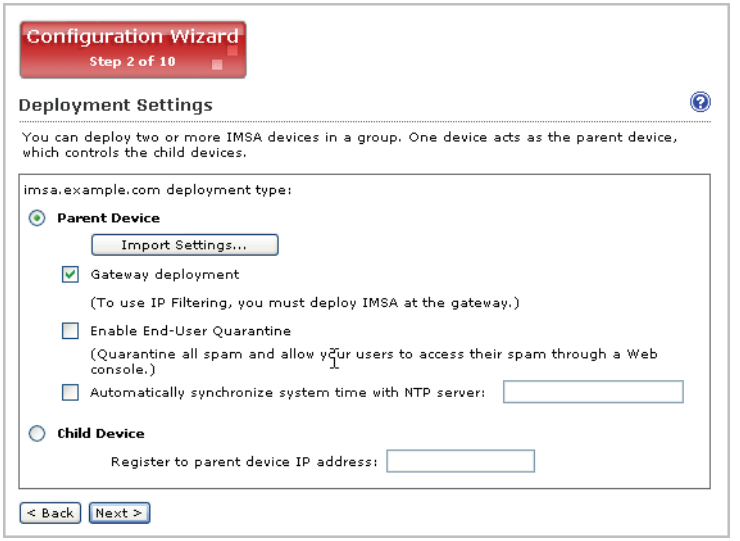
---

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

---

## Step 2: Configuring Deployment Settings

1. Click **Next**. The Deployment Settings screen appears.



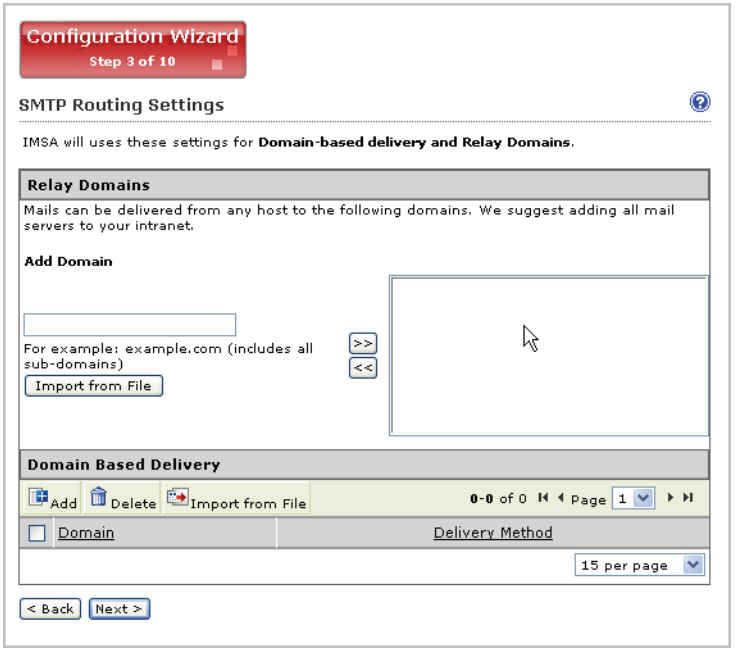

2. Select **Parent Device** or **Child Device**. If this is the first device you are setting up, you must select **Parent Device**. You can configure additional child devices at a later time.

   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 SMTP Routing Settings

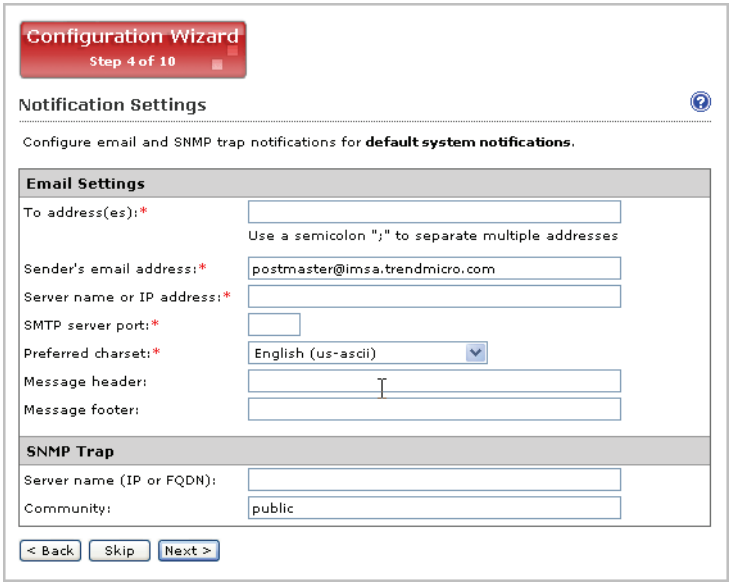
1. Click **Next**. The SMTP Routing Settings screen appears.




2. Add all SMTP server domains and their corresponding SMTP server names to the relay domain list. IMSVA needs this information to pass email to SMTP servers for delivery.

## Step 4: Configuring Notification Settings

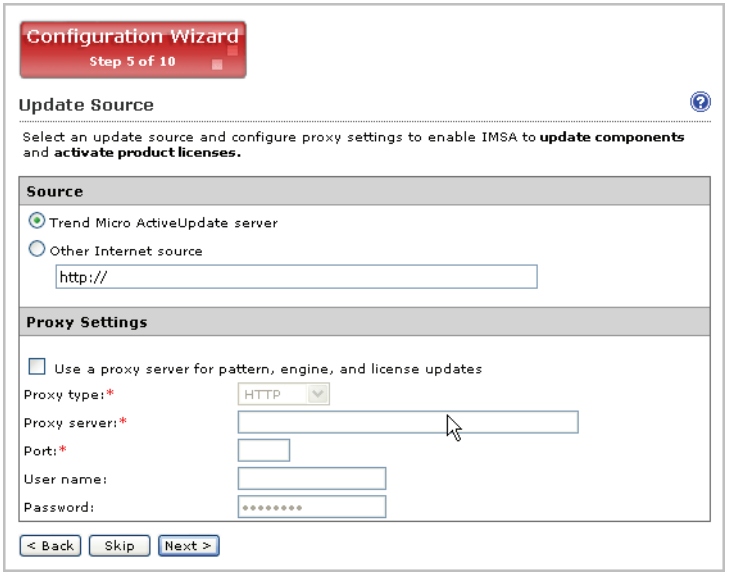
1. Click **Next**. The Notification Settings screen appears.




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

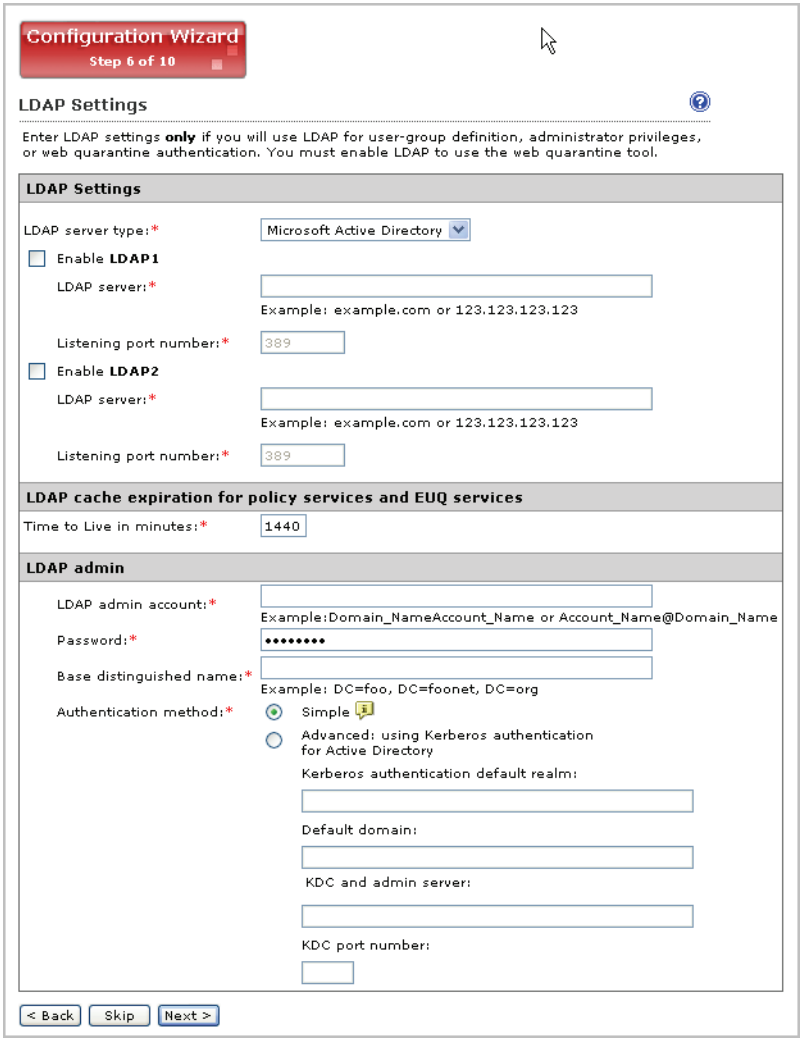
1. Click **Next**. The Update Source screen appears.




