TREND MICRO™

9.1 InterScan™ Messaging Security Virtual Appliance

Installation Guide

Hybrid SaaS Email Security

Messaging Security

Document Part No.: MSEM97320_160201

Release Date: June 2016

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

Chapter 2: Component Descriptions

Chapter 3: Planning for Deployment

Chapter 4: Installing IMSVA 9.1

Chapter 5: Upgrading from Previous Versions

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

Index

Preface

About this Manual

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

Refer to the *IMSVA 9.1 Administrator's Guide* for information about configuring IMSVA settings and the Online Help in the management console for detailed information about each field on the user interface.

Topics include:

What's New

TABLE 1. IMSVA 9.1 New Features

NEW FEATURE	DESCRIPTION
Syslog integration	To provide enterprise-class logging capabilities, IMSVA supports sending logs through the syslog protocol to multiple external syslog servers in a structured format. On the IMSVA management console, you can add, delete, import and export syslog servers.
Multiple Virtual Analyzer servers	To achieve better load balancing and failover capabilities, IMSVA allows you to add multiple servers for Virtual Analyzer. You can also enable, disable and delete Virtual Analyzer servers on the IMSVA management console.
SMTP Traffic Throttling	SMTP Traffic Throttling blocks messages from a single IP address or sender for a certain time when the number of connections or messages reaches the specified maximum.
Audit log support	As an enhanced log category of system events, **Audit log** replaces **Admin activity** on the IMSVA management console. Audit logs record various administrator operations and provide a way to query activities of specified administrator accounts.
Enhanced queue management	IMSVA uses mail transfer agent (MTA) queues to store messages that just arrived, messages ready to be delivered to the next MTA, messages deferred due to delivery failure, and messages kept on hold for later manual delivery. Specific actions can be taken on the messages in MTA queues.
Enhanced Smart Protection	IMSVA supports both Trend Micro Smart Protection Network and Smart Protection Server as smart protection sources. Smart Protection Servers are supported to localize smart protection services to the corporate network to reduce outbound traffic and optimize efficiency.

New Feature	Description
External database support	IMSVA allows you to use not only the internal but also external PostgreSQL database as the admin database or the EUQ database.
Time-of-Click Protection	IMSVA provides time-of-click protection against malicious URLs in email messages. If you enable Time-of-Click Protection, IMSVA rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious.
Connected Threat Defense	Configure IMSVA to subscribe to the suspicious object lists on the Trend Micro Control Manager server. Using the Control Manager console, you can specify customized actions for objects detected by the suspicious object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment. Control Manager facilitates the investigation of targeted attacks and advanced threats using suspicious objects. Files and URLs that have the potential to expose systems to danger or loss will be detected.
DomainKeys Identified Mail (DKIM) signature	IMSVA supports adding DKIM signatures to outgoing email messages. On the IMSVA management console, you can add or delete DKIM signatures and import or export DKIM signature files.
Report delivery through email	IMSVA allows you to send newly generated reports and archived reports through email. Detailed views of reports will be included.
Keyword and expression enhancement	To improve visibility of triggered keywords and expressions, the entity name (where the keyword expression appears in a message) and the matched expressions now appear in the policy event log query details page. Administrators can also add a description to new keyword expressions for better tracking.

New Feature	Description
Attachment names supported by message tracking logs	Message tracking logs include attachment names as a new attribute. Multiple attachment names can be specified to query message tracking logs.
Logon notice support	Customizable logon notices are available both on the administrator logon page and End-User Quarantine logon page.
Quarantine event summary	IMSVA provides quarantine event logs and reports for users to learn information about quarantine events, for example, the percentage of release events in all the quarantine events.
LDAPS support	IMSVA supports LDAP over SSL (LDAPS) that provides users a secure and encrypted channel to communicate with LDAP servers.
Ransomware detection	IMSVA gives you more visibility on ransomware detected by IMSVA. You can either query ransomware detections in logs or add a widget for ransomware detections on the dashboard.
Virtual Analyzer integration improvement	IMSVA allows you to define rules to send email messages with specified attachment names or extensions to Virtual Analyzer for analysis.

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
- Transport Layer Security

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:

Administrator's Guide
Helps you get IMSVA up and running with post-installation instructions on how to configure and administer IMSVA.

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

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

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

The documentation is available at:

http://docs.trendmicro.com

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

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

Chapter 1

Introducing InterScan™ Messaging Security 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

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.
Graymail	Graymail refers to solicited bulk email messages that are not spam. IMSVA detects marketing messages and newsletters and social network notifications as graymail.	IMSVA manages graymail separately from common spam to allow administrators to identify graymail messages. IP addresses specified in the graymail exception list bypass scanning.
Regulatory compliance	Administrators can meet government regulatory requirements using the new default policy scanning conditions *Compliance templates*.	Compliance templates provide administrators with regulatory compliance. For a detailed list of available templates, see http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.
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: • 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	Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of these compressed files. Because there is the possibility that IntelliTrap may 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. By default, IntelliTrap is turned on as one of the scanning conditions for an antivirus policy, and is configured to quarantine message attachments that may be classified as security risks.	IntelliTrap helps reduce the risk that a virus compressed using different file compression schemes will enter your network through email.
Content management	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 Sender 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
Mass mailing virus containment	Email-borne viruses that may automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users. When IMSVA detects a mass-mailing virus, the action performed against this virus can be different from the actions against other types of viruses. For example, if IMSVA detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if IMSVA detects a mass-mailing virus, the program can automatically delete the entire message.	By auto-deleting messages that contain mass-mailing viruses, you avoid using server resources to scan, quarantine, or process messages and files that have no redeeming value. The identities of known mass-mailing viruses are in the Mass Mailing Pattern that is updated using the TrendLabs℠ ActiveUpdate Servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.
Protection from spyware and other types of grayware		
Spyware and other types of grayware	Other than viruses, your clients are at risk from potential threats such as spyware, adware and dialers. For more information, see *About Spyware/ Grayware on page 1-12*.	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.
Integrated anti-spam features		

Feature	Descriptions	Benefits
Spam Prevention Solution (SPS)	Spam Prevention Solution (SPS) is a licensed product from Trend Micro that provides spam detection services to other Trend Micro products. To use SPS, obtain an SPS Activation Code. For more information, contact your sales representative. SPS works by using a built-in spam filter that automatically becomes active when you register and activate the SPS license.	The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high-performance, real-time detection that is highly adaptable, even as spam senders change their techniques.
Spam Filtering with IP Profiler, Email Reputation and SMTP Traffic Throttling	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. SMTP Traffic Throttling blocks messages from a single IP address or sender for a certain time when the number of connections or messages reaches the specified maximum. **Note** Activate SPS before you configure IP Profiler and Email Reputation.	With the integration of Sender Filtering, which includes IP Profiler, Email Reputation and SMTP Traffic Throttling, IMSVA can block spammers at the IP level.

Feature	Descriptions	Benefits
Social Engineering Attack Protection	Social Engineering Attack Protection detects suspicious behavior related to social engineering attacks in email messages.	When Social Engineering Attack Protection is enabled, the Trend Micro Antispam Engine scans for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information. If the Antispam Engine detects behavior associated with social engineering attacks, the Antispam Engine returns details about the message to IMSVA for further action, policy enforcement, or reporting.
Administration and integration		
LDAP and domain-based policies	You can configure LDAP settings if you are using LDAP directory services such as Lotus Domino™ or Microsoft™ Active Directory™ for user-group definition and administrator privileges.	Using LDAP, you can define multiple rules to enforce your company's email usage guidelines. You can define rules for individuals or groups, based on the sender and recipient addresses.
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.

Feature	Descriptions	Benefits
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. IMSVA allows you to send both one-time and scheduled reports through email.
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.
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.
Clustered architecture	The current version of IMSVA has been designed to make distributed deployment possible.	You can install the various IMSVA components on different computers, and some components can exist in multiples. For example, if your messaging volume demands, you can install additional IMSVA scanner components on additional servers, all using the same policy services.

Feature	Descriptions	Benefits
Integration with Virtual Analyzer	IMSVA integrates with Virtual Analyzer, which is an isolated virtual environment used to manage and analyze samples in Deep Discovery Advisor and Deep Discovery Analyzer.	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™ (TMCM) is a software management solution that gives you the ability to control antivirus and content security programs from a central location regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus and content security policy.	Outbreak Prevention Services delivered through Trend Micro Control Manager™ reduces the risk of outbreaks. When a Trend Micro product detects a new email-borne virus, TrendLabs issues a policy that uses the advanced content filters in 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.
Integration with syslog servers	IMSVA integrates with syslog servers that use the syslog protocol to receive log messages. Syslog protocol is a network logging standard supported by a wide range of network devices and contains information on network events and errors.	Syslog server integration implements centralized log collection and management for multiple IMSVA servers and consolidates log data from all over the network into a single central repository. Collecting and analyzing syslog messages is essential for maintaining network stability and auditing network security.

Feature	Descriptions	Benefits
Time-of-Click Protection	IMSVA provides time-of-click protection against malicious URLs in email messages.	If you enable Time-of-Click Protection, IMSVA rewrites URLs in email messages for further analysis. Trend Micro analyzes those URLs at the time of click and will block them if they are malicious.

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	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Programs	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Helps hackers enter computers
Remote Access Tools	Helps hackers remotely access and control computers
Password Cracking Applications	Helps hackers decipher account user names and passwords
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.

Type	Description
Higher risk of legal liability	If hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties.

About Web Reputation Services

Trend Micro web reputation technology helps break the infection chain by assigning websites a "reputation" based on an assessment of the trustworthiness of an URL, derived from an analysis of the domain. Web reputation protects against web-based threats including zero-day attacks, before they reach the network. Trend Micro web reputation technology tracks the lifecycle of hundreds of millions of web domains, extending proven Trend Micro anti-spam protection to the Internet.

About 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 1-14* and *Advanced on page 1-15*.

Email Reputation: Standard

This service helps block spam by validating requested IP addresses against the Trend Micro reputation database, powered by the Trend Micro Smart

Protection Network. This ever-expanding database currently contains over 1 billion IP addresses with reputation ratings based on spamming activity. Trend Micro spam investigators continuously review and update these ratings to ensure accuracy.

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

Tip

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

Email Reputation: Advanced

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

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

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

incoming email stream is spam. The more spam you receive, the higher the percentage of blocked connections you will see.

How Email Reputation Technology Works

Trend Micro Email reputation technology is a Domain Name Service (DNS) query-based service. The following process takes place after 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.

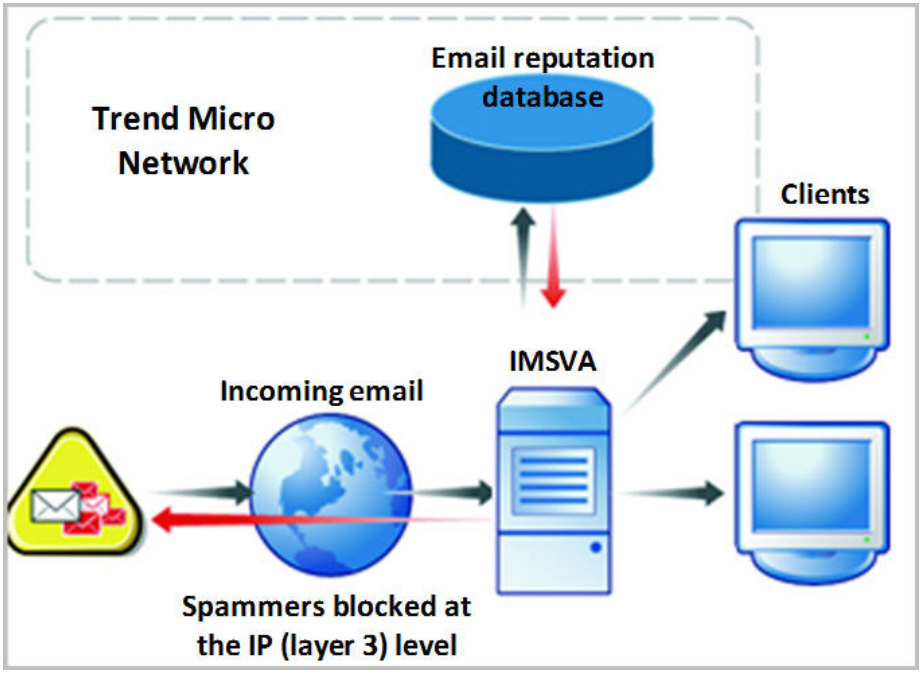


FIGURE 1-1. How Email reputation works

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

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?
Two-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.

Feature	Description	Supported?
Outbreak Prevention Policy	The Outbreak Prevention Policy (OPP) is a quick response to an outbreak developed by TrendLabs that contains a list of actions 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
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.

Feature	Description	Supported?
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
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: 1. Go to **Administration** > **Connections**. 2. Click the **TMCM 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 Graymail Scanning

Graymail refers to solicited bulk email messages that are not spam. IMSVA detects marketing messages and newsletters and social network notifications as graymail. IMSVA identifies graymail messages in two ways:

- Email Reputation Services scoring the source IP address
- Trend Micro Anti-Spam Engine identifying message content

Note

Note that while IMSVA detects these kinds of email messages, these messages are not tagged as spam.

Administrators define the rule criteria to take an action on those email messages. Every graymail message rule has an exception list containing address objects that bypass message filtering. An address object is a single IP address or address range (IPv4 or IPv6), or the Classless Inter-Domain Routing (CIDR) block.

Administrators have several options to understand graymail message traffic in the network. Reports illustrate the highest senders and recipients of graymail messages from external or internal sources. Administrators can also query detailed log information or view the email quarantine and release messages identified as permitted graymail messages when necessary.

The graymail exception list can be exported and imported.

Note

Ensure that IMSVA can query external DNS servers for graymail scanning. If you change any DNS server settings, restart the scanner server to load the new settings.

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.

Topics include:

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.

About Sender Filtering

IMSVA includes optional Sender Filtering, which consists of three parts:

IP Profiler

Allows you to configure threshold settings used to analyze email traffic. When traffic from an IP address violates the settings, IP

Profiler adds the IP address of the sender to its database and then blocks incoming connections from the IP address.

IP profiler detects any of these four potential Internet threats:

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

Email Reputation

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

SMTP Traffic Throttling

Blocks messages from a single IP address or sender for certain time when the number of connections or messages reaches the specified maximum.

How IP Profiler Works

IP Profiler proactively identifies IP addresses of computers that send email messages containing threats mentioned in the section *About Sender Filtering on page 2-3*. You can customize several criteria that determine when IMSVA starts 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.

How SMTP Traffic Throttling Works

SMTP Traffic Throttling identifies IP addresses or sender addresses that deliver connection requests or email messages too frequently and blocks these addresses if they trigger specific rules. You can customize IP-based and sender-based throttling rules to monitor behaviors of all IP addresses and senders and take actions on them if necessary. The rule criteria include the duration to monitor, maximum number of connections or messages allowed, and block duration. The difference is that sender-based throttling does not allow you to specify the maximum number of connections while IP-based throttling does.

The following process takes place after IMSVA receives a connection request from a sending mail server or a sender:

1. SMTP Traffic Throttling records the number of connections from this IP address in the specified duration to monitor.
2. SMTP Traffic Throttling records the number of email messages from this IP address in the specified duration to monitor.
3. SMTP Traffic Throttling records the number of email messages from this sender in the specified duration to monitor.
4. When the number of connections or messages from this IP address reaches the threshold you set, SMTP Traffic Throttling will add this IP address to the Blocked List and block subsequent connections or messages from this IP address temporarily.

5. When the number of messages from this sender reaches the threshold you set, SMTP Traffic Throttling will add this sender to the Blocked List and block subsequent messages from this sender temporarily.

About End-User Quarantine (EUQ)

IMSVA provides web-based EUQ to improve spam management. The Web-based EUQ service allows end users to manage their own spam quarantine. Messages that Spam Prevention Solution (licensed separately from IMSVA), 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). IMSVA allows you to send both one-time and scheduled reports through email.

Chapter 3

Planning for Deployment

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

Topics include:

Deployment Checklist

The deployment checklist provides step-by-step instructions on the pre-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	*IMSVA Deployment with Cloud Pre-Filter on page 3-5*

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		*Deployment at the Gateway or Behind the Gateway on page 3-6*
	Behind the gateway		*Deployment at the Gateway or Behind the Gateway on page 3-6*
	Without a firewall		
	In front of a firewall		
	Behind a firewall		
	In the De-Militarized Zone		

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.		
	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.		
	Sender Filtering Rules	Yes	Sender Filtering Service section of the Administrator's Guide
	SMTP Routing		Scanning SMTP Messages section of the Administrator's Guide
	POP3 Settings	Yes	Scanning POP3 Messages section of the Administrator's Guide
	Policy and scanning exceptions		Managing Policies section of the *Administrator's Guide*
	Perform a manual update of components and configure scheduled updates		Updating Scan Engine and Pattern Files section of the Administrator's Guide
	Log settings		Configuring Log Settings section of the Administrator's Guide

7. Back up 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 Sender Filtering with the device. IMSVA is deployed at the gateway to provide antivirus, content filtering, spam prevention and Sender 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 Sender Filtering with at least one of the devices. You can enable or disable services on different devices. See the following: • *Figure 3-3: IMSVA group at the gateway on page 3-8* • *Service Selection on page 3-14*
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 3-7*.	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: • *Figure 3-4: IMSVA group behind the gateway on page 3-8* • *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.		

