



8.5 InterScan™ Messaging Security Virtual Appliance

Installation Guide

Hybrid SaaS Email Security



Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, please review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

<http://docs.trendmicro.com/en-us/enterprise/interscan-messaging-security.aspx>

Trend Micro, the Trend Micro t-ball logo, Control Manager, eManager, InterScan, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

© 2014. Trend Micro Incorporated. All Rights Reserved.

Document Part No.: MSEM85912/130322

Release Date: May 2014

Protected by U.S. Patent No.: Patents pending

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Preface	v
What's New	vi
Audience	xiii
InterScan Messaging Security Virtual Appliance Documentation	xiii
Document Conventions	xiv

Chapter 1: Introducing InterScan Messaging Security Virtual Appliance

About InterScan Messaging Security Virtual Appliance	1-2
IMSVa Main Features and Benefits	1-2
About Cloud Pre-Filter	1-10
About Email Encryption	1-10
About Spyware/Grayware	1-10
How Spyware/Grayware Gets into your Network	1-11
Potential Risks and Threats	1-11
About Trend Micro Control Manager	1-12
Control Manager Support	1-13
About Trend Micro Smart Protection	1-15
The Need for a New Solution	1-16
Trend Micro Smart Protection Network	1-17
About Command & Control (C&C) Contact Alert Services	1-17

Chapter 2: Component Descriptions

About IMSVA Components	2-2
Cloud Pre-Filter Service Overview	2-2
Sender Filtering	2-2

Reputation-Based Source Filtering	2-2
Virus and Spam Protection	2-2
About Spam Prevention Solution	2-3
Spam Prevention Solution Technology	2-3
Using Spam Prevention Solution	2-3
IP Filtering	2-3
How IP Profiler Works	2-4
Email Reputation	2-5
Types of Email Reputation	2-5
How Email Reputation Technology Works	2-6
About End-User Quarantine (EUQ)	2-7
About Centralized Reporting	2-8

Chapter 3: Planning for Deployment

Deployment Checklist	3-2
Network Topology Considerations	3-5
IMSVa Deployment with Cloud Pre-Filter	3-6
Deployment at the Gateway or Behind the Gateway	3-6
Installing without a Firewall	3-9
Installing in Front of a Firewall	3-10
Installing Behind a Firewall	3-11
Installing in the De-Militarized Zone	3-12
About Device Roles	3-13
About Device Services	3-13
Service Selection	3-14
Deployment with IP Filtering	3-14
Understanding Internal Communication Port	3-14
Understanding POP3 Scanning	3-15
Requirements for POP3 Scanning	3-16
Configuring a POP3 Client that Receives Email Through IMSVA	3-16
Opening the IMSVA Management Console	3-17

Setting Up a Single Parent Device	3-18
Step 1: Configuring System Settings	3-19
Step 2: Configuring Deployment Settings	3-21
Step 3: Configuring SMTP Routing Settings	3-22
Step 4: Configuring Notification Settings	3-24
Step 5: Configuring the Update Source	3-25
Step 6: Configuring LDAP Settings	3-26
Step 7: Configuring Internal Addresses	3-29
Step 8: Configuring Control Manager Server Settings	3-31
Step 9: Activating the Product	3-33
Step 10: Reviewing the Settings	3-34
Setting Up a Child Device	3-35
Verifying Successful Deployment	3-36

Chapter 4: Installing IMSVA 8.5

System Requirements	4-2
Additional Requirements and Tools	4-3
Installing IMSVA	4-5

Chapter 5: Upgrading from Previous Versions

Upgrading from an Evaluation Version	5-2
Upgrading from IMSVA 8.2 Service Pack 2	5-4
Upgrading a Single IMSVA	5-5
Upgrading a Distributed Environment	5-8
Batch Upgrade	5-10
Offline Upgrade	5-23
Verifying the Upgrade Using SSH	5-28
Rolling Back an Upgrade	5-28
Migrating from Previous Versions	5-29
Migration Process	5-29
Migrating from IMSS for Windows	5-32
Migrating from IMSS for Linux	5-33
Migrating from IMSVA 8.0 Patch 2 or IMSVA 8.2 Service Pack 2	5-34

Exporting Debugging Files	5-35
---------------------------------	------

Chapter 6: Troubleshooting and Support Information

Troubleshooting	6-2
Troubleshooting Utilities	6-2
Installation Troubleshooting Issues	6-3
Support Information	6-5
Troubleshooting Resources	6-5
Contacting Trend Micro	6-7
Sending Suspicious Content to Trend Micro	6-8
Other Resources	6-9

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

Creating a New Virtual Machine	A-2
--------------------------------------	-----

Appendix B: Creating a New Virtual Machine Under Microsoft Hyper-V for IMSVA

Understanding Hyper-V Installation	B-2
IMSVA Support for Hyper-V	B-2
Hyper-V Virtualization Modes	B-2
Installing IMSVA on Microsoft Hyper-V	B-2
Creating a Virtual Network Assignment	B-3
Creating a New Virtual Machine	B-6
Using Para-Virtualization Mode	B-18
Using NTP on IMSVA	B-21

Index

Index	IN-1
-------------	------

Preface

Preface

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

Refer to the IMSVA 8.5 Administrator's Guide for information on how to configure IMSVA settings and the Online Help in the management console for detailed information on each field on the user interface.

What's New

IMSV A 8.5 New Features

The following table provides an overview of new features available in IMSVA 8.5.

TABLE 1. IMSVA 8.5 New Features

NEW FEATURE	DESCRIPTION
Command & Control (C&C) Contact Alert Services	Command & Control (C&C) Contact Alert Services provides IMSVA with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.
Smart Scan	Smart Scan facilitates a more efficient scanning process by offloading a large number of threat signatures previously stored on the IMSVA server to the cloud.
SMTP authentication support for End-User Quarantine	SMTP authentication provides users another option for enabling the End-User Quarantine feature.
Web Reputation enhancement	The Web Reputation filter has been enhanced to enable detection of URLs that have not been rated by Trend Micro. This functionality helps increase protection against advanced threats that leverage short-lived malicious websites.

IMSV A 8.2 Service Pack 2 New Features

The following table provides an overview of new features available in IMSVA Service Pack 8.2.

TABLE 2. IMSVA 8.2 Service Pack 2 New Features

NEW FEATURE	DESCRIPTION
Advanced anti-malware protection	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks.

NEW FEATURE	DESCRIPTION
Integration with Deep Discovery Advisor	Trend Micro™ Deep Discovery Advisor is a separately licensed product that provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. IMSVA integrates with the Virtual Analyzer in Deep Discovery Advisor.
Distribution list End-User Quarantine (EUQ) management	The web-based EUQ service also allows end-users to manage the spam quarantine of distribution lists that they belong to.
EUQ digest inline action links	IMSVA enables users to apply actions to quarantined messages through links in the EUQ digest.

IMSVA 8.2 New Features

The following table provides an overview of new features available in IMSVA 8.2.

TABLE 3. IMSVA 8.2 New Features

NEW FEATURE	DESCRIPTION
Email encryption	<p>Trend Micro Email Encryption integrates with IMSVA to protect sensitive email content by encrypting inbound and outbound email messages according to specific policies.</p> <p>IMSVA can also scan encrypted messages for threats.</p> <p>IMSVA provides reports and notifications to monitor encrypted email traffic.</p>
Multiple LDAP server support	IMSVA supports using more than one LDAP server and has support for more LDAP server types.
Dashboard and widgets	<p>Real-Time summaries have been replaced with a dashboard and widgets. This will provide administrators with more flexibility when viewing IMSVA data.</p> <p>The System Summary has been renamed "System Status" and appears in the left menu.</p>

NEW FEATURE	DESCRIPTION
Regulatory compliance support	IMSVa provides support for regulatory compliance in policies.
Expanded platform support	IMSVa can now be installed on Hyper-V platforms.
Cloud Pre-Filter enhancements	<p>Cloud Pre-Filter now supports protection against directory harvest attacks (DHA).</p> <p>Accounts other than the "admin" account can be granted access to Cloud Pre-Filter</p>
Expanded Control Manager support	IMSVa now supports registering to Control Manager 5.5.
Microsoft Hyper-V support	IMSVa now supports installation on Microsoft Hyper-V.
EUQ enhancement	EUQ now supports single sign-on with Kerberos and synchronized messages with Cloud Pre-Filter.
New migration Tools	New tools have been provided to help customers migrating from previous product versions.


IMSVa 8.0 New Features

The following table provides an overview of new features available in IMSVa 8.0.

TABLE 4. IMSVa 8.0 New Features

NEW FEATURE	DESCRIPTION
Cloud Pre-Filter	Cloud Pre-Filter is a hosted email security service that can filter all of your email messages before they reach your network. Pre-filtering your email messages can save you time and money.
Smart Search Text Box	Allows users to quickly navigate to screens on the web console by typing the name of the screen or feature in the Smart Search text field.

NEW FEATURE	DESCRIPTION
Common Policy Objects	<p>Several information objects that can be used by policies have been removed from policy creation and given their own areas for configuration:</p> <ul style="list-style-type: none"> • Address Groups • BATV Keys • Keywords & Expressions • Policy Notifications • Stamps • DKIM Approved List • Web Reputation Approved List
Web Reputation	Protect your clients from malicious URLs embedded in email messages with Web reputation.
BATV Support	Bounce Address Tag Validation (BATV) protects your clients from bounced email message attacks.
NRS Terminology Change	Network Reputation Service (NRS) has been changed to Email reputation.
Detection Capability Enhancement	Use DomainKeys Identified Mail (DKIM) enforcement, with the DKIM Approved List, in policies to assist in phishing protection and to reduce the number of false positives regarding domains.
X-Header Support	Insert X-Headers into email messages to track and catalog the messages.
Expanded File Scanning Support	IMSVa now supports scanning Microsoft® Office 2007 and Adobe® Acrobat® 8 documents.
Scan Exception Enhancement	IMSVa now supports configuring custom policy settings for encrypted messages and password protected zip attachments. Special actions can be taken on encrypted messages or password protected zip files sent/received by specified users or groups.

NEW FEATURE	DESCRIPTION
EUQ Enhancement	IMSVa now allows users to review and delete or approve messages that are quarantined by administrator-created content filters and those quarantined by the Spam Prevention Solution.
EUQ Single Sign-on (SSO)	<p>IMSVa now allows users to log in once to their domain and then to EUQ without re-entering their domain name and password.</p> <hr/> <p> Note IMSVa 8.0 only supports Internet Explorer and Firefox with Windows Active Directory as the LDAP server.</p> <hr/>
Antispoofing filter	With this filter, a message that has the sender domain that is the same as the recipient(s) domain, and the message does not come from an internal IP address, IMSVa takes action on the message.
New Migration Tools	New tools have been provided to help customers migrating from previous product versions.

IMSVa 7.0 New Features

The following table provides an overview of new features available in IMSVa 7.0.

TABLE 5. IMSVa 7.0 New Features

NEW FEATURE	DESCRIPTION
Data port redundancy	A second data port to connect to your network if a problem arises with the main data port. The second data port has the same IP address as the main data port, but a different MAC address.
New hard disks	Two 250GB raid hard disks.

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 IMSV a 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. IMSV a 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. IMSV a's new CLI interface offers stronger console security by preventing unauthorized access to the OS shell. The IMSV a CLI is modeled after industry standard CLI syntax and navigation formats to greatly reduce the learning time.
Multiple Network Interfaces Support Route Configuration	IMSVa supports multiple network interfaces, and provides a user interface to configure the route for users to deploy IMSV a more conveniently.
Multiple Antivirus and Malware Policies	Multiple IMSV a policies with LDAP support help you configure filtering settings that apply to specific senders and receivers based on different criteria.
Centralized Logging and Reporting	A consolidated, detailed report provides top usage statistics and key mail usage data.
Centralized Archive and Quarantine Management	IMSVa provides an easy way to search multiple IMSV a quarantine and archive areas for messages.
Scalable Web End-User Quarantine (Web EUQ)	Multiple Web EUQ services offer end-users the ability to view quarantined email messages that IMSV a detected as spam. Together with EUQ notification, IMSV a will help lower the cost of helpdesk administrative tasks.

NEW FEATURE	DESCRIPTION
Multiple Spam Prevention Technologies	Three layers of spam protection: <ul style="list-style-type: none"> • Email reputation filters spam senders at the connection layer. • IP Profiler helps protect the mail server from attacks with smart profiles (SMTP IDS). • Trend Micro Anti-spam engine detects and takes action on spam.
IntelliTrap	IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus in a compressed file will enter your network through email.
Delegated Administration	LDAP-integrated account management allows users to assign administrative rights for different configuration tasks.
Easy Deployment with Configuration Wizard	An easy-to-use configuration wizard to get IMSVA up and running.
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 migrated with minimum effort during setup.
Mail Auditing and Tracking	IMSVA provides detailed logging for all messages to track and identify message flow related issues.
Integration with Trend Micro Control Manager TM	Perform log queries on Email reputation detections from Control Manager, in addition to other supported features.
Supports 8 bit to 7 bit-MIME transformation	IMSVA 7.0 Service Pack 1 supports the transformation of 8 bit to 7 bit-MIME according to the standard defined in RFC 1652 SMTP Service Extension for 8bit-MIME transport. In the event that the next hop of the SMTP server does not support 8 bit MIME, IMSS will convert the message from 8 bit MIME to 7 bit MIME.

Audience

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

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

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

InterScan Messaging Security Virtual Appliance Documentation

The 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 File

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



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



<http://docs.trendmicro.com>

Document Conventions

The documentation uses the following conventions:

TABLE 6. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
Navigation > Path	The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface
 Note	Configuration notes
 Tip	Recommendations or suggestions

CONVENTION	DESCRIPTION
 Important	Information regarding required or default configuration settings and product limitations
 WARNING!	Critical actions and configuration options

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 InterScan Messaging Security Virtual Appliance on page 1-2*
- *IMSVa Main Features and Benefits on page 1-2*
- *About Cloud Pre-Filter on page 1-10*
- *About Email Encryption on page 1-10*
- *About Spyware/Grayware on page 1-10*
- *About Trend Micro Control Manager on page 1-12*
- *About Trend Micro Smart Protection on page 1-15*
- *About Command & Control (C&C) Contact Alert Services on page 1-17*

About InterScan Messaging Security Virtual Appliance

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.

IMSVA Main Features and Benefits

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

TABLE 1-1. Main Features and Benefits


FEATURE	DESCRIPTIONS	BENEFITS
Data and system protection		
Cloud-based pre-filtering of messages	Cloud Pre-Filter integrates with IMSVA to scan all email traffic before it reaches your network.	Cloud Pre-Filter can stop significant amounts of spam and malicious messages (up to 90% of your total message traffic) from ever reaching your network.
Email encryption	Trend Micro Email Encryption integrates with IMSVA to encrypt or decrypt all email traffic entering and leaving your network.	Trend Micro Email Encryption provides IMSVA the ability to encrypt all email messages leaving your network. By encrypting all email messages leaving a network administrators can prevent sensitive data from being leaked.

FEATURE	DESCRIPTIONS	BENEFITS
Advanced anti-malware protection	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and aggressive heuristic scanning to detect document exploits and other threats used in targeted attacks.	ATSE identifies both known and unknown advanced threats, protecting your system from new threats that have yet to be added to patterns.
Command & Control (C&C) Contact Alert Services	C&C Contact Alert Services allows IMSVA to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects.	C&C Contact Alert Services provides IMSVA with enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks.
Regulatory compliance	Administrators can meet government regulatory requirements using the new default policy scanning conditions <i>Compliance templates</i> .	Compliance templates provide administrators with regulatory compliance for the following: <ul style="list-style-type: none"> • GLBA • HIPAA • PCI-DSS • SB-1386 • US PII
Smart Scan	Smart Scan facilitates a more efficient scanning process by off-loading a large number of threat signatures previously stored on the IMSVA server to the cloud.	Smart Scan leverages the Smart Protection Network to: <ul style="list-style-type: none"> • Enable fast, real-time security status lookup capabilities in the cloud • Reduce the time necessary to deliver protection against emerging threats • Lower memory consumption on the server

FEATURE	DESCRIPTIONS	BENEFITS
IntelliTrap	<p>Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files.</p> <p>Because there is the possibility that IntelliTrap may identify a non-threat file as a security risk, Trend Micro recommends quarantining message attachments that fall into this category when IntelliTrap is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature.</p> <p>By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be classified as security risks.</p>	IntelliTrap 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.
Real-time Statistics and Monitor	Administrators can monitor the scan performance and IP filtering performance of all IMSVA devices (within a group) on the 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.
Protection against other email threats		

FEATURE	DESCRIPTIONS	BENEFITS
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.
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.

FEATURE	DESCRIPTIONS	BENEFITS
<p>Mass mailing virus containment</p>	<p>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.</p> <p>When IMSVA detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses.</p> <p>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.</p>	<p>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.</p> <p>The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabsSM ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.</p>
<p>Protection from spyware and other types of grayware</p>		
<p>Spyware and other types of grayware</p>	<p>Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see About Spyware/Grayware on page 1-10.</p>	<p>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.</p>
<p>Integrated anti-spam features</p>		

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

FEATURE	DESCRIPTIONS	BENEFITS
Web-based management console	The management console allows you to conveniently configure IMSVA policies and settings.	The management console is SSL-compatible. Being SSL-compatible means access to IMSVA is more secure.
End-User Quarantine (EUQ)	IMSVA provides web-based EUQ to improve spam management. The web-based EUQ service allows end-users to manage the spam quarantine of their personal accounts and of distribution lists that they belong to. IMSVA quarantines messages that it determines are spam. The EUQ indexes these messages into a database. The messages are then available for end-users to review, delete, or approve for delivery.	With the web-based EUQ management console, end-users can manage messages that IMSVA quarantines. IMSVA also enables users to apply actions to quarantined messages and to add senders to the Approved Senders list through links in the EUQ digest.
Delegated administration	IMSVA offers the ability to create different access rights to the management console. You can choose which sections of the console are accessible for different administrator logon accounts.	By delegating administrative roles to different employees, you can promote the sharing of administrative duties.
Centralized reporting	Centralized reporting gives you the flexibility of generating one time (on demand) reports or scheduled reports.	Helps you analyze how IMSVA is performing. 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 and SNMP notification on detection of system failure allows you to take immediate corrective actions and minimize downtime.

FEATURE	DESCRIPTIONS	BENEFITS
POP3 scanning	You can choose to enable or disable POP3 scanning from the management console.	In addition to SMTP traffic, IMSVA can also scan POP3 messages at the gateway as messaging clients in your network retrieve them.
Integration with Deep Discovery Advisor	Trend Micro™ Deep Discovery Advisor is a separately licensed product that provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. IMSVA integrates with the Virtual Analyzer in Deep Discovery Advisor.	IMSVA sends suspicious messages, including attachments, to Virtual Analyzer for further analysis. Virtual Analyzer performs content simulation and analysis in an isolated virtual environment to identify characteristics commonly associated with many types of malware. In particular, Virtual Analyzer checks if files attached to messages contain exploit code.
Integration with Trend Micro Control Manager™	Trend Micro Control Manager™ (TMCN) is a software management solution that gives you the ability to control antivirus and content security programs from a central location regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus and content security policy.	Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in 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.

About Cloud Pre-Filter

Cloud Pre-Filter is a cloud security solution that integrates with IMSVA to provide proactive protection in the cloud with the privacy and control of an on-premise, virtual appliance.

Cloud Pre-Filter reduces inbound email volume up to 90% by blocking spam and malware outside your network. Cloud Pre-Filter is integrated with IMSVA at the gateway allowing flexible control over sensitive information. And local quarantines ensure your email stays private. No email is stored in the cloud. With Cloud Pre-Filter, you can reduce complexity and overhead to realize significant cost savings.

About Email Encryption

Trend Micro Email Encryption provides IMSVA with the ability to perform encryption and decryption of email. With Email Encryption, IMSVA has the ability to encrypt and decrypt email regardless of the email client or platform from which it originated. The encryption and decryption of email on Trend Micro Email Encryption is controlled by a Policy Manager that enables an administrator to configure policies based on various parameters, such as sender and recipient email addresses, keywords or where the email (or attachments) contain credit card numbers. Trend Micro Email Encryption presents itself as a simple mail transfer protocol (SMTP) interface and delivers email out over SMTP to a configured outbound mail transport agent (MTA). This enables easy integration with other email server-based products, be them content scanners, mail servers or archiving solutions.

About Spyware/Grayware

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

TABLE 1-2. Types of Grayware

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

How Spyware/Grayware Gets into your Network

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

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

Potential Risks and Threats

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

TABLE 1-3. Types of Risks

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

About Trend Micro Control Manager

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

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

Control Manager Support

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

TABLE 1-4. Supported Control Manager Features

FEATURE	DESCRIPTION	SUPPORTED?
2-way communication	Using 2-way communication, either IMSVA or Control Manager may initiate the communication process.	No. 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 perform to reduce the likelihood of the IMSVA server or its clients from becoming infected. Trend Micro ActiveUpdate Server deploys this policy to IMSVA through Control Manager.	Yes

FEATURE	DESCRIPTION	SUPPORTED?
Log upload for query	Uploads IMSVA virus logs, Content Security logs, and Email reputation logs to Control Manager for query purposes.	Yes
Single Sign-on	Manage IMSVA from Control Manager directly without first logging on to the IMSVA management console.	No. You need to first log on to the IMSVA 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 pattern files used by IMSVA from Control Manager	Yes
Engine update	Update engines used by IMSVA from Control Manager.	Yes
Product component update	Update IMSVA product components such as patches and hot fixes from Control Manager.	No. Refer to the specific patch or hot fix readme file for instructions on how to update the product components.
Configuration by user interface redirect	Configure IMSVA through the IMSVA management console accessible from Control Manager.	Yes
Renew product registration	Renew IMSVA product license from Control Manager.	Yes
Customized reporting from Control Manager	Control Manager provides customized reporting and log queries for email-related data.	Yes

FEATURE	DESCRIPTION	SUPPORTED?
Control Manager agent installation/uninstallation	Install or uninstall IMSVA Control Manager agent from Control Manager.	No. IMSVA Control Manager agent is automatically installed when you install IMSVA. To enable/disable the agent, do the following from the IMSVA management console: <ol style="list-style-type: none"> 1. Go to Administration > Connections. 2. Click the TCCM Server tab. 3. To enable/disable the agent, select/clear the check box next to Enable MCP Agent.
Event notification	Send IMSVA event notification from Control Manager.	Yes
Command tracking for all commands	Track the status of commands that Control Manager issues to IMSVA.	Yes

About Trend Micro Smart Protection

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

Smart protection services include:

File Reputation Services

File reputation decouples the pattern file from the local scan engine and conducts pattern file lookups to the Trend Micro Smart Protection Network.

High performance content delivery networks ensure minimum latency during the checking process and enable more immediate protection.

