



InterScan™ Messaging Security Virtual Appliance⁷

Comprehensive Email Protection at the Gateway

Administrator's Guide



Messaging Security

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

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

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

Copyright© 2008 Trend Micro, Incorporated. All rights reserved.

Document Part No. MSEM73780/80804

Release Date: September 2008

Patents Pending

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

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

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

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

Contents

Preface

InterScan™ Messaging Security Virtual Appliance Documentation	x
Audience	x
Document Conventions	xi

Chapter 1: Getting Started

Opening the IMSVA Web Management Console	1-2
Using the Online Help	1-3
Viewing the Web Management Console Using Secure Socket Layer	1-3
Creating an SSL certificate	1-3
Performing Basic Configuration with the Configuration Wizard	1-5
Accessing the Configuration Wizard	1-5
Setting Up a Child Device	1-17
IMSVa Services	1-19
Starting or Stopping Services	1-21

Chapter 2: Configuring IMSVA Settings

IP Filtering Service	2-2
Using Network Reputation Services	2-2
Using the SPS Activation Code	2-2
Preparing Your Message Transfer Agent for Use With Network Reputation Services	2-3
Using the NRS Management Console	2-4
Configuring IP Filtering	2-5
Step 1: Enabling NRS and IP Profiler	2-5
Step 2: Enabling IP Profiler Rules	2-6
Step 3: Configuring NRS	2-14
Step 4: Adding IP Addresses to the Approved List	2-15
Step 5: Adding IP Addresses to the Blocked List	2-16
Displaying Suspicious IP Addresses and Domains	2-18
Scanning SMTP Messages	2-19
Configuring SMTP Routing	2-19

Configuring SMTP Settings	2-19
Configuring Connections Settings	2-20
Configuring Message Rule Settings	2-22
Configuring Domain-based Delivery Settings	2-25
Scanning POP3 Messages	2-27
Understanding POP3 Scanning	2-27
Requirements	2-28
Enabling POP3 Scanning	2-28
Configuring POP3 Settings	2-29
Managing Policies	2-30
How the Policy Manager Works	2-31
Understanding Address Groups	2-33
Managing Address Groups	2-34
Adding an Address Group	2-34
Editing or Deleting an Address Group	2-36
Searching for an LDAP User or Group	2-38
Configuring Internal Addresses	2-40
Adding Policies	2-42
Specifying a Route	2-42
Configuring the Route	2-45
Configuring Exceptions for Routes	2-47
Specifying Scanning Conditions	2-47
Selecting Scanning Conditions for Spam	2-52
Configuring Approved and Blocked Sender Lists	2-54
Configuring Spam Text Exemption Rules	2-55
Selecting Scanning Conditions for Attachments	2-56
Selecting Scanning Conditions for Message Size	2-58
Managing Expression Lists	2-58
Configuring an Expression	2-59
Specifying Actions	2-60
Creating a Tag Subject	2-65
Finalizing a Policy	2-66
Policy Example 1	2-68
Policy Example 2	2-72
Using the Asterisk Wildcard	2-76
Setting Scan Exceptions	2-77
Configuring Exceptions for Security Settings Violations	2-78

Setting Scan Actions for Security Setting Violations	2-78
Setting Scan Actions for Encrypted Messages	2-79
Setting Scan Actions for Password Protected Zip Files	2-80
Setting Scan Actions for Other Scanning Exceptions	2-82
Managing the Notifications List	2-83
Adding or Modifying a Policy Notification	2-83
Updating Scan Engine and Pattern Files	2-85
Specifying an Update Source	2-85
Performing a Manual Update	2-86
Rolling Back a Component Update	2-87
Configuring Scheduled Update	2-88
Updating the System and Application Files	2-90
Configuring Log Settings	2-91

Chapter 3: Backing Up, Restoring, and Replicating Settings

Import/Export Notes	3-2
Backing Up IMSVA	3-3
Restoring IMSVA	3-4
Settings That Cannot Be Restored	3-5
Replicating Settings	3-5
Enabling Control Manager Agent	3-5
Replicating Settings from Control Manager	3-6