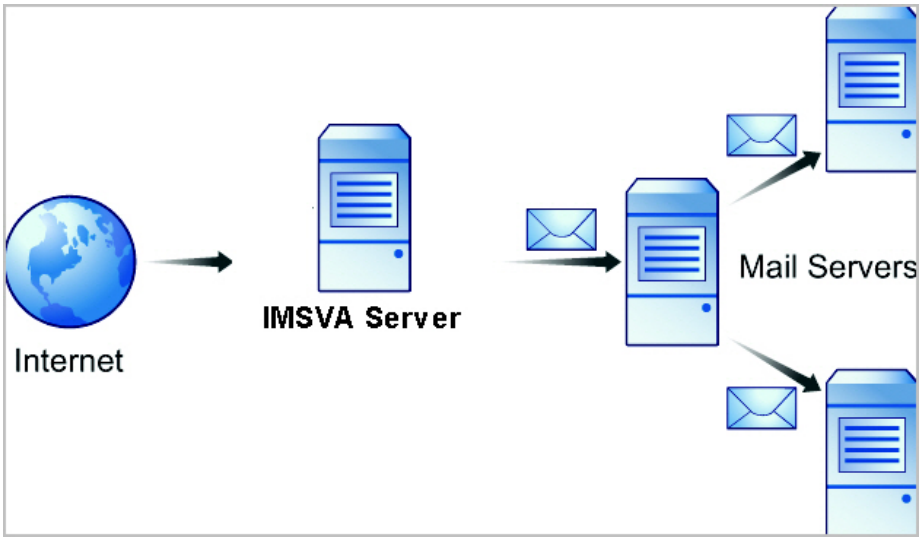


FIGURE 3-1. Single IMSVA device at the gateway

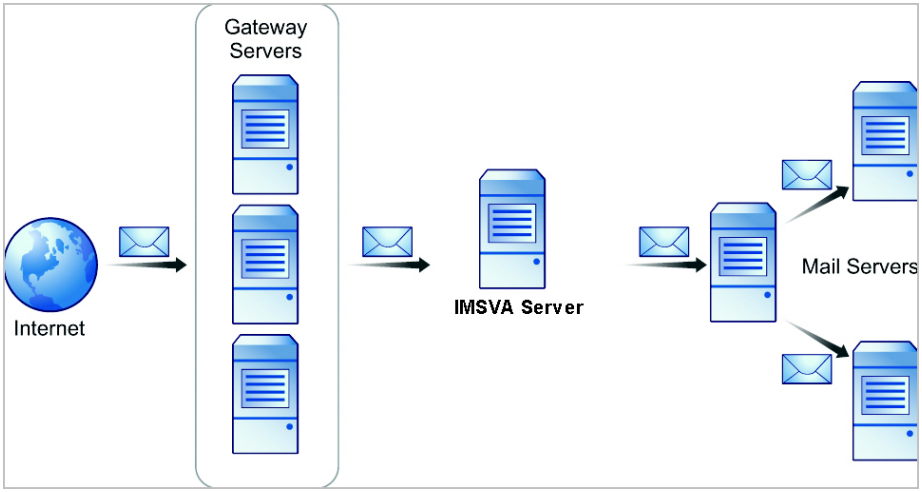


FIGURE 3-2. Single IMSVA device behind the gateway

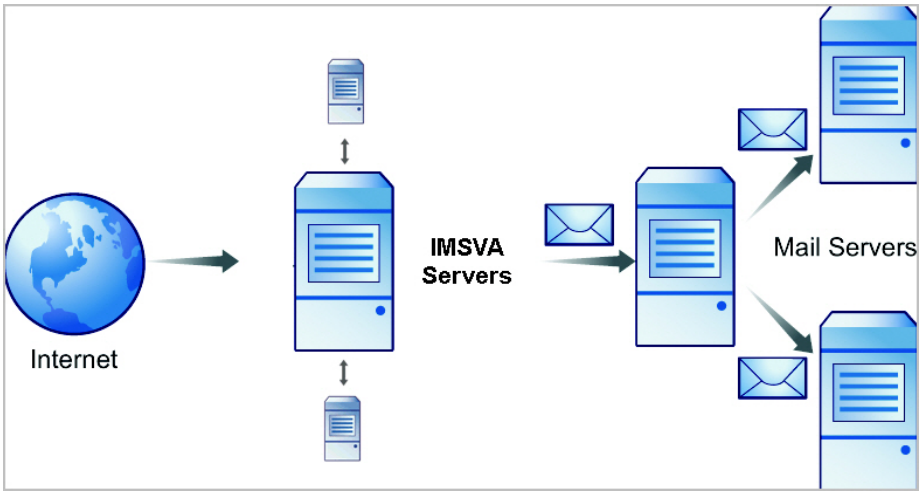


FIGURE 3-3. IMSVA group at the gateway

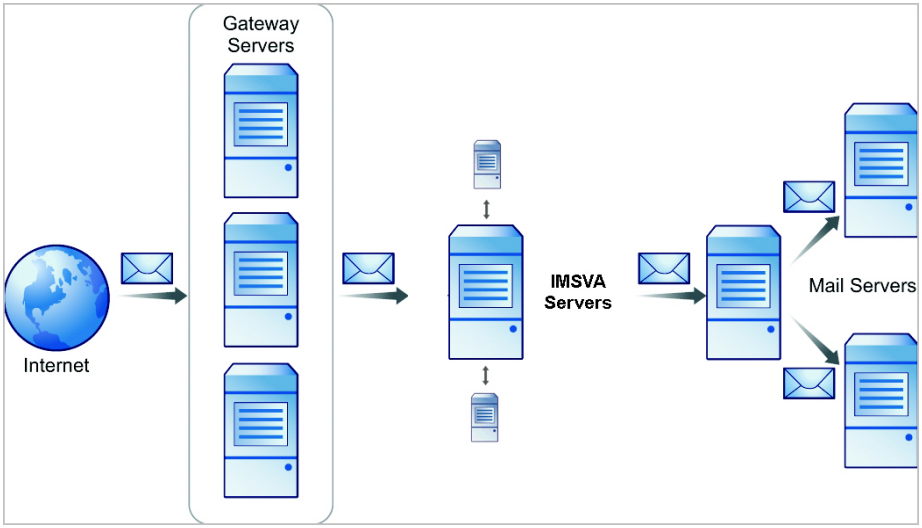


FIGURE 3-4. IMSVA group behind the gateway

Installing without a Firewall

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

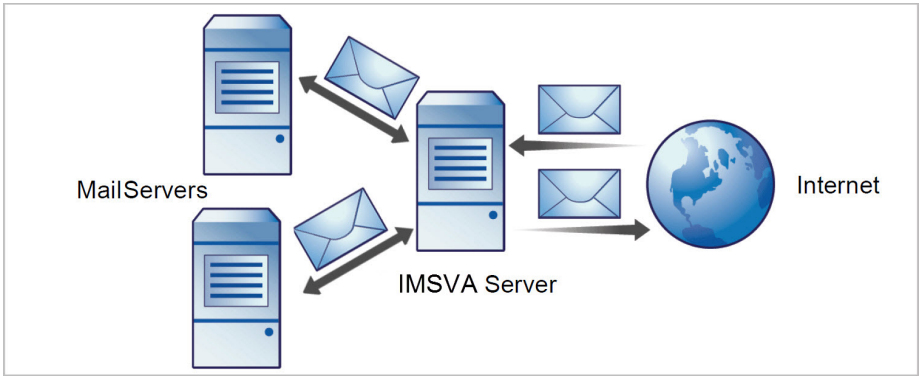


FIGURE 3-5. Installation topology: no firewall

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.

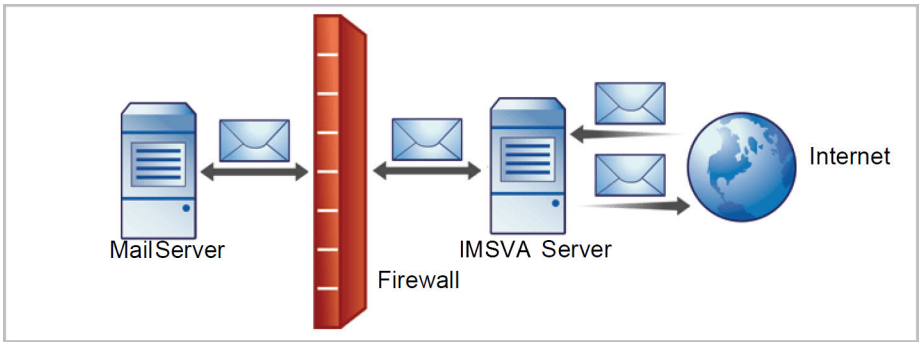


FIGURE 3-6. Installation topology: in front of the firewall

Incoming Traffic

- Configure IMSVA to reference your SMTP server(s) and 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.
- Configure IMSVA to allow internal SMTP gateways to relay 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 behind your firewall.

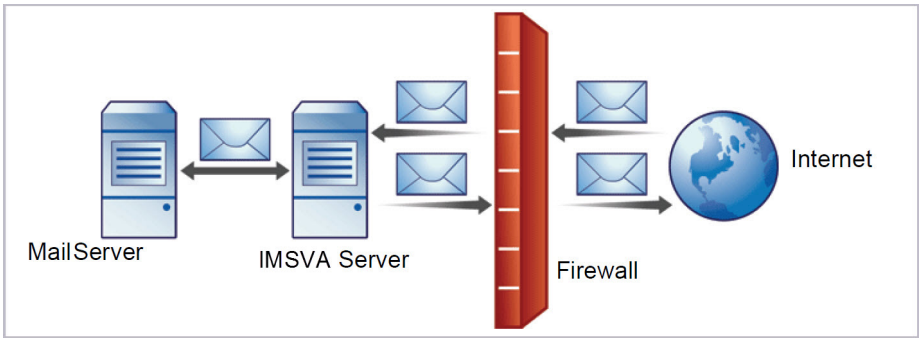


FIGURE 3-7. Installation scenario: behind a firewall

Incoming Traffic

- Configure your proxy-based firewall, as follows:
  - Incoming SMTP messages go 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 IMSVA servers.

- If you are replacing your SMTP gateway with IMSVA, configure your internal mail server to send outgoing messages to IMSVA servers.
- Configure 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 in the De-Militarized Zone (DMZ).

Incoming Traffic

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

Outgoing Traffic

- Configure your internal mail server 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 IMSVA.
- Configure IMSVA to allow internal SMTP gateways to relay to any domain through 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 Sender Filtering

The Trend Micro Sender Filtering, which includes IP Profiler, Email Reputation and SMTP Traffic Throttling, blocks connections at the IP level.

To use Sender Filtering, any firewall between IMSVA and the edge of your network must not modify the connecting IP address as Sender Filtering is not compatible with networks using network address translation (NAT). If IMSVA accepts SMTP connections from the same source IP address, for instance, Sender Filtering will not work, as this address would be the same for every received message and the sender 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**.

WARNING!

To prevent unauthorized changes to your policies, Trend Micro recommends that you set a new logon password immediately after deployment and change the password regularly.

Note

If you are using Internet Explorer (IE) 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 website** to proceed.

Chapter 4

Installing IMSVA 9.1

This chapter explains how to install IMSVA under different scenarios.

Topics include:

System Requirements

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

TABLE 4-1. System Requirements

SPECIFICATION	DESCRIPTION
Operating System	IMSVA provides a self-contained installation that uses a standard 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. **Note** 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).
CPU	• Recommended: 8-core Intel™ Xeon™ processor or equivalent • Minimum: dual-core Intel™ Xeon™ processor or equivalent
Memory	• Recommended: 8GB RAM • Minimum: 4GB RAM
Disk Space	• Recommended: 250GB **Note** IMSVA automatically partitions the detected disk space based on recommended Linux practices. • Minimum: 120GB **Note** IMSVA automatically partitions the detected disk space based on recommended Linux practices.
Monitor	Monitor that supports 800 x 600 resolution with 256 colors or higher

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	REMARKS
SSH communications application	SSH protocol version 2	To adequately view the IMSVA CLI through an SSH connection, set the terminal window size to 80 columns and 24 rows.
VMware™ ESX server	• VMware ESXi 5.0 Update 3 • VMware ESXi 5.5 Update 2 • VMware ESXi 6.0	To install IMSVA as virtual machine, install IMSVA on a VMware ESXi 5.0, VMware ESXi 5.5 or VMware ESXi 6.0.
Hyper-V	• Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2012 R2 • Microsoft Hyper-V Server 2008 R2 SP1 • Microsoft Hyper-V Server 2012 R2	IMSVA supports Hyper-V on Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Microsoft Hyper-V Server 2008 R2 SP1, and Microsoft Hyper-V Server 2012 R2.
Internet Explorer™	• Version 9.0 • Version 10.0 • Version 11.0	To access the web console, which allows you to configure all IMSVA settings, use Internet Explorer 9.0 or above, Firefox 45.0 or above, or Microsoft Edge 31 or above. Using the data port IP address you set during initial configuration, enter the following URL:`https://[IP Address]:8445`
Mozilla Firefox™	Version 45.0	
Microsoft Edge™	Version 31	
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.

Application	System Requirements	Remarks
PostgreSQL database	Version 9.2	The IMSVA admin database and EUQ database can be installed either on the internal or external database server.
Trend Micro Control Manager	• Version 5.5 SP1 Patch 4 or later • Version 6.0 SP3 Patch 1 or later	Install Trend Micro Control Manager 6.0 SP3 Patch 1 hot fix build 3262 so that Data Loss Prevention policies can be deployed to IMSVA 9.1.

Installing IMSVA

IMSVA 9.1 supports upgrading only from IMSVA 9.0 and migrates existing configuration and policy data during the upgrade.

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 erased during the installation process. Back up any existing data on the system (if any) before installing IMSVA.

Procedure

1. Start the IMSVA installation.

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

   - On a Bare Metal Server

     a. Make sure the Bare Metal server supports CentOS 6.4 x86_64.

b. Insert the IMSVA Installation DVD into the DVD drive of the desired server.

c. Power on the Bare Metal server.

- On a VMware ESX Virtual Machine

  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-9.1-xxxx-x86_64.iso` file. The `IMSVA-9.1-xxxx-x86_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.

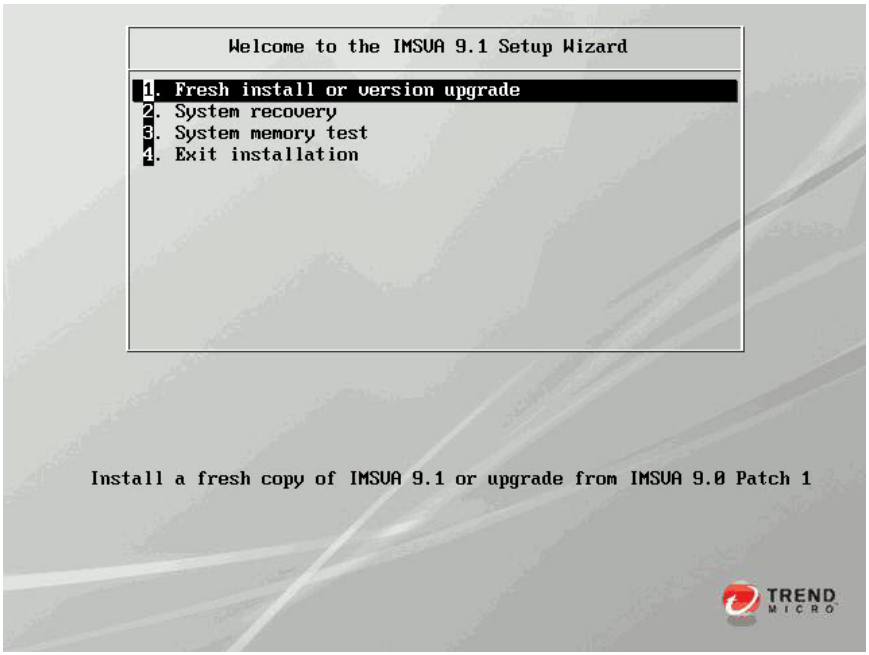
For both a VMware ESX Virtual Machine and a Bare Metal Server installation, a page appears displaying the **IMSVA 9.1 Setup Wizard** with the following options:

- **Fresh Install or version upgrade**: Select this option to install IMSVA onto the new hardware or virtual machine or upgrade the existing IMSVA.

- **System recovery**: Select this option to fix operating system errors and recover administrative passwords.

- **System memory test**: Select this option to perform memory diagnostic tests.

- **Exit installation**: Select this option to exit the installation process and to boot from the local disk.

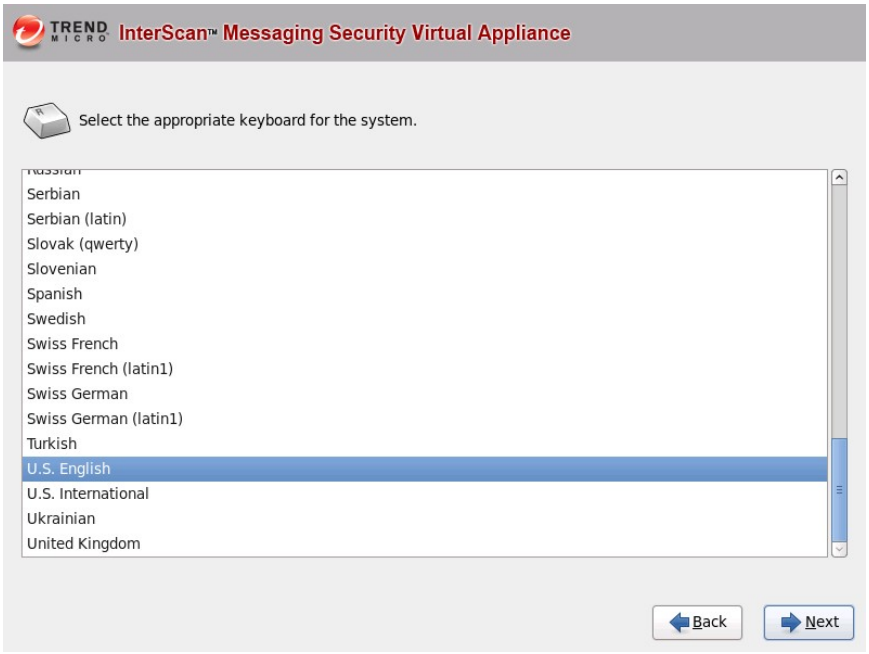


2. Select **Fresh install or version upgrade**.

The **License Agreement** page appears.

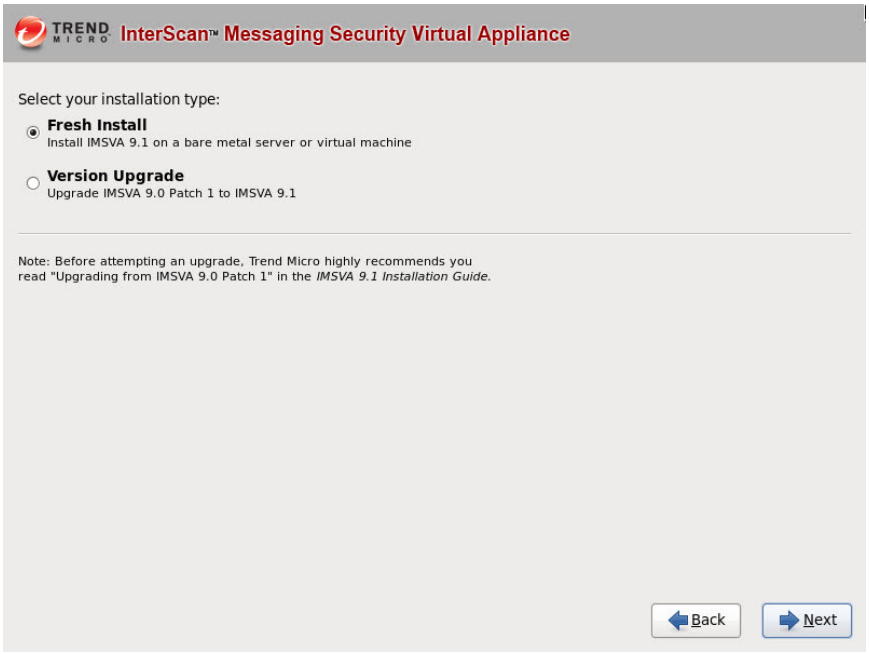
3. Click **Accept** to continue.

A keyboard language selection screen appears.



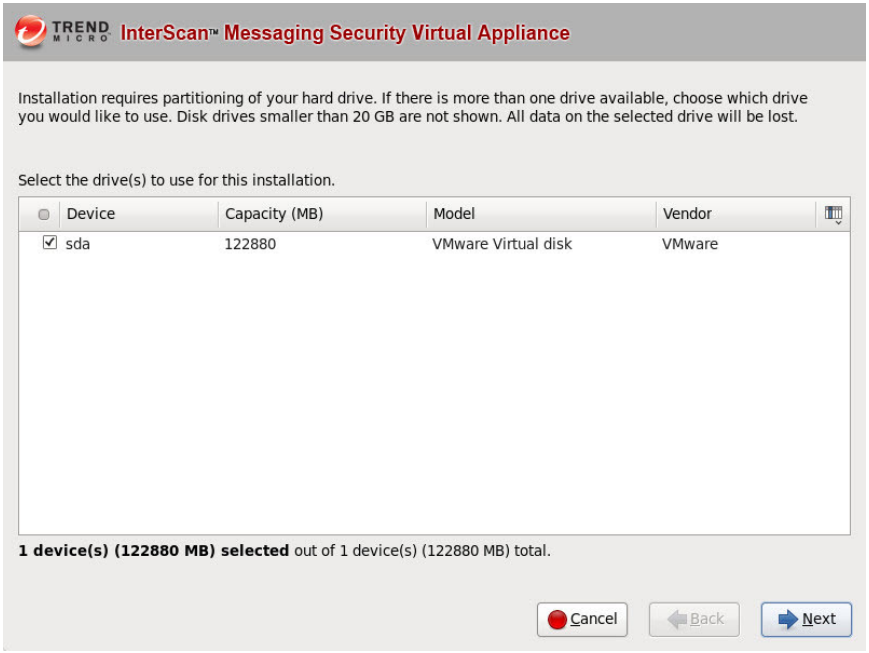
4. Select the keyboard language for the system, and then click **Next**.

A screen appears for you to select your installation type.



5. Select **Fresh Install**, and then click **Next**.

A screen appears for you to select the drive used for installation.

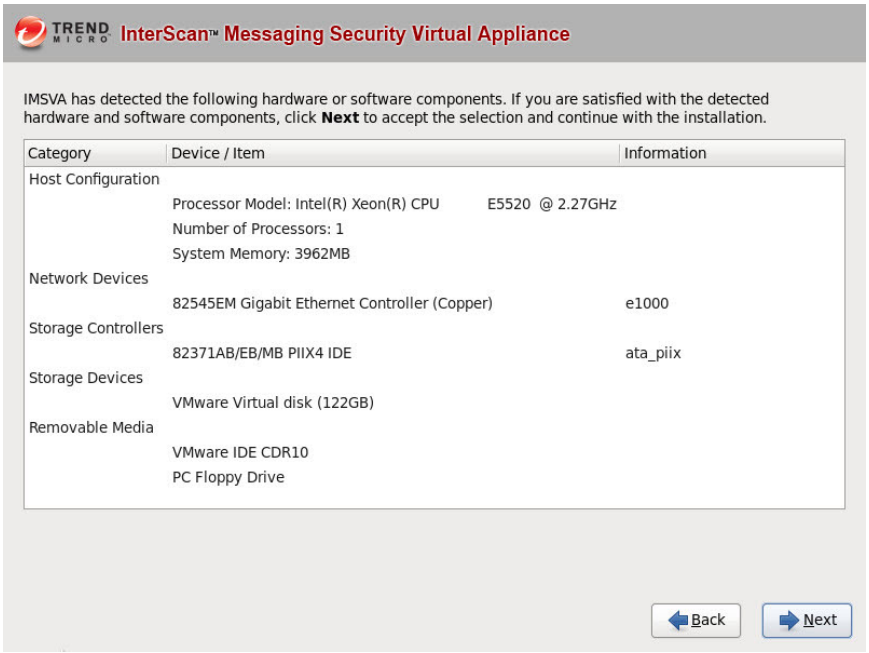


6. Select the drive, and then click **Next**.

   A warning dialog box appears.