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

Web Reputation Services

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

Web reputation technology prevents users from:

- Accessing compromised or infected sites
- Communicating with Command & Control (C&C) servers used in cybercrime

The Need for a New Solution

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

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

Trend Micro™ Smart Protection Network™

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

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

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

The Smart Protection Network provides Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. A client sends web reputation queries to the Smart Protection Network to check the reputation of websites that a user is attempting to access. The client correlates a website's reputation with the specific web reputation policy enforced on the computer to determine whether access to the site is allowed or blocked.

For more information on the Smart Protection Network, visit:

www.smartprotectionnetwork.com

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

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

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

Chapter 2

Component Descriptions

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

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 sections provide an overview of each component.

Cloud Pre-Filter Service Overview

Cloud Pre-Filter service is a managed email security service powered by the Trend Micro Email Security Platform. By routing your inbound messages through the service, you protect your domains against spam, phishing, malware, and other messaging threats before the threats reach your network.

Sender Filtering

By approving senders, Cloud Pre-Filter Service subscribers automatically allow messages from trusted mail servers or email addresses. Messages from approved senders are not checked for spam or source reputation. Messages from approved senders are scanned for viruses.

By blocking senders, subscribers automatically block messages from untrusted sources.

Reputation-Based Source Filtering

With Trend Micro Email Reputation, Cloud Pre-Filter service verifies email sources against dynamic and self-updating reputation databases to block messages from the latest botnets and other IP addresses controlled by spammers, phishers, and malware distributors.

Virus and Spam Protection

With Trend Micro antivirus technology, Cloud Pre-Filter Service protects against infectious messages from mass-mailing worms or manually crafted messages that contain Trojans, spyware, or other malicious code.

Cloud Pre-Filter Service checks messages for spam characteristics to effectively reduce the volume of unsolicited messages.

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. The SPS license is included in the **Trend Micro Antivirus and Content Filter** license. 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 **Spam Prevention Solution** license.

IP Filtering

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

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

IP profiler detects any of these four potential Internet threats:

- **Spam:** Email with unwanted advertising content.

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

How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email containing threats mentioned in the section [IP Filtering on page 2-3](#). 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.

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.

Email Reputation

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

Types of Email Reputation

There are two types of Email reputation: *Standard on page 2-5* and *Advanced on page 2-5*.

Email Reputation: Standard

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

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

Email Reputation: Advanced

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

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

Like Email reputation: Standard, Email reputation: Advanced is a DNS query-based service, but two queries can be made to two different databases: the standard reputation

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

How Email Reputation Technology Works

Trend Micro Email reputation technology is a Domain Name Service (DNS) query-based service. The following process takes place after 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 Email reputation DNS servers and queries the Reputation Database. If the IP address had already been reported as a source of spam, a record of the address will already exist in the database at the time of the query.
3. If a record exists, Email reputation instructs 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.

The figure below illustrates how Email reputation works.

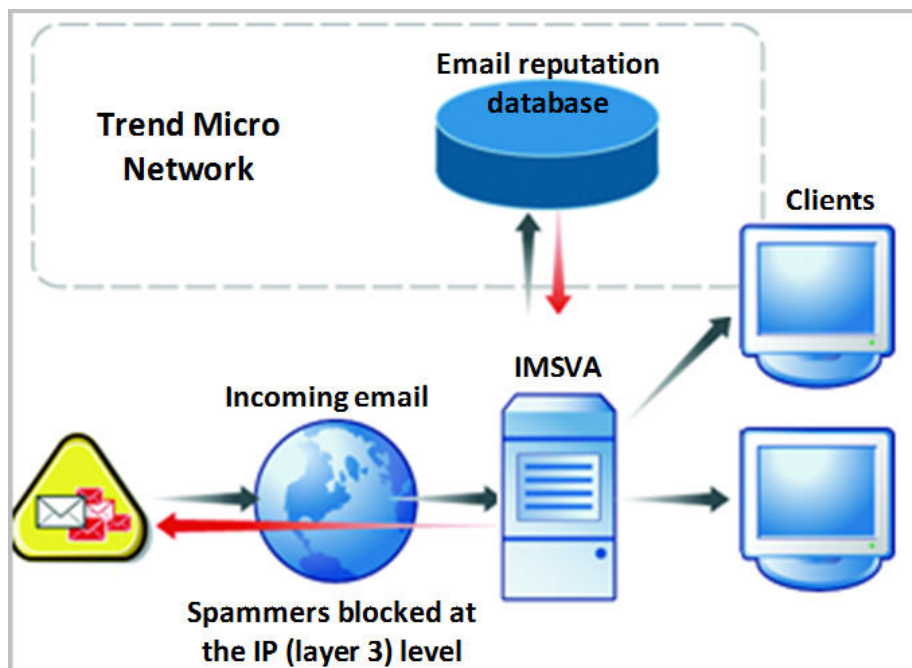


FIGURE 2-1. How Email reputation works

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

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 IMSV), or administrator-created content filters, determine to be spam, are placed into quarantine. These messages are

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

About Centralized Reporting

To help you analyze how IMSVA 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 Quick StartGuide in the carton or the PDF version on the included Solutions DVD for IMSVA 5000. For instructions on performing initial configuration, see the Administrator's Guide.

Deployment Checklist

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

1. Deploy IMSVA with Cloud Pre-Filter

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Deploy with Cloud Pre-Filter	Yes	<i>IMSVA Deployment with Cloud Pre-Filter on page 3-6</i>

2. Identify the location of IMSVA

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Select one of the following locations on your network where you would like to install IMSVA.		
	At the gateway		<i>Deployment at the Gateway or Behind the Gateway on page 3-6</i>
	Behind the gateway		<i>Deployment at the Gateway or Behind the Gateway on page 3-6</i>
	Without a firewall		<i>Installing without a Firewall on page 3-9</i>

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	In front of a firewall		Installing in Front of a Firewall on page 3-10
	Behind a firewall		Installing Behind a Firewall on page 3-11
	In the De-Militarized Zone		Installing in the De-Militarized Zone on page 3-12

3. Plan the scope

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Decide whether you would like to install a single IMSVA device or multiple devices.		
	Single device installation		About Device Roles on page 3-13
	Multiple IMSVA devices		About Device Roles on page 3-13

4. Deploy or Upgrade

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Deploy a new IMSVA device or upgrade from a previous version.		

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Upgrade from a previous version		Upgrading from Previous Versions on page 5-1

5. Start services

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Activate IMSVA services to start protecting your network against various threats.		
	Scanner		IMSVA Services section of the Administrator's Guide
	Policy		
	EUQ	Yes	

6. Configure other IMSVA settings

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

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	POP3 Settings	Yes	Scanning POP3 Messages section of the Administrator's Guide
	Policy and scanning exceptions		Managing Policies section of the Administrator's Guide
	Perform a manual update of components and configure scheduled updates		Updating Scan Engine and Pattern Files section of the Administrator's Guide
	Log settings		Configuring Log Settings section of the Administrator's Guide

7. Back up IMSVA

TICK WHEN COMPLETED	TASKS	OPTIONAL	REFERENCE
	Perform a backup of IMSVA as a precaution against system failure.		
	Back up IMSVA settings		Backing Up IMSVA section of the Administrator's Guide

Network Topology Considerations

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

IMSVA Deployment with Cloud Pre-Filter

Cloud Pre-Filter has no impact on how IMSVA should be deployed.



Note

Cloud Pre-Filter uses port 9000 as the web service listening port. This port must be open on the firewall for IMSVA to connect to Cloud Pre-Filter.

However, when adding Cloud Pre-Filter policies you must change the MX records, of the domain specified in the policy, to that of the Cloud Pre-Filter inbound addresses. The address is provided on the bottom of Cloud Pre-Filter Policy List screen. Click Cloud Pre-Filter in the IMSVA management console to display the Cloud Pre-Filter Policy List screen.



Tip

Trend Micro recommends adding IMSVA's address to the domain's MX records, and placing IMSVA at a lower priority than Cloud Pre-Filter. This allows IMSVA to provide email service continuity as a backup to Cloud Pre-Filter.

Deployment at the Gateway or Behind the Gateway

TABLE 3-1. 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: Single IMSVA device at the gateway on page 3-7 .	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: <ul style="list-style-type: none"> • Figure 3-3: IMSVA group at the gateway on page 3-8 • Service Selection on page 3-14

	SINGLE DEVICE	MULTIPLE DEVICES
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: Single IMSVA device behind the gateway on page 3-8 .	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: <ul style="list-style-type: none"> • Figure 3-4: IMSVA group behind the gateway on page 3-9 • Service Selection on page 3-14
Trend Micro Control Manager scenario		
If you have multiple groups, you can use Trend Micro Control Manager (TMCM) to manage the devices.		

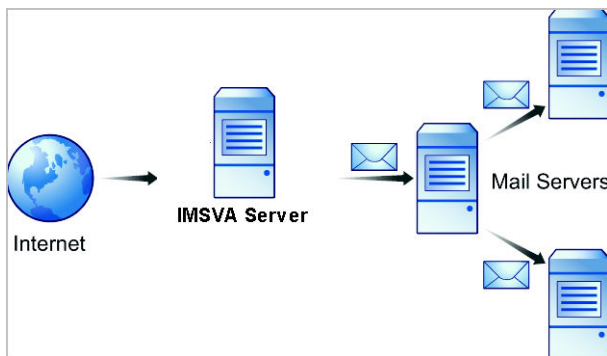


FIGURE 3-1. Single IMSVA device at the gateway

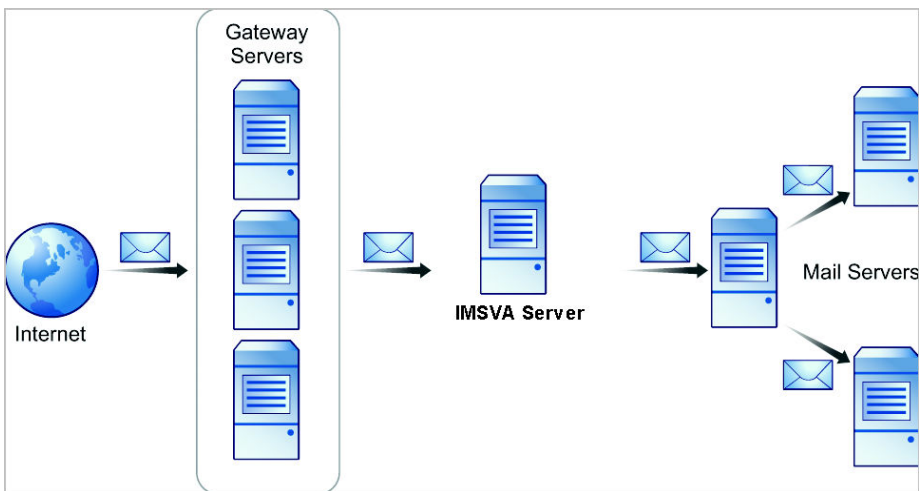


FIGURE 3-2. Single IMSVA device behind the gateway

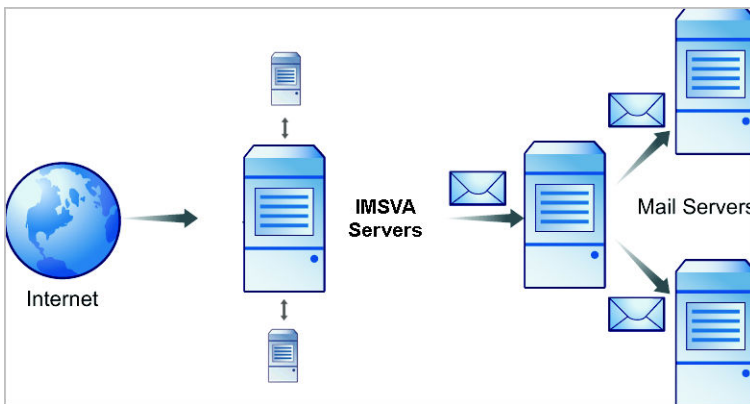


FIGURE 3-3. IMSVA group at the gateway

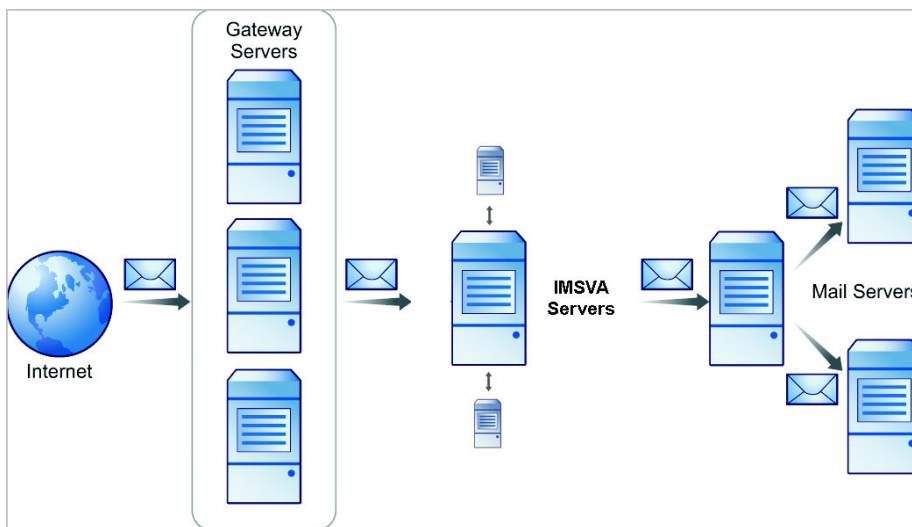


FIGURE 3-4. IMSVA group behind the gateway

Installing without a Firewall

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

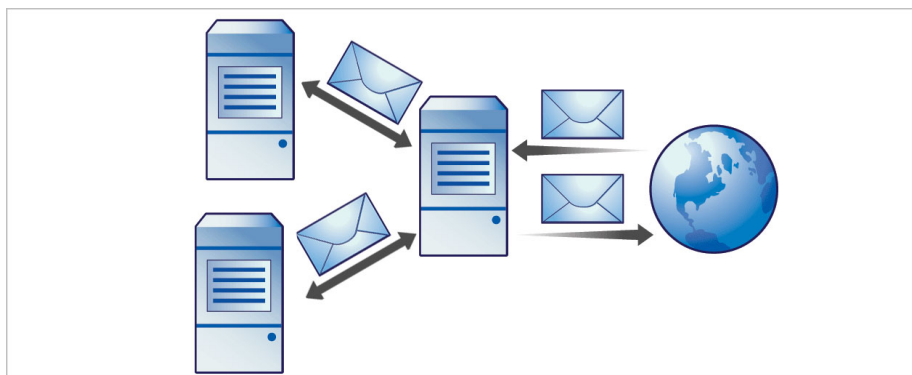


FIGURE 3-5. Installation topology: no firewall

**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

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

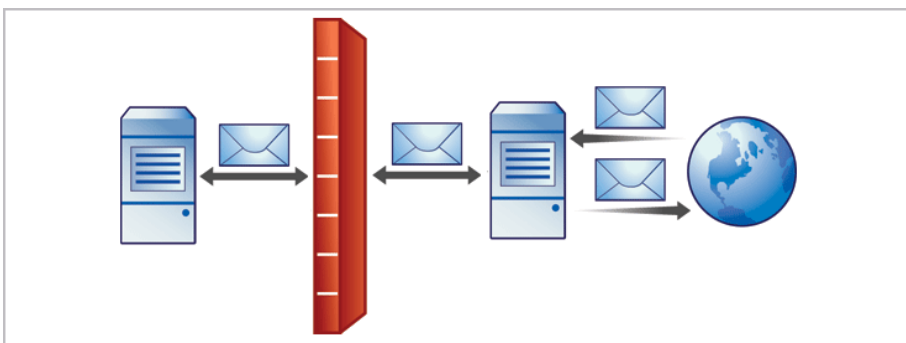


FIGURE 3-6. Installation topology: in front of the firewall

Incoming Traffic

- Postfix should receive incoming messages first, then transfer 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 messages to IMSVA servers.

- Incoming SMTP messages 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 the **Configuring SMTP Routing** section of the *IMSVA Administrator's Guide*.

Installing Behind a Firewall

The following figure illustrates how to deploy IMSVA and Postfix behind your firewall.

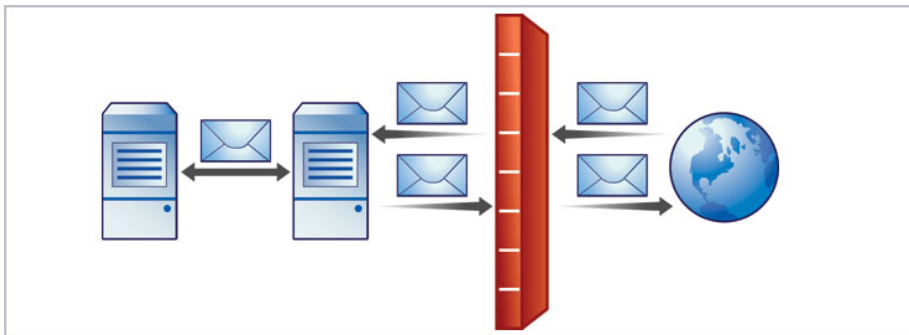


FIGURE 3-7. Installation scenario: behind a firewall

Incoming Traffic

- Configure your proxy-based firewall, as follows:
 - Outgoing SMTP messages go to Postfix first and then to the IMSVA server or the switch performing load balancing between scanners.
 - Incoming SMTP messages go first to Postfix, then to IMSVA, and then to the SMTP servers in the domain.
- Configure IMSVA to route messages destined for your local domain(s) to the SMTP gateway or your internal mail server.

- Configure relay restriction to only allow relay for local domain(s).

Outgoing Traffic

- Configure all internal SMTP gateways to send outgoing messages to Postfix and then to IMSVA servers.
- If you are replacing your SMTP gateway with IMSVA, configure your internal mail server to send outgoing messages through Postfix and then to IMSVA servers.
- Configure Postfix and IMSVA to route all outgoing messages (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 the **Configuring SMTP Routing** section of the *IMSVA Administrator's Guide*.

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 messages destined for your local domain(s) to the SMTP gateway or your internal mail server.

Outgoing Traffic

- Configure Postfix to route all outgoing messages (destined for domains 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 the **Configuring SMTP Routing** section of the *IMSVA 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:** Managed by a single parent device and uses all global settings that you configure through the parent device's management 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 (management 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 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.

Service Selection

You can enable different types of services on parent and child devices. For example, to increase throughput, add more child devices, enable all their services 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 3-15](#) for more information.

Deployment with IP Filtering

The Trend Micro IP Filtering, which includes IP Profiler and Email Reputation 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 management 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 management console, the management console service on the Internal Communication Port needs to be enabled. By default, the management 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 only IMSVA 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

For example: user

Opening the IMSVA Management 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: **imsva**

Type the logon credentials the first time you open the console and click **Log on**. 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 management 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.

Procedure

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 3.5 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: imsva

The **Configuration Wizard** screen appears.

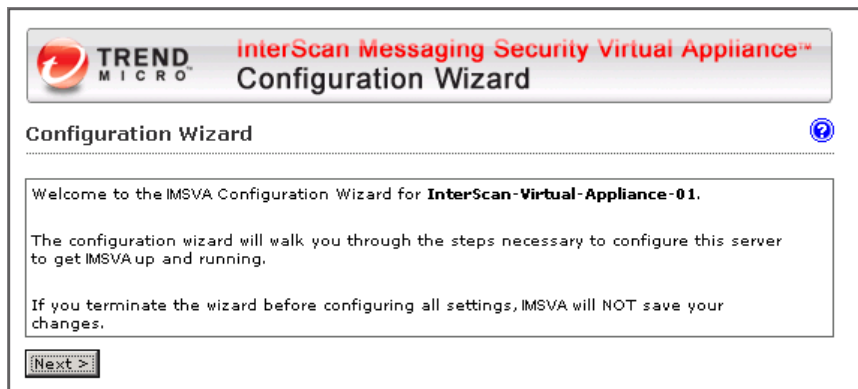


FIGURE 3-8. Configuration Wizard screen

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

Step 1: Configuring System Settings

Procedure

1. After you read the welcome screen, click **Next**. The **Local System Settings** screen appears.

Configuration Wizard
 Step 1 of 10

Local System Settings

The following settings for network and system time will be applied to **local system** immediately when you click the Save/Next button

Network Settings

IPv6 Configuration

Enable IPv6

Network interface configuration

Device name	IP Address and Mask
eth0	IPv4: * <input style="width: 150px;" type="text"/> / <input style="width: 100px;" type="text"/> IPv6: <input style="width: 150px;" type="text"/> / <input style="width: 50px;" type="text"/>

Internal Communication Port

Device name:

Network subsystem configuration

Host name: *

Default IPv4 gateway: *

Primary IPv4 DNS server: *

Secondary IPv4 DNS server:

Default IPv6 gateway:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

System Time

You can enable NTP on the Deployment Settings screen. A child device uses the NTP settings of its parent device. If you do not enable NTP on the Deployment Settings screen for the parent device, child devices cannot use NTP.

Local Time Zone: *

Continent Country/Region Province/City

Date and time: *

mm/dd/yyyy hh:mm:ss

FIGURE 3-9. Local System Settings

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

Procedure

1. Click **Next**.

The **Deployment Settings** screen appears.

Configuration Wizard
Step 2 of 10

Deployment Settings

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

dean85.com deployment type:

Parent Device

Import Settings...

Gateway deployment ⓘ

Automatically synchronize system time with NTP server:

Child Device

Register to parent device IP address:

< Back Next >

Steps

1. System Settings
- 2. Deployment Settings**
3. SMTP Routing
4. Notification Settings
5. Update Source
6. LDAP Settings
7. Internal Addresses
8. TCMC Settings
9. Product Activation
10. Review Settings

FIGURE 3-10. Deployment Settings

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 the NTP service.

Step 3: Configuring SMTP Routing Settings

Procedure

1. Click **Next**.

The **SMTP Routing Settings** screen appears.

Configuration Wizard
 Step 3 of 10

?

SMTP Routing Settings

IMSSVA uses the following domain-based settings for receiving and sending messages.

Incoming Message Settings

Add Domain

 For example: example.com

Note: To ensure that IMSSVA receives incoming messages, Trend Micro recommends adding all internal domains in your network.

test.com

Message Delivery Settings

<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Import"/>	1-1 of 1 Page 1
Domain	Mail Server
Other domains	Determined by DNS
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Import"/>	1-1 of 1 Page 1
Rows per page: 15 per page	

FIGURE 3-11. SMTP Routing Settings

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

Step 4: Configuring Notification Settings

Procedure

1. Click **Next**.

The **Notification Settings** screen appears.