2. Configure the following update settings, which will determine from where IMSVA will receive its component updates and through which proxy (if any) IMSVA 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 LDAP Settings

1. Click **Next**. The LDAP Settings screen appears.



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 3-3 for a guide on what to specify for the LDAP admin settings.

| LDAP SERVER | LDAP ADMIN ACCOUNT (EXAMPLES) | BASE DISTINGUISHED NAME (EXAMPLES) | AUTHENTICATION METHOD |
|---|---|---|---|
| Active Directory | Without Kerberos:<br>user1@domain.com (UPN) or domain\user1<br>With Kerberos:<br>user1@domain.com | dc=domain, dc=com | Simple<br>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 3-3. LDAP admin settings**

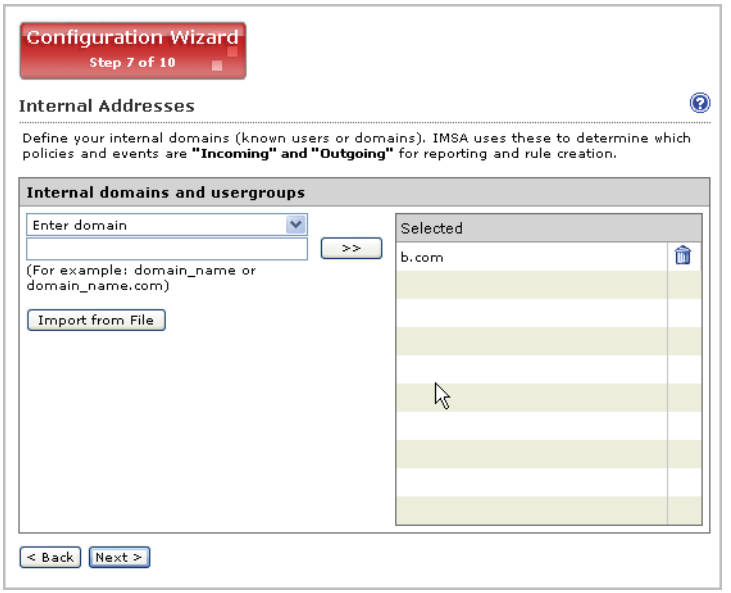
   f. For **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos

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 Internal Addresses

1. Click **Next**. The Internal Addresses screen appears.




2. IMSVA 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 IMSVA, do the following:
   a. Select **Enable TMCM Agent** (included with IMSVA 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.

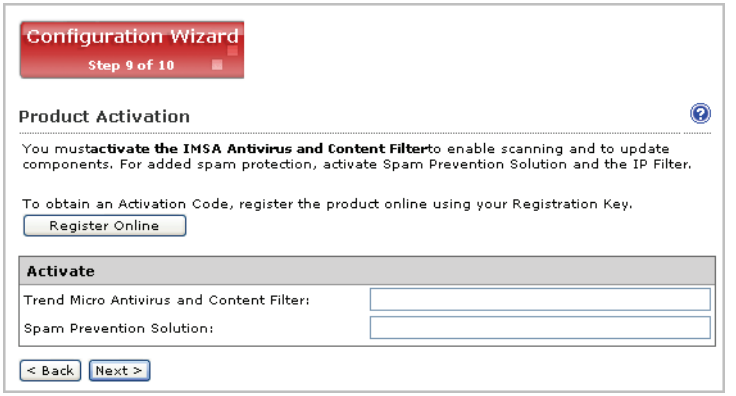
d. Under **Web server authentication**, type the user name and password for the Web server if it requires authentication.

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

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

## Step 9: Activating the Product

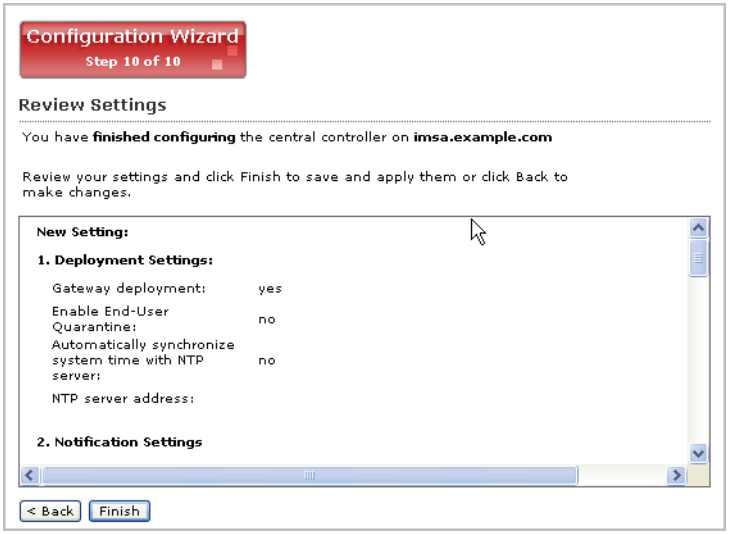
1. Click **Next**. The Product Activation screen appears. You must activate the Antivirus and Content Filter to enable scanning and security updates. If you want to scan email traffic for spam or use IP Filtering (NRS and IP Profiler), provide the SPS Activation Code.




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. IMSVA 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 3-16), 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 > IMSVA Configuration > Connections > Child IP**.

d. Under **Add IP Address**, add the IP address for the **Internal Communication Port** 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 IMSVA 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 IP address for the **Internal Communication Port** of the parent device.

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 mark  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:

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

d. Choose **Redistribute all** or **Only redistribute approved senders**. Trend Micro recommends choosing **Redistribute all**.

e. 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 IMSVA devices, the services should start automatically.

**To verify that IMSVA 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.

# Chapter 4

# Installing and Upgrading

This chapter explains how to install and upgrade IMSVA under different scenarios.

Topics include:

# Installing IMSVA

IMSVA only supports new installations — upgrading an existing IMSS or IMSA installation is not supported. IMSVA supports migrating existing configuration and policy data from previous InterScan messaging products.

The IMSVA installation process formats your existing system to install IMSVA. The installation procedure is basically the same for both a Bare Metal and a VMware ESX virtual machine platform. The Bare Metal installation boots off of the IMSVA installation CD to begin the procedure and the VMware installation requires the creation of a virtual machine before installation. The additional VMware virtual machine configuration is described in Appendix A, Creating a New Virtual Machine Under VMware ESX for IMSVA.