7. Click **Yes** to proceed.

   The IMSVA installation program scans your hardware and software to determine if the minimum requirements have been met and displays the results. If the hardware or software contains any components that do not meet the minimum requirements, the installation program highlights those components and the installation stops.



8. Make sure the hardware and software information is correct, and then click **Next**.

The network devices configuration screen appears.

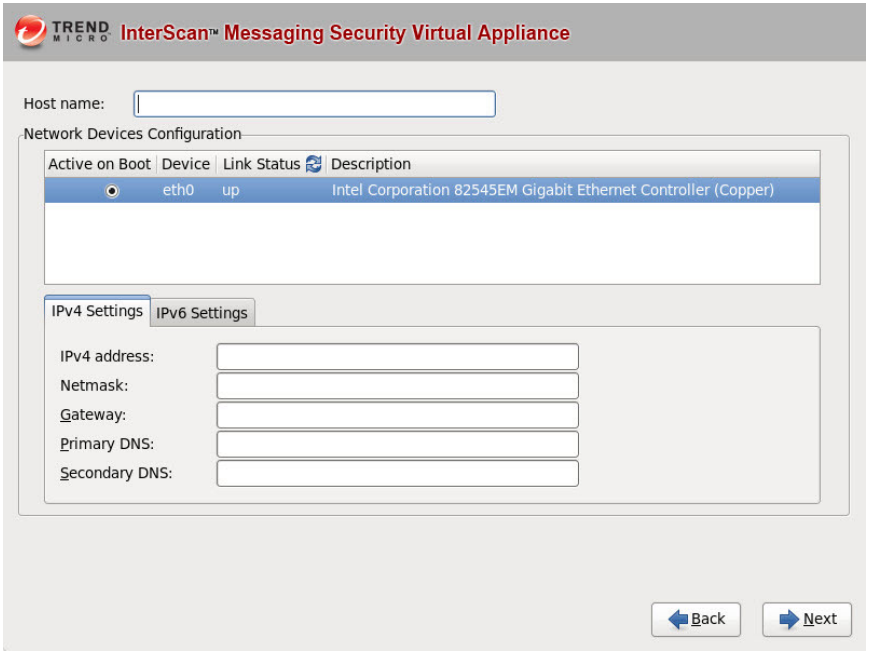


TABLE 4-3. Network Device Configuration

CONFIGURATION PARAMETER	DESCRIPTION
IPv4 Address	Type the IMSVA management IP address and subnet mask.
Hostname	Type in the applicable FQDN for this IMSVA host.
Gateway	Type the applicable IP address as the gateway for this IMSVA installation.
Primary DNS	Type the applicable IP address as the primary DNS server for this IMSVA installation.

Configuration Parameter	Description
Secondary DNS	Type the applicable IP address as the secondary DNS server for this IMSVA installation.

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

   The time zone configuration screen appears.

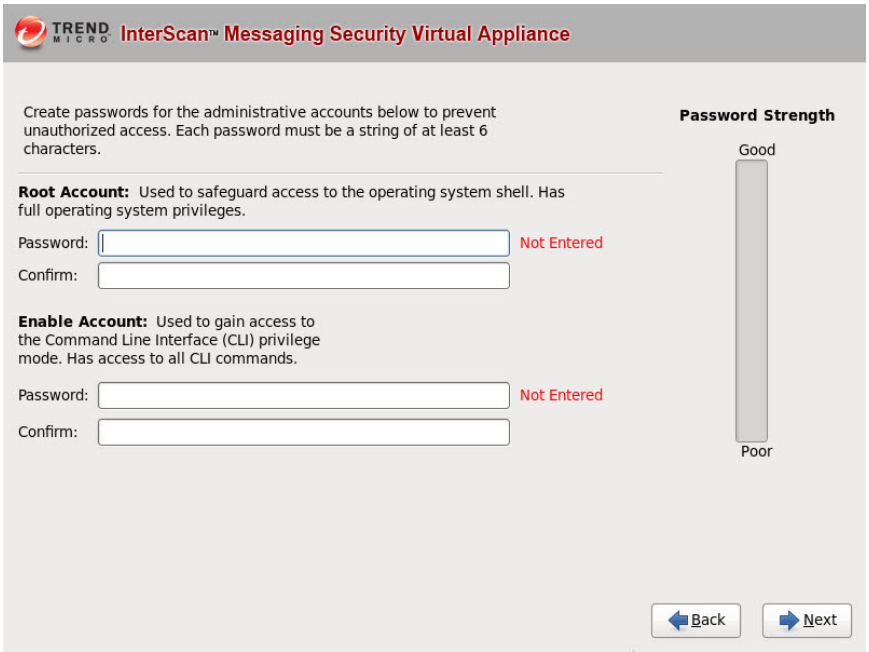
10. Specify the IMSVA server's time and clock settings

    a. Select the location of the IMSVA server.

    b. Specify whether the server's system clock uses UTC or not by selecting or clearing the **System clock uses UTC** check box.

11. Click **Next**.

The account settings screen appears.



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

    IMSVA uses two different levels of administrator accounts to secure the system.

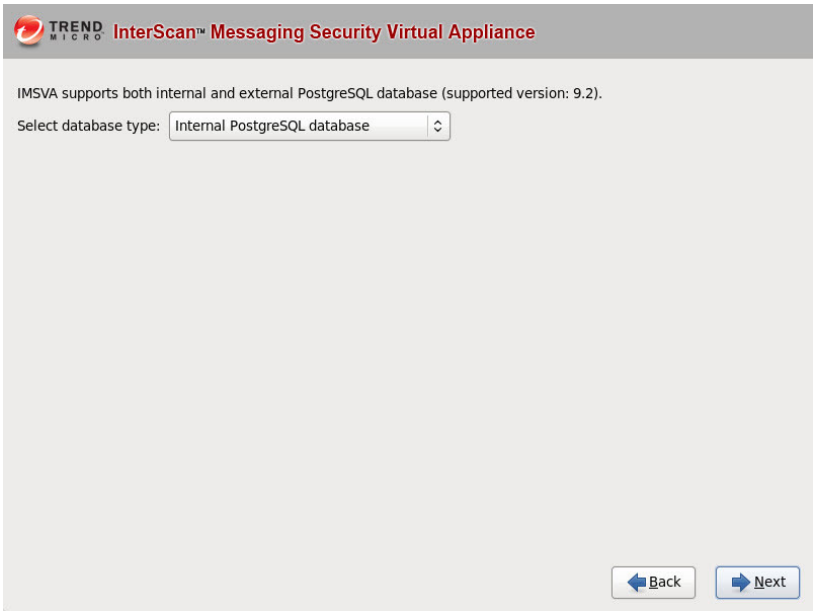
    The password must be a minimum of 6 characters and a maximum of 32 characters.

Tip

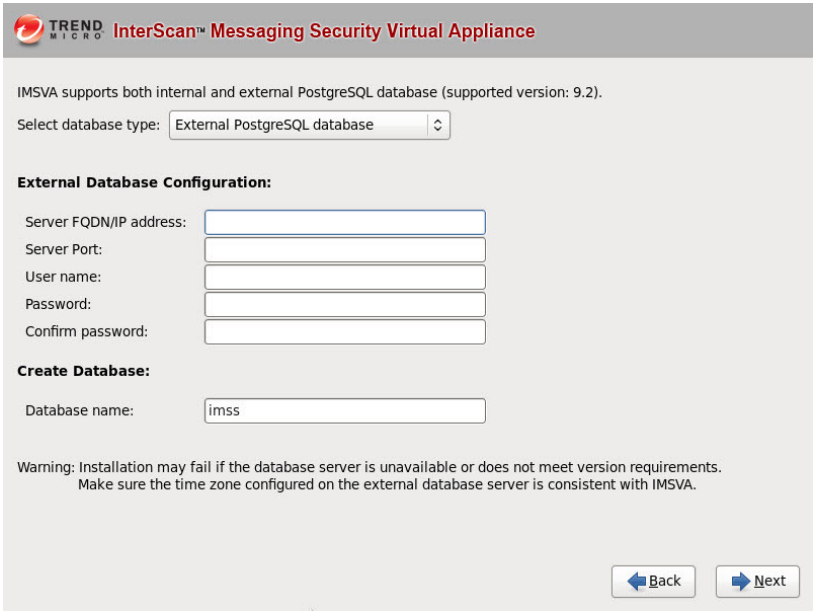
For the best security, create a highly unique password only known to you. You can use both upper and lower case alphabetic characters, numerals, and any special characters found on your keyboard to create your passwords.

- **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.

13. Select a database from the following:
    - **Internal PostgreSQL database**: This is the default database used.



- **External PostgreSQL database**: If you select this option, provide external database information as required.



Note

To use the external database, do the following:

a. Make sure the account used to install the IMSVA admin database has the superuser role.

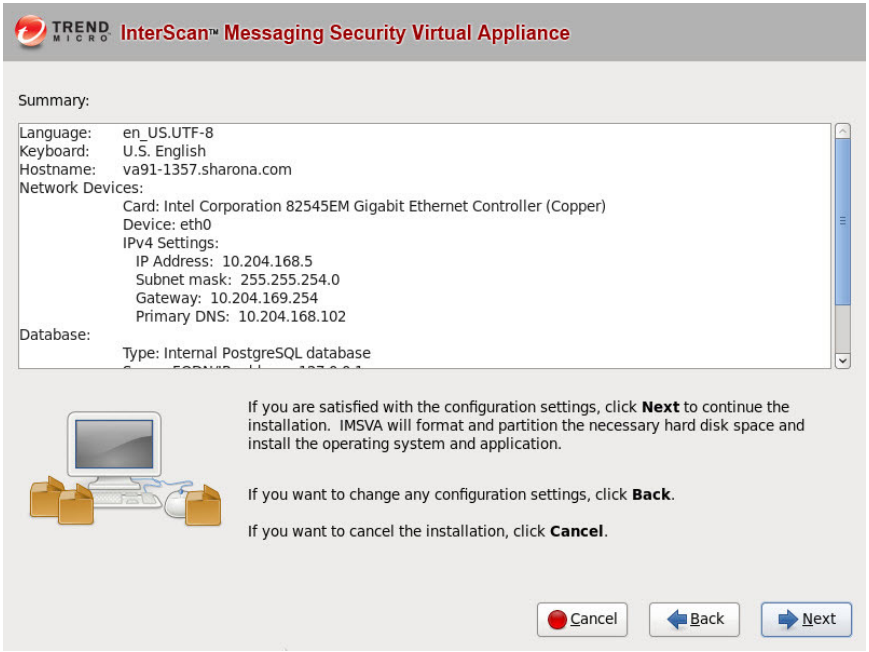
b. Manually change the maximum number of database connections to 600:

```
vi /var/lib/pgsql/9.2/data/postgresql.conf

max_connection = 600 (default 100)

restart DB service (service postgresql-9.2 restart OR
systemctl restart postgresql)
```

c. Make sure that IMSVA and the external database server use the same timezone and time settings; otherwise, some unexpected issues may happen.

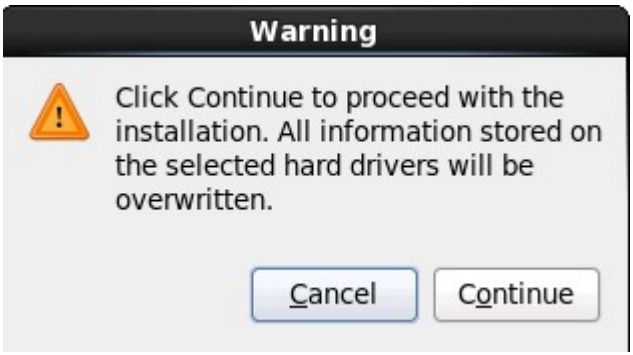
14. Click **Next**.

A screen appears, showing a summary of your configuration settings.



15. Verify settings, and then click **Next**.

    A dialog box appears, asking you whether to continue the installation.



Important

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.

16. 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 completes, a summary screen appears. The installation log saves to the `/var/app_data/installlog` file for reference.

17. Click **Restart** to restart the system.

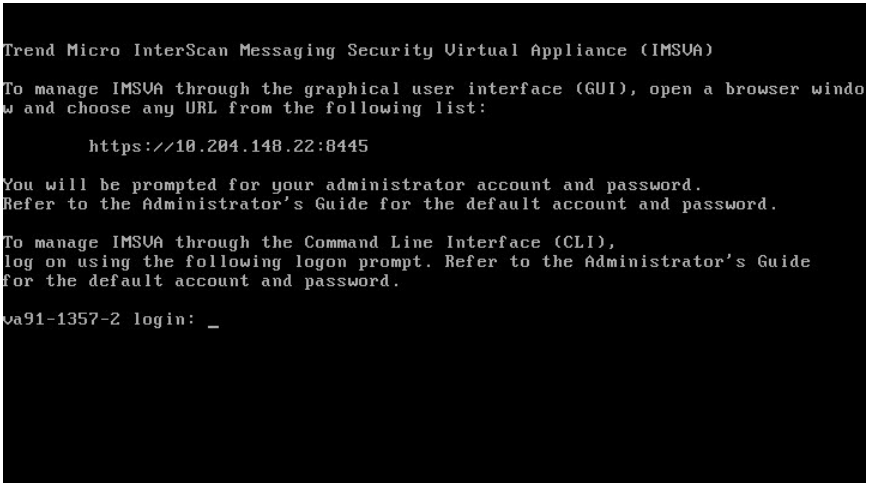
    - Bare Metal installation:

      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.



18. Log on through either the CLI or IMSVA management console to launch IMSVA.

Tip

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

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, Firefox or Microsoft Edge.
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.

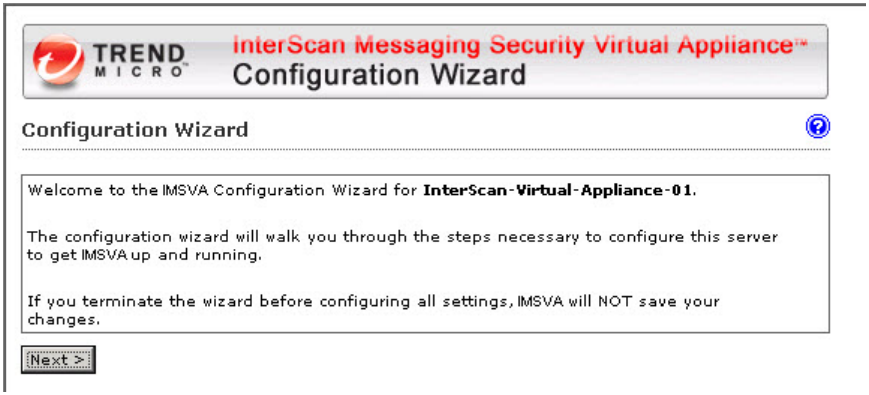


FIGURE 4-1. Configuration Wizard screen

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.

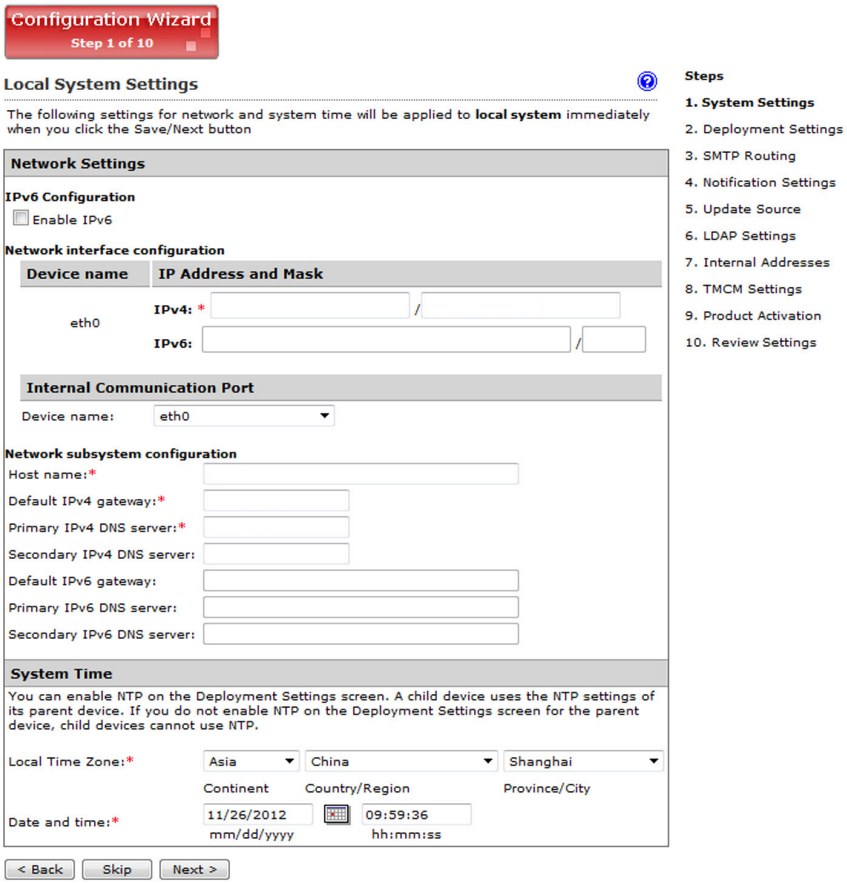


FIGURE 4-2. Local System Settings

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.

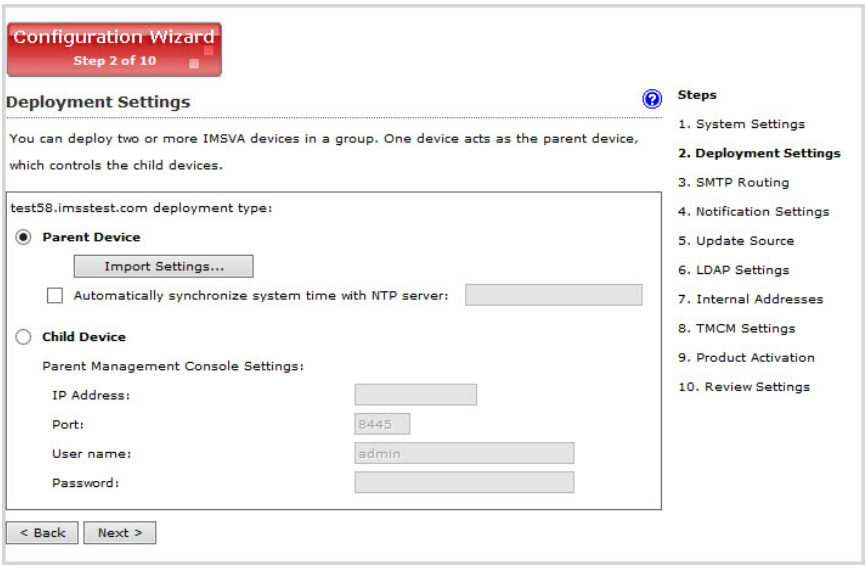


FIGURE 4-3. Deployment Settings

2. Select **Parent Device** or **Child Device**.

   - **Parent Device**: If this is the first device you are setting up, you must select this option. You can configure additional child devices at a later time. Also, decide if you want to use the NTP service.
   - **Child Device**: If you select this option, specify the parent management console settings. Make sure the user account you use here has full administration rights.

Step 3: Configuring SMTP Routing Settings

Procedure

1. Click **Next**.

The **SMTP Routing Settings** screen appears.