The screenshot shows the 'Configuration Wizard' interface at 'Step 4 of 10'. The main heading is 'Notification Settings' with a help icon. Below the heading is the instruction: 'Configure email and SNMP trap notifications for default system notifications.' The form is divided into two sections: 'Email Settings' and 'SNMP Trap'. The 'Email Settings' section includes fields for 'To address(es):*' (with a note to use semicolons), 'Sender's email address:*' (pre-filled with 'postmaster@imsva.trendmicro.com'), 'Server name or IP address:*' (pre-filled with '127.0.0.1'), 'SMTP server port:*' (pre-filled with '10026'), 'Preferred charset:*' (a dropdown menu set to 'UTF-8 (utf-8)'), 'Message header:', and 'Message footer:'. The 'SNMP Trap' section includes 'Server name (IP or FQDN):' and 'Community:' (pre-filled with 'public'). At the bottom are three buttons: '< Back', 'Skip', and 'Next >'.

FIGURE 3-12. Notification Settings

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

Procedure

1. Click **Next**.

The **Update Source** screen appears.

Configuration Wizard
Step 5 of 10

Update Source

Select an update source and configure proxy settings to enable IMSVA to **update components** and **activate product licenses**.

Source

Trend Micro ActiveUpdate server

Other Internet source

http://

Proxy Settings

Use a proxy server for updates to patterns, engines, licenses, Web Reputation queries, Cloud Pre-Filter, and Trend Micro Email Encryption.

Proxy type:* HTTP

Proxy server:*

Port:*

User name:

Password: *****

< Back Skip Next >

FIGURE 3-13. Update Source

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 `http://<TMC server address>/TvcDownload/ActiveUpdate/`, 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

Procedure

1. Click **Next**.

The **LDAP Settings** screen appears.

Configuration Wizard
 Step 6 of 10

LDAP Settings ?

Enter LDAP settings **only** if you will use LDAP for user-group definition, administrator privileges, or web quarantine authentication. You must enable LDAP to use the web quarantine tool. If you need to define more than one LDAP servers, please follow this link: [Administration > Connections > LDAP](#)

LDAP Descriptions

Description:*

LDAP Settings

LDAP server type:* Microsoft Active Directory

Enable LDAP1

LDAP server:*
Example: example.com or 123.123.123.123

Listening port number:* 389
Note: Please use the global catalog port 3268 if the LDAP server type is Microsoft Active Directory.

Enable LDAP2 !

LDAP server:*
Example: example.com or 123.123.123.123

Listening port number:* 389
Note: Please use the global catalog port 3268 if the LDAP server type is Microsoft Active Directory.

LDAP cache expiration for policy services and EUQ services

Time to Live in minutes:* 1440

LDAP admin

LDAP admin account:*
Example: Domain_Name\Account_Name or Account_Name@Domain_Name

Password:*

Base distinguished name:*
Example: DC=foo, DC=foonet, DC=org

Authentication method:*

Simple !

Advanced: using Kerberos authentication for Active Directory

Kerberos authentication default realm:

Default domain:

KDC and admin server:

KDC port number:

< Back
Skip
Next >

FIGURE 3-14. LDAP Settings

2. Type a meaningful description for the LDAP server.
3. 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:
 - **Domino**
 - **Microsoft Active Directory**
 - **Microsoft AD Global Catalog**
 - **OpenLDAP**
 - **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 the following table for a guide on what to specify for the LDAP admin settings.

TABLE 3-2. LDAP admin settings

LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory	Without Kerberos: user1@domain.com (UPN) or domain \user1 With Kerberos: user1@domain.com	dc=domain, dc=com	Simple Advanced (with Kerberos)

LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory Global Catalog	Without Kerberos: user1@domain.com (UPN) or domain \user1 With Kerberos: user1@domain.com	dc=domain, dc=com dc=domain1,dc=com (if multiple unique domains exist)	Simple Advanced (with Kerberos)
Lotus Domino	cn=manager, dc=test1, dc=com	dc=test1, dc=com	Simple
Lotus Domino	user1/domain	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	Simple

- 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.

Step 7: Configuring Internal Addresses

Procedure

1. Click **Next**.

The **Internal Addresses** screen appears.

Configuration Wizard
Step 7 of 10

Internal Addresses

Define your internal domains (known users or domains). IMSVA uses these to determine which policies and events are **"Incoming"** and **"Outgoing"** for reporting and rule creation.

Internal domains and usergroups

Enter domain

(For example: domain_name or domain_name.com)

Selected

FIGURE 3-15. Internal Addresses

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 Control Manager Server Settings

Procedure

1. Click **Next**.

The **TCMC Server Settings** screen appears.

Configuration Wizard
Step 8 of 10

TCMC Server Settings

Trend Micro™ Control Manager™ (TCMC) is a software management solution that gives you the ability to control IMSVA devices and other antivirus and content security programs from a central location.

TCMC Server Settings

To manage IMSVA with Control Manager, enable the Control Manager MCP agent and configure all Control Manager server settings.

Enable MCP Agent

Server:*

Communication protocol:*
 HTTP Port:
 HTTPS Port:

Web server authentication:

User name:

Password:

Enable proxy

Proxy type:*

Proxy server:*

Port:*

User name:

Password:

< Back Skip Next >

FIGURE 3-16. TCMC Server Settings

2. If you will use Control Manager to manage IMSVA, do the following:
 - a. Select **Enable MCP Agent** (included with IMSVA by default).
 - b. Next to **Server**, type the Control Manager 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.

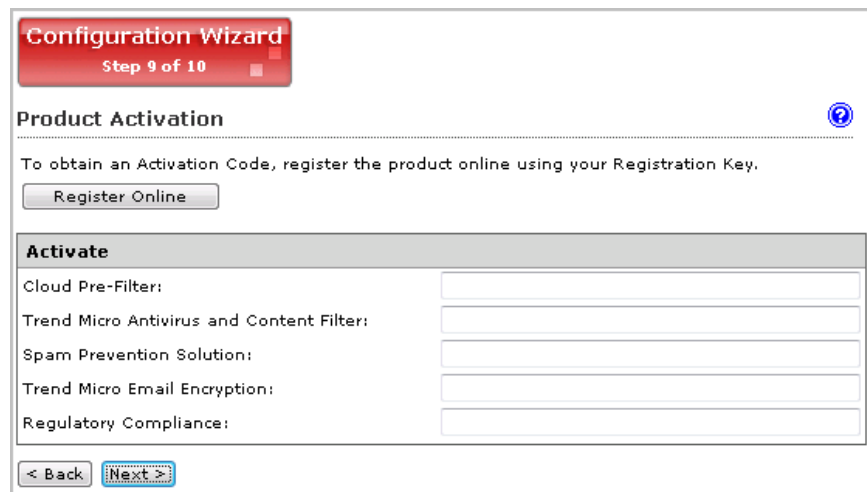
- d. Under **Web server authentication**, type the user name and password for the web server if it requires authentication.
 - e. If a proxy server is between IMSVA and Control Manager, select **Enable proxy**.
 - f. Type the proxy server port number, user name, and password.
-

Step 9: Activating the Product

Procedure

1. Click **Next**.

The **Product Activation** screen appears.



The screenshot shows a web-based configuration wizard. At the top, a red banner reads "Configuration Wizard Step 9 of 10". Below this, the title "Product Activation" is displayed with a help icon. The main text instructs the user to register the product online using their Registration Key, with a "Register Online" button. A section titled "Activate" contains five input fields for: Cloud Pre-Filter, Trend Micro Antivirus and Content Filter, Spam Prevention Solution, Trend Micro Email Encryption, and Regulatory Compliance. At the bottom, there are "< Back" and "Next >" navigation buttons.

FIGURE 3-17. Product Activation

2. Type the Activation Codes for the products or services 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

Procedure

1. Click **Next**.

The **Review Settings** screen appears.



FIGURE 3-18. Review Settings

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.

Procedure

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 3-18*), make sure the parent device is operational.
 - b. Log on to the management console. Make sure that you are logging on the parent device management console.
 - c. Navigate to **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 management console. All IMSVA devices have the same default management 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. Navigate to **System Status**.

- 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:
 - a. On the parent device, navigate to **Administration > End-User Quarantine**.
The **EUQ Management** tab appears by default.
 - b. Select **Redistribute all** or **Only redistribute approved senders**. Trend Micro recommends selecting **Redistribute all**.
 - c. Click **Redistribute**.



Note

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

Trend Micro recommends the following:

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

Verifying Successful Deployment

After you have set up the IMSVA devices, the services should start automatically.

Procedure

1. Navigate to **System Status**.
 2. 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 IMSVA 8.5

This chapter explains how to install IMSVA under different scenarios.


Topics include:



- *System Requirements on page 4-2*
- *Installing IMSVA on page 4-5*

System Requirements

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

TABLE 4-1. System Requirements

SPECIFICATION	DESCRIPTION
Operating System	<p>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.</p> <hr/> <p> Note</p> <p>IMSVA uses a 64-bit operating system. When installing a 64-bit OS on ESX/ESXi, you need to enter the BIOS and enable VT (Virtualization Technology).</p>
CPU	<ul style="list-style-type: none"> • Recommended: Four Intel™ Xeon™ processors • Minimum: Two Intel™ Xeon processors
Memory	<ul style="list-style-type: none"> • Recommended: 8GB RAM • Minimum: 4GB RAM


SPECIFICATION	DESCRIPTION
Disk Space	<ul style="list-style-type: none"> <li data-bbox="512 253 720 321">• Recommended: 250GB <hr/> <div data-bbox="561 370 1180 464">  Note IMSVA automatically partitions the detected disk space as per recommended Linux practices </div> <hr/> <ul style="list-style-type: none"> <li data-bbox="512 488 659 557">• Minimum: 120GB <hr/> <div data-bbox="561 605 1180 699">  Note IMSVA automatically partitions the detected disk space as per recommended Linux practices </div> <hr/>
Monitor	Monitor that supports 800 x 600 resolution with 256 colors or higher
Trend Micro Control Manager	<ul style="list-style-type: none"> <li data-bbox="512 805 1085 831">• Version 5.5 (Service Pack 1 Patch 3 or later version) <li data-bbox="512 849 928 875">• Version 6.0 (Patch 3 or later version)

Additional Requirements and Tools

The following table lists the minimum application requirements to access the CLI and management console interfaces and to manage IMSVA with Control Manager.

TABLE 4-2. Minimum Software Requirements

APPLICATION	SYSTEM REQUIREMENTS	DETAILS
SSH communication 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.

APPLICATION	SYSTEM REQUIREMENTS	DETAILS
VMware™ ESX server	Version 4.0/4.1	If you want to install IMSVA as virtual machine, install IMSVA on a VMware ESX server 4.0/4.1.
Hyper-V	<ul style="list-style-type: none"> Windows Server 2008 R2 Windows Server 2008 R2 with SP1 or later 	IMSVA only supports Hyper-V on Windows Server 2008 R2 and Windows Server 2008 R2 with SP1 or later.
Internet Explorer™	<ul style="list-style-type: none"> Version 8.0 Version 7.0 Version 6.0 SP2 	<p>To access the web console, which allows you to configure all IMSVA settings, use Internet Explorer 6.0 SP 2 or above or Firefox 3.5 or above. Using the data port IP address you set during initial configuration, enter the following URL: <code>https://[IP Address]:8445</code></p> <hr/> <p> Note</p> <p>When accessing the Dashboard using Internet Explorer 9.0, Compatibility Mode must be used to correctly render the screen.</p> <p>To Compatibility Mode for the Dashboard when using Internet Explorer 9.0, in Internet Explorer click Page > Compatibility View Settings, and add IMSVA to the list.</p> <hr/>
Mozilla Firefox™	<ul style="list-style-type: none"> Version 5.0 Version 4.0 Version 3.6 Version 3.5 	
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 5.5	Use Trend Micro Control Manager 5.5 to manage IMSVA.

Installing IMSVA

IMSVA only supports upgrading from IMSVA 8.5. IMSVA supports migrating existing configuration and policy data from other InterScan Messaging Security 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 DVD to begin the procedure and the VMware installation requires the creation of a virtual machine before installation.



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.

Procedure

1. Start the IMSVA installation:
 - On a Bare Metal Server
 - a. Insert the IMSVA Installation DVD into the DVD drive of the desired server.
 - b. Power on the Bare Metal server.
 - On a VMware ESX Virtual Machine



WARNING!

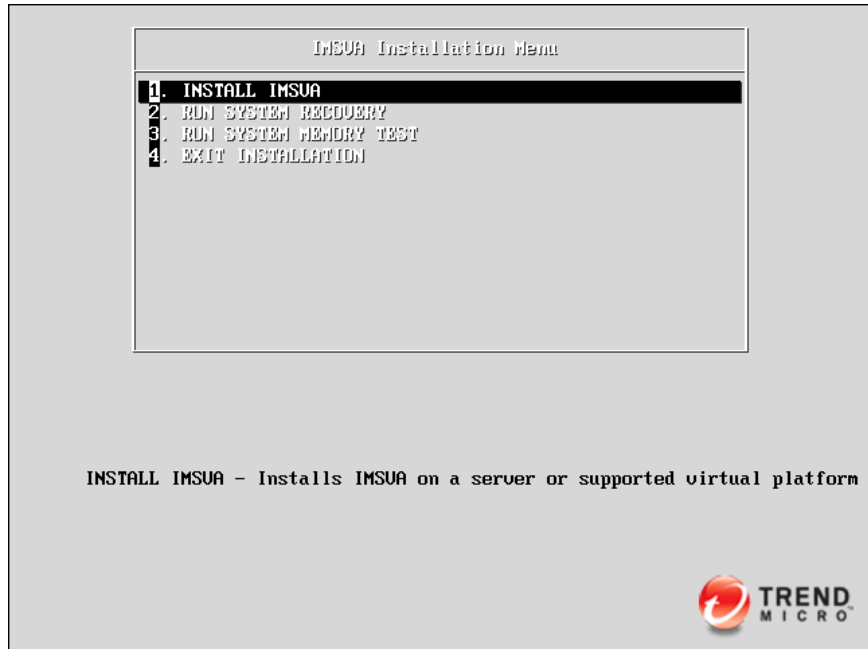
If you install IMSVA on an ESX server, disable the snapshot feature for the virtual machine because the snapshot will exhaust hard disk space.

- a. Create a virtual machine on your VMware ESX server.
- b. Start the virtual machine.
- c. Insert the IMSVA Installation DVD into the virtual DVD drive with any one of the following methods.

- Insert the IMSVA Installation DVD into the physical DVD drive of the ESX server, and then connect the virtual DVD drive of the virtual machine to the physical DVD drive.
 - Connect the virtual DVD drive of the virtual machine to the IMSVA-8.2.xxxx-86_64.iso file. The IMSVA-8.2.xxxx-86_64.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.

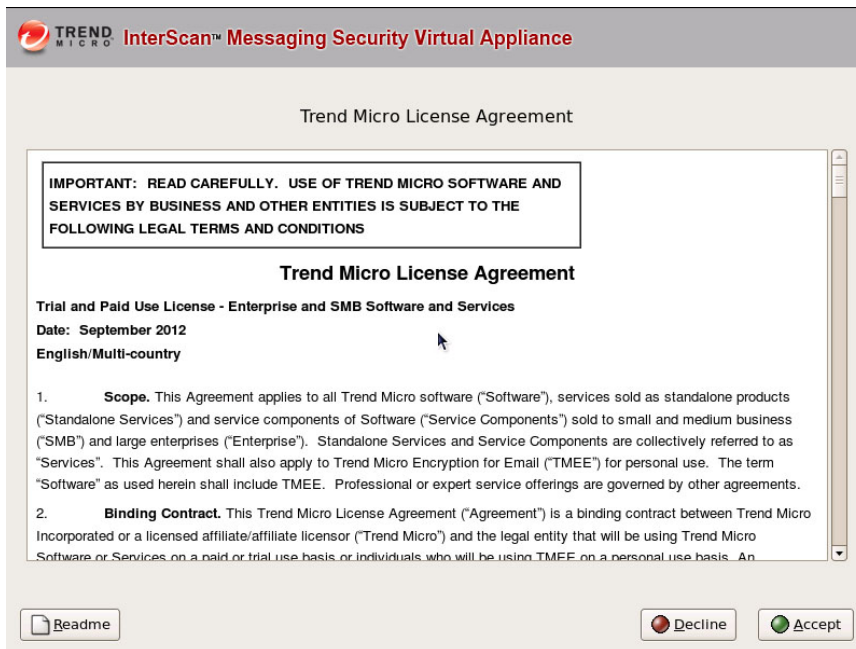
For both a VMware ESX Virtual Machine and a Bare Metal Server installation, a page appears displaying the **IMSVA Installation Menu** with the following options:

- **Install IMSVA:** Select this option to install IMSVA onto the new hardware or virtual machine
- **System Recovery:** Select this option to recover the 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.



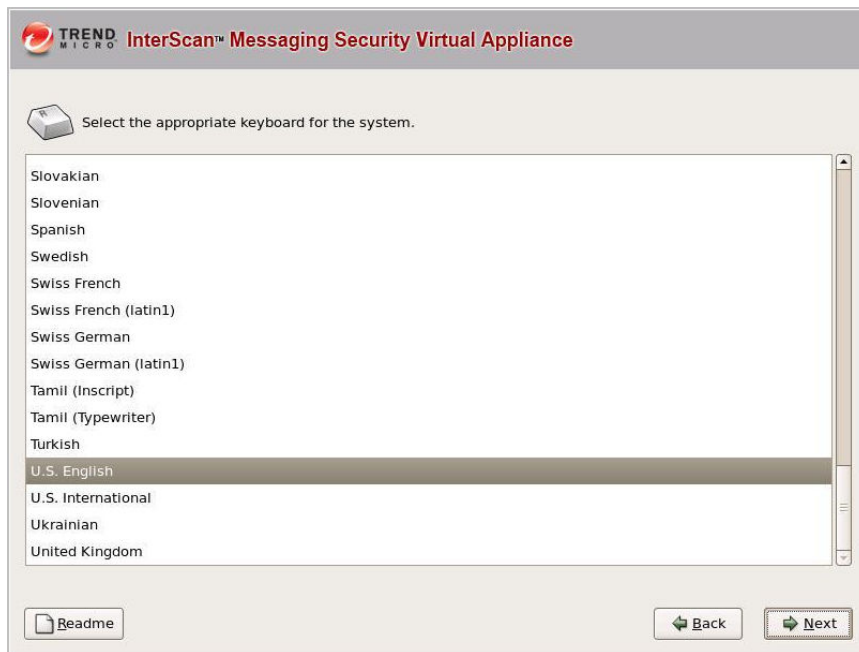
2. Select **Install IMSVA**.

The **License Agreement** page appears. From this page, you can access the readme (**Readme** button).

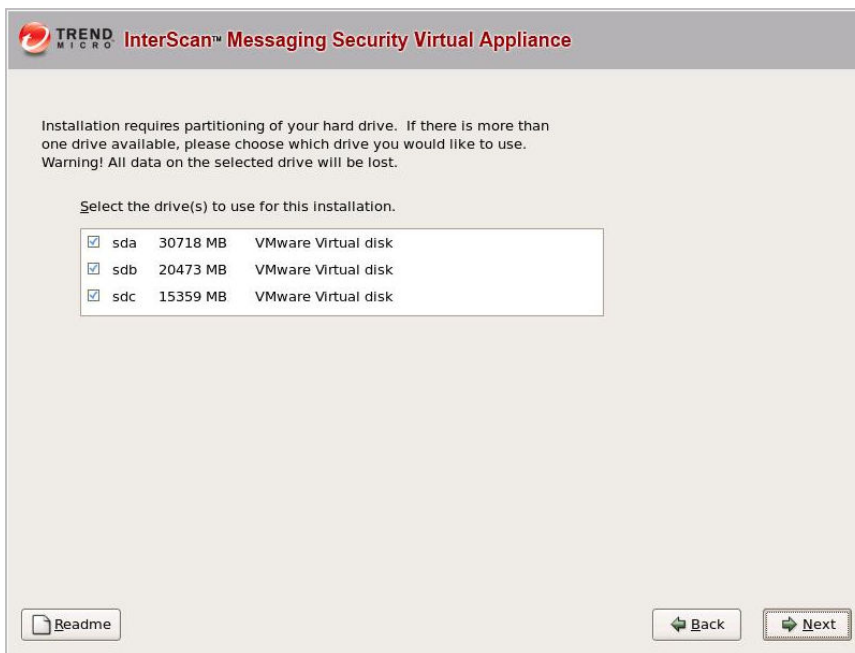


3. Click **Accept** to continue.

A page appears where you select the keyboard language.

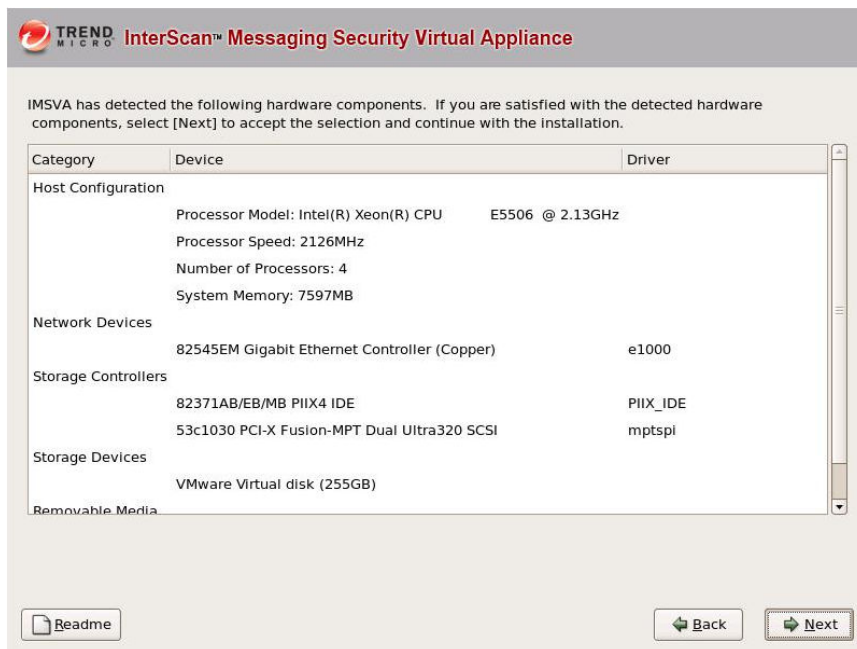


4. Select the keyboard language for the system and then click **Next**.
5. Specify the drive or drives IMSVA uses for installation and normal operation and then click **Next**.



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.