---

**WARNING!** **Any existing data or partitions are removed during the installation process. Back up any existing data on the system (if any) before installing IMSVA.**

---

### To install IMSVA:

1. Start the IMSVA installation:

   #### On a Bare Metal Server

   a. Insert the IMSVA Installation CD into the CD/DVD drive of the desired server.

   b. Power on the Bare Metal server.

   #### On a VMware ESX Virtual Machine

   ---

   **WARNING!** **If you install IMSVA on an ESX server, disable the snapshot feature for the virtual machine because the snapshot will exhaust hard disk space.**

   ---

   a. Create a virtual machine on your VMware ESX server

      See Appendix A, Creating a New Virtual Machine Under VMware ESX for IMSVA.

   b. Start the virtual machine.

c. Insert the IMSVA Installation CD into the virtual CD/DVD drive with any one of the following methods.

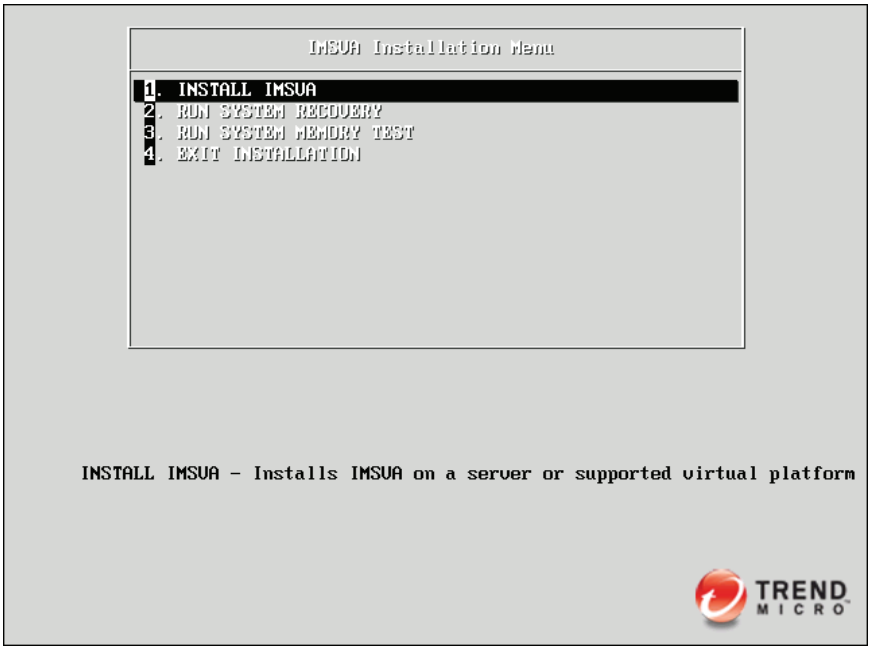
   - Insert the IMSVA Installation CD into physical CD/DVD drive of the ESX server, and then connect the virtual CD/DVD drive of the virtual machine to the physical CD/DVD drive.
   - Connect the virtual CD/DVD drive of the virtual machine to IMSVA-7.0.xxxx-1-i386-CD.iso file. The IMSVA-7.0.xxxx-1-i386-CD.iso file is available at:

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

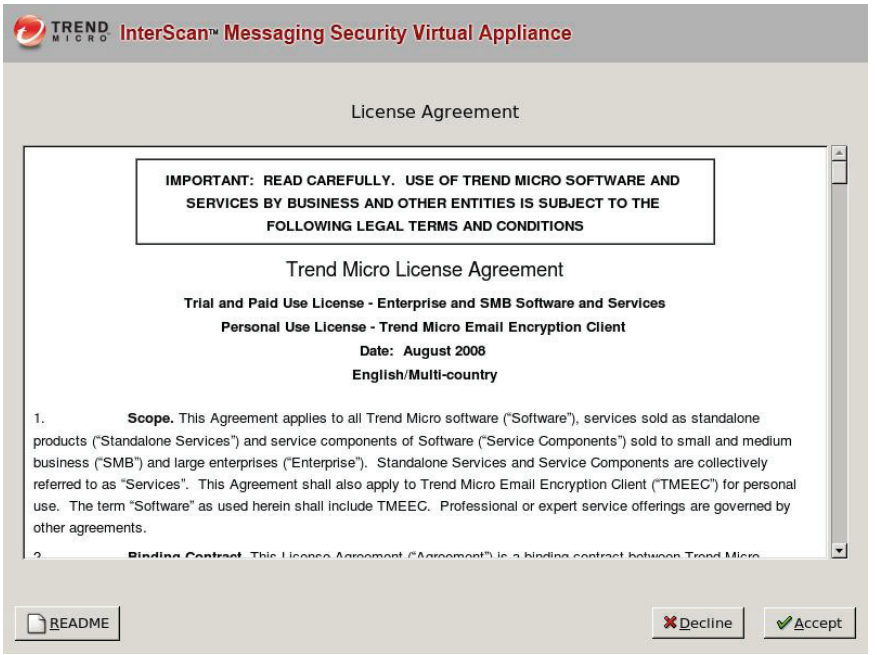
d. Restart the virtual machine by clicking **VM > Send Ctrl+Alt+Del** on the VMware Web console.

For both a **VMware ESX Virtual Machine** and a **Bare Metal Server** installations a page appears displaying IMSVA Installation Menu with the following options:

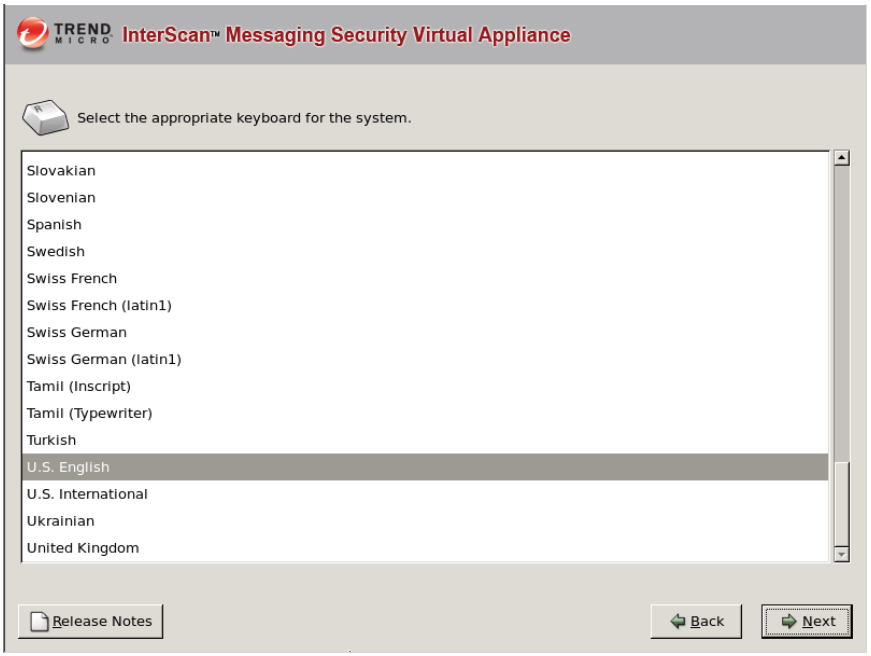
- **Install IMSVA**: Select this option to install IMSVA onto the new hardware or virtual machine
- **System Recovery**: Select this option to recover an IMSVA system in the event that the administrative passwords cannot be recovered.
- **System Memory Test**: Select this option to perform memory diagnostic tests to rule out any memory issues
- **Exit Installation**: Select this option to exit the installation process and to boot from the local disk.




2. Select **Install IMSVA**. The license acceptance page appears. From this page, you can access the readme (**Readme** button).