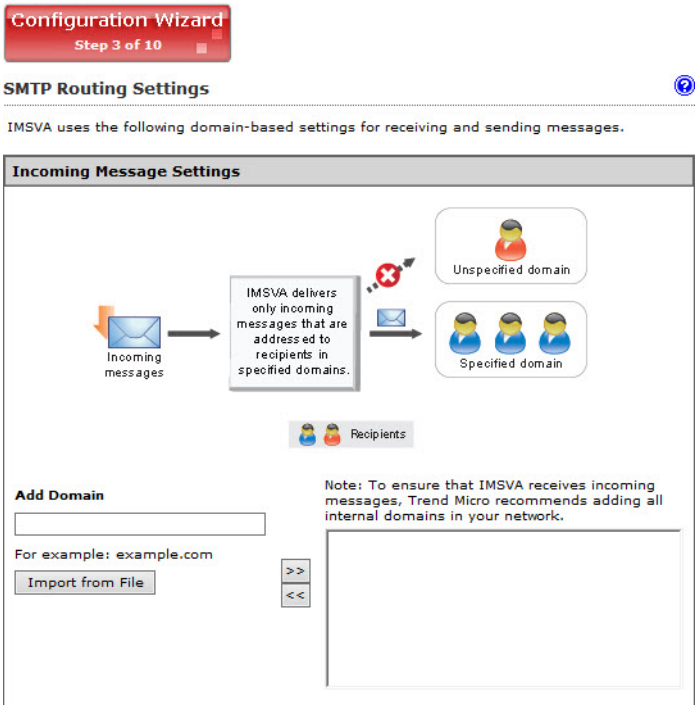
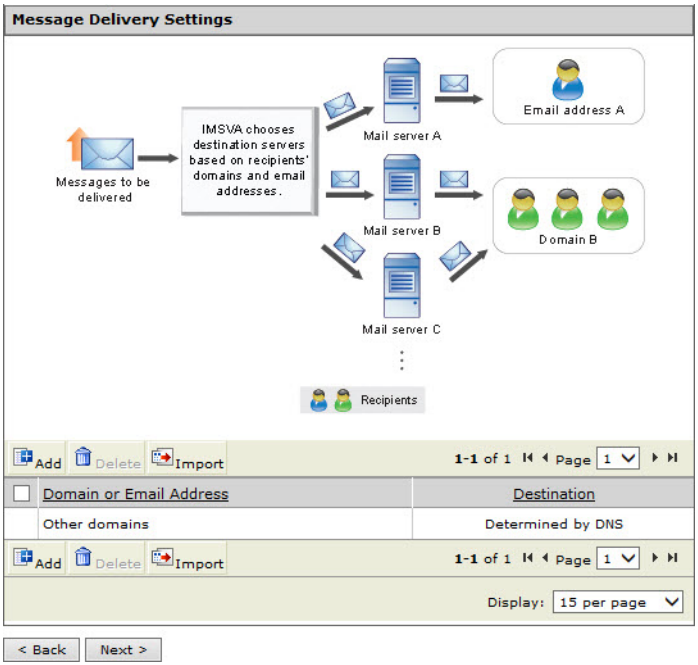


FIGURE 4-4. SMTP Routing Settings



2. Specify the incoming message settings.
3. Specify the message delivery settings.

Step 4: Configuring Notification Settings

Procedure

1. Click **Next**.

The **Notification Settings** screen appears.

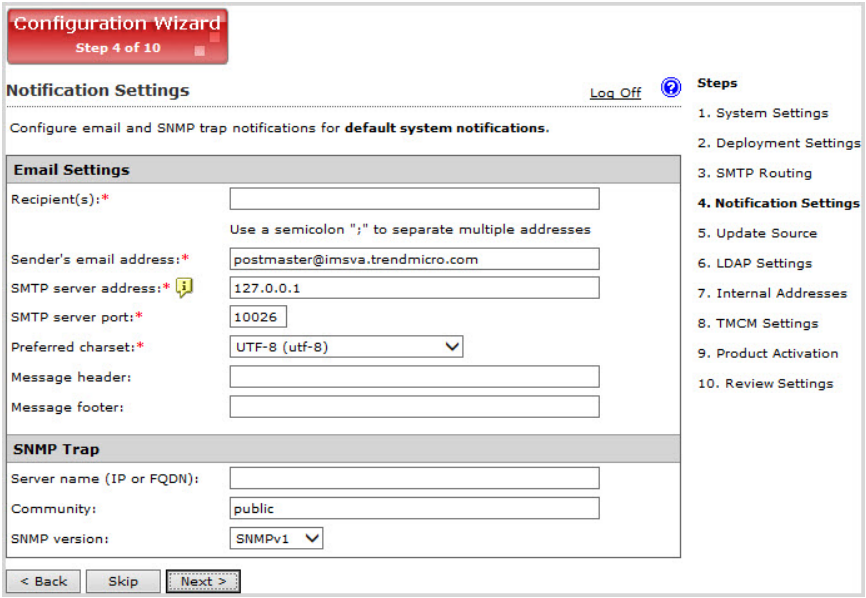


FIGURE 4-5. Notification Settings

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.

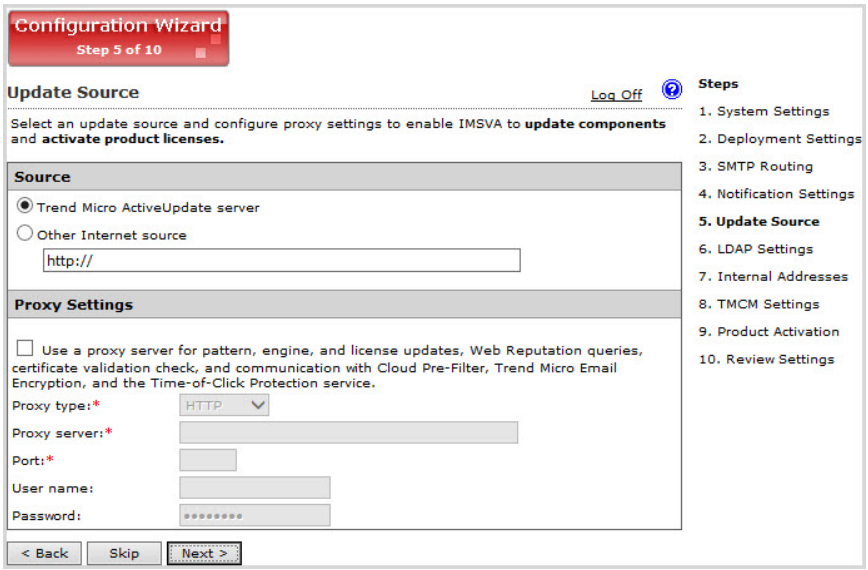


FIGURE 4-6. Update Source

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://<TMCM server address>/TvcsDownload/ActiveUpdate/`, if applicable.

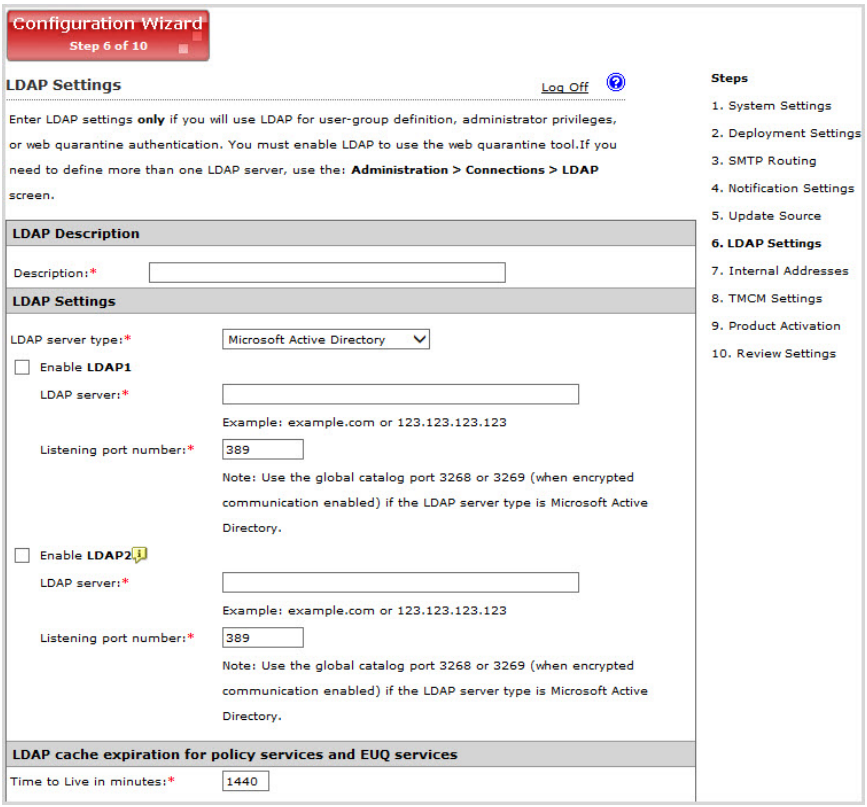
   - **Proxy Settings**: Select the **Use proxy server** check box and configure the proxy type, server name, port, user name, and password.

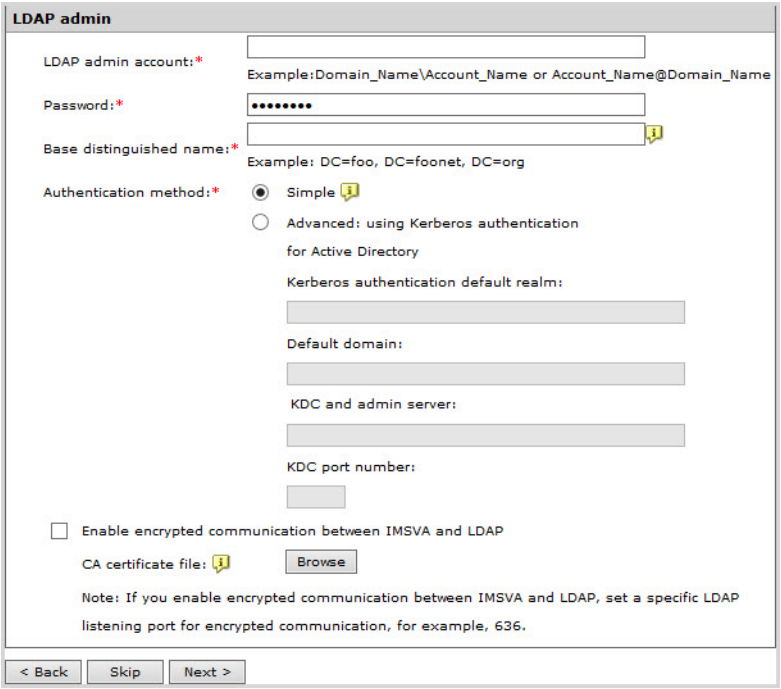
Step 6: Configuring LDAP Settings

Procedure

1. Click **Next**.

   The **LDAP Settings** screen appears.





2. Specify a meaningful description for the LDAP server.
3. Complete the following to enable LDAP settings:
   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. Specify 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 4-4. 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)
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
Open LDAP	cn=manager, dc=test1, dc=com	dc=test1, 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.

g. Select the **Enable encrypted communication between IMSVA and LDAP** check box and click **Browse** to upload a CA certificate file.

Step 7: Configuring Internal Addresses

Procedure

1. Click **Next**.

The **Internal Addresses** screen appears.

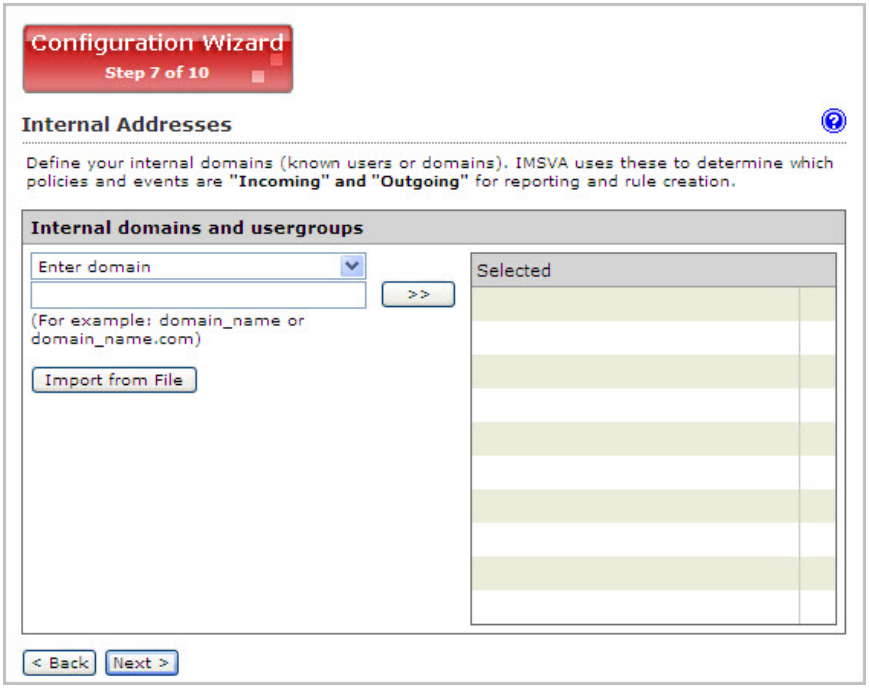


FIGURE 4-7. Internal Addresses

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 **TMCM Server Settings** screen appears.

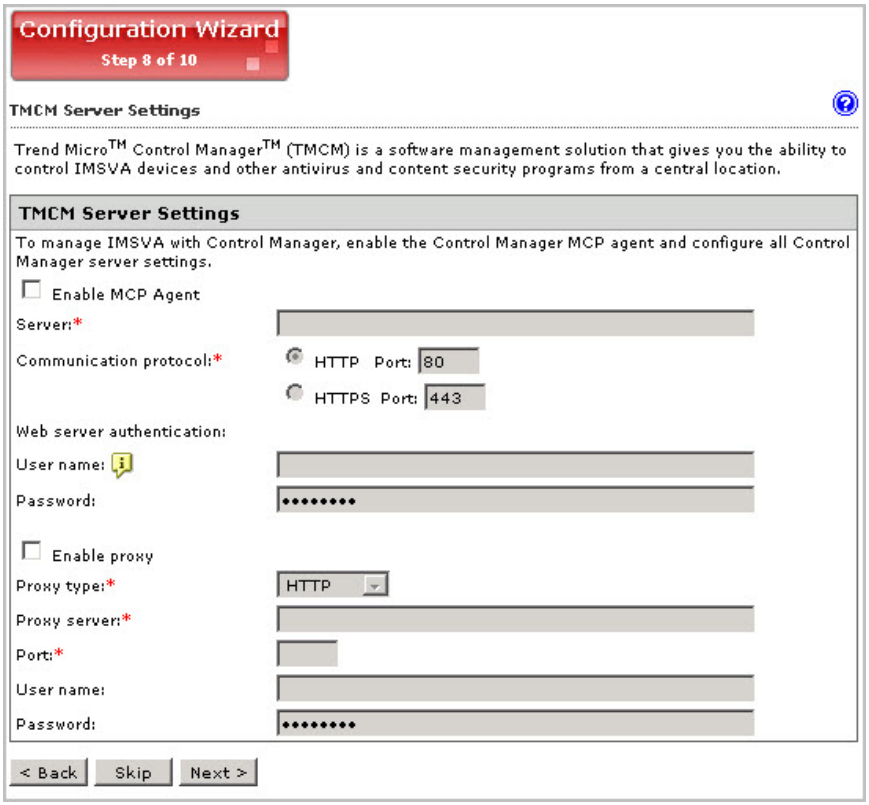


FIGURE 4-8. TMCM Server Settings

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.

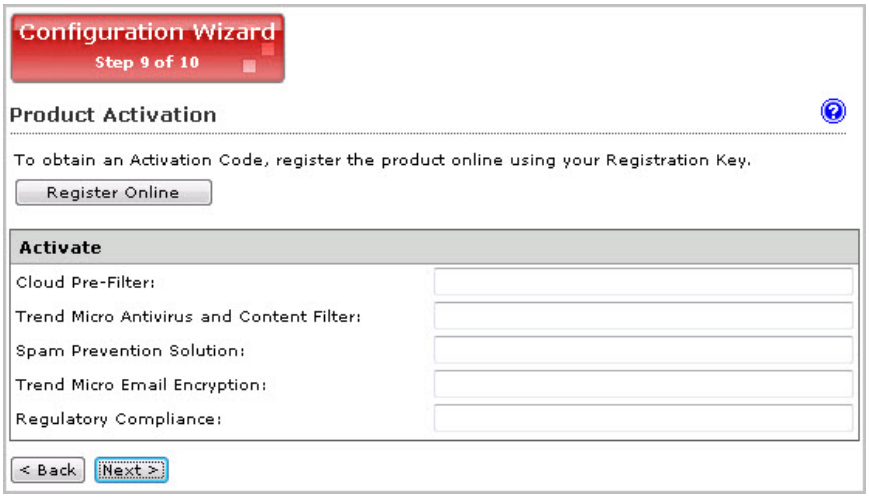


FIGURE 4-9. Product Activation

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 website.

Step 10: Reviewing the Settings

Procedure

1. Click **Next**.

   The **Review Settings** screen appears.

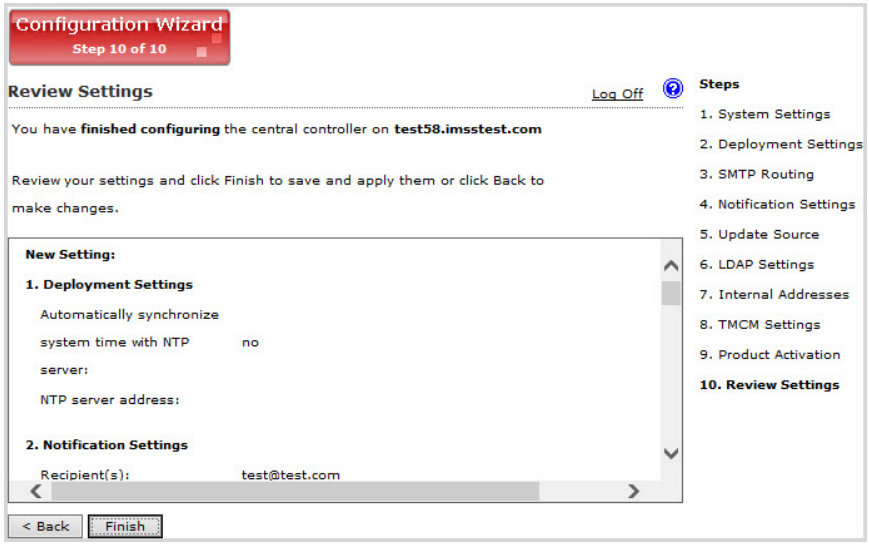


FIGURE 4-10. Review Settings

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 4-21*), 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. Go 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 logon credentials.
   b. In the **Setup Wizard**, configure the local system settings and then click **Next>**.
   c. On the **Deployment Settings** screen, select **Child Device** and specify the IP address, port, logon user name and password for the management console of the parent device.

Note

The logon user account that you specified must have full administration rights.

d. Click **Finish**.

4. On the parent device, do the following:

   a. Go 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. Go 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 5

Upgrading from Previous Versions

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

Topics include:

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.

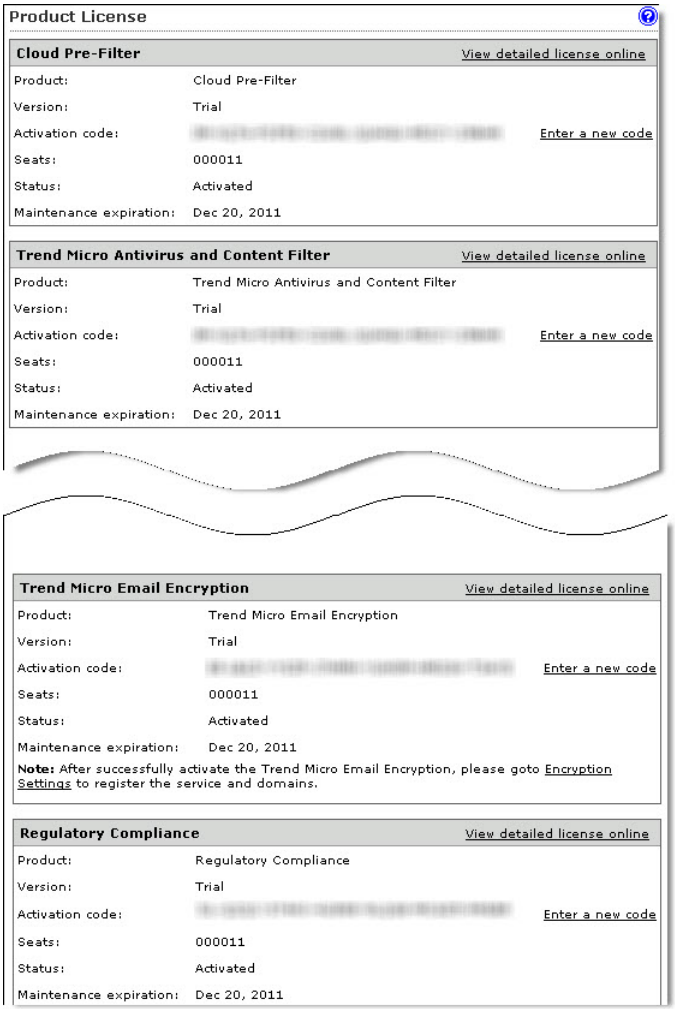
Fourteen (14) days prior to the expiry of the evaluation period, IMSVA will display a warning message on the management console alerting you of the impending expiration.

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

Procedure

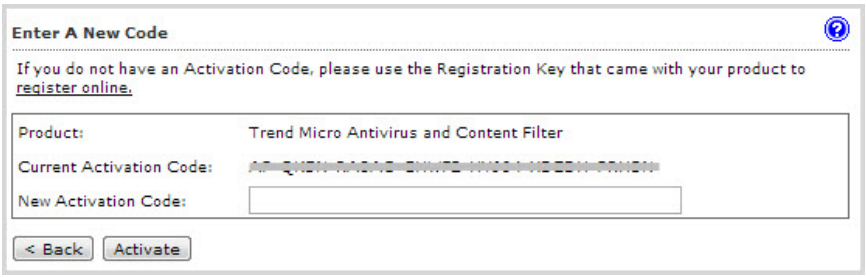
1. Go to **Administration** > **Product Licenses**.