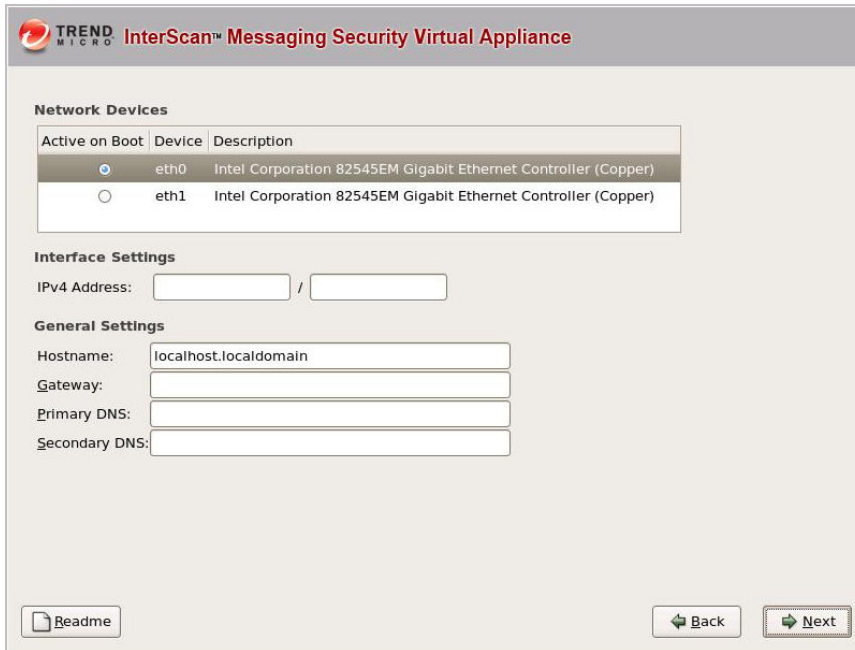


6. Click **Next**.

The IMSVA installer detects hard disk drives and displays all available hard disk drives. At least one drive must be selected for IMSVA installation.

7. Select the drive(s) for IMSVA installation and then click **Next**.

The **Network Settings** screen appears.



TREND MICRO InterScan™ Messaging Security Virtual Appliance

Network Devices

Active on Boot	Device	Description
<input checked="" type="radio"/>	eth0	Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
<input type="radio"/>	eth1	Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

Interface Settings

IPv4 Address: /

General Settings

Hostname:

Gateway:

Primary DNS:

Secondary DNS:



Note

During installation only the default network device (**eth0**) can be selected. To use a different ethernet card, use the Configuration Wizard to specify the ethernet card you want to use, after IMSVA installs.

The table below describes the information required.

TABLE 4-3. Network Device Settings

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.
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.

8. Provide all the information to install IMSVA, and click **Next**.

The **NTP settings** screen appears.



9. 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** check box.
10. Click **Next**.

The **Account Settings** screen appears.

TREND MICRO InterScan™ Messaging Security Virtual Appliance

Please setup passwords for the administrative accounts below to against unauthorized access. The password must be as least six characters longs.

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: Not Entered

Confirm:

Enable Account: Used to gain access to the Command Line Interface (CLI) privilege mode. Has access to all CLI commands.

Password: Not Entered

Confirm:

Password Strength

Good

Poor

- Specify passwords for the **root** and **enable** accounts.

IMSVA uses two 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.

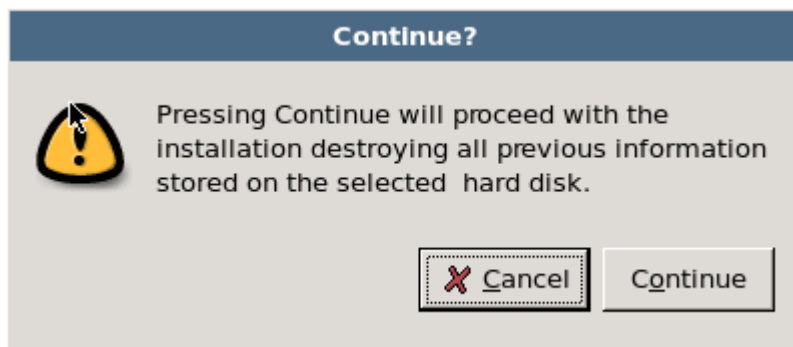
As you type the passwords, the password strength meter on the right indicates how strong the selected password is.

12. Click **Next**.

The **Review Settings** screen appears.

13. 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.

14. 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.



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

- Bare Metal installation:

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

- Virtual machine installation:

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

After IMSVA reboots, the initial CLI login screen appears.

```
Trend Micro InterScan Messaging Security Virtual Appliance (IMSVA)

To manage the IMSVA through the management interface, open a
browser window and choose any URL from following list:

    https://10.204.169.31:8445

You will be prompted for your administrator account and password.
Please have your administrator account and password ready for authentication.
Refer to the Administrator's Guide for the default account and password informat
ion.

To manage IMSVA through the Command Line Interface (CLI),
log on using the Logon prompt below. Refer to the Administrator's Guide
for the default account and password information.

imsva-31 login: _
```



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.

16. Log on either in the CLI or in the IMSVA management console to launch IMSVA.
Log on to the CLI shell if you need to perform additional configuration, troubleshooting, or housekeeping tasks.

Chapter 5

Upgrading from Previous Versions

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

Topics include:

- *Upgrading from an Evaluation Version on page 5-2*
- *Upgrading from IMSVA 8.2 Service Pack 2 on page 5-4*
- *Migrating from Previous Versions on page 5-29*

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 management console alerting you of the impending expiration.

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

Procedure

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

Product License		
Cloud Pre-Filter		View detailed license online
Product:	Cloud Pre-Filter	
Version:	Trial	
Activation code:	<input type="text" value="XXXXXXXX-XXXX-XXXX-XXXX-XXXX"/>	Enter a new code
Seats:	000011	
Status:	Activated	
Maintenance expiration:	Dec 20, 2011	
Trend Micro Antivirus and Content Filter		View detailed license online
Product:	Trend Micro Antivirus and Content Filter	
Version:	Trial	
Activation code:	<input type="text" value="XXXXXXXX-XXXX-XXXX-XXXX-XXXX"/>	Enter a new code
Seats:	000011	
Status:	Activated	
Maintenance expiration:	Dec 20, 2011	
Trend Micro Email Encryption		View detailed license online
Product:	Trend Micro Email Encryption	
Version:	Trial	
Activation code:	<input type="text" value="XXXXXXXX-XXXX-XXXX-XXXX-XXXX"/>	Enter a new code
Seats:	000011	
Status:	Activated	
Maintenance expiration:	Dec 20, 2011	
Note: After successfully activate the Trend Micro Email Encryption, please goto Encryption Settings to register the service and domains.		
Regulatory Compliance		View detailed license online
Product:	Regulatory Compliance	
Version:	Trial	
Activation code:	<input type="text" value="XXXXXXXX-XXXX-XXXX-XXXX-XXXX"/>	Enter a new code
Seats:	000011	
Status:	Activated	
Maintenance expiration:	Dec 20, 2011	

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

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



Enter A New Code

If you do not have an Activation Code, please use the Registration Key that came with your product to [register online](#).

Product: Cloud Pre-Filter

Current Activation Code: [blurred]

New Activation Code:

< Back Activate

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 by email. To prevent mistakes when typing the Activation Code (in the format xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx), you can copy the Activation Code from the email and paste it in the box provided.

4. Click **Activate**.
5. Repeat steps 2 to 5 for all the products or services you want to activate.

Upgrading from IMSVA 8.2 Service Pack 2

IMSVA 8.2 Service Pack 2 can be upgraded as a single device or an entire distributed environment can be upgraded.

**Important**

You must install Hot Fix 1698, Critical Patch 1700, or later fixes before upgrading to IMSVA 8.5. For more information, see [Step 1: Installing the Hot Fix or Critical Patch on page 5-12](#).

Do not restart IMSVA until you have completed the upgrade process.

Upgrading a Single IMSVA

This procedure upgrades a single IMSVA to version 8.5.

Procedure

1. Back up IMSVA 8.2 Service Pack 2 to safeguard against any issues that may occur during the upgrade.

**Tip**

IMSVA 8.2 Service Pack 2 backs up the configuration settings and performs an auto-rollback if the upgrade is not successful. However Trend Micro recommends backing up IMSVA 8.2 Service Pack 2 in one of the following ways, before attempting to upgrade to IMSVA 8.5:

- Ghost the entire computer where IMSVA 8.2 Service Pack 2 is installed.
- Clone IMSVA 8.2 Service Pack 2 if it is installed on a virtual machine.
- Back up the IMSVA 8.2 Service Pack 2 `app_data` partition. To perform this task, open the operating system shell console and run the following commands:

```
/opt/trend/imss/script/imssctl.sh stop  
  
service crond stop  
  
cp -rf --preserve /var/app_data/* /var/udisk/  
app_data_backup/
```

-
2. Download the IMSVA 8.5 upgrade package. (for example, `IMSVA-Upgrade-Pkg-82SP2-To-85_1128.tgz` and `run.sh`).
 3. Use the following command in the CLI console to verify there are no messages in the Postfix queue:

```
postqueue -p
```

4. Stop all IMSVA services, except the database, using the following commands:

```
/opt/trend/imss/script/imssctl.sh stop
```

```
/opt/trend/imss/script/dbctl.sh start
```

5. Navigate to the directory where the upgrade package is stored and type the following command:

```
./run.sh
```

The upgrade script launches and performs a pre-installation check. If the pre-installation check is not successful, installation stops.

The upgrade package reboots IMSVA automatically after it finishes the pre-installation check.

After rebooting IMSVA, the upgrade package installs IMSVA 8.5. Wait until the installation completes.



Note

The IMSVA 8.5 upgrade process allows you to add a parameter after `./run.sh` (for example, `/root/list.txt`) for specifying important files that you need to back up. The file path in `list.txt` should be an absolute path.

```
#vi /root/list.txt:
```

```
/etc/named.conf
```

```
/var/spool/cron/root
```

```
/etc/init.d/rcFirewall
```

6. Use the following commands to check the upgrade status:

```
# grep "\[IMSVA Upgrade\]" /mnt/backup/upgrade_log/imsva-upgrade.log; tail -f -- lines=0
```

```
/mnt/backup/upgrade_log/imsva-upgrade.log | grep "\[IMSVA Upgrade\]"
```

You can find the following status information when the upgrade completes:

```
[IMSVa Upgrade] IMSVA upgrade is complete.
```

7. Once IMSVA 8.5 installation completes, restart IMSVA services from the CLI console with the following command:

```
/mnt/backup/upgrade/dry_run.sh
```

8. Verify that IMSVA is working correctly after the upgrade.
9. To roll back to IMSVA 8.2 Service Pack 2, use the following commands:

```
/mnt/backup/upgrade/confirm.sh
```

```
"no"
```

10. If the IMSVA is working correctly after the upgrade, use the following commands to complete the upgrade:

```
/mnt/backup/upgrade/confirm.sh
```

```
"yes"
```

If you do not roll back to IMSVA 8.2 Service Pack 2 within 2 hours, all IMSVA services will stop automatically. You must then decide to roll back to IMSVA 8.2 Service Pack 2, or to complete the upgrade using the following command:

```
/mnt/backup/upgrade/confirm.sh
```

Type **yes** to complete the upgrade or **no** to roll back.

**Note**

IMSVa does not automatically generate reports if you roll back to a previous version. To enable automated reports, run the following command on the IMSVA CLI:

```
service crond start
```

Automated reports resume after approximately one hour. If waiting is not an option, reboot the device immediately after the rollback process.

Upgrading a Distributed Environment

IMSVa now supports upgrading an entire distributed deployment. For example, in a network where IMSVA is being used in a parent-child deployment.

Procedure

1. Backup IMSVA 8.2 Service Pack 2 to safeguard against any issues that may occur during the upgrade.



Tip

IMSVa 8.2 Service Pack 2 backs up the configuration settings and performs an auto-rollback if the upgrade is not successful. However Trend Micro recommends backing up IMSVA 8.2 Service Pack 2 in one of the following ways, before attempting to upgrade to IMSVA 8.5:

- Ghost the entire computer where IMSVA 8.2 Service Pack 2 is installed.
- Clone IMSVA 8.2 Service Pack 2, if it is installed on a virtual machine.
- Back up the IMSVA 8.2 Service Pack 2 `app_data` partition. To perform this task, open the operating system shell console and run the following commands:

```
/opt/trend/imss/script/imssctl.sh stop

service crond stop

cp -rf --preserve /var/app_data/* /var/udisk/
app_data_backup/
```

-
2. Download the IMSVA 8.5 upgrade package (for example, `IMSVa-Upgrade-Pkg-82SP2-To-85_1128.tgz` and `run.sh`).
 3. Use the following command in the CLI console to verify there are no messages in the Postfix queue:

```
postqueue -p
```

4. Stop all IMSVA services, except the database, using the following commands:

```
/opt/trend/imss/script/imssctl.sh stop

/opt/trend/imss/script/dbctl.sh start
```


5. On the Parent IMSVA, navigate to the directory where the upgrade package is stored and type the following command:

```
./run.sh
```

The upgrade script launches and performs a pre-installation check. If the pre-installation check is not successful, installation stops.

The upgrade package reboots IMSVA automatically after it finishes the pre-installation check.

After rebooting IMSVA, the upgrade package installs IMSVA 8.5. Wait until the installation completes.

6. Use the following commands to check the upgrade status:

```
# grep "\[IMSVA Upgrade\]" /mnt/backup/upgrade_log/imsva-  
upgrade.log; tail -f -- lines=0
```

```
/mnt/backup/upgrade_log/imsva-upgrade.log | grep "\[IMSVA  
Upgrade\]"
```

You can find the following status information when the upgrade completes:

```
[IMSVA Upgrade] IMSVA upgrade is complete.
```



WARNING!

Do not restart IMSVA services after upgrading the Parent IMSVA.

7. Upgrade all the Child IMSVAs one at a time, a few at a time, or all at once.



WARNING!

Do not restart IMSVA services until all IMSVAs have been upgraded.

If one of the Child IMSVAs encounters issues while upgrading, you can unregister the Child using the CLI, or if you are able to resolve the issue, you can retry the upgrade.

8. After upgrading all IMSVAs, restart IMSVA services for each IMSVA from the CLI console with the following command:

```
/mnt/backup/upgrade/dry_run.sh
```

9. Verify that IMSVA is working correctly after the upgrade.
10. To roll back to IMSVA 8.2 Service Pack 2, first roll back all Child IMSVAs and then the Parent with the following commands:

```
/mnt/backup/upgrade/confirm.sh
```

```
"no"
```

11. If the IMSVA is working correctly after the upgrade, use the following commands to complete the upgrade:

```
/mnt/backup/upgrade/confirm.sh
```

```
"yes"
```

If you do not roll back to IMSVA 8.2 Service Pack 2 within 2 hours, all IMSVA services will stop automatically. You must then decide to roll back to IMSVA 8.2 Service Pack 2, or to complete the upgrade, using the following command:

```
/mnt/backup/upgrade/confirm.sh
```

Type **yes** to complete the upgrade or **no** to roll back.

Batch Upgrade

Batch upgrade allows upgrading of two or more batches of parent and child devices. This option reserves log information during the upgrade process and does not cause any downtime.

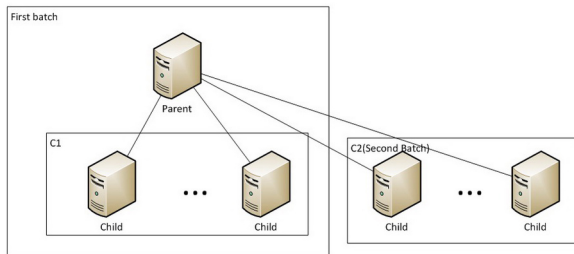


Tip

Trend Micro recommends performing batch upgrade when mail traffic is at a minimum. Evaluate if the IMSVA devices to be upgraded after the first batch can accommodate the total mail traffic during the upgrade process.

Batch upgrade is best performed between 4:00 and 22:00. The daemon service on the child devices may be restarted outside the recommended time period, preventing these devices from connecting to the parent device.

The following is an overview of the batch upgrade process:



1. Select the first batch of child devices to be upgraded.
2. Block connections between parent and child devices (with IP table or firewall), except devices selected in Step 1.



Note

At this stage, child devices should not be able to connect to the parent device but the parent device can connect to the child devices to conduct a pre-upgrade check.

3. Perform offline upgrade for the parent and child devices selected in Step 1.
4. Deploy the upgraded devices to production.
5. Perform offline upgrade for the rest of the child devices.
6. Restore the connection between the upgraded parent and child devices.
7. Deploy the upgraded devices to production.
8. Repeat the steps until all parent and child devices are upgraded.



Note

During the batch upgrade process, it is important to block the connection between parent and child devices.

Configure the firewall of the parent and child devices to block the second batch of child device upgrades. The child devices cannot be restarted unless the connection is blocked.

Step 1: Installing the Hot Fix or Critical Patch

Procedure

1. Upload the hot fix package or extract the critical patch package content.
 - Hot fix:
 - a. Copy the hot fix or patch package to the device from which you access the IMSVA management console.
 - b. Log on to the IMSVA management console.
 - c. Navigate to **Administration > Updates > System & Applications**.
 - d. Under **Upload**, click **Browse** and navigate to the folder that contains the hot fix or patch package.
 - e. Select the package and click **Open**.
 - f. Click **Upload**.
 - Critical patch:
 - a. Extract the files for the critical patch to a local folder.
2. Install the hot fix or critical patch.
 - Hot fix:
 - a. Navigate to **Administration > Updates > System & Applications**.
 - b. Under **Current Status**, select **IMSVa** and click **Update**.
 - c. Check the description and click **Install**.
 - d. Wait for the installation result. Update the screen as necessary.
 - Critical patch:
 - a. On the command line interface, run the following command:

```
cd ./imsva_82_criticalpatch17000
```
 - b. Run the following command:

```
./imssinst
```

Follow the screen prompts to complete the installation.

The following message appears after the system completes the installation:

“Installation is complete and related services are started.”

3. Check the installation result.
 - a. Navigate to **Administration > Updates > System & Applications**.
 - b. Check the **Current Status** section.
-

Step 2: Backing Up IMSVA 8.2 on Parent and Child Devices

Trend Micro recommends backing up IMSVA 8.2 using one of the following methods before attempting to upgrade to version 8.5.

- Clone the drive on which IMSVA 8.2 is installed.
- Back up the IMSVA 8.2 app_data partition. Open the operating system shell console and run the following commands:

```
# /opt/trend/imss/script/imssctl.sh stop  
  
# service crond stop  
  
# cd /var  
  
# mkdir udisk  
  
# cd udisk  
  
# mkdir app_data_backup  
  
# cp -rf --preserve /var/app_data/* /var/udisk/  
app_data_backup/  
  
# /opt/trend/imss/script/imssctl.sh start
```

Step 3: Preparing for Inline Upgrade

Procedure

1. Back up important settings.
 - a. The following files may be modified after upgrading or installing IMSVA 8.2.

Add the full path of the following files to the backup file list to prevent them from being modified during the installation or upgrade process.

```
#vi /root/list.txt  
  
/etc/named.conf  
  
/var/spool/cron/root  
  
/etc/init.d/rcFirewall
```



Note

Trend Micro recommends adding other important files to `list.txt`.

- b. Disable IP Profiler before performing inline upgrade. If IP Profiler is left enabled, child devices will attempt to connect to parent devices to obtain the results of the IP Profiler scan.
2. Stop scheduled component updates.

Perform this step to prevent the child daemon from restarting automatically.

 - a. Log on to the IMSVA 8.2 management console.
 - b. Navigate to **Administration > Updates > Components**.
 - c. Deselect **Enable scheduled update**.
 - d. Click **Save**.
-

Step 4: Blocking Connections Between Parent and Child Devices

Procedure

1. Select the first batch of devices to be upgraded (referred to hereafter as C1).
 - a. Select a parent device.
 - b. Select child devices.
 - c. Modify the DNS record to stop sending messages to the selected devices.
2. Configure the second batch of child devices (referred to hereafter as C2).

- a. Check the configuration of the C2 child devices.

```
# vi /opt/trend/imss/config/imss.ini
```

```
[policy_server]
```

```
disableldap=yes
```

```
disablePeriodicalQueryFromDB=yes
```

```
[general]
```

```
proc_max_connections = -1
```

- b. Restart the IMSVA service.

```
# /opt/trend/imss/script/imssctl.sh restart
```

- c. Stop the message tracing service.

```
# S99MSGTRACING stop
```

- d. Stop the monitor service.

```
# S99MONITOR stop
```

- e. Stop the manager service.

```
# S99MANAGER stop
```

- f. If EUQ is disabled, start the database services.

```
#/opt/trend/imss/script/dbctl.sh start
```

3. Change the iptables on the C2 child devices.

- a. Change the iptables.

```
# vi /etc/init.d/rcFirewall
```

At the end of start(), add the following rules:

```
iptables -I INPUT -s [parent's IP] -j DROP
```

```
iptables -I INPUT -s [C1's IP] -j DROP
```

```
iptables -I INPUT -s [parent's IP] -p tcp --sport 5432 -  
j ACCEPT
```

```
iptables -I INPUT -s [parent's IP] -p tcp --dport 5432 -  
j ACCEPT
```

- b. Apply the added rules.

```
# /etc/init.d/rcFirewall restart
```

4. Change the iptables on the parent and C1 devices.

- a. Change the iptables on both parent and C1 child devices.

```
# vi /etc/init.d/rcFirewall
```

- At the end of start(), add the following rule:

```
iptables -I INPUT -s [C2's IP] -j DROP
```

- On parent device, add the following rule:

```
iptables -I INPUT -s [C2's IP] -p tcp --sport 5432 -  
j ACCEPT
```

- b. Apply the added rules.

```
# /etc/init.d/rcFirewall restart
```

Step 5: Performing Inline Upgrade

Procedure

1. Verify that there are no messages in the Postfix queue on both parent and C1 devices.

- a. Check if there is sufficient disk space for the inline upgrade.

```
# df -m
```



Note

Ensure that the available disk space in `/dev/mapper/IMSVA-Snapshot` is greater than the used disk space in `/dev/mapper/IMSVA-Root1`.

- b. On the CLI console, check the Postfix queue.

```
# postqueue -p
```

The upgrade will continue only if the Postfix queue is empty. Otherwise, you may lose messages in the Postfix queue.

2. Stop all IMSVA services except the database services on both parent and C1 devices.

- a. Run the following commands:

```
# /opt/trend/imss/script/imssctl.sh stop
```

```
# /opt/trend/imss/script/dbctl.sh start
```

3. Perform inline upgrade to IMSVA 8.5.

Perform the upgrade first on the parent devices and then on the C1 devices.

- a. Download the IMSVA 8.5 upgrade package to the parent and child devices (for example, `IMSVA-Upgrade-Pkg-82SP2-To-85_1164.tgz`).

- b. Navigate to the directory in which the upgrade package is stored, and then run the following command:

```
# ./run.sh /root/list.txt
```

- c. Use the following commands to check the upgrade status:

```
# grep "\[IMSVa Upgrade\]" /mnt/backup/upgrade_log/
imsva-upgrade.log; tail -f -- lines=0

/mnt/backup/upgrade_log/imsva-upgrade.log | grep "\
\[IMSVa Upgrade\]"
```

You can find the following status information when the upgrade completes:

```
[IMSVa Upgrade] IMSVA upgrade is complete.
```

- d. After the parent completes the inline upgrade, proceed to upgrading the C1 devices.