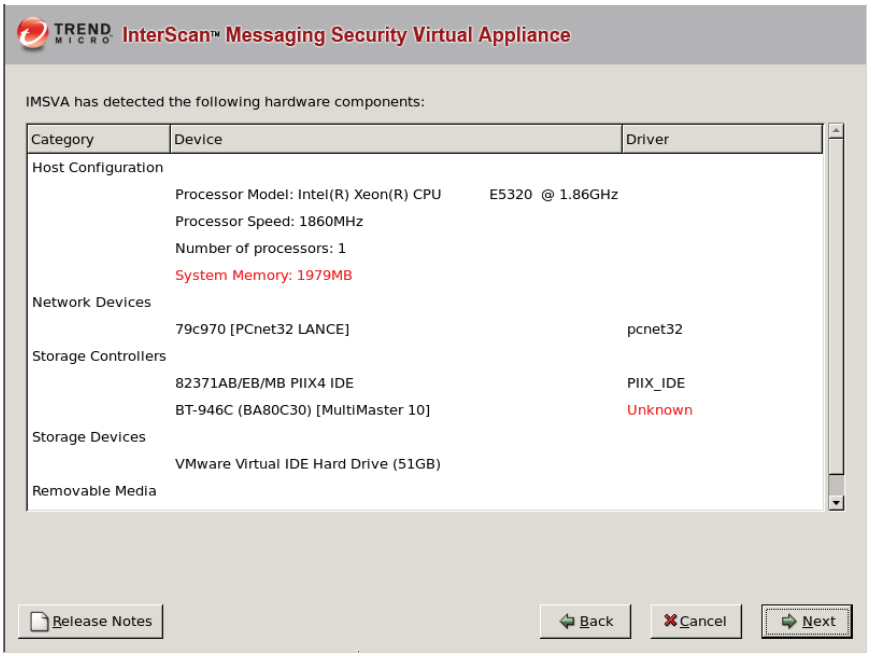



**3.** Click **Accept** to continue. A page appears where you choose the keyboard language.

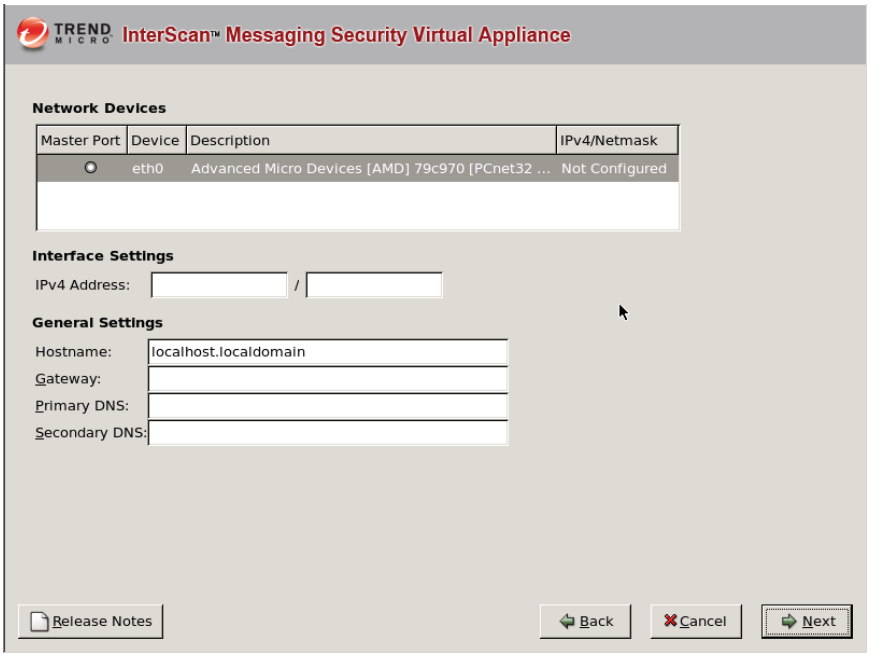



4. Select the keyboard language for the system and then click **Next**.

   The IMSVA installer scans your hardware to determine if the minimum specifications have been met and displays the results as illustrated below. If the host hardware contains any components that do not meet the minimum specifications, the installation program will highlight the non-conforming components and the installation will stop.




5. Click **Next**. The IMSVA installer detects hard disk drives and displays all available hard disk drives. At least one drive must be selected for IMSVA installation.
6. Select the drive(s) for IMSVA installation and then click **Next**. The Network Settings screen appears.




The table below describes the information required.

**TABLE 4-1. Deployment Option 1: Transparent Bridge Mode**

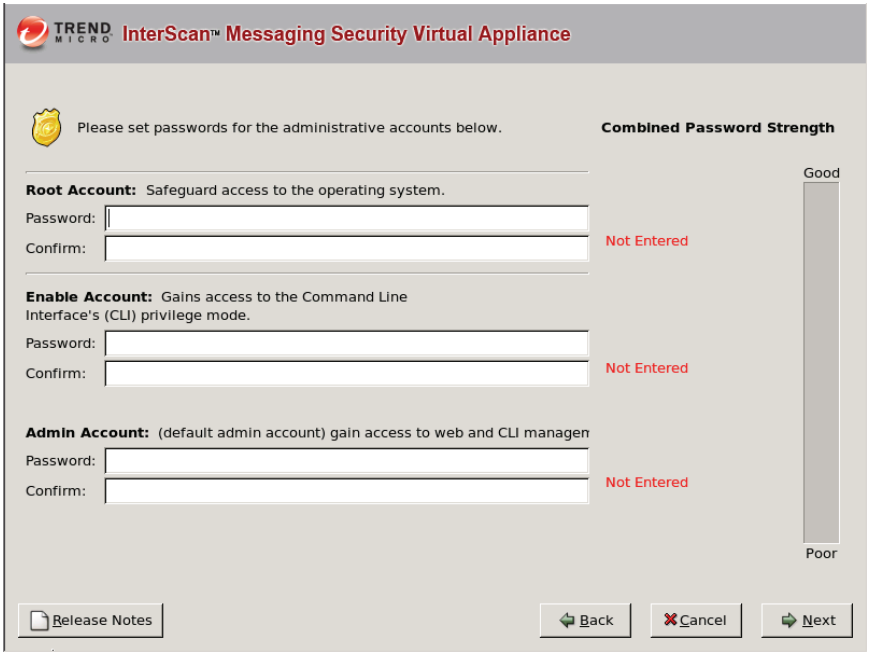
| CONFIGURATION PARAMETER | DESCRIPTION |
|---|---|
| IPv4 Address | This is the IP address of the IMSVA management interface. Type in the IP address and appropriate subnet mask to complete the configuration. |
| Hostname | Type in the applicable FQDN hostname for this IMSVA host. |
| Gateway | Type in the applicable IP address to be used as the gateway for this IMSVA installation. |

**TABLE 4-1. Deployment Option 1: Transparent Bridge Mode**

| CONFIGURATION PARAMETER | DESCRIPTION |
|---|---|
| Primary DNS | Type in the applicable IP address to be used as the primary DNS server for this IMSVA installation. |
| Secondary DNS | Type in the applicable IP address to be used as the secondary DNS server for this IMSVA installation. |
| Internal Interface | Select which network adapter should be used for the internal connection of the transparent bridge. |
| External Interface | Select which network adapter should be used for the external connection of the transparent bridge. |

7. Provide all the information to install IMSVA, and click **Next**. The NTP settings screen appears.


8. Specify the IMSVA server's time and clock settings
   a. Select the location of the IMSVA server.
   b. Specify whether the server's system clock uses UTC or GMT by selecting or clearing the **System clock uses UTC** checkbox.
9. Click **Next**. The Account Settings screen appears.




**10.** Specify passwords for the root, enable, and admin accounts.

IMSVA uses three different levels of administrator types to secure the system.

The password must be a minimum of 6 characters and a maximum of 32 characters.