The **Product License** screen appears.



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

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



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

Note

When you purchase the full licensed version of 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 9.0 Patch 1

Upgrade IMSVA 9.0 Patch 1 as a single device or an entire distributed environment can be upgraded.

Note

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

During the upgrade, no customized operating system settings migrate, except the host, network, and gateway settings. To retain the original settings, do the following:

1. Mount the original root partition to a path on the upgraded server, for example, `/root/original_root`:

   ```
   mount /dev/mapper/IMSVA-Root1 /root/original_root
   ```

2. Find the original settings in the mounted path.
3. Add the original settings to the upgrade server.

Backing Up IMSVA 9.0 Patch 1

IMSVA 9.0 Patch 1 backs up the configuration settings and performs an auto-rollback if the upgrade is not successful. However, Trend Micro recommends backing up IMSVA 9.0 Patch 1 before attempting to upgrade to IMSVA 9.1:

Procedure

1. Do any of the following tasks to back up IMSVA 9.0 Patch 1:

- Ghost the entire computer where IMSVA 9.0 Patch 1 is installed.
- Take a snapshot for IMSVA 9.0 Patch 1 if it is installed on a virtual machine.
- Back up the IMSVA 9.0 Patch 1 app_data partition.

  a. Open the operating system shell console and run the following commands:

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

  service crond stop
  ```

  b. Mount an external disk to `/var/udisk`.

c. Copy all files to the disk:

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

2. Start all IMSVA services after backup.

Upgrading a Single IMSVA

This procedure explains how to upgrade a single IMSVA to version 9.1.

Procedure

1. Back up IMSVA 9.0 Patch 1.

   Note

   For details, see *Backing Up IMSVA 9.0 Patch 1 on page 5-5*.

2. Use the following command in the CLI console to verify there are no messages in the Postfix queue:

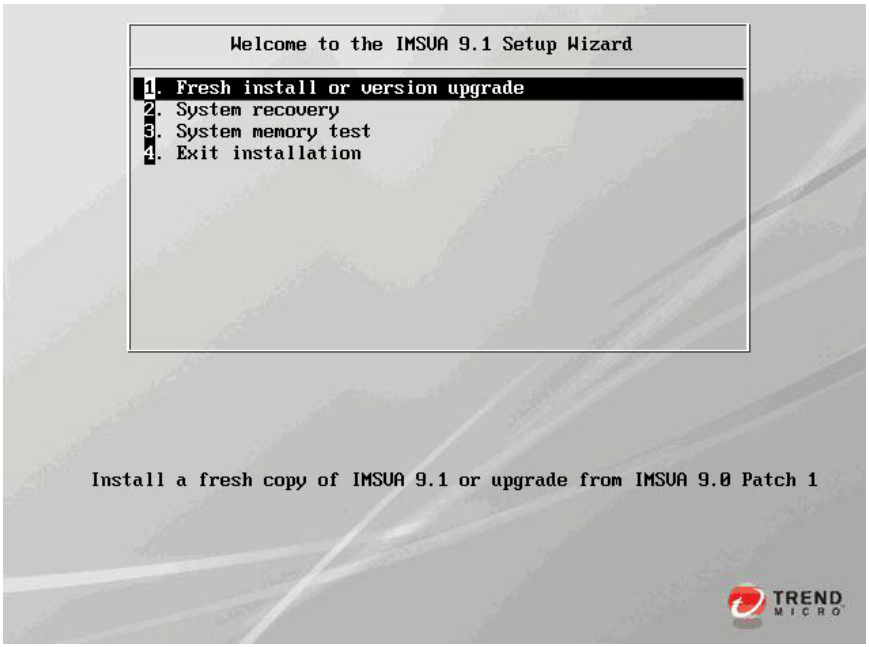
   ```
   postqueue -p
   ```

3. Restart the server that you want to upgrade with the IMSVA Installation DVD.

   Note

   For details, see Step 1 in *Installing IMSVA on page 4-4*.

The **IMSVA 9.1 Setup Wizard** screen appears.

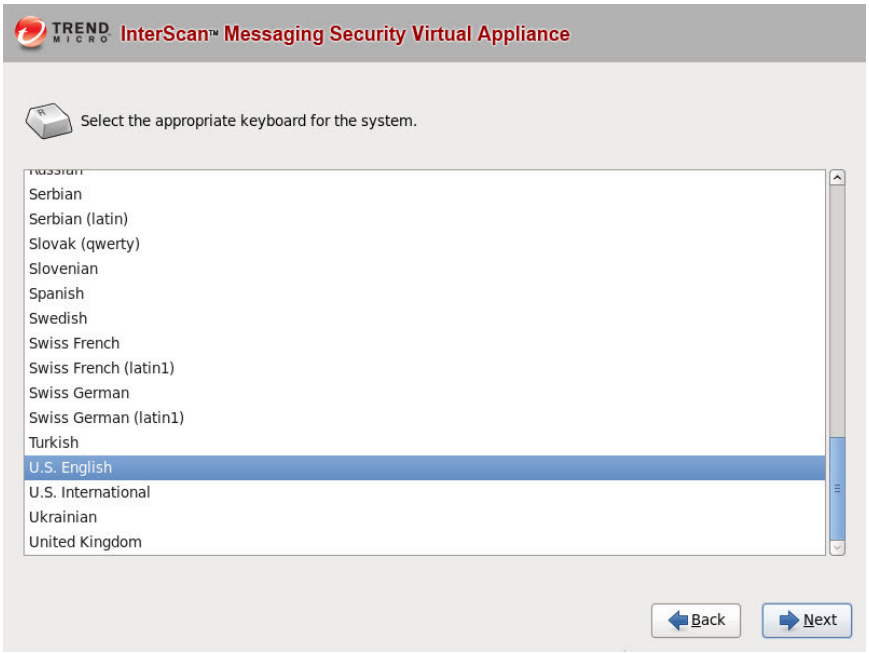


4. Select **Fresh install or version upgrade**.

The **License Agreement** screen appears.

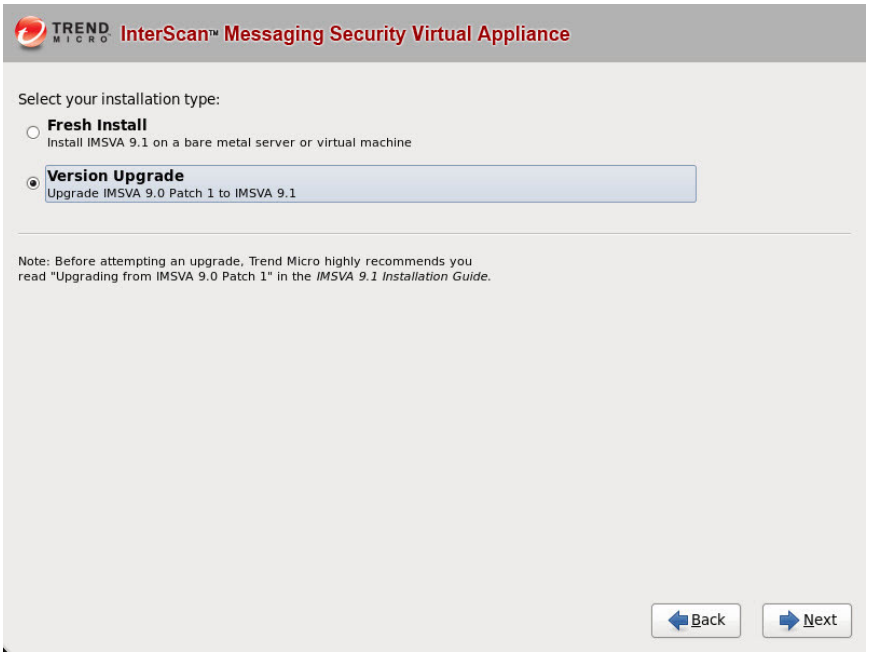
5. Click **Accept** to continue.

A keyboard language selection screen appears.



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

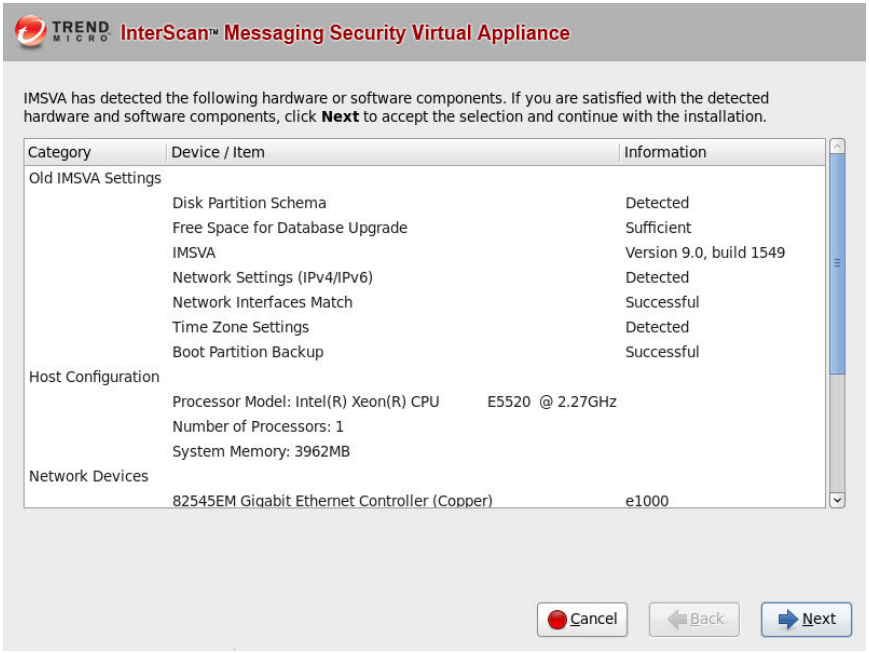
A screen appears for you to select your installation type.



7. Select **Version Upgrade**, and then click **Next**.

   The IMSVA upgrade program scans your hardware and software to determine if the minimum requirements have been met and displays the results. If the hardware or software contains any components that do not

meet the minimum requirements, the upgrade program highlights those components and the upgrade stops.

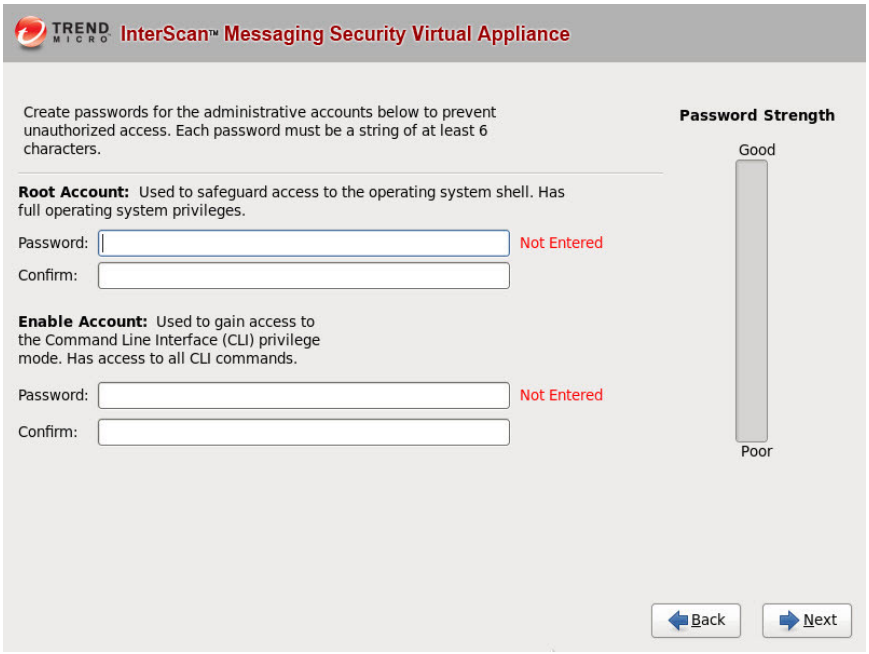


Note

If the free space for database upgrade is insufficient, remove old log files from `/var/app_data/imss/log` and try again. Make sure that the free disk space on `/var/app_data` is at least 1.25 times the disk space on `/var/imss`.

8. Make sure the hardware and software information is correct, and then click **Next**.

The **Account Settings** screen appears.



9. 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.

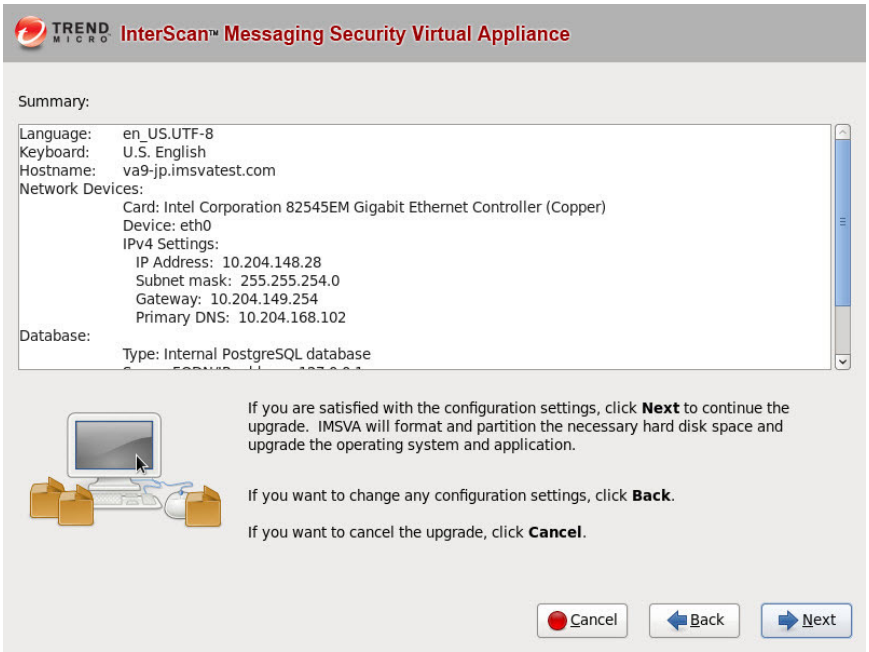
Tip

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 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.

10. Click **Next**.

    A screen appears, showing a summary of your configuration settings.



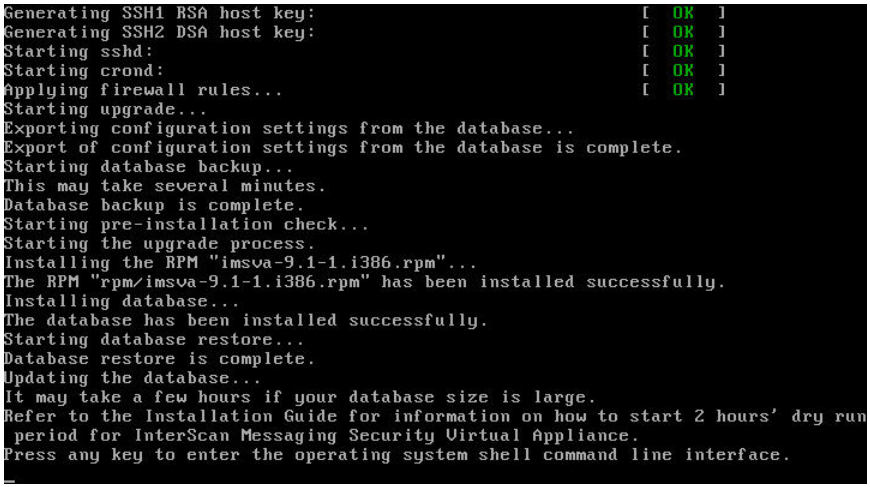
11. Verify settings, and then click **Next**.

A screen appears that provides the formatting status of the local drive for the IMSVA upgrade.

Once the formatting is complete, a summary screen appears.

12. Click **Restart** to restart the system.

The upgrade continues after the system restarts. When the following information appears, the upgrade is complete.



Note

To avoid any unexpected error, do not restart your machine in any of the following steps.

13. Press any key to enter the system shell command line interface.
14. Use the following command to verify the upgrade:

    ```
    # tail -1 /var/app_data/installlog
    ```

15. Once IMSVA upgrade completes, restart IMSVA services from the CLI console with the following command:

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

16. Verify that IMSVA is working properly after the upgrade.
17. To roll back to IMSVA 9.0 Patch 1, use the following commands:

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

"no"

18. If the IMSVA is working properly after the upgrade, use the following commands to complete the upgrade:

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

    "yes"

    If you do not roll back to IMSVA 9.0 Patch 1 within 2 hours, all IMSVA services will stop automatically. You must then decide whether to roll back to IMSVA 9.0 Patch 1, or to complete the upgrade using the following command:

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

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

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. Prepare for the upgrade.

   a. Back up IMSVA 9.0 Patch 1.

   Note

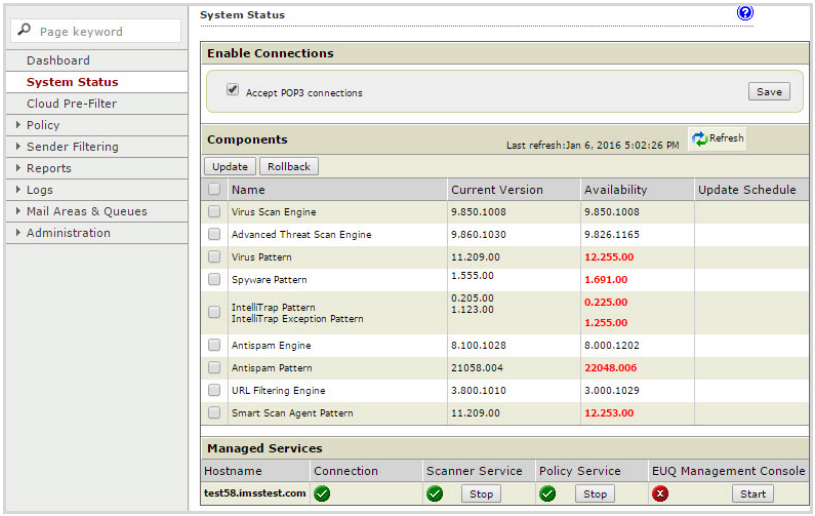
   For details, see *Backing Up IMSVA 9.0 Patch 1 on page 5-5*.

   b. Use the following command in the CLI console to verify there are no messages in the Postfix queue:

      ```
      postqueue -p
      ```

   c. Make sure that all IMSVA services are working properly on the management console.

On the **System Status** screen, all the services under **Managed Services** are active.



d. Stop all services on child devices using the following command:

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

Note

In a distributed deployment, the parent device must be upgraded before child devices.

WARNING!

Performing this step will interrupt your email traffic. If you want to avoid traffic interruption, perform *Batch Upgrade on page 5-20* or *Offline Upgrade on page 5-28*.

e. Start the database service on child devices using the following command:

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

2. Upgrade the parent and child devices.

   a. Upgrade the parent device. See steps 3 to 13 in *Upgrading a Single IMSVA on page 5-6*.

   b. Use the following command to verify that the database is working properly on the parent device:

      ```
      # ps -ef |grep imss
      ```

      Information similar to the following appears:

      ```
      imss 5602 0.0 0.2 63412 3376 ? S Oct14 1:09 /opt/trend/
      imss/PostgreSQL/bin/postgres -D /var/imss/pgdata -i
      ```

   c. Upgrade all the child devices one at a time, a few at a time, or all at once.

      WARNING!

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

      Do not run `/mnt/backup/dry_run.sh` or `/mnt/backup/confirm.sh` on any of the parent or child device before you finish upgrading all the devices.

      If one of the child devices encounters issues while upgrading, unregister the child device using the CLI.

3. Verify that the upgrade is successful.

   a. Open the installation log file using the following command:

      ```
      # tail -1 /var/app_data/installlog
      ```

   b. Check the installation logs for information indicating the upgrade success.

4. Complete the upgrade.

   a. After upgrading all devices, restart IMSVA services on the parent device and then on the child devices with the following command:

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

b. Verify that IMSVA is working properly after the upgrade.

c. To roll back to IMSVA 9.0 Patch 1, first roll back all child devices and then the parent device with the following commands:

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

```
“no”
```

d. If the IMSVA is working properly after the upgrade, use the following commands to complete the upgrade:

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

```
“yes”
```

If you do not roll back to IMSVA 9.0 Patch 1 within 2 hours, all IMSVA services will stop automatically. You must then decide to roll back to IMSVA 9.0 Patch 1, or to complete the upgrade, using the following command:

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

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

Batch Upgrade

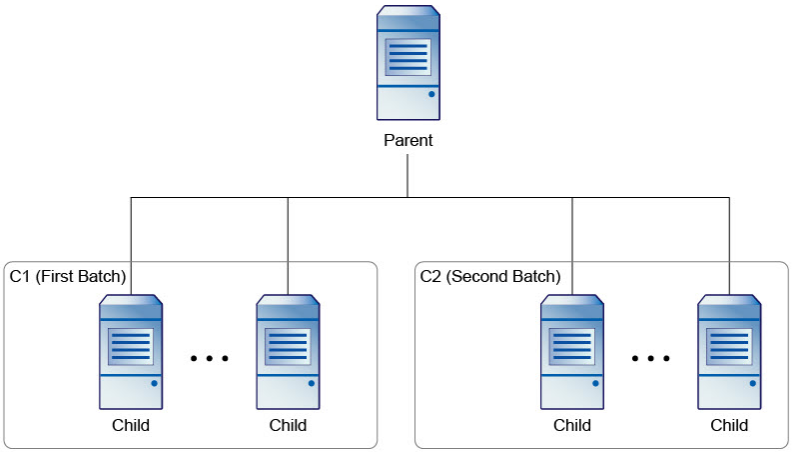
Batch upgrade allows upgrading of two or more parent and child devices. This option reserves log information during the upgrade process and does not cause any downtime.

Tip

Trend Micro recommends performing batch upgrade when email traffic is at a minimum. Evaluate if the IMSVA devices to be upgraded after the first batch can accommodate the total email 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 upgrade.
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. However, 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: Blocking Connections Between Parent and Child Devices

Note

In this procedure, C1 refers to the first batch of child devices to be upgraded, and C2 refers to the second batch of 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. Change the iptables on the second batch of child devices (referred to hereafter as C2).
   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 REJECT

iptables -I INPUT -s [C1's IP] -j REJECT

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

iptables -I OUTPUT -d [C1's IP] -j REJECT

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

b. Apply the added rules.

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

3. Change the iptables on the parent device.

a. On the 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 2: Performing Inline Upgrade

Note

In this procedure, C1 refers to the first batch of child devices to be upgraded, and C2 refers to the second batch of child devices.

Procedure

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

a. 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 C1 devices using the following commands:

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

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

3. Perform inline upgrade to IMSVA 9.1.

Note

For detailed upgrade procedure, see *Upgrading a Single IMSVA on page 5-6*.

4. Perform a test deployment of IMSVA 9.1.

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='9.1.0.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 3: Performing Inline Upgrade for Other Child Devices on page 5-26* (substep 4-b). Then, replace `9.1.0.xxxx` with the number of the IMSVA 9.1 build that you intend to install.

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

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

Note

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

5. Check the build number.

   a. Go to **Administration** > **Updates** > **System & Applications**.

   b. Under **Current Status**, check if the application version is 9.1.0.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/confirm.sh
   ```

   “yes”

   b. To roll back to IMSVA 9.0, first roll back all child devices, then the parent devices.