Chapter 4: Maintenance

Monitoring Your Network	4-2
Viewing the Real-time Statistics	4-2
Interpreting the Real-time Statistics	4-3
System Overview	4-3
IMSVa Scan Performance	4-5
Viewing System Summary Statistics	4-6
IP Filtering Performance	4-8
Generating Reports	4-10
Types of Report Content	4-10
Managing One-time Reports	4-11
Adding One-time Reports	4-12
Using Scheduled Reports	4-15
Configuring Scheduled Reports	4-15

Logs	4-18
Querying Logs	4-18
Configuring Log Settings	4-24
Quarantine and Archive	4-26
Configuring Quarantine and Archive Settings	4-26
Managing Quarantine Areas	4-27
Querying Messages	4-29
Viewing a Quarantined Message	4-34
Viewing Archived Messages	4-35
Viewing Postponed Messages	4-36
Viewing Deferred Messages	4-36
Configuring User Quarantine Access	4-38
Using EUQ	4-39
Event Notifications	4-41
Configuring Delivery Settings	4-42
Configuring Event Criteria and Notification Message	4-44
Configuring Web EUQ Digest Settings	4-46
Editing Notifications	4-47
Configuring NTP Settings	4-47
Configuring Database Maintenance Schedule	4-48
Managing Administrator Accounts	4-49
Adding Administrator Accounts	4-49
Editing or Deleting Administrator Accounts	4-51
Configuring Connection Settings	4-53
Configuring LDAP Settings	4-53
Configuring POP3 Settings	4-56
Configuring TMCM Settings	4-58
Configuring Child IP Settings	4-59
Changing the Web Console Password	4-59
Managing Product Licenses	4-60
Viewing Your Product Licenses	4-60
Renewing or Activating a License	4-61
Activating Products	4-62

Chapter 5: Using End User Quarantine

About EUQ	5-2
Step 1: Configuring and Enabling LDAP	5-2

Step 2: Enabling EUQ	5-5
Step 3: Starting the EUQ Service	5-7
Step 4: Enabling End-User Access	5-8
Step 5: Opening the End-User Quarantine Console	5-10
Logon Name Format	5-10
Disabling EUQ	5-11

Chapter 6: Using the Command Line Interface

Using the CLI	6-2
Entering the CLI	6-2
CLI Overview	6-3
Entering the OS Shell	6-3
Command Line Interface Commands	6-4
configure adminUI disable	6-4
configure adminUI enable	6-5
configure adminUI enable all	6-5
configure date	6-6
configure dns	6-6
configure hostname	6-7
configure interface	6-7
configure password enable	6-8
configure role change-parent	6-8
configure role unregister	6-9
configure route add	6-9
configure route default	6-10
configure route del	6-10
configure ssh disable	6-11
configure ssh enable	6-11
configure ssh enable all	6-12
configure timezone	6-12
enable	6-13
exit	6-13
help	6-14
history	6-14
logout	6-15
ping	6-15
postfix drop	6-16

postfix flush	6-16
postfix queue	6-17
postfix start	6-17
postfix stop	6-18
reboot	6-18
rescue	6-19
resolve	6-19
service	6-20
show arp	6-21
show connections	6-21
show date	6-22
show disk partition	6-22
show firewall	6-23
show hostname	6-23
show ip dns	6-24
show ip interface	6-24
show ip route	6-25
show kernel	6-25
show log	6-26
show ntp	6-26
show open-ports	6-27
show process	6-27
show role	6-28
show statistics	6-28
show status	6-29
show timezone	6-29
show uptime	6-30
show version	6-30
shutdown	6-31
stop process	6-31
traceroute	6-32

Chapter 7: Modifying IMSVA Deployment

Internal Communication Port	7-2
Adding and Removing Devices	7-3
Adding a Child Device to a Group	7-3
Removing a Child Device from a Group	7-3
Resetting Child Devices When the Parent-Child Connection is Broken	7-4
Changing Device Roles	7-4
Changing the Device Role from Parent to Child	7-4
Changing the Device Role from Child to Parent	7-5
Changing the Deployment	7-5
Changing the Deployment from Gateway to Non-Gateway	7-5
Changing the Deployment from Non-Gateway to Gateway	7-6
Changing IP Addresses	7-7
Changing the Parent's Internal Communication Port IP Address	7-7
Changing the Child Internal Communication Port IP Address	7-7