---

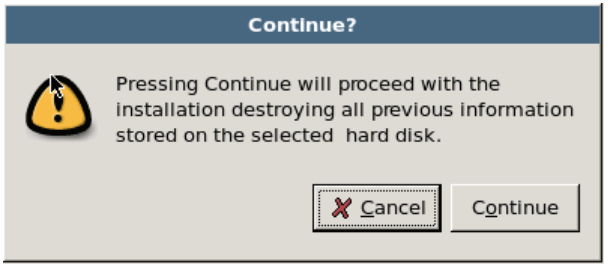
**Tip:** For the best security, create a highly unique password only known to you. You can use both upper and lower case alphabetic characters, numerals, and any special characters found on your keyboard to create your passwords.

---

- **Root Account:** Used to gain access to the operating system shell and has all rights to the server. This is the most powerful user on the system.
- **Enable Account:** Used to gain access to the command line interface's privilege mode. This account has all rights to execute any CLI command.
- **Admin Account:** The default administration account used to access the IMSVA Web and CLI management interfaces. It has all rights to the IMSVA application, but no access rights to the operating system shell.

As you type the passwords, the password strength meter on the right indicates how strong the selected password is.

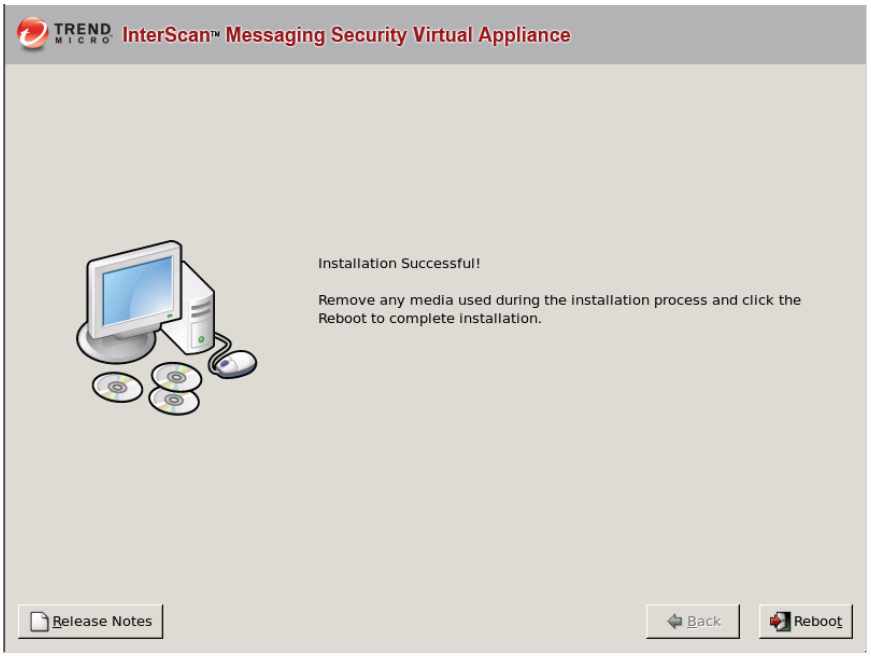
11. Click **Next**. The Review Settings screen appears.
12. Confirm that the selected values are correct and then click **Next**. The installation process prompts you to begin the installation.




Selecting **Continue** erases any data on the hard disk partition and formats the hard disk. If you have data on the hard disk that you would like to keep, cancel the installation and back up the information before proceeding.

13. Click **Continue**. A screen appears that provides the formatting status of the local drive for the IMSVA installation. When formatting completes, the IMSVA installation begins.


Once the installation is complete a summary screen appears. The installation log is saved in the `/root/install.log` file for reference.




14. Click **Reboot** to restart the system.

    **Bare Metal installation:**

    The CD automatically ejects. Remove the CD from the drive to prevent reinstallation.

    **Virtual machine installation:**

    Trend Micro recommends disconnecting the CD-ROM device from the virtual machine now that IMSVA is installed.

    After IMSVA reboots, the initial CLI login screen appears.

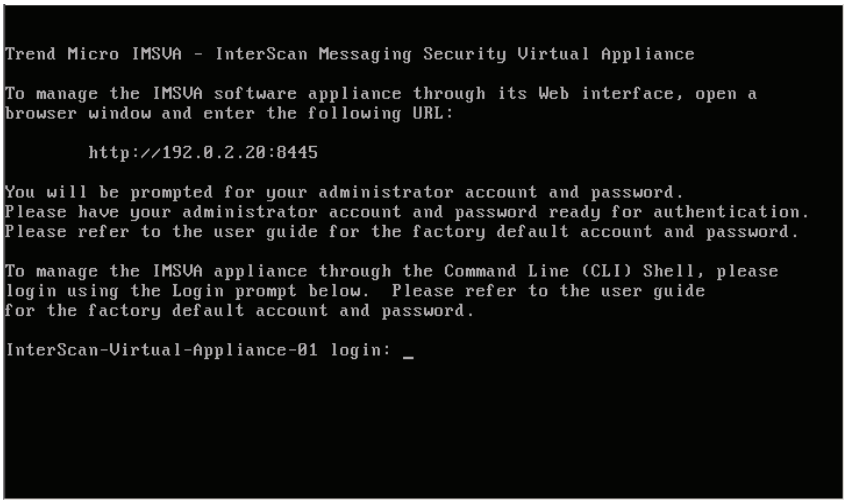



**FIGURE 4-1 The initial CLI login screen**

---

**Note:** During installation, you may receive the following messages:

```
for crash kernel (0x0 to 0x0) notwhitin permissible range
powernow-k8: bios error -no psb or acpi_pss objects
```

Both of these messages are normal. The latter message indicates that the system BIOS is not reporting or presenting any PSB or ACPI objects or hooks to the Linux kernel. Either the CPU or BIOS does not support PSB or ACPI objects or hooks, or they are simply disabled.

---

**15.** Log on either in the CLI or in the IMSVA Web console to launch IMSVA.

Log on to the CLI shell if you need to perform additional configuration, troubleshooting, or housekeeping tasks.

# Upgrading from an Evaluation Version

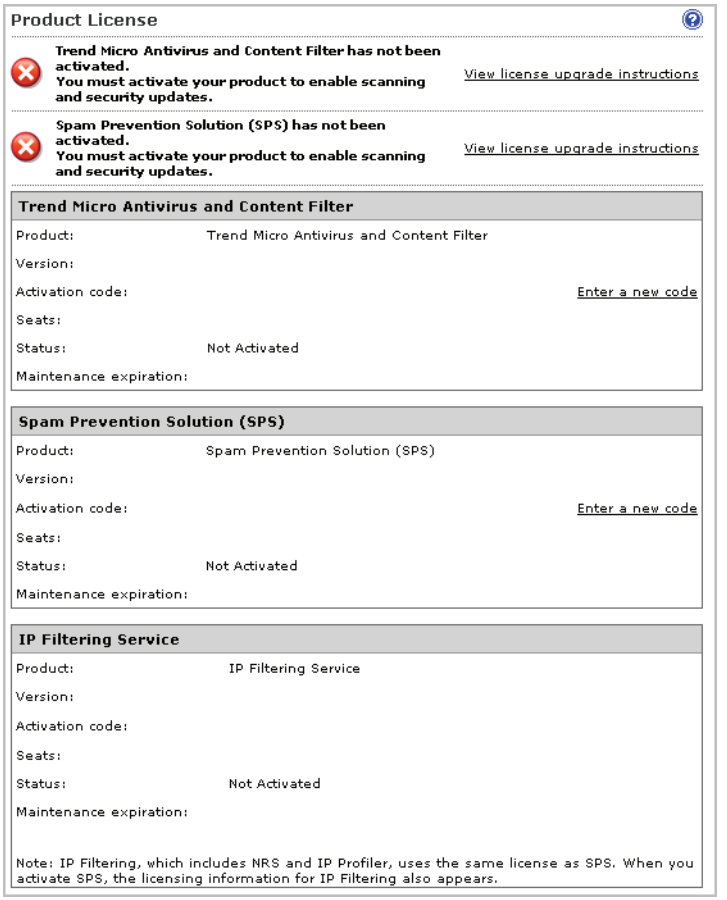
If you provided an evaluation Activation Code to activate IMSVA previously, you have started an evaluation period that allows you to try the full functionality of the product. The evaluation period varies depending on the type of Activation Code used.