4. Perform a test deployment of IMSVA 8.5.

- a. After successfully upgrading the C1 devices, modify the iptables on the parent device to establish a connection with a remote server. You can update the parent device's database data from this remote server.

```
# iptables -I INPUT -s [Remote server's IP] -p tcp --
sport 5432 -j ACCEPT

# iptables -I INPUT -s [Remote server's IP] -p tcp --
dport 5432 -j ACCEPT
```

- b. Log on to the parent device SQL database and update the table.

```
# select * from tb_component_list;

# update tb_component_list set app_ver='8.5.0.xxxx'
where ip_addr='[C2's IP]';
```



Note

This step enables IMSVA to bypass the check performed before the dry run.

Record the original IMSVA version (`app_ver`) of the C2 devices for reference in [Step 6: Performing Inline Upgrade for the Other Child Devices on page 5-20](#) (substep 2-c). Then, replace `8.5.0.xxxx` with the number of the IMSVA 8.5 build that you intend to install.

- c. Modify the iptables for the parent device:

```
# vi /etc/init.d/rcFirewall
```

At the end of start(), delete the following rule:

```
iptables -I INPUT -s [C2's IP] -p tcp --sport 5432 -j
ACCEPT
```

```
# /etc/init.d/rcFirewall restart
```

- d. On the CLI console, restart all IMSVA services.

```
# /mnt/backup/upgrade/dry_run.sh
```



Note

Restart the parent device first, and then all child devices.

5. Check the build number.
 - a. Navigate to **Administration > Updates > System & Applications**.
 - b. Under **Current Status**, check if the application version is 8.5.0.xxxx.
 6. Complete the inline upgrade.
 - a. To complete the upgrade on all parent and C1 devices, run the following command (first on the parent, and then on the C1 devices):


```
#/mnt/backup/upgrade/confirm.sh
"yes"
```
 - b. To roll back to IMSVA 8.2, first roll back all child devices, then the parent devices.


```
# /mnt/backup/upgrade/confirm.sh
"no"
```
 - c. Modify the DNS record to start sending messages to the upgraded parent and C1 devices, and to stop sending messages to the C2 devices.
-

Step 6: Performing Inline Upgrade for the Other Child Devices

**Note**

Child devices be upgraded individually or in batches.

Procedure

1. Verify that there are no messages in the Postfix queue.
 - a. Check if there is sufficient disk space for the inline upgrade.

```
# df -m
```
 - b. On the CLI console, check the Postfix queue.

```
# postfixqueue -p
```
2. Modify the settings for the C2 devices.
 - a. Restore the configuration of `imss.ini`.

```
# vi /opt/trend/imss/config/imss.ini

[policy_server]

disableldap=no

disablePeriodicalQueryFromDB=no

[general]

#proc_max_connections = -1
```
 - b. To bypass the inline upgrade check, change the iptables on the parent device.

```
# iptables -I INPUT -s [C2's IP] -p tcp --dport 5432 -j
ACCEPT
```
 - c. Change the IMSVA version for the C2 devices on the parent database.

```
# select * from tb_component_list;
```

```
# update tb_component_list set app_ver='8.2.0.xxxx'
where ip_addr='[C2's IP]';
```

**Note**

The IMSVA version (`app_ver`) should reflect the version that you recorded in [Step 5: Performing Inline Upgrade on page 5-17](#) (substep 4-b).

3. Stop all C2 IMSVA services, except the database service.

```
# /opt/trend/imss/script/imssctl.sh stop
# /opt/trend/imss/script/dbctl.sh start
```

4. Perform inline upgrade to IMSVA 8.5.

- a. Download the IMSVA 8.5 upgrade package to the C2 devices (for example, `IMSVA-Upgrade-Pkg-82SP2-To-85_1164.tgz`).

- b. Navigate to the directory in which the upgrade package is stored, and then run the following command:

```
# ./run.sh /root/list.txt
```

- c. Use the following commands to check the upgrade status:

```
# grep "\[IMSVA Upgrade\]" /mnt/backup/upgrade_log/
imsva-upgrade.log; tail -f -- lines=0
```

```
/mnt/backup/upgrade_log/imsva-upgrade.log | grep "\
\[IMSVA Upgrade\]"
```

You can find the following status information when the upgrade completes:

```
[IMSVA Upgrade] IMSVA upgrade is complete.
```

5. Perform a test deployment of IMSVA 8.5.

- a. Modify the iptables for the parent and C1 devices.

```
# vi /etc/init.d/rcFirewall
```

- At the end of `start()`, remove the following rule:

```
iptables -I INPUT -s [C2's IP] -j DROP
```

- Apply the above rules:

```
# /etc/init.d/rcFirewall restart
```

- b. Modify the iptables on the C2 devices:

```
# vi /etc/init.d/rcFirewall
```

- At the end of start(), delete the following rule:

```
iptables -I INPUT -s [parent's IP] -j DROP
```

```
iptables -I INPUT -s [C1's IP] -j DROP
```

```
iptables -I INPUT -s [parent's IP] -p tcp --sport  
5432 -j ACCEPT
```

```
iptables -I INPUT -s [parent's IP] -p tcp --dport  
5432 -j ACCEPT
```

- Apply the added rules:

```
# /etc/init.d/rcFirewall restart
```

- c. On the CLI console, restart all IMSVA services:

```
# /mnt/backup/upgrade/dry_run.sh
```

6. Check the build number.

- a. Navigate to **Administration > Updates > System & Applications**.
- b. Under **Current Status**, check if the application version is 8.5.0.xxxx.

7. Complete the inline upgrade.

- a. To complete the upgrade on all devices, run the following command:

```
#/mnt/backup/upgrade/confirm.sh
```

```
"yes"
```

- b. To roll back to IMSVA 8.2, run the following command:

```
# /mnt/backup/upgrade/confirm.sh
```

“no”

8. Restore the C2 devices.
 - a. Modify the DNS record and start sending messages to the C2 devices.
 - b. Continue upgrading the other child devices until the batch upgrade process is completed .
-

Offline Upgrade

During offline upgrade, a temporary IMSVA device is used to process email traffic. IMSVA logs all information and does not experience any downtime during the upgrade process.



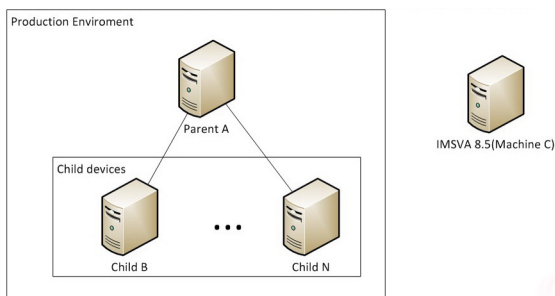
Tip

Trend Micro recommends performing offline upgrade when mail traffic is at a minimum. Evaluate if the temporary IMSVA device can accommodate the total mail traffic during the upgrade process.

When using offline upgrade:

1. Back up your files before deploying IMSVA to virtual machines.
 2. Use an NTP server to ensure that the production IMSVA devices and the temporary IMSVA device use the same system time.
-

The following is an overview of the offline upgrade process:



1. Install IMSVA 8.5 on a temporary device.
2. Import the configuration settings from the production IMSVA devices.
3. Modify the DNS MX record to redirect mail traffic to the temporary device.
4. Disconnect the production devices from the network.
5. Upgrade the devices.
6. Redirect mail traffic back to the production devices.
7. Copy the logs and queue folders from the temporary device to one of the production child devices.



Note

Data gaps may occur after restoring the data to the child devices. If Deep Discovery Advisor notifications are enabled, you may receive Deep Discovery Advisor service messages after data is restored.

Step 1: Installing IMSVA 8.5 on a Temporary Device

Procedure

1. Install IMSVA 8.5 on a temporary device using an ISO file.
2. Back up the default settings of the temporary IMSVA 8.5 device.
 - a. Log on to the parent device management console.
 - b. Navigate to **Administration > Import/Export**.
 - c. Click **Export** and save the exported files.
3. Export the settings of the existing parent and child devices.
 - a. Log on to the parent device management console.
 - b. Navigate to **Administration > Import/Export**.
 - c. Click **Export** and save the exported files.

4. Import the parent device settings to the temporary device.
 - a. Log on to the temporary device management console.
 - b. Navigate to **Administration > Import/Export**.
 - c. Click **Import**.
-

**Note**

If problems occur during the import process, restore the IMSVA 8.5 default settings using the backup file created in Step 2.

Step 2: Redirecting Mail Traffic to the Temporary IMSVA Device

Trend Micro recommends upgrading the production server when email traffic is minimal.

Procedure

1. Modify the DNS MX record to redirect the mail traffic to the temporary IMSVA device.
 2. Stop sending messages to the parent and child devices.
-

Step 3: Performing Offline Upgrade

Procedure

1. Upgrade the parent and child devices while offline. For more information, see [Upgrading a Distributed Environment on page 5-8](#).
2. Modify the DNS MX record to redirect mail traffic to the parent and child devices, with the exception of one child device.
3. Configure any customized settings that were lost in the upgrade process.

4. Stop sending messages to the temporary IMSVA device.
-

Step 4: Copying IMSVA 8.5 Logs and Queue Folder to a Child Device

Procedure

1. Stop the monitor, manager, and message tracing services on the child device (referred to as Machine B hereafter).

```
[root@machine B ~]# S99MONITOR stop
```

```
[root@machine B ~]# S99MANAGER stop
```

```
[root@machine B ~]# S99CMAGENT stop
```

```
[root@machine B ~]# S99MSGTRACING stop
```

2. If you enabled Deep Discovery Advisor on the temporary device, verify that there are no messages in the Deep Discovery Advisor upload folder.

```
[root@machine C ~]# ls -l /var/app_data/imss/dtas_upload/
```



Note

Trend Micro recommends disabling Deep Discovery Advisor on the temporary IMSVA device to prevent receiving notifications after log import. Ignore the notifications if you intend to keep Deep Discovery Advisor enabled.

3. Copy and merge the queue folder from the temporary IMSVA device to the Child B device.

```
[root@machine C ~]# scp -r /opt/trend/imss/queue  
root@machine B:/opt/trend/imss/
```

```
[root@machine B ~]# chown -R imss:imss /opt/trend/imss/  
queue
```

4. Copy the temporary IMSVA device policy event logs and append at the end of the latest Child B policy event logs.

For example:

```
[root@machine C ~]# scp /opt/trend/imss/log/polevt.imss.20130325.0001 root@machine B:/root/
```

```
[root@machine B ~]# cat /root/polevt.imss.20130325.0001 >> /opt/trend/imss/log/polevt.imss.20130325.0001
```

5. Copy the temporary IMSVA device mail logs and append at the end of the Child B mail logs.

```
[root@machine C ~]# scp /var/log/maillog root@machine B:/root/
```

```
[root@machine B ~]# cat /root/maillog >> /var/log/maillog
```

6. Copy the temporary IMSVA device fox* log and append at the end of the latest Child B fox* log.

For example:

```
[root@machine C ~]# scp /opt/trend/imss/log/foxmsg.20130325.0001 root@machine B:/root/
```

```
[root@machine B ~]# cat /root/foxmsg.20130325.0001 >> /opt/trend/imss/log/foxmsg.20130325.0001
```

7. On the Child B device, start the monitor, manager, and message tracking services. The appended log will be imported to the database shortly.

```
[root@machine B ~]# S99MANAGER start
```

```
[root@machine B ~]# S99MONITOR start
```

```
[root@machine B ~]# S99CMAGENT start
```

```
[root@machine B ~]# S99MSGTRACING start
```

8. After importing the appended log into the database, restore the Child B device settings by modifying the DNS MX record.

Verifying the Upgrade Using SSH

Procedure

1. Use the following command to check the upgrade status:

```
grep "\[IMSVA Upgrade\]" /mnt/backup/upgrade_log/imsva-  
upgrade.log; tail -f --lines=0 /mnt/backup/upgrade_log/  
imsva-upgrade.log | grep "\[IMSVA Upgrade\]"
```

Rolling Back an Upgrade

IMSVA rolls back automatically if there are problems during the upgrade process. However, if the automatic rollback encounters issues, you need to perform a manual rollback.

Procedure

1. If you created a ghost image or have a virtual machine image of your original IMSVA, replace the upgraded image with the original image.
2. If you backed up the data using `backup app_data`:

- a. Start the manual rollback with the following command:

```
/mnt/backup/upgrade/manual_rollback.sh
```

- b. Remove the data under `/var/app_data`.
- c. Copy your backup data to IMSVA, using the following commands:

```
cp -rf --preserve /var/udisk/App_data_backup/* /var/  
app_data/
```

- d. Reboot IMSVA.
-

Migrating from Previous Versions

IMSSVA 8.5 supports migration from previous versions of IMSS and IMSSVA.

The following table lists the minimum versions that support migration to IMSSVA 8.5:

TABLE 5-1. Supported Migration Platform and Versions

PLATFORM	VERSION
IMSS for Solaris	7.0 Service Pack 1 Patch 4
IMSS for Linux	7.1 Patch 3
IMSS for Windows	7.1 Patch 2
IMSSVA	8.0 Patch 2
IMSSVA	8.2 Service Pack 2

Migration Process

The migration process requires the following tasks:


- **Step 1:** Exporting the settings from previous versions of IMSS or IMSSVA
- **Step 2:** Importing the settings to IMSSVA 8.5

Exporting Settings from Previous Versions of IMSS or IMSSVA

The following settings do not migrate:

TABLE 5-2. Settings that Cannot Migrate

MTA SETTINGS	SETTINGS NOT MIGRATED
MTA Settings	IP address of SMTP Interface

MTA SETTINGS	SETTINGS NOT MIGRATED
Configuration Settings	Database settings (example: Internal file path)
	Management console password
	Control Manager settings
	Activation Codes
	 Note IMSVA 8.0 will migrate the Cloud Pre-Filter Activation Code to IMSVA 8.5



Important

When exporting configuration settings, ensure that the IMSS or IMSVA server is:

- Not performing database-related tasks.
- Not stopped or started.

Procedure

1. Navigate to **Administration > Import/Export** from the IMSS servers or IMSVA to migrate from.

The **Import/Export** screen appears.

2. Click **Export**.

The configuration settings export to a package that IMSVA can import.

Exporting Settings from IMSS 7.0 Service Pack 1 Patch 4 for Solaris

Procedure

1. Copy the migration tool package (`export_tool_sol_70.tar.gz`) on to the IMSS 7.0 for Solaris server.

2. Extract the export tool using the following command.

```
gzip -d export_tool_sol_70.tar.gz
tar xf export_tool_sol_70.tar
```

**Note**

The tool exports configuration settings to an encrypted package that can be used to duplicate these settings on other InterScan Messaging Security products.

3. Change the current working directory using the following command.

```
cd export70sol
```

4. Run the following command.

```
./export_tool_70.sh
```

The tool creates the exported settings package (`imss_config_70.tar.gz`) and a detailed log file (`export_70.<xxxxxxxx>.log`) in the current directory.

Importing Settings to IMSVA 8.5

Procedure

1. Perform a fresh installation of IMSVA 8.5.

**Tip**

Trend Micro recommends importing configuration packages to a fresh installation of IMSVA 8.5, because the imported configuration settings overwrite all existing settings.

2. Retrieve the package that contains the configuration settings that you wish to migrate.
3. Navigate to **Administration > Import/Export** on the IMSVA 8.5 management console.

The **Import/Export** screen appears.

4. Import the configuration package.

Migrating from IMSS for Windows

To migrate from IMSS for Windows to IMSVA 8.5, see [Migration Process on page 5-29](#).

IMSS 7.1 for Windows Settings that Change

The following table provides information on all settings for IMSS 7.1 for Windows that change during migration.

TABLE 5-3. IMSS 7.1 for Windows Settings that Change

SETTING	CHANGE
Email Reputation	During migration IMSVA 8.5 changes all customized actions to Default intelligent action , unless the customized action is Connection rejected with in which case the setting remains unchanged.
Transport Layer Security (TLS)	<ul style="list-style-type: none"> • Enable TLS on messages entering IMSS changes to the following in IMSVA 8.5: Enable incoming Transport Layer Security • Server Certificate settings are contained in the Private key <code>key.pem</code> and SMTP server certification <code>cert.pem</code> in IMSVA 8.5 • Trusted CA Certificate settings do not migrate. The settings must be retrieved from the IMSS 7.1 for Windows console and applied manually to the postfix settings. • The TLS IP Address/Domain List does not migrate. • All TLS Messages Exiting IMSS settings, except for the status, do not migrate. The status migrates to Enable outgoing Transport Layer Security.

SETTING	CHANGE
Domain-Based Delivery	<ul style="list-style-type: none"> • Default Delivery with Smart Host set, changes to * smtp:[IP]:port • If several Smart Hosts of a Domain were set, only the first Smart Host in the list migrates to IMSVA 8.5
Message Rule settings	The maximum date size/messages per connection settings are reduced.
Other settings	<p>The following Administration > Connections > Components internal ports do not migrate:</p> <ul style="list-style-type: none"> • IMSS manager port • Policy service port
Notifications	<p>Free disk space on any scanner less than changes to the following in IMSVA 8.5:</p> <p>Data partition on free space on any host less than</p>
Policy migration	The BATV rule and all related settings do not migrate.

Migrating from IMSS for Linux

To migrate from IMSS for Linux to IMSVA 8.5, see [Migration Process on page 5-29](#).

IMSS 7.1 for Linux Settings that Change

The following table provides information on all settings for IMSS 7.1 for Windows that change during migration.

TABLE 5-4. IMSS 7.1 for Linux Settings that Change

SETTING	CHANGE
Notifications	<p>The Administration > Notifications > Events notification:</p> <p>Free disk space on any scanner less than changes to the following in IMSVA 8.5:</p> <p>Data partition on free space on any host less than</p>

Migrating from IMSVA 8.0 Patch 2 or IMSVA 8.2 Service Pack 2

To migrate from previous IMSVA versions to IMSVA 8.5, see [Migration Process on page 5-29](#).

IMSVA 8.0 Settings that Change

All IMSVA 8.0 settings migrate to IMSVA 8.5.

IMSVA 8.2 Settings that Change

All IMSVA 8.2 settings migrate to IMSVA 8.5 except the following:

- All Control Manager agent settings
- Administrator account user name and password
- Patterns and engines
- SMTP interface and port number
- Some internal settings that affect system performance
- Encryption settings
- Deep Discovery Advisor settings

Exporting Debugging Files

If you need to analyze the debug files for troubleshooting purposes, you can export debug logs for up to the past two days for the parent device or any device that is registered to the parent device.



Note

The debug logs are contained in a password protected zip file. The default password for the file is `trend`.

Procedure

1. Navigate to **Administration > Export Debugging Files**.
2. Next to **Scanner**, select a device.
3. Select the number of days to export.
4. Click **Export**.

The process might take 10 minutes to 1 hour or more depending on the total log file size.

Chapter 6

Troubleshooting and Support Information

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

Troubleshooting

For common issues that you might encounter when installing IMSVA, see [Installation Troubleshooting Issues on page 6-3](#). 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

Installation Troubleshooting Issues

ISSUE	SUGGESTED RESOLUTION
Devices in a group cannot communicate	<p>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:</p> <ul style="list-style-type: none">• 5060: Policy service• 15505: IMSVA control service• 53 UDP/TCP: IP Profiler• 5432: Database service• 8009: EUQ internal service• 389: LDAP local cache service <p>Also, verify the following:</p> <ul style="list-style-type: none">• The current firewall settings in “iptables”.• The firewall configuration files in <code>/etc/conf/fw.rules</code>.• 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. <p>Also, verify that all the necessary port IMSVA uses are accessible for the relevant services (see).</p>

ISSUE	SUGGESTED RESOLUTION
Child device has trouble registering to a parent	<p>Do the following:</p> <ol style="list-style-type: none">1. Open the parent device's management console and navigate to Administration > IMSVA Configuration > Connections > Child IP.2. Verify that the IP address of the child is on the Child IP Address List.3. In the Configuration Wizard, verify that Child is selected for the device role.4. Verify that the Admin Database is accessible.5. Unregister the MCP agent (if MCP agent is enabled).6. Verify that no other child device registered to the parent has the same IP address as the device you are trying to register.7. Remove all the logs and quarantined messages.8. Change the configuration and restart the services. <p>The parent device management 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:</p> <pre data-bbox="498 943 1076 992">/opt/trend/imss/script/cfgtool.sh reg IPADDR sa postgresQL</pre>

ISSUE	SUGGESTED RESOLUTION
<p>Child device has trouble unregistering from the parent</p>	<p>Do the following:</p> <ol style="list-style-type: none"> 1. Connect to the child device through the command line interface. 2. Check whether the Admin Database is accessible. If yes, remove the child device from the Child IP list on the parent management console and update the trusted child list. 3. Rescue the device, which will forcibly unregister it from the parent. 4. Update the patches. <p>To verify that a child is unregistered from its parent, try to access the management console on the child device. If the console is accessible, the device is successfully unregistered.</p> <p>You can also run the following command:</p> <pre data-bbox="596 781 1072 802">/opt/trend/imss/script/cfgtool.sh dereg</pre>

Support Information

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

<http://community.trendmicro.com/>

Using the Support Portal

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

Procedure

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

The **Technical Support** product page appears.

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

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

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

Security Intelligence Community

Trend Micro cyber security experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to <http://www.trendmicro.com/us/security-intelligence/index.html> to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media
- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to <http://www.trendmicro.com/vinfo> to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

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

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

- Worldwide support offices:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Trend Micro product documentation:
<http://docs.trendmicro.com>

Speeding Up the Support Call

To improve problem resolution, have the following information available:

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

Sending Suspicious Content to Trend Micro

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

File Reputation Services

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

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

Record the case number for tracking purposes.

Email Reputation Services

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

<https://ers.trendmicro.com/>

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

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

Web Reputation Services

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

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

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

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

<http://trendedge.trendmicro.com/>

Download Center

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

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

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

TrendLabs

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

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

Learn more about TrendLabs at:

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

Appendix A

Creating a New Virtual Machine Under VMware ESX for IMSVA

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

Topic included:

- *Creating a New Virtual Machine on page A-2*

Creating a New Virtual Machine

The actual installation of ESX 4.1/4.0 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.

Procedure

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

The **New Virtual Machine Wizard** appears.