Chapter 8: Updating and Rescuing the System and Application

Updating the System and Application	8-2
Rescuing IMSVA	8-4
Application Rescue Overview	8-4
Rescuing the Application	8-4

Chapter 9: Troubleshooting, FAQ, and Support

Troubleshooting	9-2
IMSVa Ports	9-11
Frequently Asked Questions	9-14
Postfix MTA Settings	9-14
Network Reputation Services	9-15
IP Profiler	9-15
Quarantine and Archive	9-16
End-User Quarantine	9-17
Transport Layer Security (TLS)	9-18
Spam Protection Service	9-19
ActiveUpdate	9-19

Others	9-19
Using the Knowledge Base	9-22
Contacting Support	9-22
TrendLabs	9-23
Security Information Center	9-23
Staying Up to Date	9-24
Send Trend Micro Your Viruses	9-24

Appendix A: IMSVA Scripts

Using IMSVA Scripts	A-2

Appendix B: Default Directory Locations

Default Mail Queues	B-2
eManager, Virus and Program Logs	B-3
Temporary Folder	B-3
Notification Pickup Folder	B-4

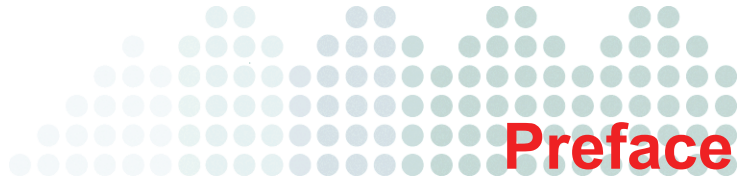
Chapter C: Transport Layer Security

How Transport Layer Security Works	C-2
Transport Layer Security Related Terms	C-2
Prerequisites to Using Transport Layer Security with IMSVA	C-3
Configuring Transport Layer Security Settings	C-4
Scenario on Configuring Site-Specific TLS Settings	C-4
Incoming Transport Layer Security Levels	C-6
Scenario on Configuring Incoming Transport Layer Security Settings	C-6
Outgoing Transport Layer Security Levels	C-7
Scenario on Configuring Outgoing Transport Layer Security Settings	C-7

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

Creating a New Virtual Machine	D-2

Index



Preface

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

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

This preface discusses the following topics:

- [InterScan™ Messaging Security Virtual Appliance Documentation on page x](#)
- [Audience on page x](#)
- [Document Conventions on page xi](#)

InterScan™ Messaging Security Virtual Appliance Documentation

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

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

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

Audience

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

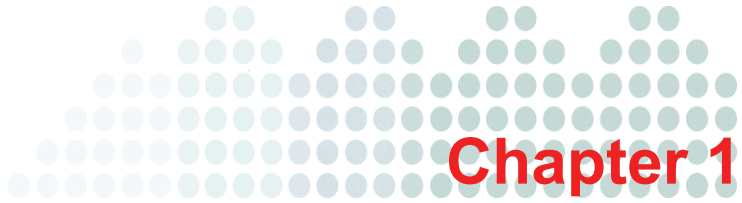
- SMTP and POP3 protocols
- Message transfer agents (MTAs), such as Postfix or Microsoft Exchange
- LDAP
- Database management

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

Document Conventions

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

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



Getting Started

This chapter explains how to log on to the Web management console and provides instructions on what to do immediately after installation to get IMSVA 7.0 up and running.

Topics include:

- [Opening the IMSVA Web Management Console on page 1-2](#)
- [Viewing the Web Management Console Using Secure Socket Layer on page 1-3](#)
- [Performing Basic Configuration with the Configuration Wizard on page 1-5](#)
- [IMSVA Services on page 1-19](#)

Opening the IMSVA Web Management Console

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

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

- `https://<target server IP address>:8445`

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

The default logon credentials are as follows:

- Administrator user name: **admin**
- Password: **<specified by user on installation>**

Type the log on credentials the first time you open the management console and click the **Enter** button.