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

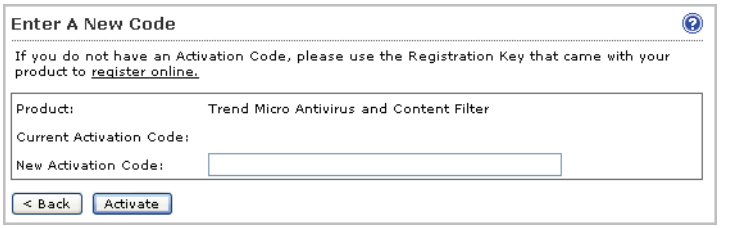
To continue using IMSVA, please purchase the full licensed product. You will then be assigned a new licensed Activation Code.

**To upgrade from the evaluation period:**

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




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




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

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

4. Click **Activate**.

# Import/Export Notes

To reuse settings from InterScan Messaging Security Appliance (IMSA) or InterScan Messaging Security Suite (IMSS) in InterScan Messaging Security Virtual Appliance 7.0, you need to export the original settings from the previous versions before performing the upgrade. Then importing these settings after the upgrade.

The configuration and policy information for the following InterScan family of products can be migrated to IMSVA 7.0:

- IMSS 5.7 Linux
- IMSS 5.7 Windows
- IMSS 5.7 Solaris
- IMSA 7.0 SP1

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 InterScan Messaging Security Virtual Appliance 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 InterScan Messaging Security Appliance or InterScan Messaging Security Virtual Appliance 7.0.

Trend Micro strongly suggests:

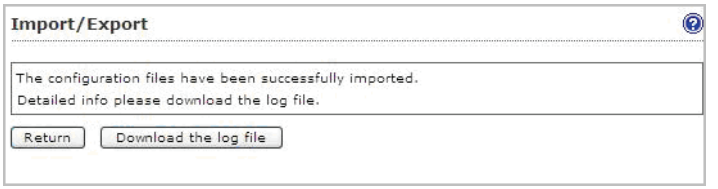
- Adjusting the component list and child device registration information after import if necessary.
- Backing up a copy of current configuration before each import operation, in order to recover from mistaken import processes.
- Performing import/export when IMSVA is idle because importing and exporting affects IMSVA performance.

## Importing Settings

To reuse the original configuration settings from IMSVA 1.0 or InterScan Messaging Security Suite 5.7 after upgrading to IMSVA 7.0, import the configuration files that you have backed up previously.

**To import device configuration files:**

1. Log on to the IMSVA 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 IMSVA 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.

If the import fails, the configuration will roll back to the original settings before the import.

## Settings that Cannot be Migrated

IMSVA will not migrate the following settings:

**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 types in the advanced content filter
- Actions for "Archive Original"
- Notifications with original mail attachments
- Forwarding original email message attachments

NRS Settings

All NRS settings cannot be migrated.

# Migrating from InterScan Messaging Security Suite 5.7 to IMSVA 7.0

If you want to reuse your policy settings from InterScan Messaging Security Suite 5.7 (Linux, Solaris, or Windows), you must first export the settings into a file. Thereafter, you can import the file into IMSVA 7.0 (see Importing Settings on page 4-19).

## Exporting from InterScan Messaging Security Suite 5.7 Linux

**To export from InterScan Messaging Security Suite 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 InterScan Messaging Security Suite 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 InterScan Messaging Security Suite 5.7 Solaris:

**To export from InterScan Messaging Security Suite 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 InterScan Messaging Security Suite 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 InterScan Messaging Security Suite 5.7 Windows

**To export from InterScan Messaging Security Suite 5.7 Windows:**

1. Upload `IMSS_5.7_Windows_GM_Export_Tool.zip` to your InterScan Messaging Security Suite 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 InterScan Messaging Security Suite 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 InterScan Messaging Security Suite 5.7

IMSVA 7.0 will only migrate certain policy settings from InterScan Messaging Security Suite 5.7. All other settings will not be migrated. The following policy settings cannot migrate:

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 types in the advanced content filter
- Actions for "Archive Original"
- Notifications with original mail attachments
- Forwarding original email message attachments

# Chapter 5

# Troubleshooting, FAQ, and Support

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

Topics include:

# Troubleshooting

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

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

## Troubleshooting Utilities

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

**TABLE 5-1. Installation Troubleshooting issues**

| ISSUE | SUGGESTED RESOLUTION |
|---|---|
| The NRS installation does not validate the NRS Activation Code | To validate the Activation Code, the NRS installation script accesses Trend Micro through the Internet.<br><br>Verify that your DNS server is operating correctly and that the computer on which you are installing NRS has access to the Internet. |
| Devices in a group cannot communicate | If several IMSVA devices are deployed in a group, they must communicate with each other. Verify that the following ports are accessible on all devices:<br>• 5060—Policy service<br>• 15505—IMSVA control service<br>• 53 UDP/TCP—IP Profiler<br>• 5432—Database service<br>• 8009—EUQ internal service<br>Also, verify the following:<br>• The current firewall settings in “iptables”.<br>• The firewall configuration files in /etc/conf/fw.rules.<br>• 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.<br>Also, verify that all the necessary port IMSVA uses are accessible for the relevant services. |

**TABLE 5-1. Installation Troubleshooting issues**

| ISSUE | SUGGESTED RESOLUTION |
|---|---|
| Child device has trouble registering to a parent | Do the following:<br>1. Open the parent device's Web console and choose **Administration > IMSVA Configuration > Connections > Child IP**.<br>2. Verify that the IP address of the child is on the Child IP Address List.<br>3. In the Configuration Wizard, verify that **Child** is selected for the device role.<br>4. Verify that the Admin Database is accessible.<br>5. Unregister the Control Manager agent (if TMCM agent is enabled).<br>6. Verify that no other child device registered to the parent has the same IP address as the device you are trying to register.<br>7. Remove all the logs and quarantined messages.<br>8. Change the configuration and restart the services.<br><br>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:<br>`/opt/trend/imss/script/cfgtool reg IPADDR sa postgreSQL` |
| Child device has trouble unregistering from the parent | Do the following:<br>1. Connect to the child device through the command line interface.<br>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.<br>3. Rescue the device, which will forcibly unregister it from the parent.<br>4. Update the patches.<br>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.<br><br>You can also run the following command:<br>/opt/trend/imss/script/cfgtool.sh dereg |

# Frequently Asked Questions

## Postfix MTA Settings

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

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

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

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

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

**Note:** "{Parameter1:{Parameter2}:…::{Parameter n}" means you can use one or more parameters by separating them using colons.

**WARNING! Use extreme caution when modifying the configuration file.**

## Importing and Exporting

### Will all IMSA 1.0 or InterScan Messaging Security Suite 5.7 settings be retained during migration?

No. Due to architectural changes in IMSVA 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.

## 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

# Appendix A

# Creating a New Virtual Machine Under VMware ESX for IMSVA

This appendix describes how to create a new virtual machine for IMSVA.

Topics include:

# Creating a New Virtual Machine

The actual installation of ESX 3.5.0 is not covered in this document. Please refer to VMware's product documentation to install this product.

The steps outlined below detail the process to create a new virtual machine under VMware ESX to install IMSVA. Please use the following steps as a guideline for creating the virtual machine for your environment. The number of CPUs, NIC cards, memory and hard disk space selected should reflect the requirements for your deployment. The values entered here are for instructional purposes.