   ```
   # /mnt/backup/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 3: Performing Inline Upgrade for Other Child Devices

Note

Upgrade child devices individually or in batches.

In this procedure, C1 refers to the first batch of child devices to be upgraded, and C2 refers to the second batch of child devices.

Procedure

1. Select child devices.
2. Modify the DNS record to stop sending messages to the selected devices.
3. Verify that there are no messages in the Postfix queue.
   a. On the CLI console, check the Postfix queue.

      ```
      # postqueue -p
      ```
4. Modify the settings for the C2 devices.
   a. To bypass the inline upgrade check, change the iptables on the C2 devices.

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

      ```
      # /opt/trend/imss/PostgreSQL/bin/psql imss sa

      # select * from tb_component_list;

      # update tb_component_list set app_ver='9.0.0.1549'
      where ip_addr='[C2's IP]';
      ```

Note

The IMSVA version (`app_ver`) should reflect the version that you recorded in *Step 2: Performing Inline Upgrade on page 5-23* (substep 4-b).

5. Perform inline upgrade to IMSVA 9.1.

Note

For detailed upgrade procedure, see *Upgrading a Single IMSVA on page 5-6*.

6. Perform a test deployment of IMSVA 9.1.
   a. On the CLI console, restart all IMSVA services:

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

7. Check the build number.
   a. Go to **Administration** > **Updates** > **System & Applications**.
   b. Under **Current Status**, check if the application version is 9.1.0.xxxx.
8. Complete the inline upgrade.
   a. To complete the upgrade on all devices, run the following command:

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

      “yes”

   b. To roll back to IMSVA 9.0, run the following command:

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

      “no”

9. 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.

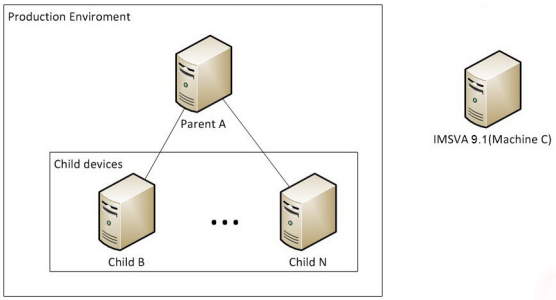
Tip

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 9.1 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 Virtual Analyzer notifications are enabled, you may receive Virtual Analyzer service messages after data is restored.

Step 1: Installing IMSVA 9.1 on a Temporary Device

Procedure

1. Install IMSVA 9.1 on a temporary device using an ISO file.
2. Back up the default settings of the temporary IMSVA 9.1 device.
   a. Log on to the parent device management console.
   b. Go 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. Go 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. Go to **Administration** > **Import/Export**.

c. Click **Import**.

Note

If problems occur during the import process, restore the IMSVA 9.1 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 5-17*.
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 9.1 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 Virtual Analyzer on the temporary device, verify that there are no messages in the Virtual Analyzer upload folder.

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

Note

Trend Micro recommends disabling Virtual Analyzer on the temporary IMSVA device to prevent receiving notifications after log import. Ignore the notifications if you intend to keep Virtual Analyzer 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.

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. Stop the cron service using the following command:

   ```
   service crond stop
   ```

3. Check the cron settings backup file `/var/spool/cron/root.bakForUpgrade`. After finding the file, restore the cron settings using the following command:

   ```
   rm -rf /var/spool/cron/root && /bin/mv -f /var/spool/cron/root.bakForUpgrade /var/spool/cron/root
   ```

4. Check the log backup file `/var/app_data/imss/log.bakForUpgrade`. After finding the backup file, restore the log file using the following command:

   ```
   rm -rf /var/app_data/imss/log/ && /bin/mv -f /var/app_data/imss/log.bakForUpgrade /var/app_data/imss/log/
   ```

5. Stop the database service using the following command:

   ```
   killall postgres
   ```

6. On the parent device, check the database backup file `/var/app_data/imss/pgdata.bakForUpgrade`. After finding the file, restore the database file using the following command:

   ```
   rm -rf /var/app_data/imss/db/pgdata && /bin/mv -f /var/app_data/imss/pgdata.bakForUpgrade /var/app_data/imss/db/pgdata
   ```

7. If not mounted, mount the root partition of IMSVA 9.0 Patch 1 using the following command:

   ```
   mkdir -p /var/tmp/orig_root

   mount -t ext3 /dev/mapper/IMSVA-Root1 /var/tmp/orig_root
   ```

8. Restore the **/boot** folder using the following command:

   ```
   /bin/cp -af /var/tmp/orig_root/boot-imsva-9.0-back-

   up-for-9.1/* /boot
   ```

9. Update the boot partition UUID.

   a. Obtain the 9.1 boot partition UUID from `/etc/fstab`.

   b. Replace 9.0 Patch 1 boot partition UUID in `/var/tmp/orig_root/etc/fstab` with 9.1 boot partition UUID.

10. Restart your machine.

Migrating from Previous Versions

IMSVA 9.1 supports migration from previous versions of IMSS and IMSVA.

The following table lists the minimum versions that support migration to IMSVA 9.1:

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 Service Pack 2
IMSS for Windows	7.1 Patch 3
IMSS for Windows	7.5
IMSVA	8.0 Patch 2

Platform	Version
IMSVA	8.2 Service Pack 2 Patch 1
IMSVA	8.5 Service Pack 1 Patch 1
IMSVA	9.0 Patch 1

Migration Process

The migration process requires the following tasks:

- **Step 1**: Exporting the settings from previous versions of IMSS or IMSVA
- **Step 2**: Importing the settings to IMSVA 9.1

Exporting Settings from Previous Versions of IMSS or IMSVA

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
Configuration Settings	Database settings (example: Internal file path)
	Management console password
	Control Manager settings
	Activation Codes **Note** All earlier versions of IMSVA will migrate the Cloud Pre-Filter Activation Code to IMSVA 9.1

Important

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

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

Certificate usage for child devices cannot be exported.

Procedure

1. Go 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 9.1

Procedure

1. Perform a fresh installation of IMSVA 9.1.

   Tip

   Trend Micro recommends importing configuration packages to a fresh installation of IMSVA 9.1, because the imported configuration settings overwrite all existing settings.

2. Retrieve the package that contains the configuration settings that you wish to migrate.

3. Go to **Administration** > **Import/Export** on the IMSVA 9.1 management console.

   The **Import/Export** screen appears.

4. Import the configuration package.

   Note

   By default, all child devices use the certificates of the parent device after migration. If you do not want to use those certificates, assign other certificates to child devices.

Migrating from IMSS for Windows

To migrate from IMSS for Windows to IMSVA 9.1, see *Migration Process on page 5-35*.

IMSS for Windows Settings that Change

The following settings of IMSS for Windows change during migration:

- During migration IMSVA 9.1 changes all customized actions to **Default intelligent action**, unless the customized action is **Connection rejected with** in which case the setting remains unchanged.
- **Default Delivery** with **Smart Host** set, changes to *****
- If several **Smart Hosts** of a Domain were set, all Smart Hosts in the list migrate to IMSVA 9.1 with Static Routing as the delivery method
- The maximum data size/messages per connection settings are reduced.
- **Free disk space on any scanner less than** changes to **Data partition on free space on any host less than** in IMSVA 9.1.

IMSS for Windows 7.1 Patch 3 Settings that Do Not Migrate

All IMSS for Windows 7.1 Patch 3 settings migrate to IMSVA 9.1 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
- Transport Layer Security settings
- Activation Code because IMSVA cannot use the Activation Code from IMSS Windows 7.1

- The following **Administration** > **Connections** > **Components** internal ports do not migrate:
  - **IMSS manager port**
  - **Policy service port**
- The BATV rule and all related settings do not migrate.

IMSS for Windows 7.5 Settings that Do Not Migrate

All IMSS for Windows 7.5 settings migrate to IMSVA 9.1 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
- Virtual Analyzer settings
- Transport Layer Security settings
- Activation Code because IMSVA cannot use the Activation Code from IMSS Windows 7.5
- The following **Administration** > **Connections** > **Components** internal ports do not migrate:
  - **IMSS manager port**
  - **Policy service port**
- The BATV rule and all related settings do not migrate.

Migrating from IMSS for Linux

To migrate from IMSS for Linux to IMSVA 9.1, see *Migration Process on page 5-35*.

IMSS for Linux Settings that Change

The following settings of IMSS for Linux change during migration:

- The **Administration** > **Notifications** > **Events** notification:

  Free disk space on any scanner less than changes to **Data partition on free space on any host less than** in IMSVA 9.1.

IMSS for Linux 7.1 SP2 Settings that Do Not Migrate

All IMSS for Linux 7.1 SP2 settings migrate to IMSVA 9.1 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
- Transport Layer Security (TLS) settings
- Activation Code because IMSVA cannot use the Activation Code from IMSS Linux 7.1
- Email addresses in the marketing message exception list

Migrating from IMSS for Solaris

To migrate from IMSS for Solaris to IMSVA 9.1, see *Migration Process on page 5-35*.

IMSS for Solaris 7.0 SP1 Patch 4 Settings that Do Not Migrate

All IMSS for Solaris 7.0 SP1 Patch 4 settings migrate to IMSVA 9.1 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
- TLS settings
- Activation Code because IMSVA cannot use the Activation Code from IMSS Solaris 7.0

Migrating from IMSVA 8.0 Patch 2, IMSVA 8.2 SP2 Patch 1, IMSVA 8.5 SP1 Patch 1 or IMSVA 9.0 Patch 1

To migrate from previous IMSVA versions to IMSVA 9.1, see *Migration Process on page 5-35*.

IMSVA 8.0 Patch 2 Settings that Do Not Migrate

All IMSVA 8.0 Patch 2 settings migrate to IMSVA 9.1 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
- TLS settings

IMSVA 8.2 SP2 Patch 1 Settings that Do Not Migrate

All IMSVA 8.2 SP2 Patch 1 settings migrate to IMSVA 9.1 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
- Virtual Analyzer settings
- TLS settings

IMSVA 8.5 SP1 Patch 1 Settings that Do Not Migrate

All IMSVA 8.5 SP1 Patch 1 settings migrate to IMSVA 9.1 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

- Virtual Analyzer settings
- TLS settings

IMSVA 9.0 Patch 1 Settings that Do Not Migrate

All IMSVA 9.0 Patch 1 settings migrate to IMSVA 9.1 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
- Virtual Analyzer 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. Go 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

This sections helps to resolves common issues that you might encounter when installing, or configuring and administering IMSVA. If you have additional problems, check the Trend Micro Knowledge Base.

Topics include:

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.

- Admin database

  Open `/opt/trend/imss/config/odbc.ini` and check the value of the key database

- EUQ database

  Open `/opt/trend/imss/config/euqodbc.ini` and check the value of the key database.

  Note

  If you use the internal database, the default password of the database is **postgreSQL**.

- Firewall setting check:

  ```
  iptables -nvxL
  ```

- PostgreSQL command line tool:

  ```
  /opt/trend/imss/PostgreSQL/bin/psql -U sa -d imss
  ```

  Note

  imss refers to the admin database name that you obtain from `/opt/trend/imss/config/odbc.ini`.

- cdt (password: "trend")—Collect the following information:
  - Configuration information
  - Logs
  - Core dumps

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

Troubleshooting Communication Between Devices in a Group

If several IMSVA devices are deployed in a group, they must communicate with each other.

Procedure

1. Verify that the following ports are accessible on all devices:
   - 5060: Policy service
   - 15505: IMSVA control service
   - 53 UDP/TCP: IP Profiler
   - 5432: Database service
   - 8009: EUQ internal service
   - 389: LDAP local cache service
   - 998/999: TLS setting service
   - 10030: Message Delivery setting service
   - 10040: SMTP Traffic Throttling service
   - 8891: DKIM setting service

2. Verify the following:
   - The current firewall settings in “iptables”.
   - The firewall configuration files in `/etc/conf/fw.rules`.
   - The table “tb_trusted_ip_list” in the database has the IP addresses of the correct devices. The IP address of any other devices trying to access this device must be in this list.
3. Verify that all the necessary ports are accessible for the relevant services.

Troubleshooting Child Device Registration

Procedure

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.
9. The parent device management console (in the Configuration Wizard) makes the initial request.

Troubleshooting Child Device Unregistration

Procedure

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.
5. To verify that a child is unregistered from its parent, to either of the following:
   - Try to access the management console on the child device. If the console is accessible, the device is successfully unregistered.
   - Run the following command:

     ```
     /opt/trend/imss/script/cfgtool.sh dereg
     ```

Troubleshooting the Hardware Identification Error

If IMSVA cannot identify your hardware such as storage or network device, load driver disks before you try to install IMSVA again.

Contact the hardware vender to obtain a hardware driver applicable to CentOS 6.4 (x86_64). Then load a driver disk by referring to the driver's installation guide.

The following is an example of loading a driver disk.

Procedure

1. Prepare your removable disk, for example, a USB diskette. Make sure the file system of your removable disk is available.

2. Copy the driver image to the USB diskette.

   ```
   cp dd.iso /mnt/usb
   ```

3. Insert the IMSVA Installation DVD into the DVD drive and start IMSVA installation.

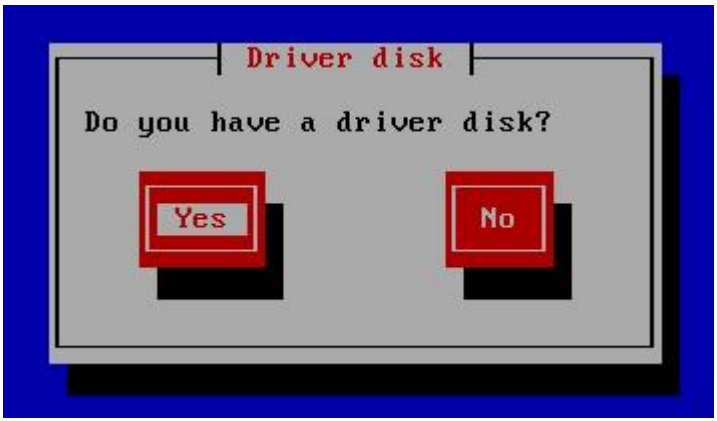
   The setup wizard screen appears.

4. Select **Fresh install or version upgrade** and press Tab to enter the edit mode.

5. Append `dd` to the information that appears at the bottom of the setup wizard screen.

6. Press Enter.

The **Driver disk** screen appears.

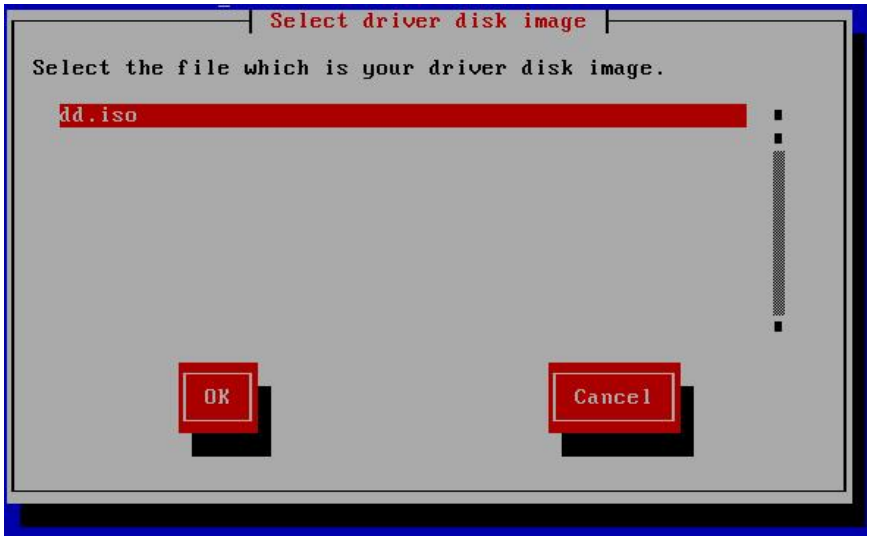


7. Insert your USB diskette and select **Yes**.

   The **Driver Disk Source** screen appears.

8. Select your USB diskette, for example, sdb, and select **OK**.

   The **Select driver disk image** screen appears.



9. Select the driver disk image.

   The **More Driver Disks** screen appears.

10. Unplug your USB diskette and click **No** to continue IMSVA installation.

Troubleshooting Network Connectivity

If a network connectivity problem occurs on your virtual machine, check whether the MAC address assigned to your NIC card changes.

Sometimes the MAC address automatically assigned to a virtual machine changes dynamically. However, the MAC address recorded either in the interface configuration files or in the udev persistent network rule files does not change. As a result, the NIC card might be unavailable.

Trend Micro recommends that you use a static MAC address. If your MAC address changes, do the following to make sure your NIC card works properly:

Procedure

1. Remove the udev rule file using the following command:

   ```
   rm -rf /etc/udev/rules.d/70-persistent-net.rules
   ```

2. Remove the following lines from the `/etc/sysconfig/network-scripts/ifcfg-eth<X>` file:

   ```
   HWADDR=<MAC>

   UUID=<UUID>
   ```

   Note

   The interface configuration files are named `/etc/sysconfig/network-scripts/ifcfg-eth<X>`, where `<X>` is a unique number corresponding to a specific card.

3. In the `/lib/udev/rules.d/75-persistent-net-generator.rules` file, find the line that contains the following information:

   ```
   ATTR{addr_assign_type}=="0"
   ```

4. Add the following information before the line you found:

```
# ignore VMWare virtual interfaces

ENV{MATCHADDR}=="00:0c:29:*|00:50:56:*",
GOTO="persistent_net_generator_end"