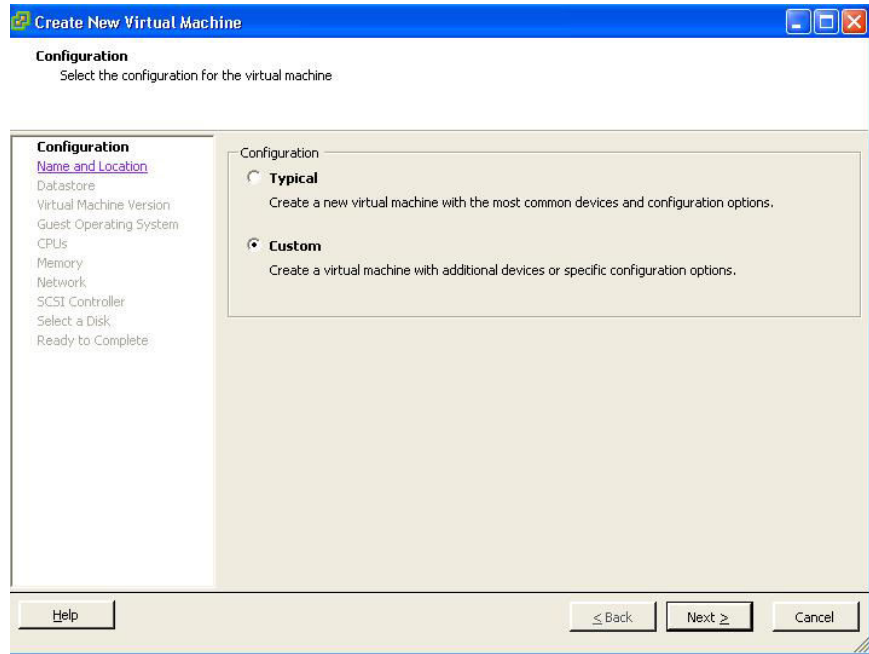


FIGURE A-1. Virtual Machine Configuration

2. Under **Virtual Machine Configuration**, leave the **Typical** radio button selected.
3. Click **Next**.

The **Name and Location** screen appears.

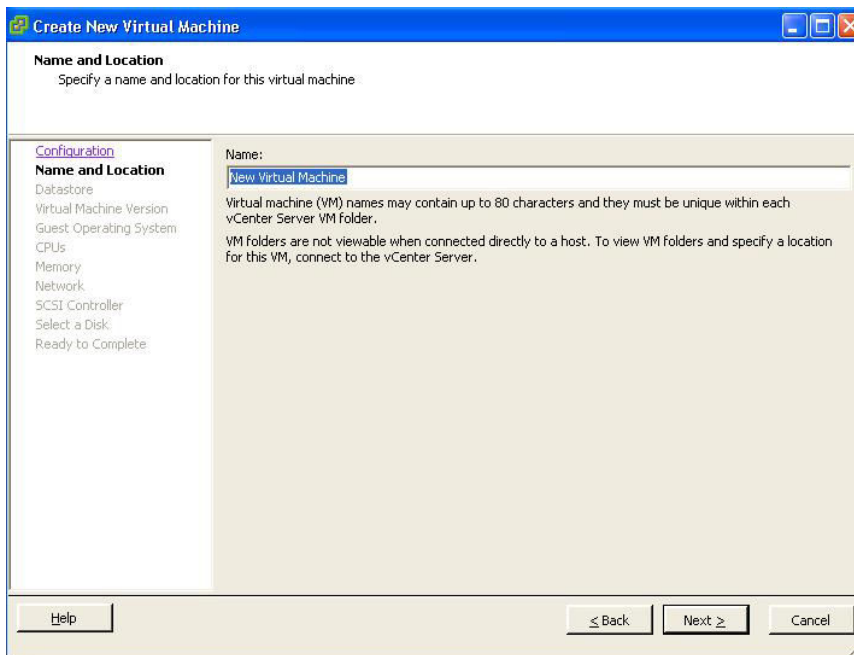


FIGURE A-2. Select a Name and Location for this Virtual Machine

4. In the **Name** field, type an appropriate machine name and then click **Next**.

The **Datastore** screen appears.

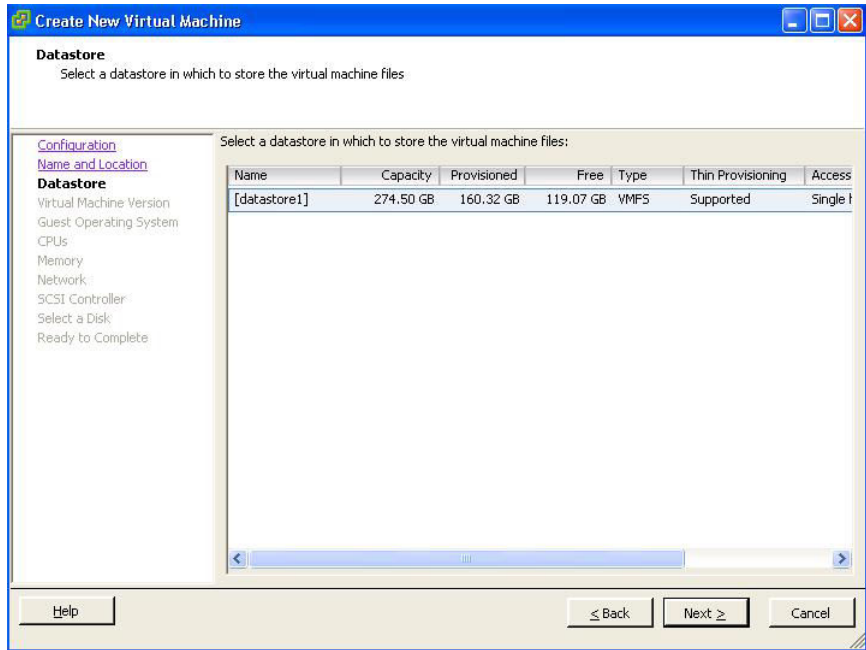
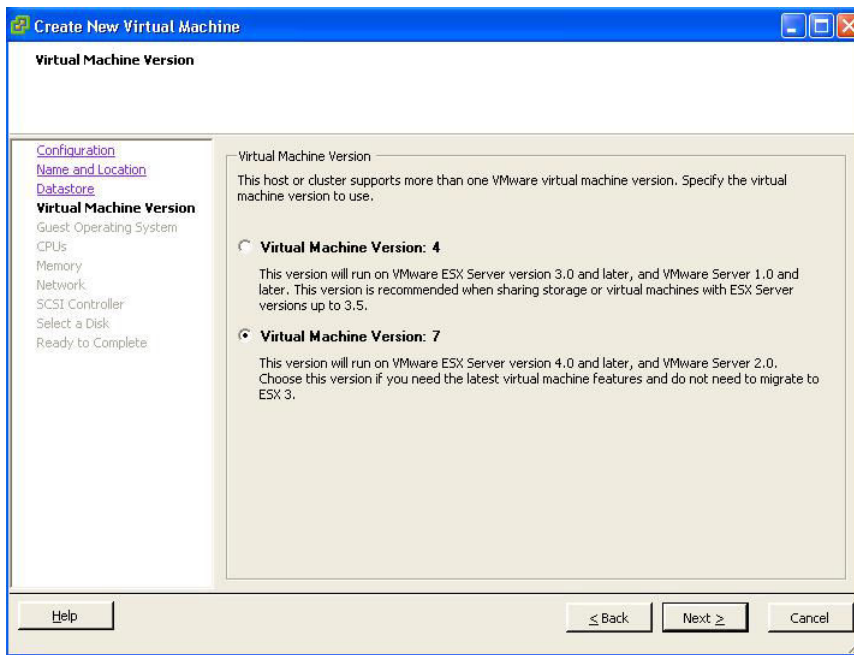


FIGURE A-3. Virtual Machine Datastore

5. Select the datastore where the virtual machine will reside.
6. Click **Next**.

The **Virtual Machine Version** screen appears.



7. Specify the virtual machine version to use.
8. Click **Next**.

The **Guest Operating System** screen appears.

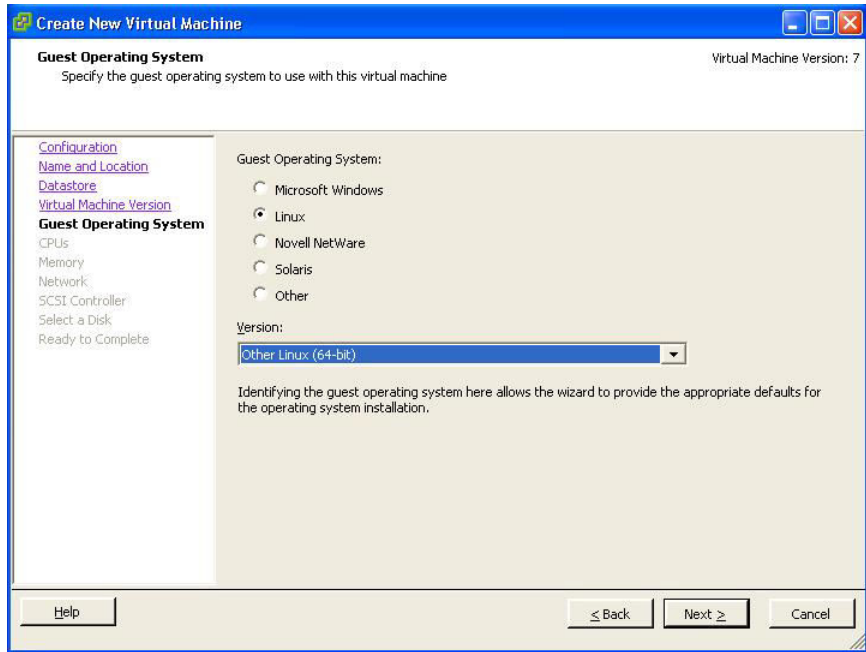


FIGURE A-4. Virtual Machine Guest Operating System

9. For the guest operating system, select **Linux > Other Linux (64-bit)**.
10. Click **Next**.

The **CPUs** screen appears.

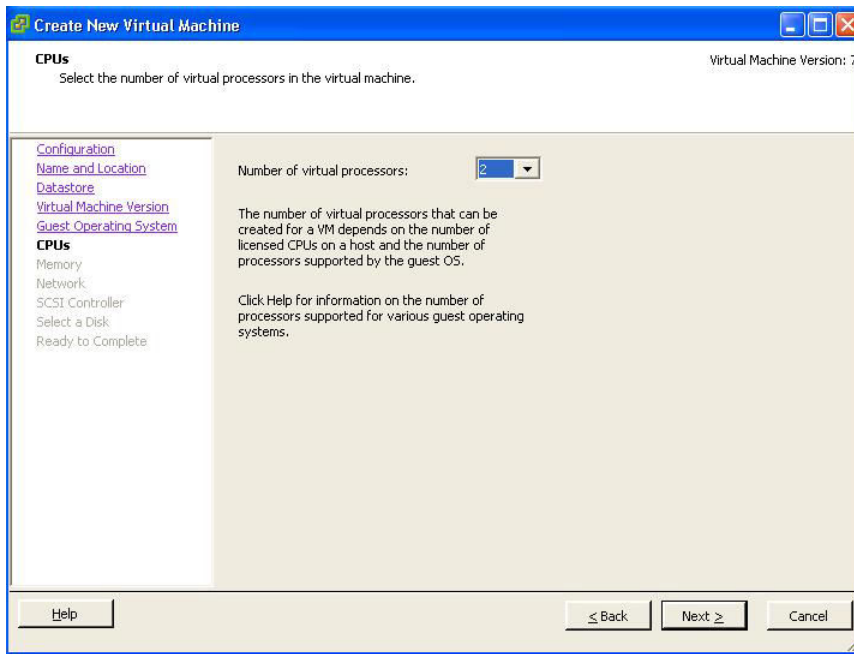


FIGURE A-5. Virtual Machine CPU

11. 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.
12. Click **Next**.

The **Memory** screen appears.

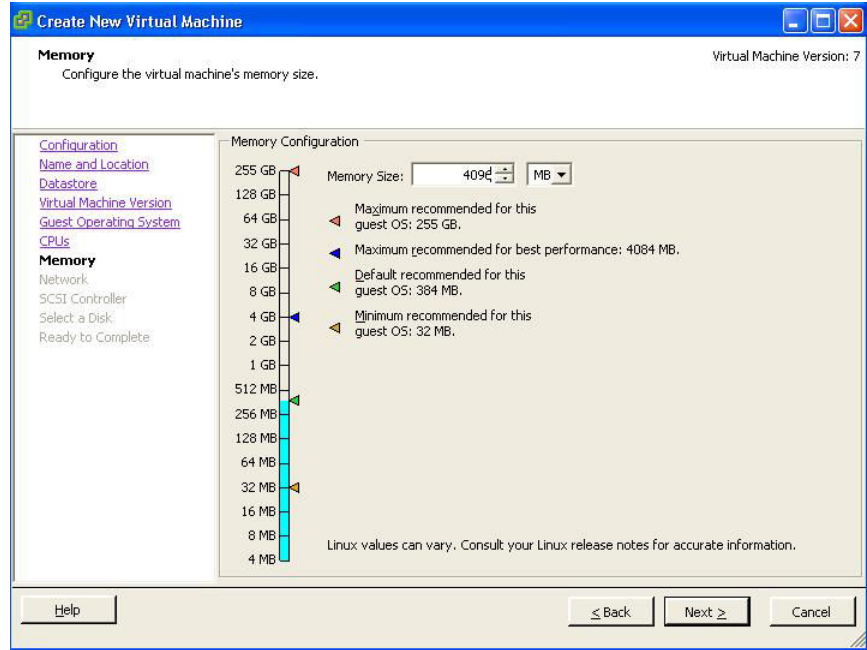


FIGURE A-6. Virtual Machine Memory

13. Allocate 4096MB of memory as a minimum for IMSVA.



Tip

For improved performance, Trend Micro recommends at least 8192MB of RAM.

14. Click **Next**.

The **Network** screen appears.

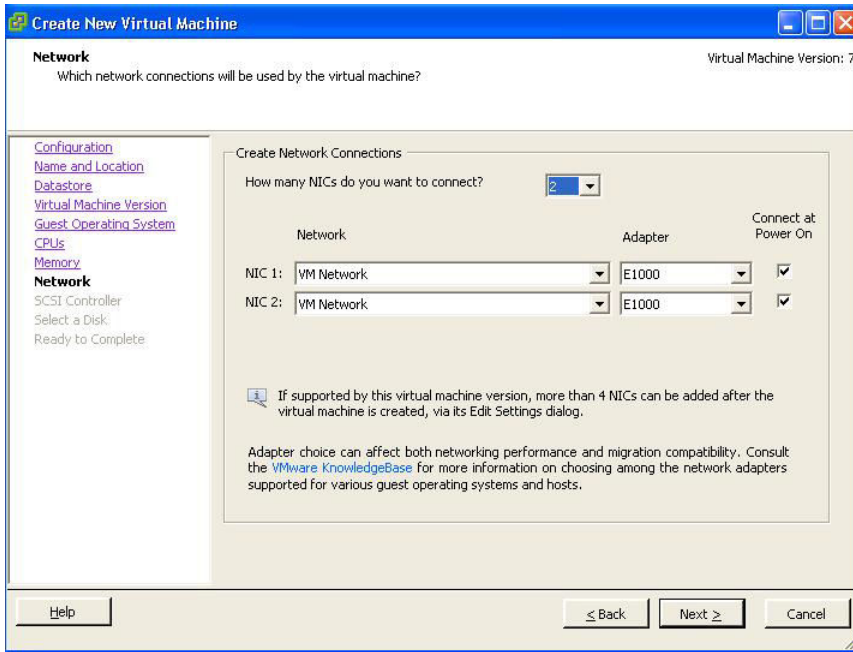
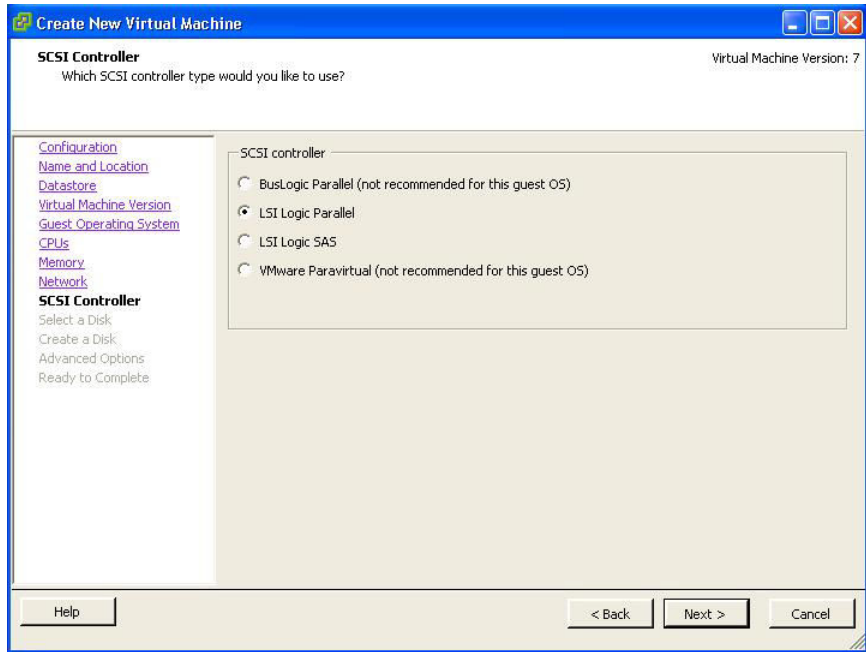


FIGURE A-7. Virtual Machine Network

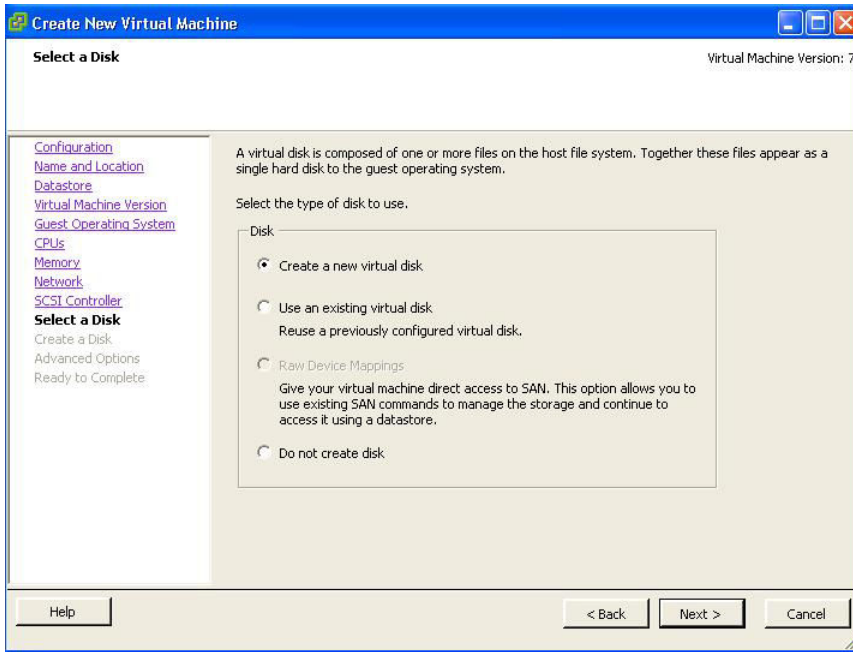
15. Accept the default network settings.
16. Click **Next**.

The **SCSI Controller** screen appears.



17. Select **LSI Logic Parallel**.
18. Click **Next**.

The **Select a Disk** screen appears.



19. Select **Create a new virtual disk**.
20. Click **Next**.

The **Create a Disk** screen appears.

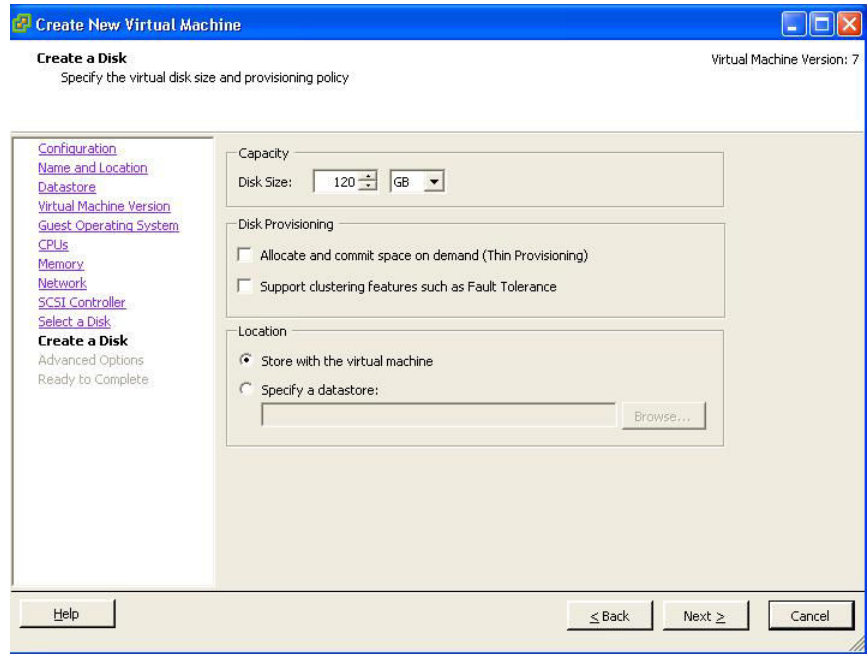


FIGURE A-8. Virtual Disk Capacity

21. Specify at least 120GB of disk space. IMSVA requires at least 120GB disk space. See for more information on disk space allocation.

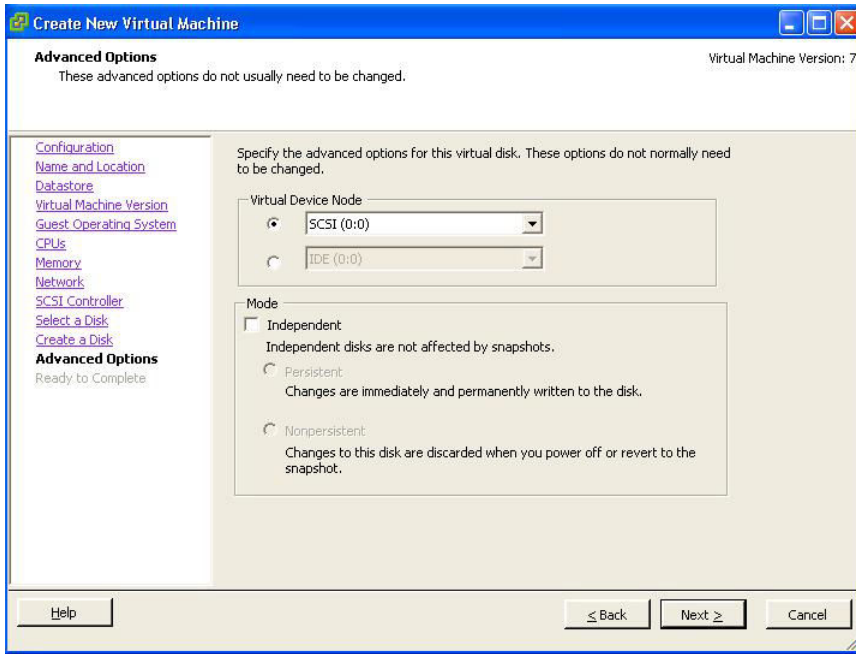


Tip

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

22. Click **Next**.

The **Advanced Options** screen appears.



23. Specify the advanced options if required. Usually these options do not need to be changed.
24. Click **Next**.

The **Ready to Complete** screen appears.