**To create the virtual machine:**

1. From the menu bar, select **File > New > Virtual Machine**. The New Virtual Machine Wizard appears.

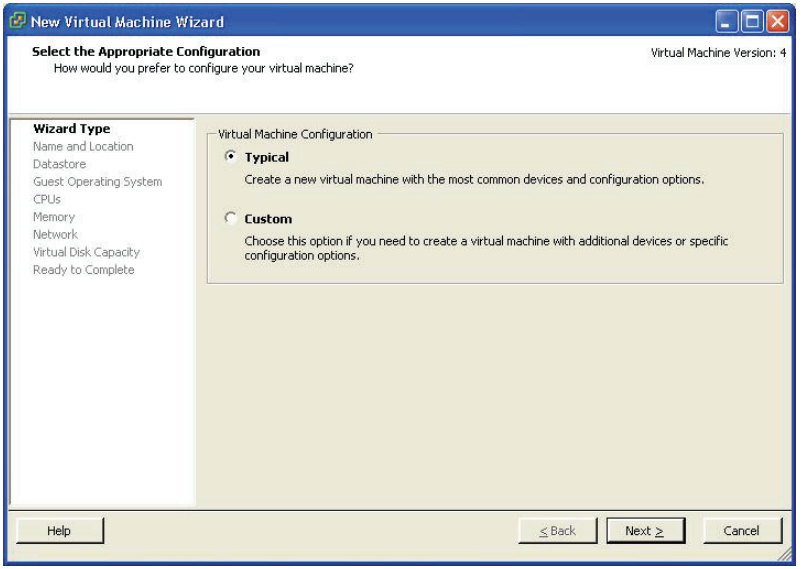



**FIGURE A-1 Virtual Machine Configuration**

2. Under **Virtual Machine Configuration**, leave the **Typical** radio button selected.
3. Click **Next**. The Select a Name and Location for this Virtual Machine page appears.

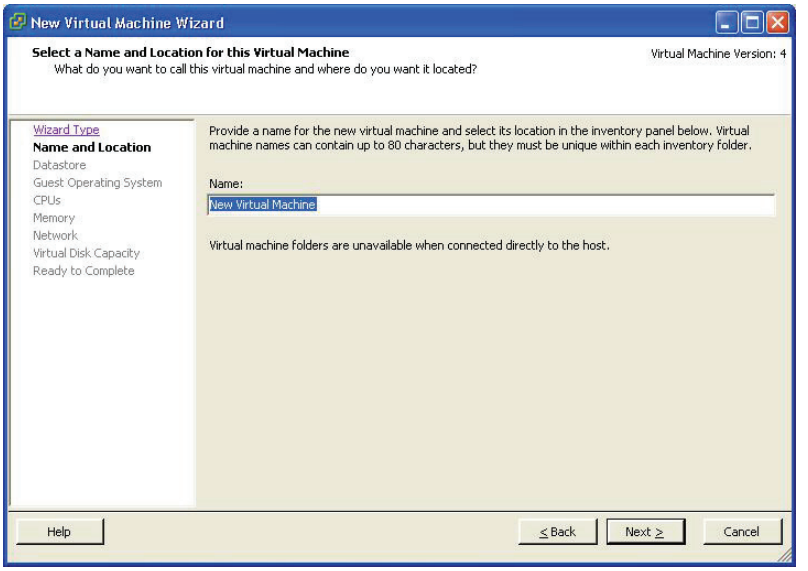



**FIGURE A-2 Select a Name and Location for this Virtual Machine**

4. In the **Name** field, type an appropriate machine name and then click **Next**. The Choose a Datastore for the Virtual Machine page appears.

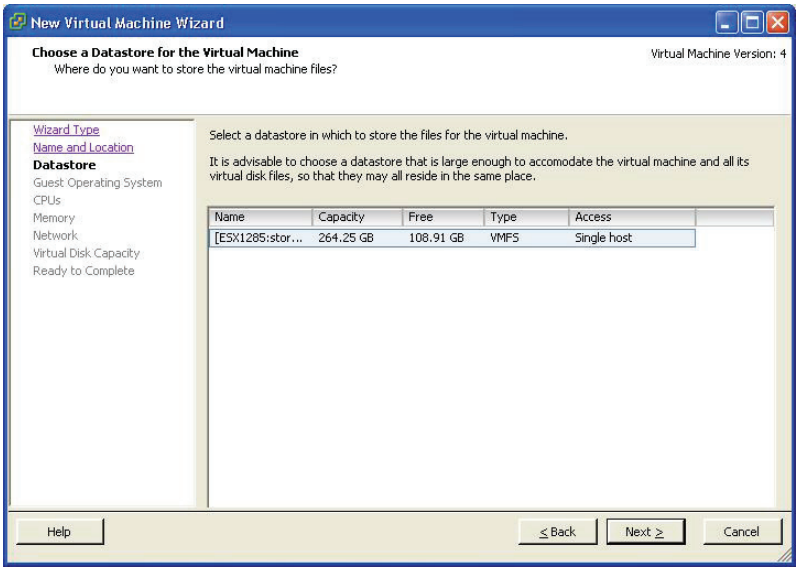



**FIGURE A-3 Virtual Machine Datastore**

5. Select the datastore where the virtual machine will reside.
6. Click **Next**. The Choose the Guest Operating System page appears.

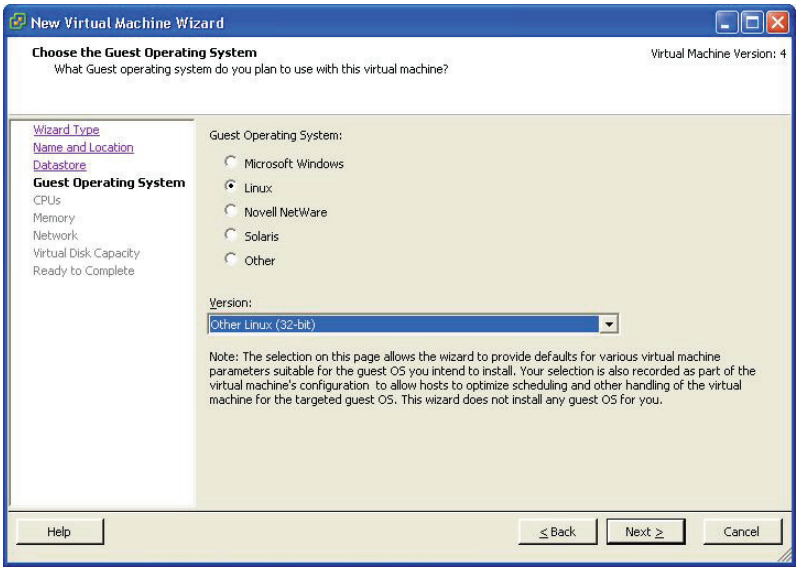



**FIGURE A-4 Virtual Machine Guest Operating System**

7. For the guest operating system, select **Linux > Other Linux (32-bit)**.
8. Click **Next**. The Virtual CPUs screen appears.

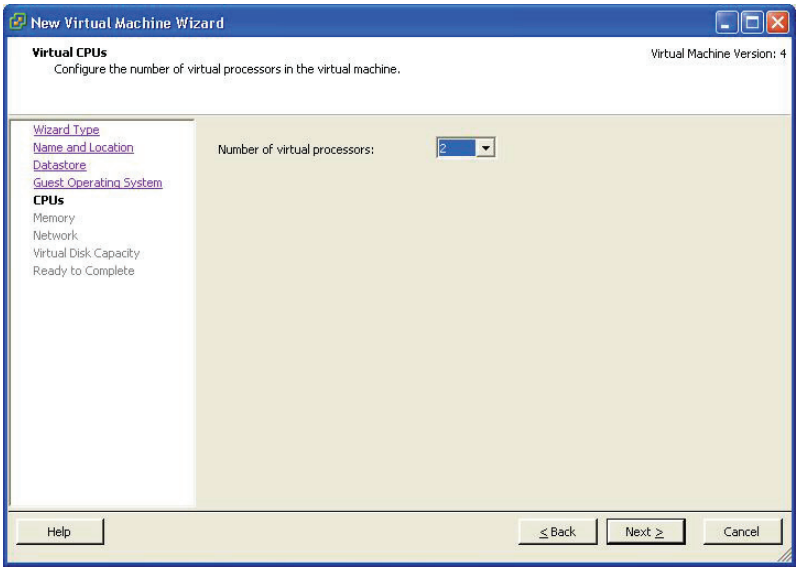



**FIGURE A-5 Virtual Machine CPU**

9. Select the number of processors for the virtual machine. IMSVA takes advantage of the Virtual SMP, so select the maximum number of virtual processors available.
10. Click **Next**. The Memory screen appears.