# ignore Hyper-V virtual interfaces

ENV{MATCHADDR}=="00:15:5d:*",
GOTO="persistent_net_generator_end"
```

5. Restart your virtual machine to verify your network connectivity.

Appendix A

Technical Support

This appendix explains various Trend Micro resources and technical support information.

Topics include:

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/1036097.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

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

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

Learn more about TrendLabs at:

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

Appendix B

Creating a New Virtual Machine Under VMware ESX for IMSVA

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

Topic includes:

Creating a New Virtual Machine

The actual installation of ESX 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.

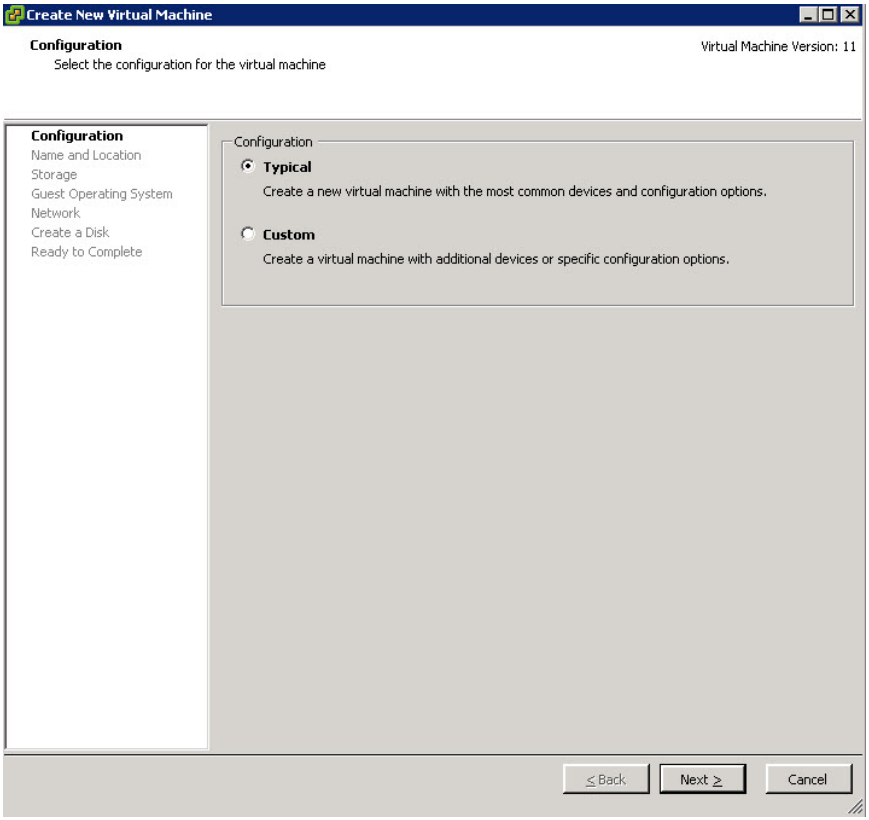


FIGURE B-1. Virtual Machine Configuration

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

3. Click **Next**.

The **Name and Location** screen appears.

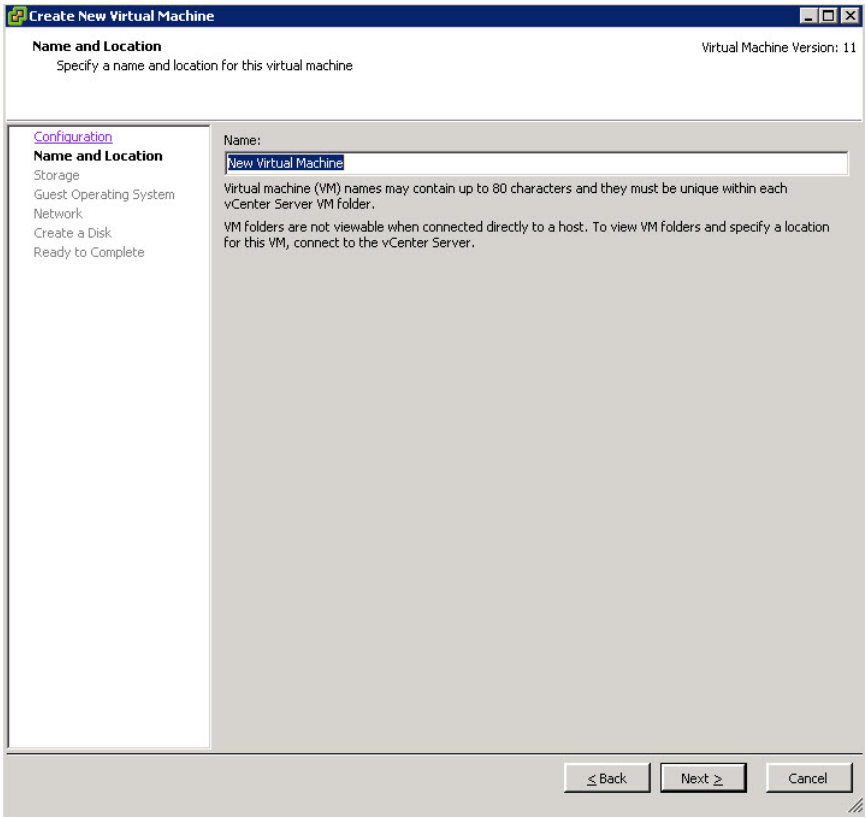


FIGURE B-2. Specify a Name and Location for this Virtual Machine

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

The **Datastore** screen appears.

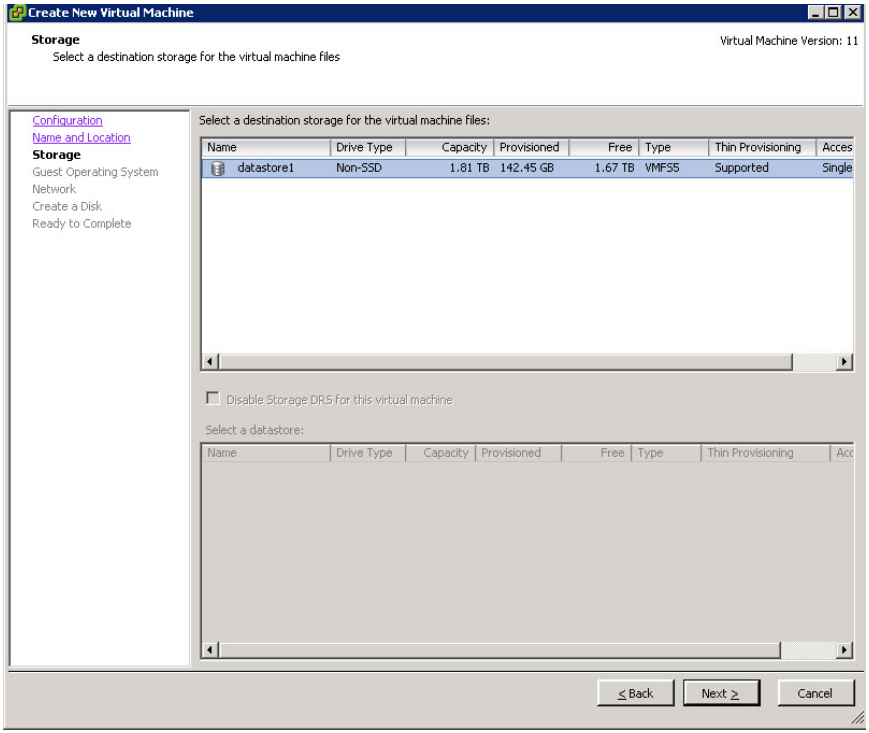


FIGURE B-3. Virtual Machine Datastore

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

The **Guest Operating System** screen appears.

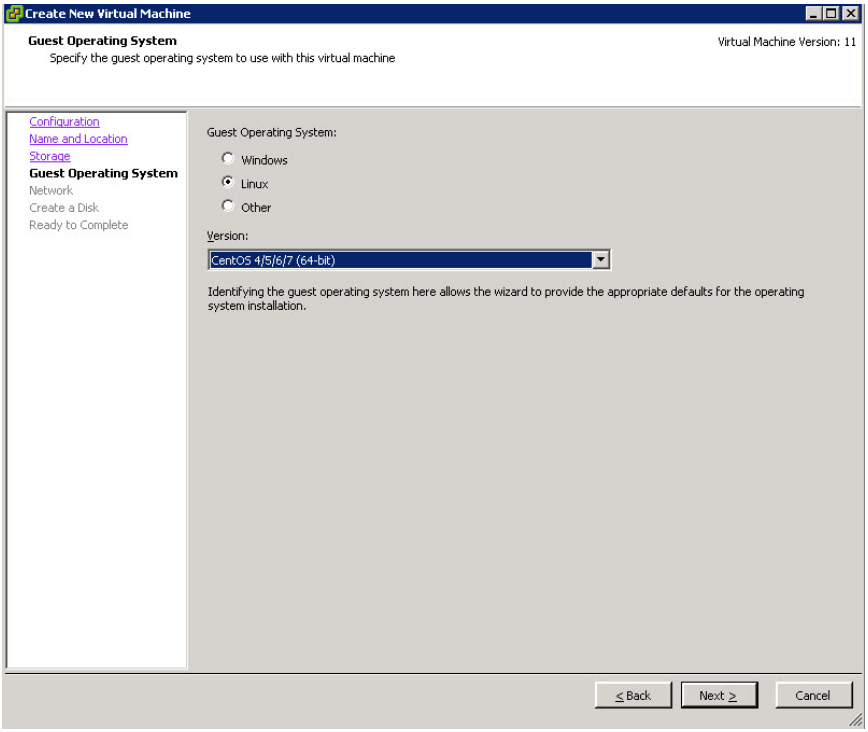


FIGURE B-4. Virtual Machine Guest Operating System

7. For the guest operating system, select **Linux** and then **Other Linux (64-bit)** or **CentOS 4/5/6/7 (64-bit)**.

8. Click **Next**.

The **Network** screen appears.

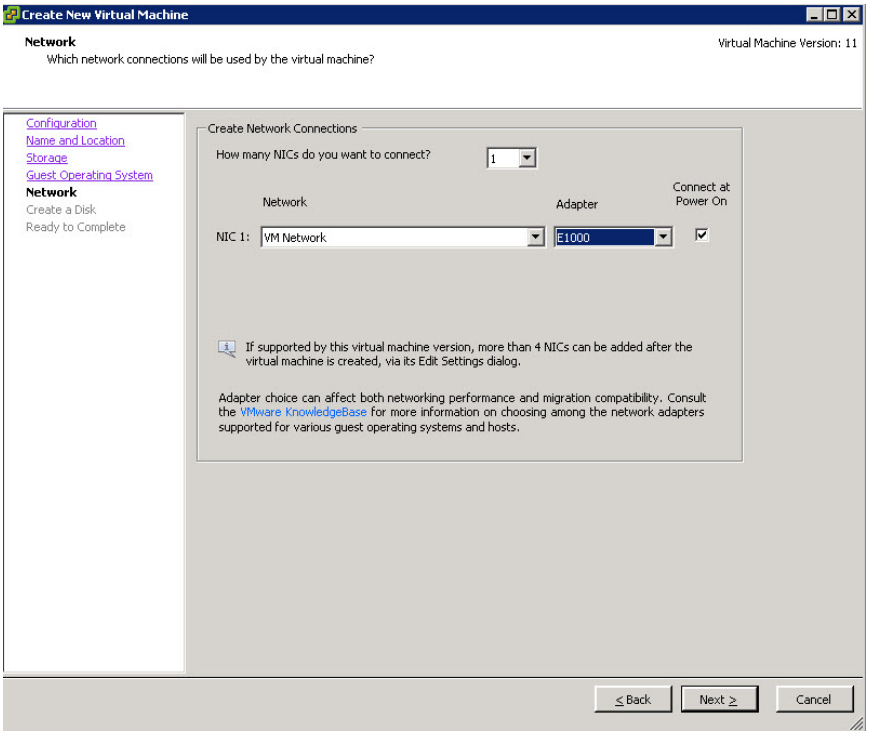


FIGURE B-5. Virtual Machine Network

9. Accept the default network settings.
10. Click **Next**.

The **Create a Disk** screen appears.

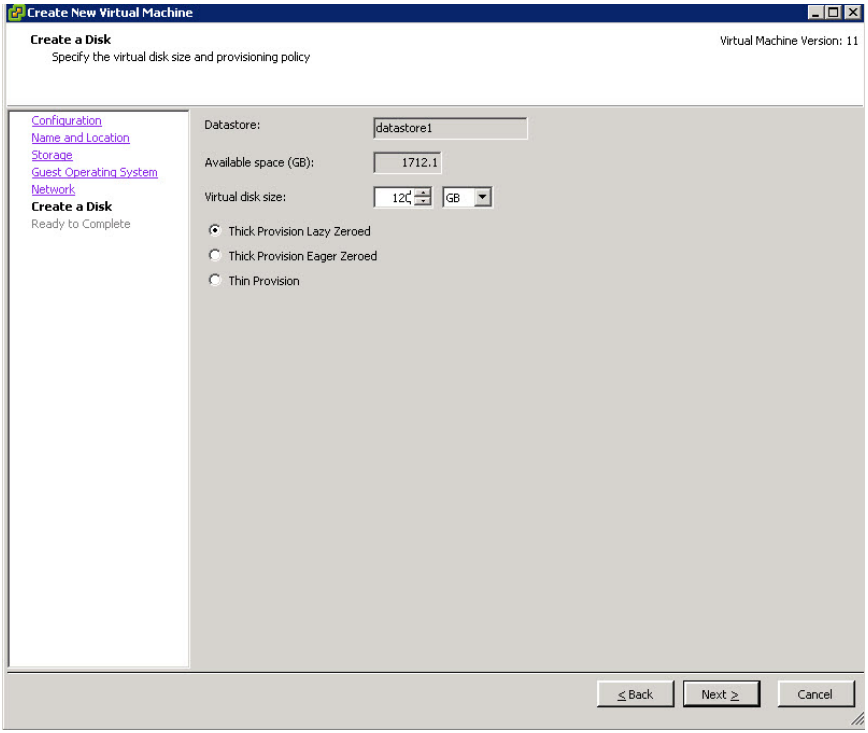


FIGURE B-6. Virtual Disk Capacity

11. Specify at least 120GB of disk space. IMSVA requires at least 120GB disk space. See *System Requirements on page 4-2* for more information on disk space allocation.

Tip

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

12. Click **Next**.

The **Ready to Complete** screen appears.

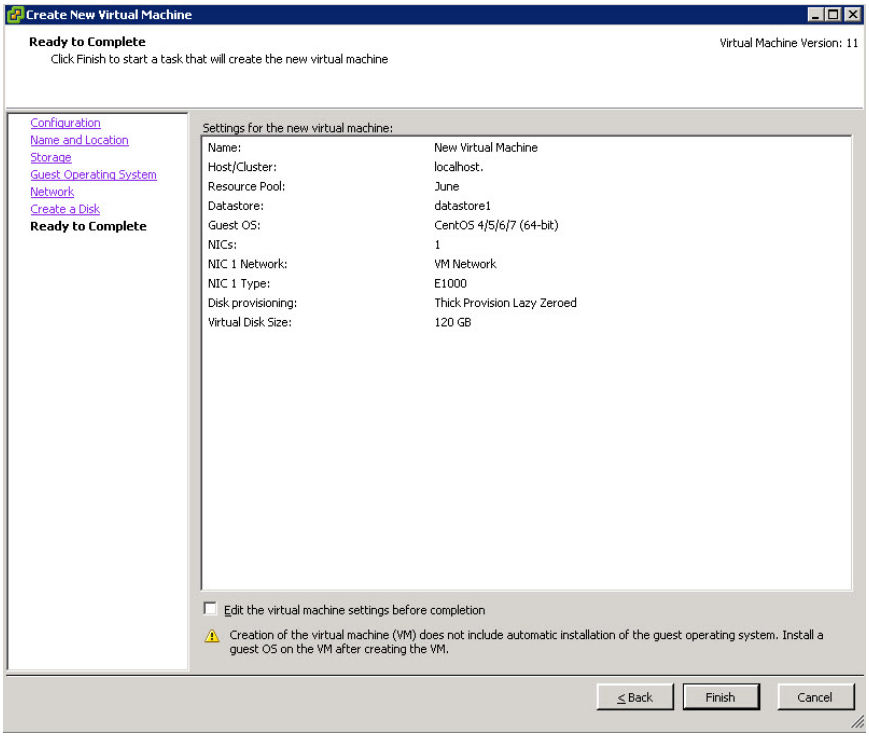


FIGURE B-7. Ready to Complete

13. Click **Finish**.

    If you want to modify the system component settings, check the **Edit the virtual machine settings before submitting** check box and then click **Continue**.

14. 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 C

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

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 Server 2012 R2 Hyper-V server.

IMSVA Support for Hyper-V

IMSVA supports Hyper-V on the following platforms:

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Microsoft Hyper-V Server 2008 R2 SP1
- Microsoft Hyper-V Server 2012 R2

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.

Creating a Virtual Network Assignment

Procedure

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

A menu appears.

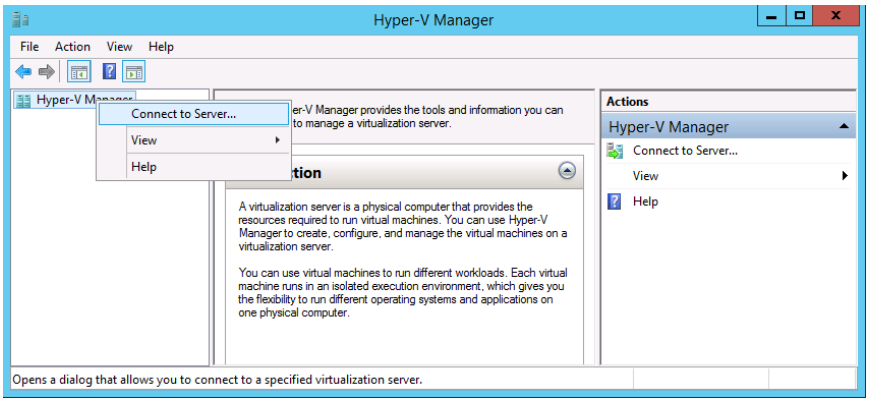


FIGURE C-1. Connect to Server

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.

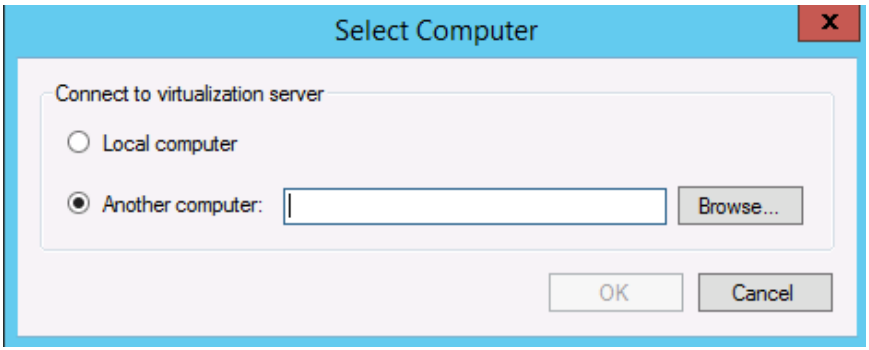


FIGURE C-2. Location of Virtualization Server

3. Specify the location of the virtualization server and click **OK**.