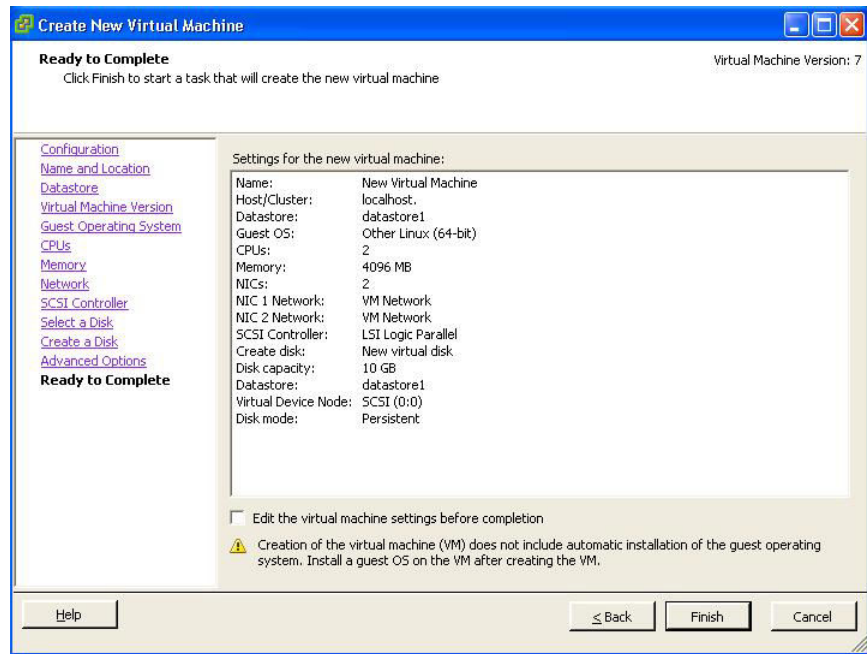


FIGURE A-9. Ready to Complete

25. 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**.

26. 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.

Appendix B

Creating a New Virtual Machine Under Microsoft Hyper-V for IMSVA

This appendix describes how to create a new virtual machine for IMSVA under Microsoft Hyper-V.

Topics include:

- *Understanding Hyper-V Installation on page B-2*
- *Installing IMSVA on Microsoft Hyper-V on page B-2*
- *Using Para-Virtualization Mode on page B-18*
- *Using NTP on IMSVA on page B-21*

Understanding Hyper-V Installation

IMSVA supports installation on Microsoft Hyper-V based virtual platforms. This appendix provides step-by-step instructions to install IMSVA on Hyper-V based virtual machines. The actual installation of Hyper-V is not covered in this document. Refer to Microsoft product documentation to install Hyper-V. The procedure outlined in this appendix describes how to install IMSVA on a Windows 2008 Server R2 Hyper-V server.

IMSVA Support for Hyper-V

IMSVA only supports Hyper-V on Windows Server 2008 R2 and Windows Server 2008 R2 with SP1 or later.

Hyper-V Virtualization Modes

Hyper-V provides two virtualization modes that support IMSVA:

- Full-virtualization
- Para-virtualization

**Tip**

Trend Micro recommends installing IMSVA in para-virtualization mode. This allows IMSVA to achieve much higher throughput performance and supports enterprise networking environments. IMSVA provides the necessary integrated Hyper-V drivers to support the installation under Hyper-V as a para-virtualization virtual machine.

Installing IMSVA on Microsoft Hyper-V

Use the following steps as a guideline for creating a 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 provided are for instructional purposes.

**Note**

Creating a New Virtual Machine on page B-6 only covers installing IMSVA on Hyper-V in full-virtualization mode. *Using Para-Virtualization Mode on page B-18* describes how to convert full-virtualization to para-virtualization.

Creating a Virtual Network Assignment

Procedure

1. From the Hyper-V **Server Manager** menu, right-click **Hyper-V Manager**.

A menu appears.

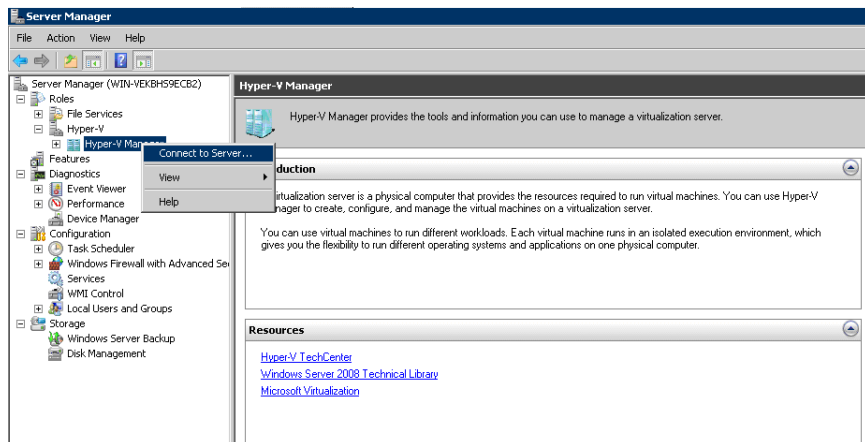


FIGURE B-1. Connect to Server

2. Select **Connect to Server**.

A dialog box appears prompting you to select the location of the virtualization server that you want to connect to.

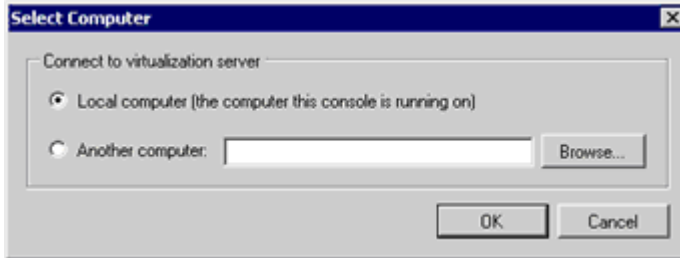


FIGURE B-2. Location of Virtualization Server

3. Specify the location of the virtualization server and click **OK**.
4. Right-click the Windows 2008 R2 server and select **Virtual Network Manager**.

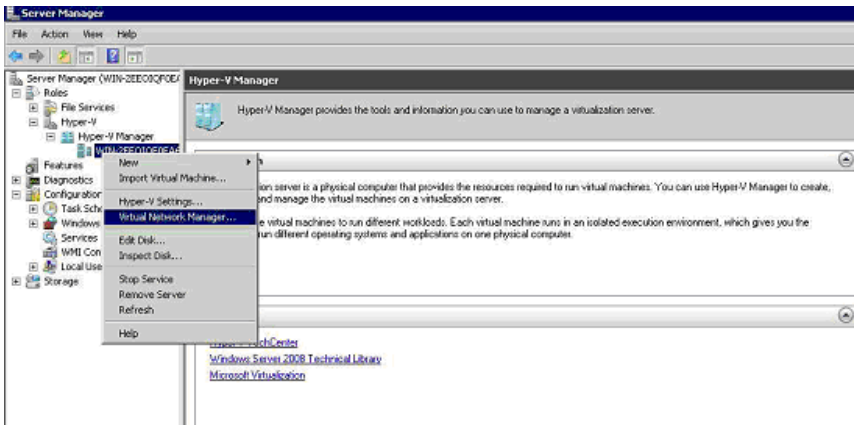


FIGURE B-3. Select Virtual Network Manager

5. Create a new virtual network by selecting **External** from the list of options and clicking **Add**.

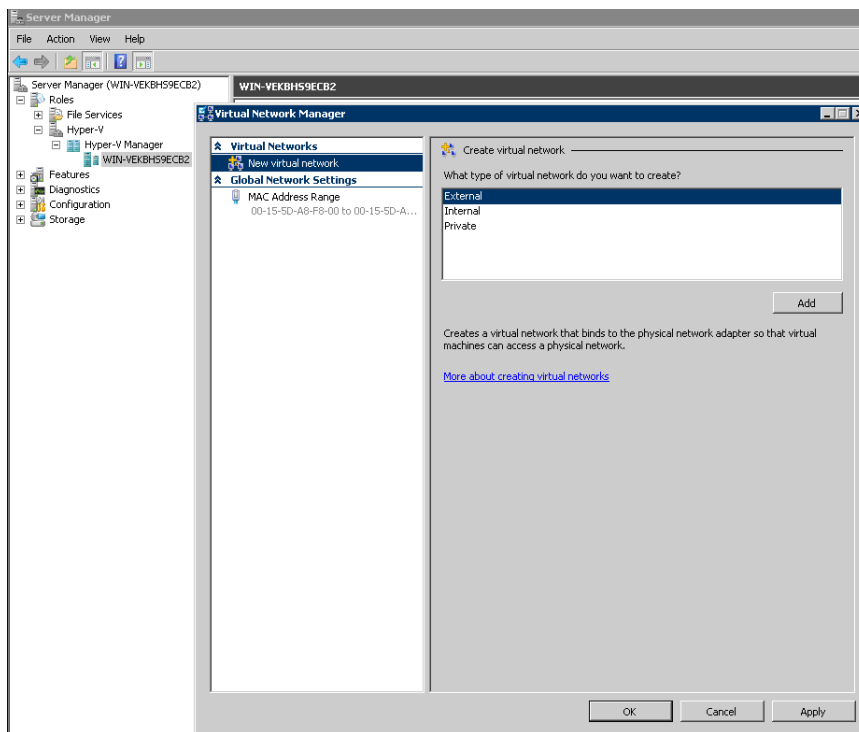


FIGURE B-4. Adding the “External” Virtual Network

- From the **External** drop-down menu, select the physical network adaptor you want to connect to.



Note

The physical adaptor must be connected to the network and have access to the corporate network and the Internet.

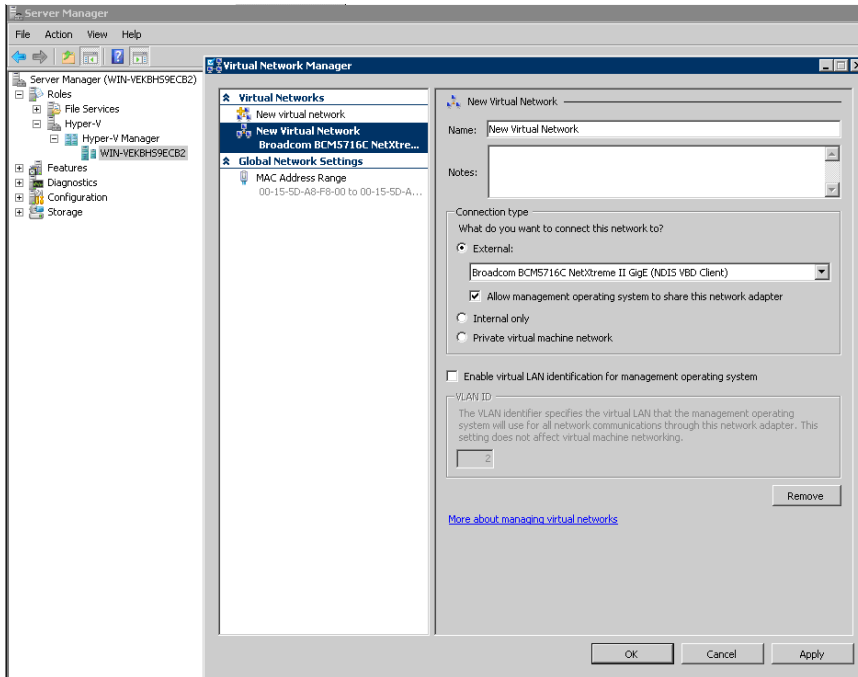


FIGURE B-5. Physical Network Adaptor Selection

Creating a New Virtual Machine

Procedure

1. From the Hyper-V Server Manager menu, right-click the Windows 2008 R2 server, and select **New > Virtual Machine**.

The **New Virtual Machine Wizard** appears.

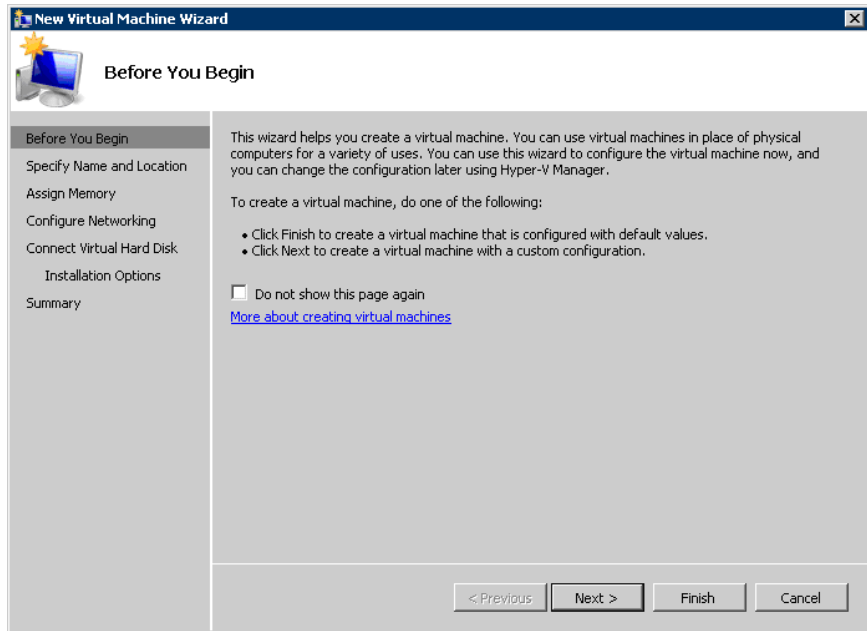


FIGURE B-6. New Virtual Machine Wizard

2. Click **Next**.

The **Specify Name and Location** screen appears.

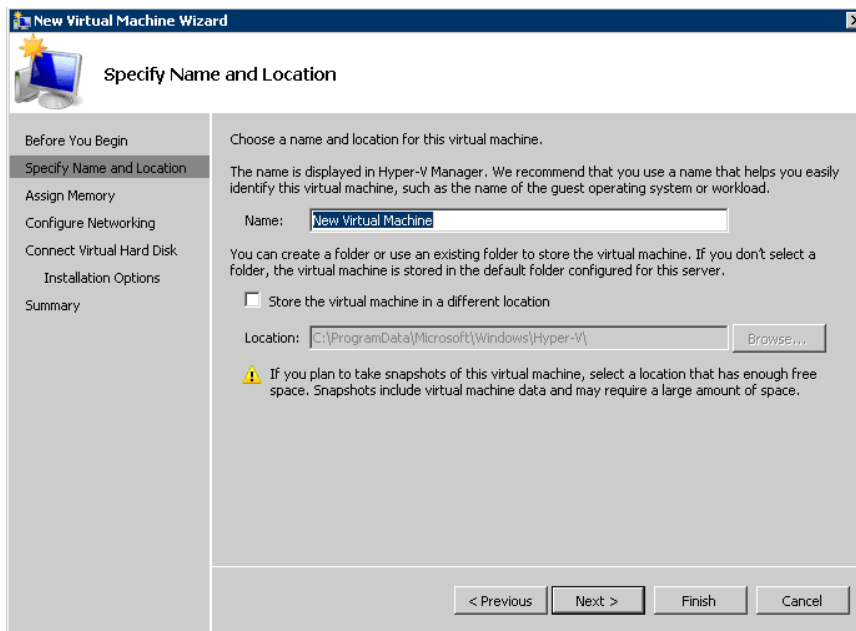


FIGURE B-7. Specify Name and Location

3. In the **Name** field, type a meaningful machine name. If you plan to store the virtual machine to another folder, select **Store the virtual machine in a different location** and provide the correct location.
4. Click **Next**.

The **Assign Memory** screen appears.

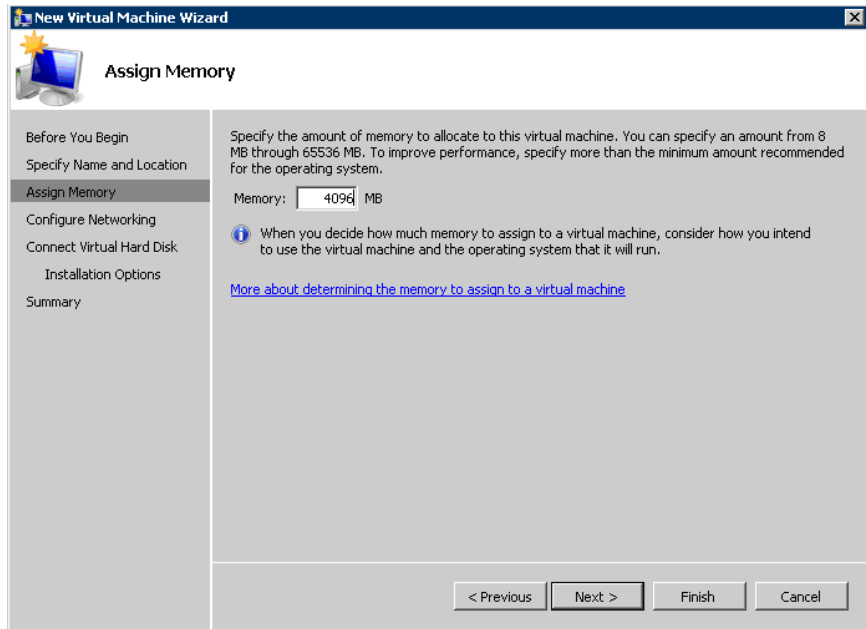


FIGURE B-8. Assign Memory

5. Allocate at least 4096MB of memory for IMSVA.



Tip

Trend Micro recommends allocating 8192MB of RAM.

6. Click **Next**.

The **Configure Networking** screen appears.

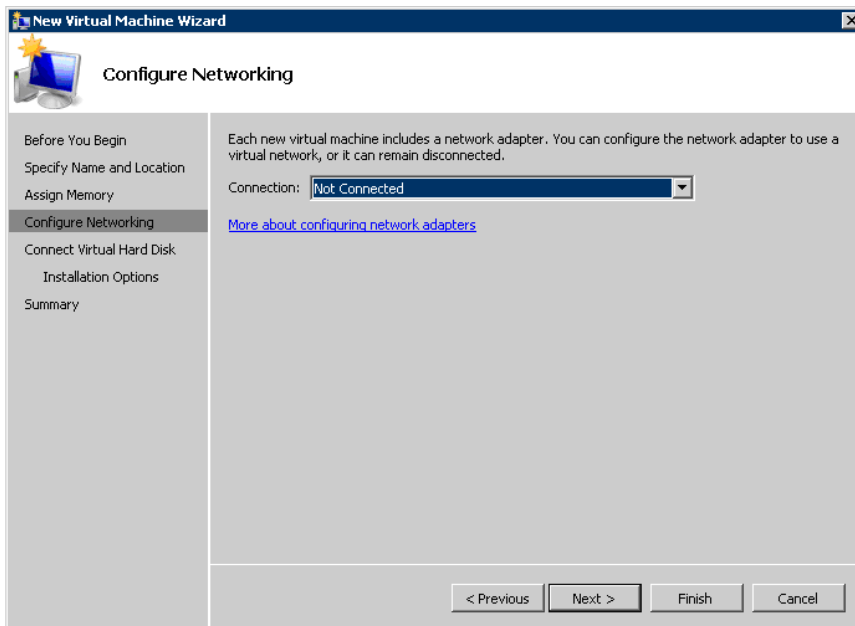


FIGURE B-9. Configure Networking

7. Keep the default network settings **Not Connected**.
8. Click **Next**.

The **Connect Virtual Hard Disk** screen appears.

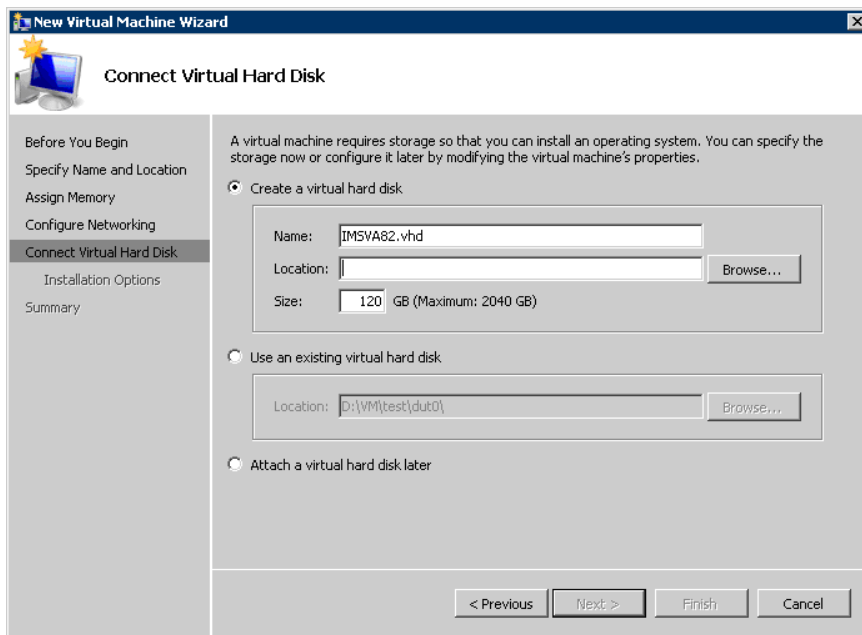


FIGURE B-10. Connect the Virtual Hard Disk

9. Specify at least 120GB disk space for IMSVA.



Tip

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

10. Specify a location to store the virtual hard disk, and click **Next**.

The **Installation Options** screen appears.

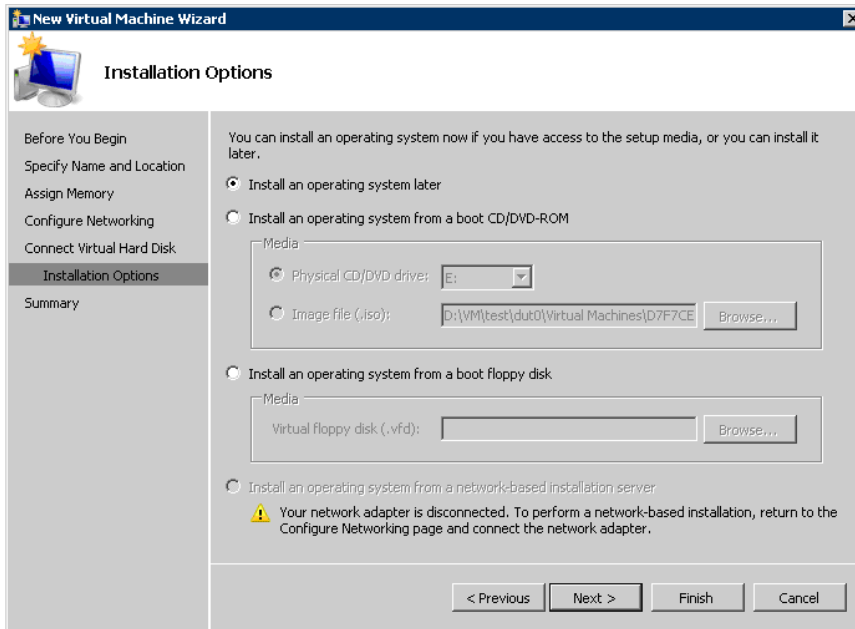


FIGURE B-11. Installation Options

11. Keep the default setting **Install an operating system later**, and click **Next**.

The **Completing the New Virtual Machine Wizard** screen appears.