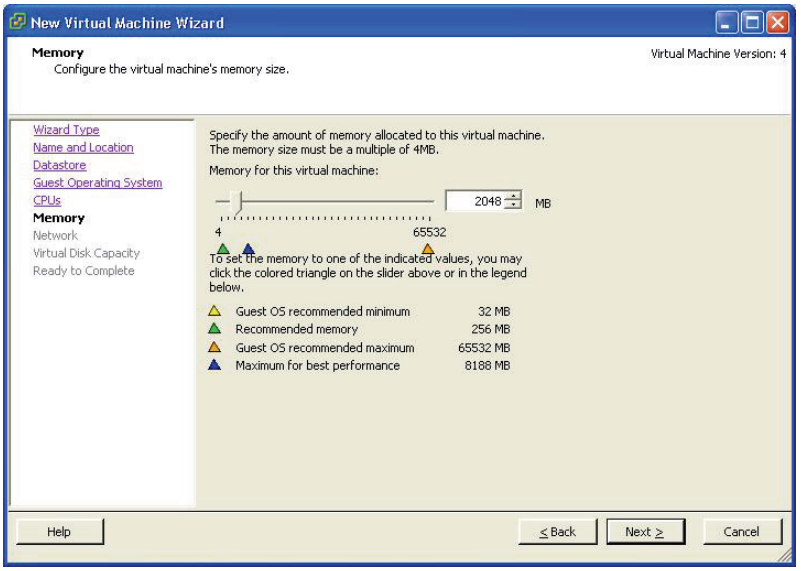



**FIGURE A-6 Virtual Machine Memory**

**11.** Allocate 2048MB of memory as a minimum for IMSVA.

**Tip:** For improved performance, Trend Micro recommends at least 4096MB of RAM.

**12.** Click **Next**. The Choose Networks screen appears.

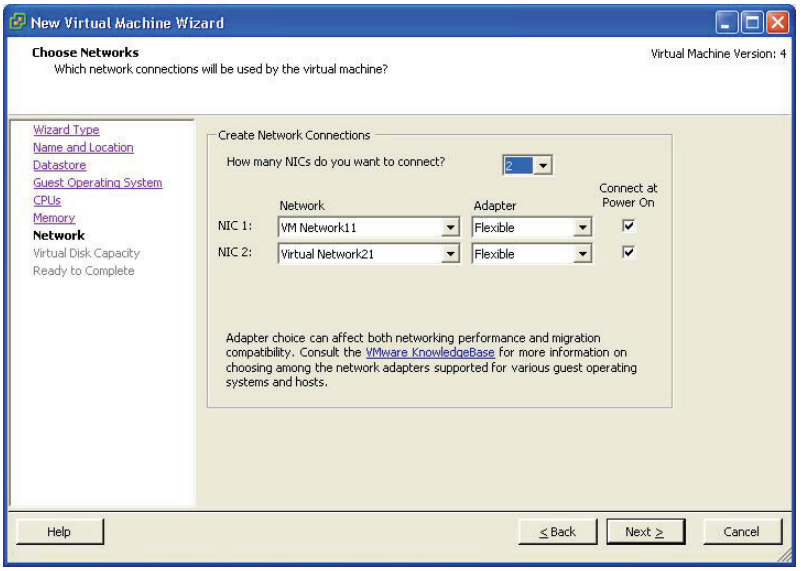



**FIGURE A-7 Virtual Machine Network**

13. Accept the default network settings and then click **Next**. The Define Virtual Disk Capacity screen appears.

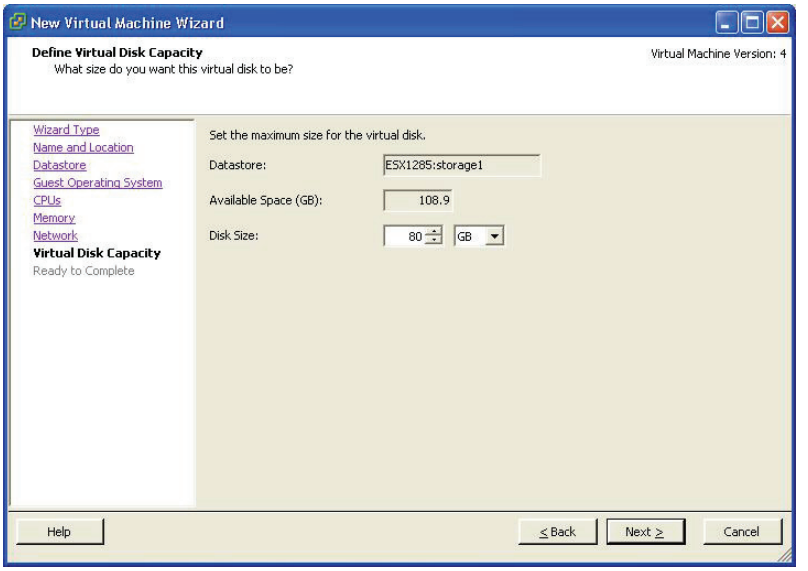



**FIGURE A-8 Virtual Disk Capacity**

14. IMSVA requires at least 80GB disk space. See System Requirements on page 2-2 for more information on disk space allocation.

---

**Tip:** Trend Micro recommends 250GB or more of disk space for message quarantine and logging purposes.

---

15. Click **Next**. The Ready to Complete New Virtual Machine screen appears.

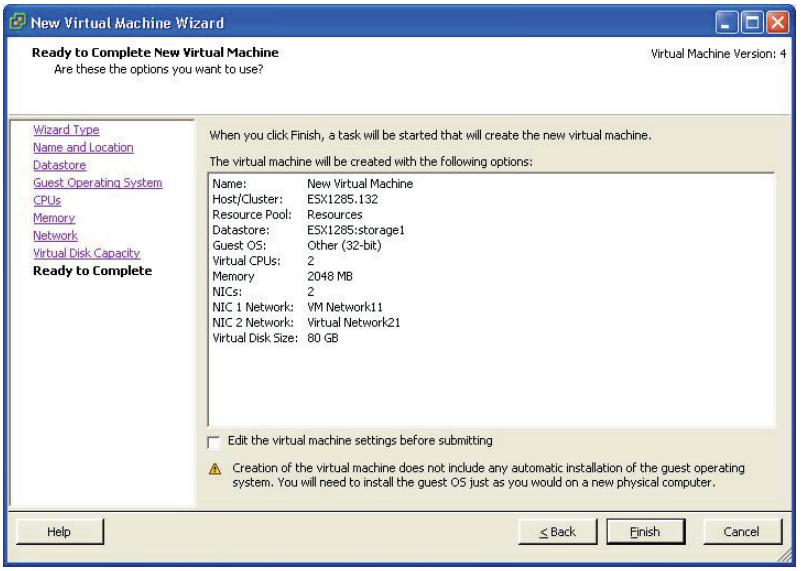



**FIGURE A-9 Ready to Complete**

16. Click **Continue**. If you want to modify the system component settings, check the **Edit the virtual machine settings before submitting** check box and then click **Continue**.
17. Verify your settings and then click **Finish**. The new Virtual Machine is now ready and configured to be powered on and begin the installation process.

# Index