4. Right-click the Windows Server 2012 R2 server and select **Virtual Switch Manager**.

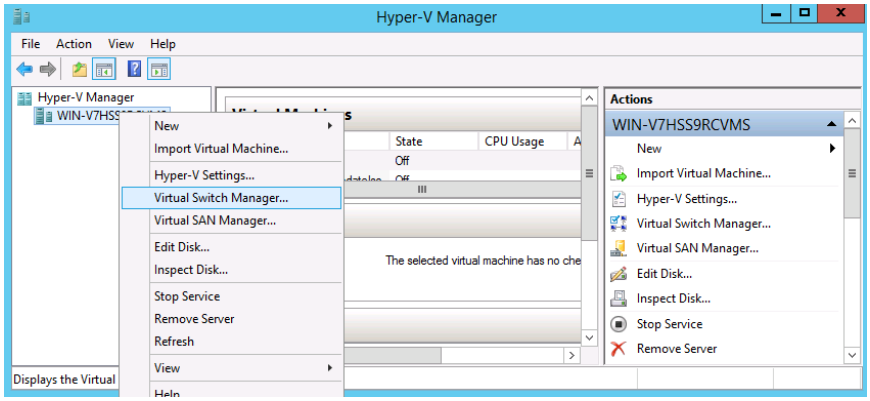


FIGURE C-3. Select Virtual Network Manager

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

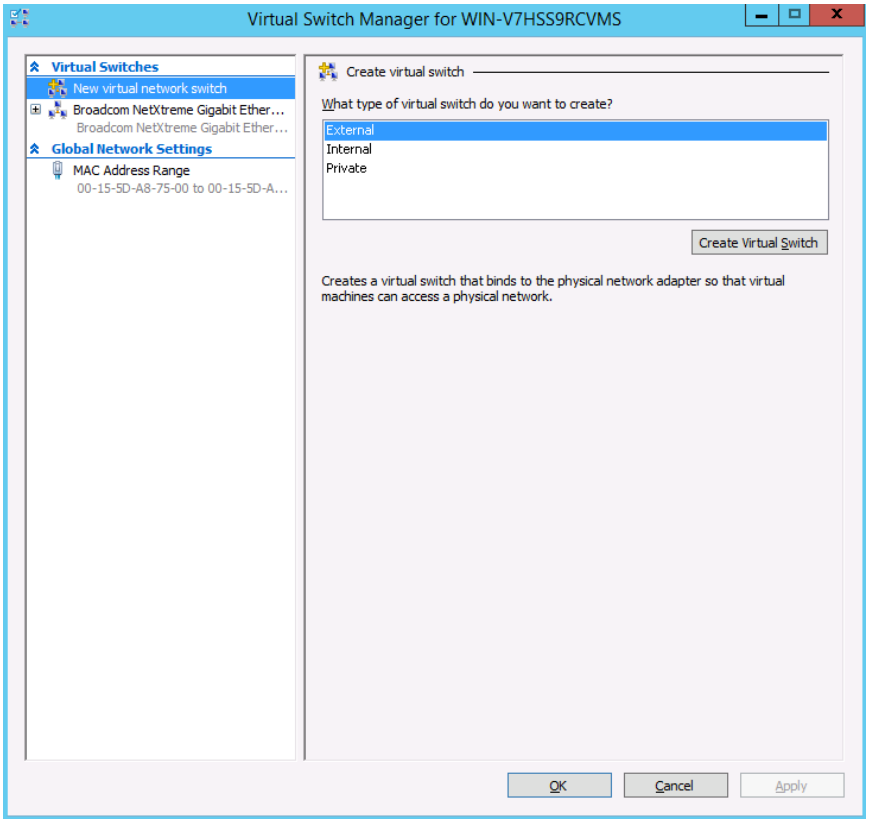


FIGURE C-4. Adding the "External" Virtual Network

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

Note

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

When you have Hyper-V running on Microsoft Windows Server 2012 or Windows Server 2012 R2 together with Broadcom NetXtreme 1-gigabit network adapters (but not NetXtreme II network adapters), you may notice one or more of the following symptoms:

- Virtual machines may randomly lose network connectivity. The network adapter seems to be working in the virtual machine. However, you cannot ping or access network resources from the virtual machine. Restarting the virtual machine does not resolve the issue.
- You cannot ping or connect to a virtual machine from a remote computer.

This is a known issue. For details, see https://support.microsoft.com/en-us/kb/2986895.

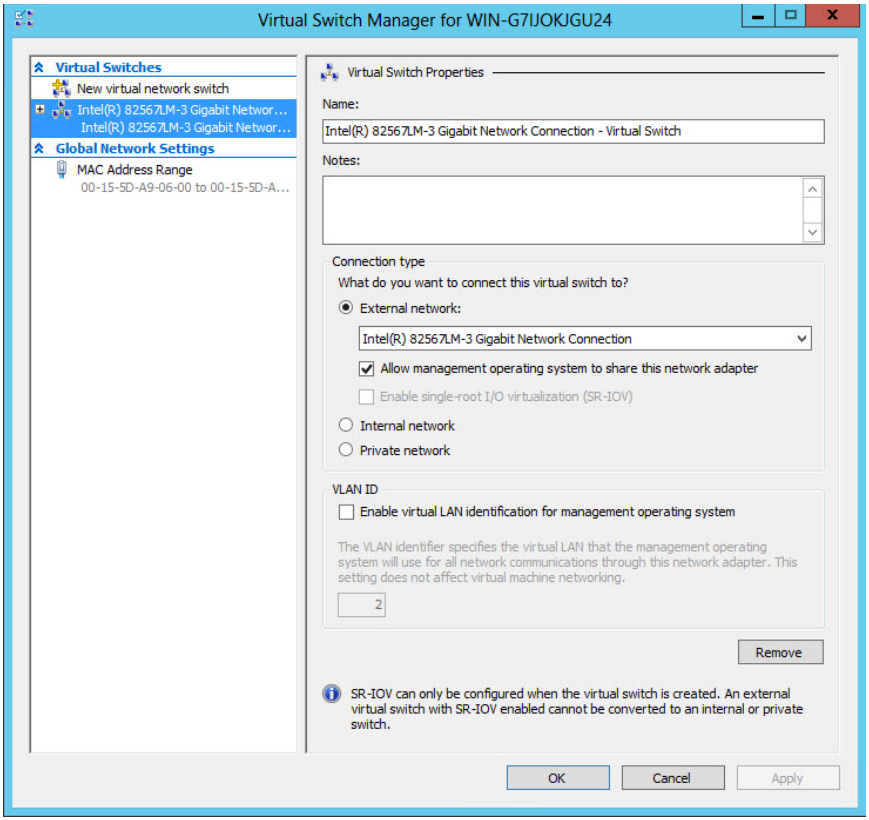


FIGURE C-5. Physical Network Adapter Selection

Creating a New Virtual Machine

Procedure

1. From the Hyper-V Server Manager menu, right-click the Windows Server 2012 R2 server, and select **New** > **Virtual Machine**.

The **New Virtual Machine Wizard** appears.

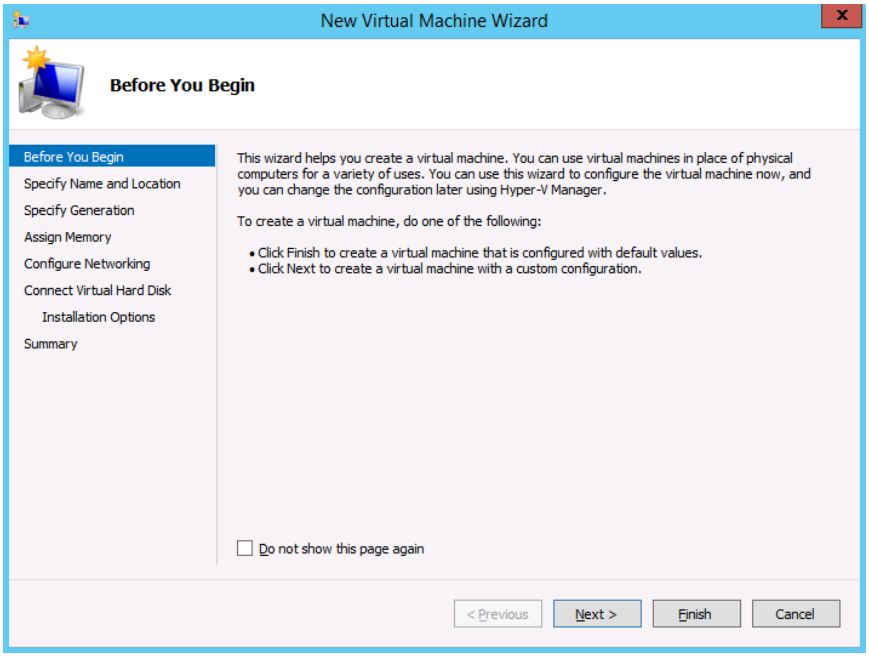


FIGURE C-6. New Virtual Machine Wizard

2. Click **Next**.

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

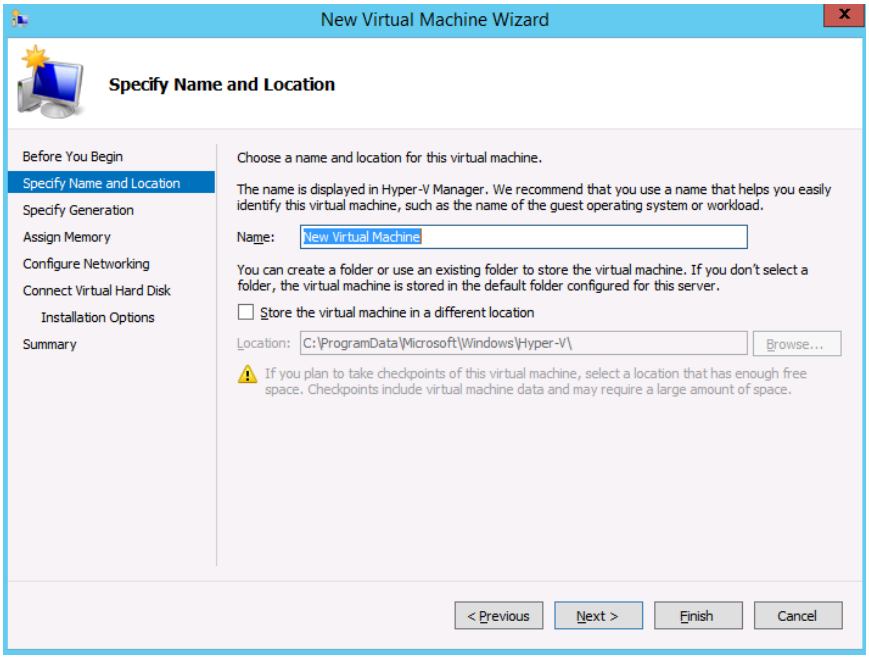


FIGURE C-7. Specify Name and Location

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 **Specify Generation** screen appears.

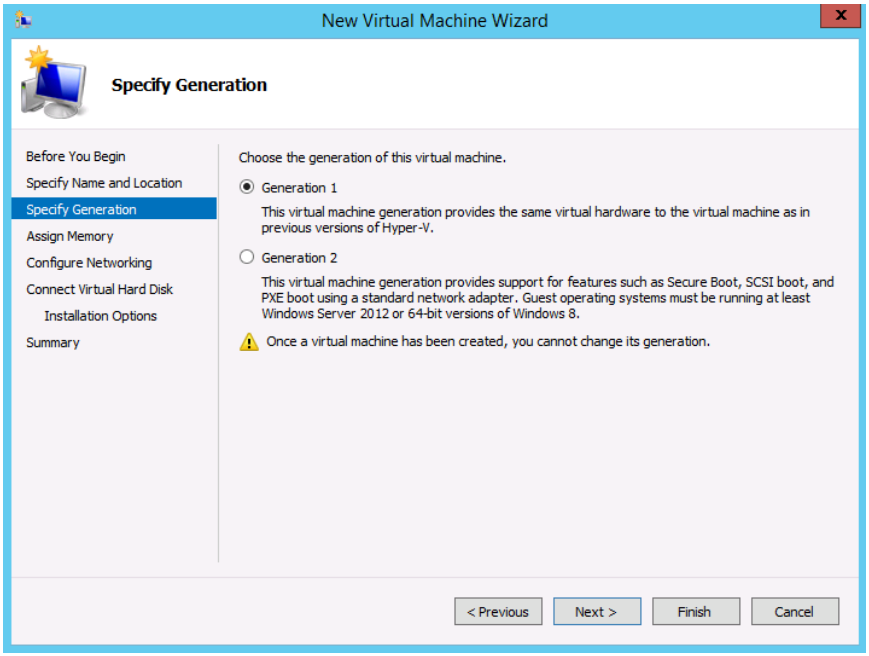


FIGURE C-8. Specify Generation

5. Select **Generation 1** and click **Next**.

The **Assign Memory** screen appears.

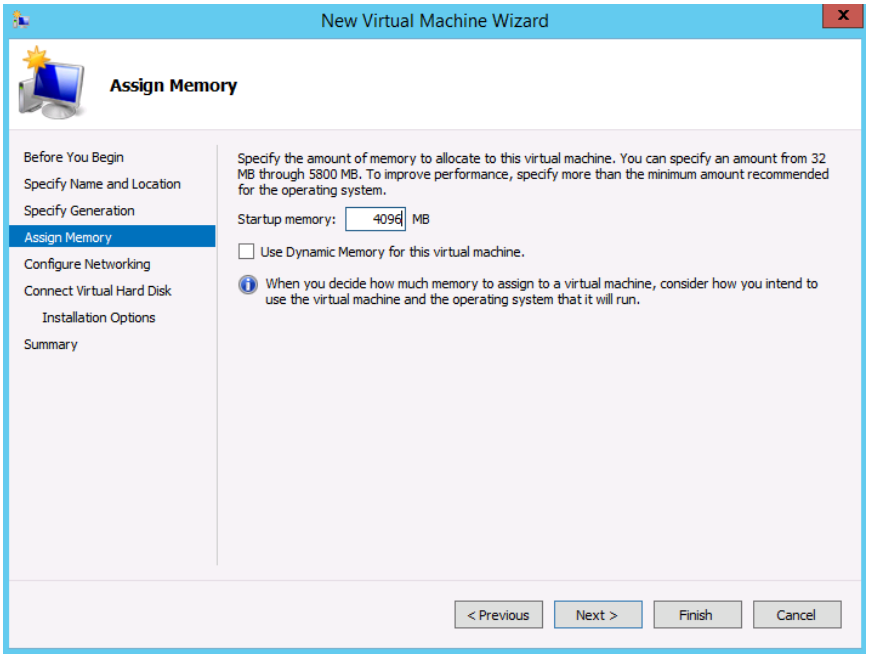


FIGURE C-9. Assign Memory

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

Tip

Trend Micro recommends allocating 8192MB of RAM.

The maximum number of virtual processors allowed on Windows 2008 R2 Hyper-V is 4. To add more than four core CPUs and more than 4096MB memory, set `numa=off` on Hyper-V and IMSVA.

7. Click **Next**.

The **Configure Networking** screen appears.

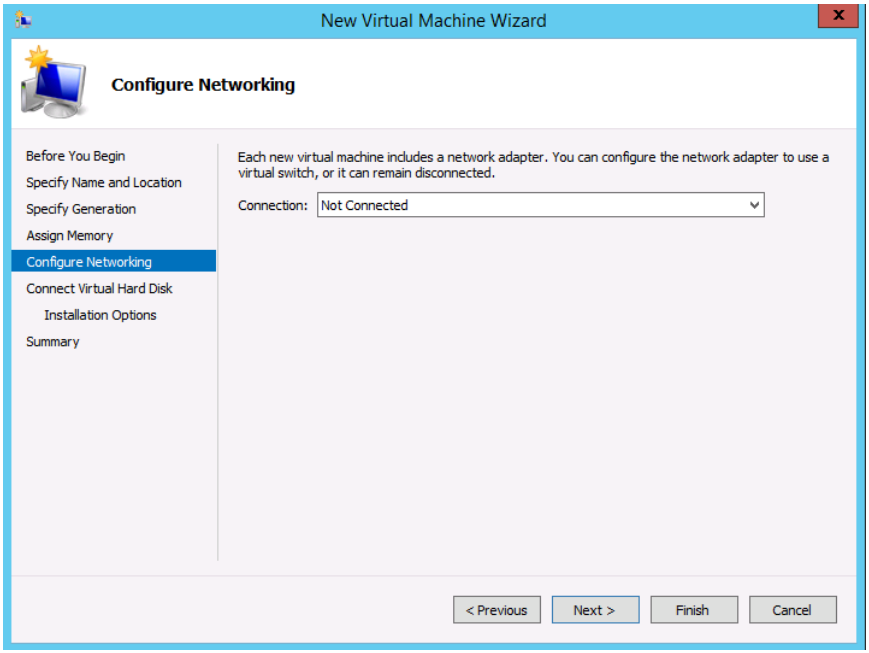


FIGURE C-10. Configure Networking

8. Select the virtual network created in *Creating a Virtual Network Assignment on page C-2*.

9. Click **Next**.

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

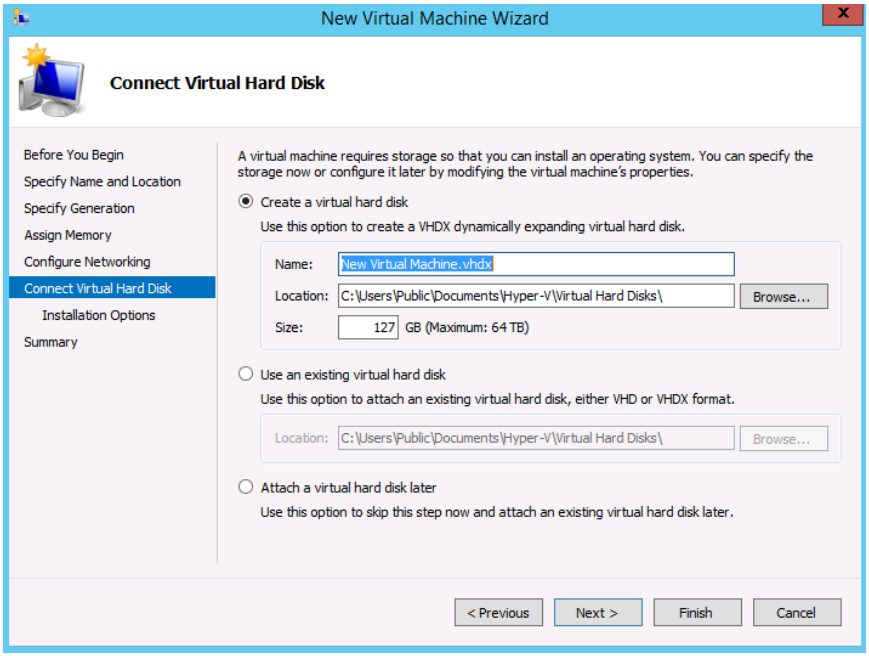


FIGURE C-11. Connect the Virtual Hard Disk

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

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

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

The **Installation Options** screen appears.

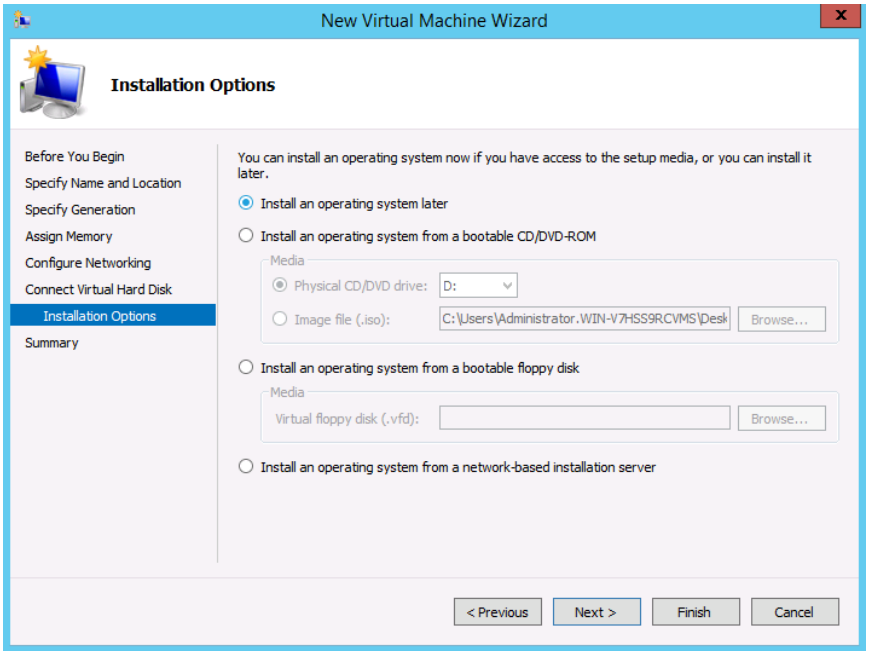


FIGURE C-12. Installation Options

12. Click **Install an operating system from a boot CD/DVD-ROM**, specify the installation ISO file for IMSVA, and then click **Next**.

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

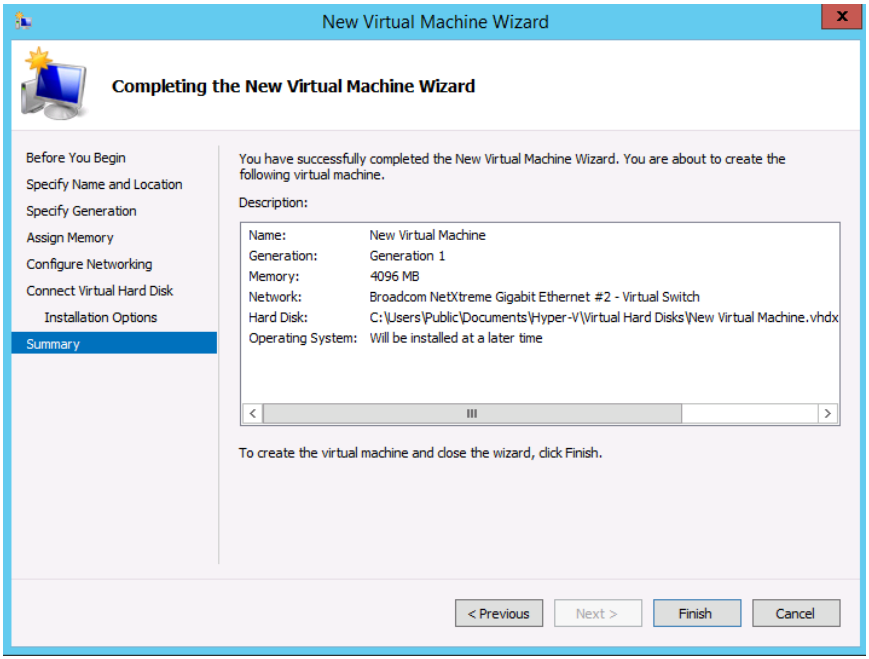


FIGURE C-13. Completing the New Virtual Machine Wizard

13. Verify your settings and click **Finish**.

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

Index

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: MSEM97320/160201