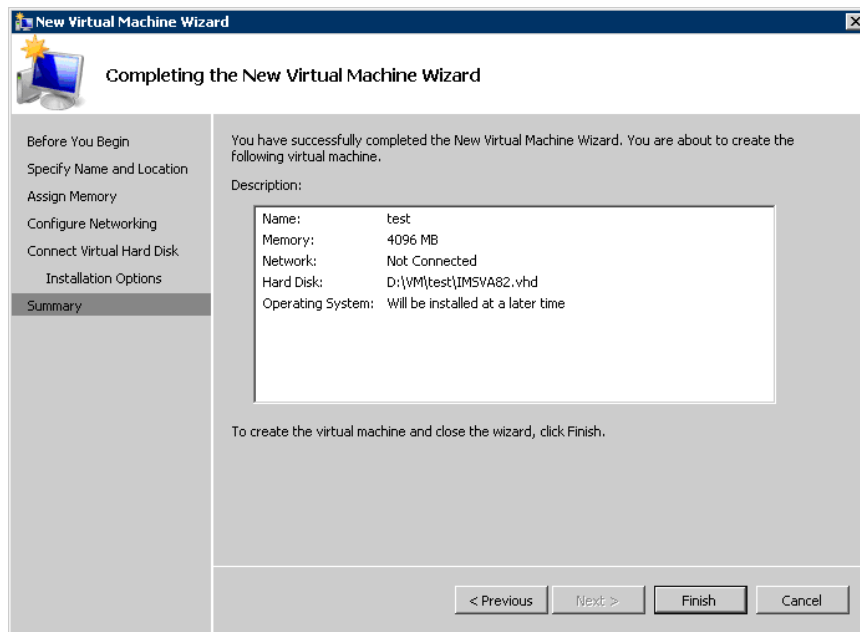


FIGURE B-12. Completing the New Virtual Machine Wizard

12. Verify your settings and click **Finish**. Some manual configuration is still required.
13. Right-click your new Virtual Machine, and select **Settings**.

The **Settings for test** screen appears.

14. Click **Add Hardware**, and select **Legacy Network Adapter**.

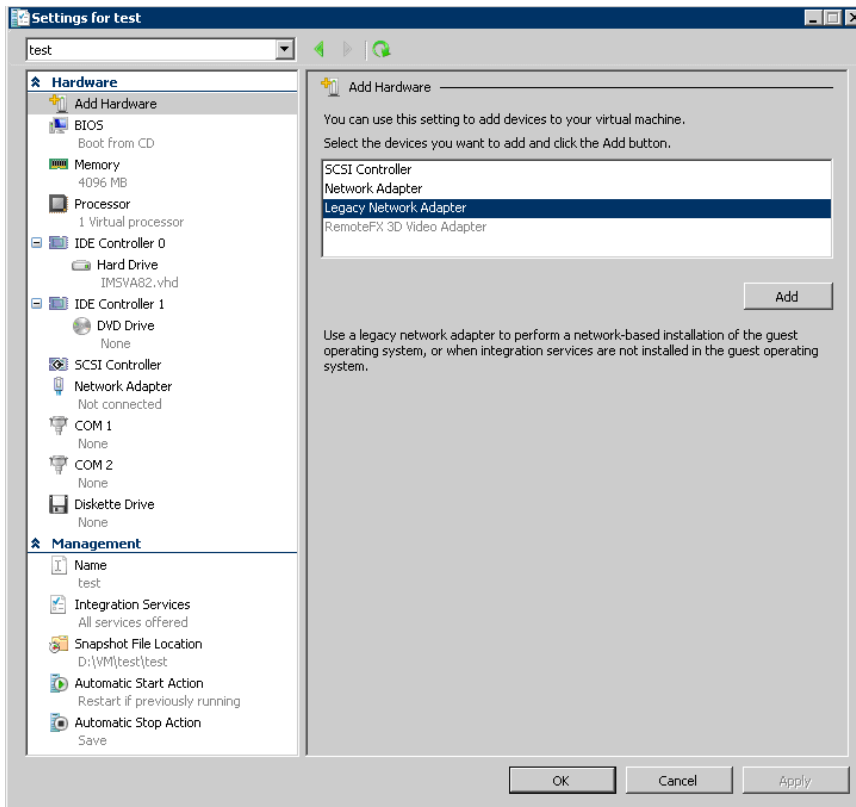


FIGURE B-13. Add Hardware: Legacy Network Adapter

15. Select the correct virtual network adapter.
16. Click **OK**.

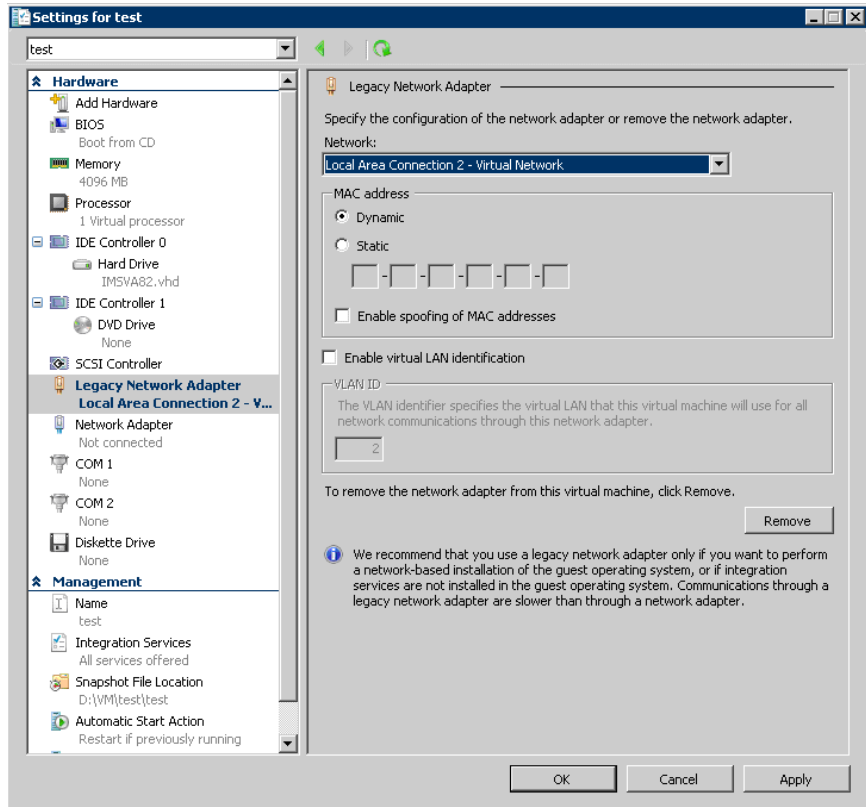


FIGURE B-14. Configure Legacy Network Adapter

17. Remove the **Network Adapter** from the Hardware list.
18. Click **OK**.

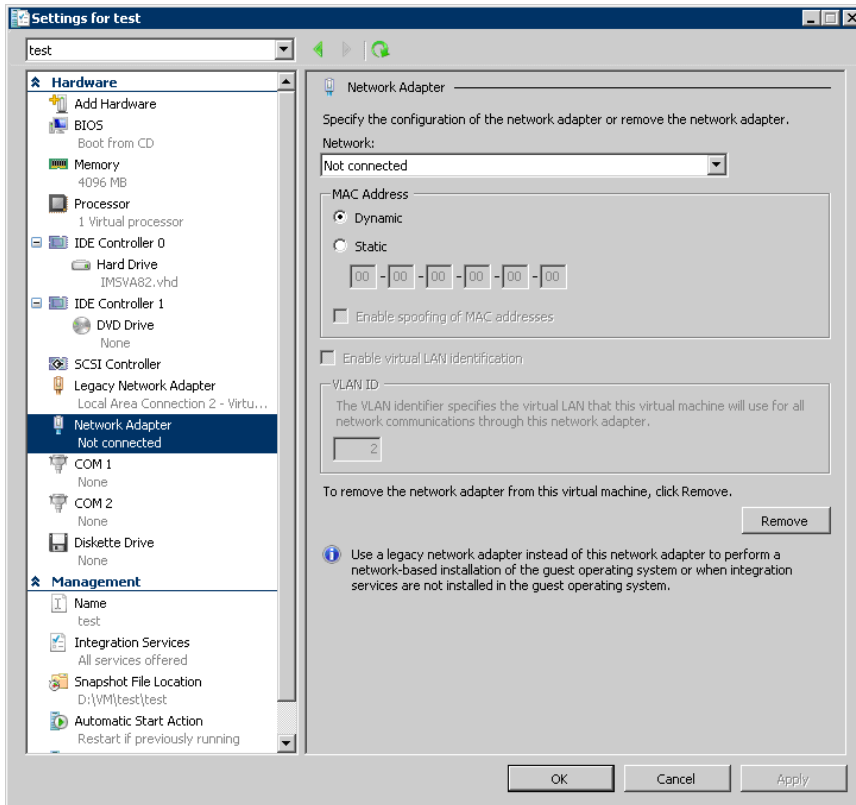


FIGURE B-15. Remove Network Adapter

19. Select the image file for IMSVA from the DVD Drive in the Hardware list.
20. Click **OK**.

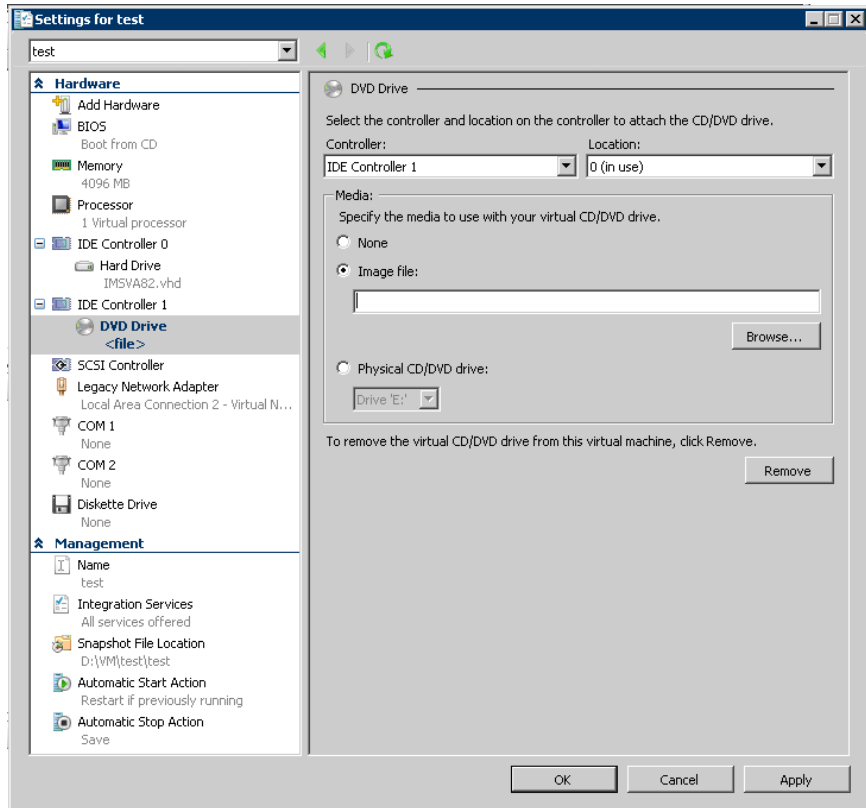


FIGURE B-16. Add Image file into DVD Drive

The virtual machine is now ready to be powered on to begin the installation process.

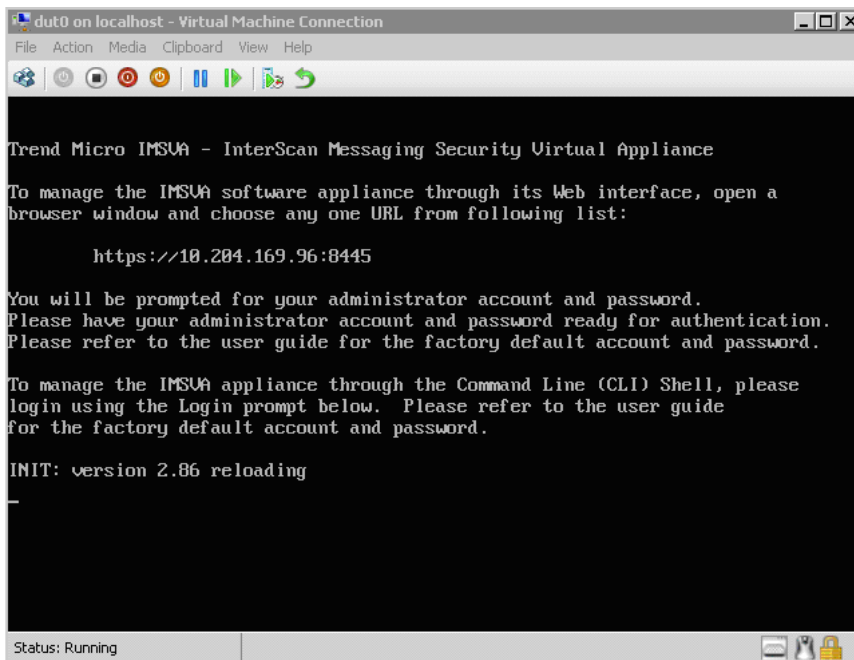


FIGURE B-17. IMSVA installed on a Hyper-V virtual machine

Using Para-Virtualization Mode

If IMSVA has been installed on a Hyper-V virtual machine with Full-Virtualization Mode, you can enable the appropriate drivers to make IMSVA enter Para-Virtualization Mode.

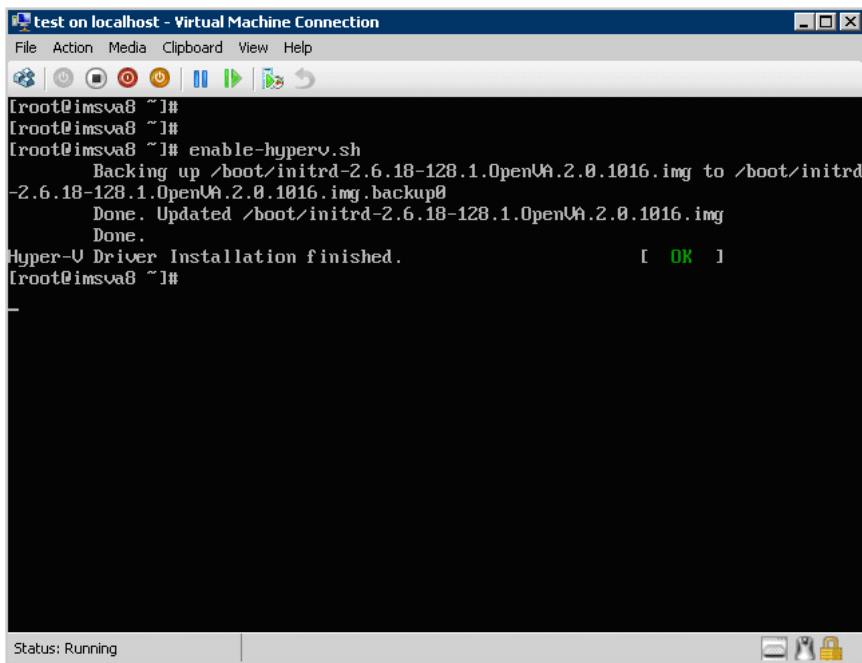
**Tip**

Trend Micro recommends using IMSVA in Para-Virtualization Mode. This allows IMSVA to achieve much higher throughput performance and supports enterprise networking environments. IMSVA provides the necessary integrated Hyper-V drivers to support the installation under Hyper-V as a para-virtualization virtual machine.

Procedure

1. Open the CLI console and backup your current network configuration.
2. Enable Hyper-V Para-Virtualization drivers using the following commands:

```
[root@imsva8 ~]# enable-hyperv.sh
Backing up /boot/initrd-2.6.18-128.1.OpenVA.2.0.1020.img to
/boot/initrd-2.6.18-128.1.OpenVA.2.0.1020.img.backup0
Done. Updated /boot/initrd-2.6.18-128.1.OpenVA.2.0.1020.img
Done.
Checking for new synthetic nics...
Hyper-V Driver Installation finished.
```



```
test on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
[root@imsva8 ~]#
[root@imsva8 ~]#
[root@imsva8 ~]# enable-hyperv.sh
    Backing up /boot/initrd-2.6.18-128.1.OpenVA.2.0.1016.img to /boot/initrd-2.6.18-128.1.OpenVA.2.0.1016.img.backup0
    Done. Updated /boot/initrd-2.6.18-128.1.OpenVA.2.0.1016.img
    Done.
Hyper-U Driver Installation finished.           [ OK ]
[root@imsva8 ~]#
Status: Running
```

FIGURE B-18. Move to Para-Virtualization Mode

3. Shut down IMSVA:

```
[root@imsva82 ~]# poweroff
```

4. Reconfigure the Virtual Network Adapter on the Virtual Machine Settings screen.
 - Remove the **Network Adapter**

- Add a network adapter with the correct virtual network adapter.

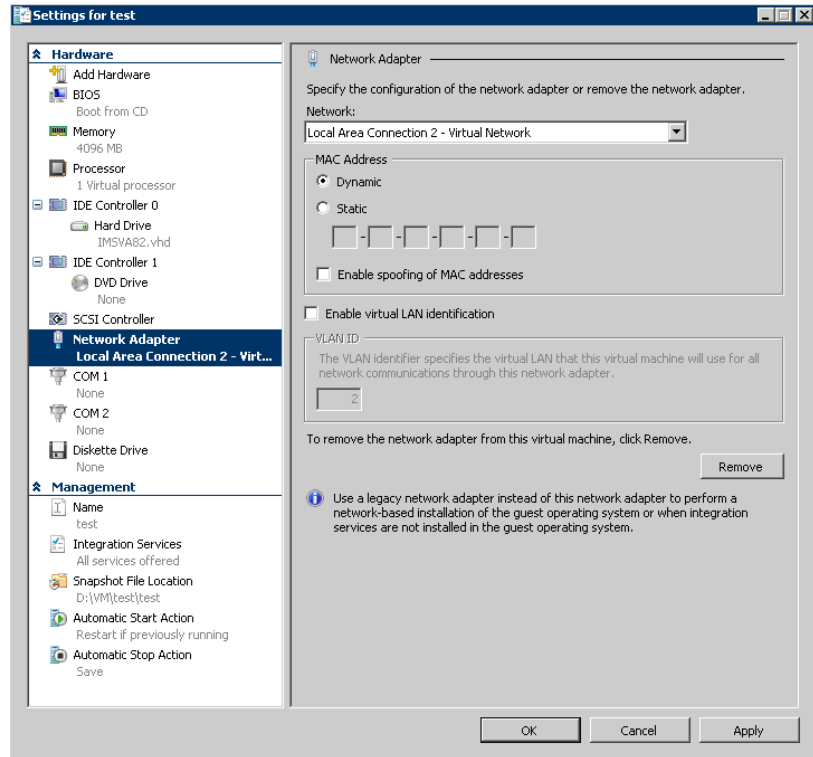


FIGURE B-19. Change Network Adapter

5. Power on the virtual machine. Open the CLI console and reconfigure the network configuration. The virtual machine is now in Para-Virtualization Mode.

Using NTP on IMSVA

Procedure

1. Disable the time synchronization service in Hyper-V.

- a. Navigate to the Hyper-V settings screen.
 - b. Under Integration Services, disable **Time synchronization**.
2. Use an SSH client to connect to IMSVA and modify the kernel boot options by editing the GRUB configuration file (/boot/grub/grub.conf). Add the following to the appropriate kernel line:

```
notsc divider=4
```

For example:

```
title IMSVA (2.6.18-128.1.OpenVA.2.0.1067)
root (hd0,0)
kernel /vmlinuz-2.6.18-128.1.OpenVA.2.0.1067
ro root=/dev/IMSVA/Root2 quiet notsc divider=4
```

**Note**

The divider accepts only values between 1 and 4.

3. Synchronize the system time manually.

```
$ service ntpd stop
$ ntpdate [ntp server]
```
 4. On another SSH session, set the hardware clock to the newly synchronized time.

```
$ hwclock --systohc
```
 5. Reboot the IMSVA device.
-

Index

A

about IMSS appliances, 1-2
 adware, 1-11
 archive, xi
 audience, xiii

C

centralized archive and quarantine, xi
 centralized logging, xi
 centralized policy, xi
 Centralized Reporting, 2-8
 Command & Control (C&C) Contact Alert Services, 1-17
 community, 6-5
 configuration wizard, xii
 Control Manager
 see Trend Micro Control Manager, 1-12
 Control Manager version requirements, 4-3
 CPU requirements, 4-2

D

dialers, 1-11
 disk space requirements, 4-3
 documentation
 IMSVA related, xiii

E

Email reputation, xii
 about, 2-5
 types, 2-5
 email threats
 spam, 1-5
 unproductive messages, 1-5
 End-User Quarantine, 2-7
 EUQ, xi

F

File Reputation Services, 1-15
 filtering, how it works, 1-7

H

hacking tools, 1-11

I

IMSS appliances
 about, 1-2
 installing
 before a firewall, 3-10
 behind a firewall, 3-11
 in the DMZ, 3-12
 no firewall, 3-9
 IP Filtering
 about, 2-3
 IP Profiler, xii
 about, 2-3
 detects, 2-3
 how it works, 2-4

J

joke program, 1-11

L

logs, xi

M

mass mailing viruses
 pattern, 1-6
 memory requirements, 4-2
 migrate
 from IMSS for Linux, 5-33
 from IMSS for Windows, 5-32
 from IMSVA, 5-34

minimum requirements, 4-2
MTA features, opportunistic TLS, xii

N

new features, vi

O

online

community, 6-5

online help, xiii

P

password cracking applications, 1-11

policy, xi

POP3

deployment planning, 3-15

Pre-Filter, viii

Pre-Filter Service, 2-2

Q

quarantine, xi

R

readme file, xiv

remote access tools, 1-11

reports, xi

requirements, 4-2

S

security risks

spyware/grayware, 1-10

Smart Protection, 1-15

Smart Protection Network, 1-17

spam prevention, xii

spyware/grayware, 1-10

adware, 1-11

dialers, 1-11

entering the network, 1-11

hacking tools, 1-11

joke program, 1-11

password cracking applications, 1-11

remote access tools, 1-11

risks and threats, 1-11

support

knowledge base, 6-6

resolve issues faster, 6-8

TrendLabs, 6-10

system requirements, 4-2

T

TrendLabs, 6-10

Trend Micro Control Manager, 1-12

agent, 1-12

server, 1-12

troubleshooting, 6-2

W

Web EUQ, xi

Web Reputation Services, 1-16

what's new, vi



TREND MICRO INCORPORATED

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

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

www.trendmicro.com

Item Code: MSEM85912/130322