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

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

Using the Online Help

The IMSVA Web management console comes with an Online Help that provides a description of each field on the user interface.

To access page-specific Online Help from the IMSVA Web management console, click the Help  icon located at the top right corner of the page.

To access the *table of contents* for the Online Help, click the Help  icon next to the **Log Off** hyperlink on the right of the page header.

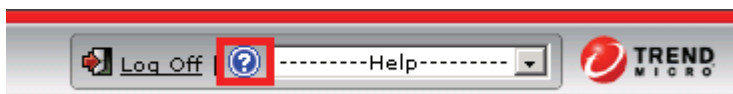


FIGURE 1-1 Table of Contents Access for Online Help

Viewing the Web Management Console Using Secure Socket Layer

The IMSVA Web management console supports encrypted communication, using SSL. After installing IMSVA, SSL communication should work because the installation contains a default certificate. Trend Micro suggests creating your own certificate to increase security.

If you want to use your own certificate, replace the following:

```
/opt/trend/imss/UI/tomcat/sslkey/.keystore
```

Creating an SSL certificate

Do the following:

1. Create the Tomcat SSL certificate as follows:

```
keytool -genkey -alias tomcat -keyalg RSA -keystore  

\opt\trend\imss\UI\tomcat\sslkey\keystore
```

For more details on SSL configuration in Tomcat, please visit:
<http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>
2. Create the Apache SSL certificate as follows:

- a. Generate a Private Key and Certificate Signing Request (CSR)

```
openssl req -new > new.cert.csr
```

- b. Remove pass-phrase from the key

```
openssl rsa -in privkey.pem -out new.cert.key
```

- c. Generate a Self-Signed Certificate

```
openssl x509 -in new.cert.csr -out new.cert.cert -req  
-signkey new.cert.key -days 1825
```

- d. Copy the certificate and key to the Apache path

```
cp new.cert.cert  
/opt/trend/imss/UI/apache/conf/ssl.crt/server.crt  
cp new.cert.key  
/opt/trend/imss/UI/apache/conf/ssl.key/server.key
```

Performing Basic Configuration with the Configuration Wizard

IMSVa provides a configuration wizard to help you configure the basic settings required to get IMSVa up and running.

The configuration wizard guides you through steps of configuring the following settings:

- Step 1: Configuring System Settings
- Step 2: Configuring Deployment Settings
- Step 3: Configuring SMTP Routing
- Step 4: Configuring Notification Settings
- Step 5: Configuring the Update Source
- Step 6: Configuring LDAP Settings
- Step 7: Configuring Internal Addresses
- Step 8: Configuring Control Manager Server Settings
- Step 9: Activating the Product
- Step 10: Verifying Settings Summary

Accessing the Configuration Wizard

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

1. On the management computer, open Internet Explorer (version 6.0 or later) or Firefox (version 2.0 or later).
2. Type the following URL (accept the security certificate if necessary):

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

The Log On screen appears.

3. Select the **Open Configuration Wizard** check box.
4. Type the following default user name and password:
 - User name: **admin**

- Password: **<specified by user on installation>**

The Configuration Wizard screen appears.



Step 1: Configuring System Settings

1. Click **Next**. The Local System Settings screen appears.

Configuration Wizard
 Step 1 of 10

Local System Settings

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

Network Settings

Network interface configuration

Device name	IP address	Netmask
eth0		

Internal Communication Port

Device name:

Network subsystem configuration

Host name: *
 Default gateway: *
 Primary DNS server: *
 Secondary DNS server:

System Time

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

Local Time Zone: *

Continent

Country/Region

Province/City

Date and time: *

mm/dd/yyyy

hh:mm:ss

< Back
Skip
Next >

2. Modify the device host name, internal communication port, IP address, and netmask if necessary. Also, configure your network settings and set the device system time.

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

Step 2: Configuring Deployment Settings

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

Configuration Wizard
Step 2 of 10

Deployment Settings ?

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

imsa.example.com deployment type:

☒ **Parent Device**

Import Settings...

☒ Gateway deployment
(To use IP Filtering, you must deploy IMSA at the gateway.)

☐ Enable End-User Quarantine
(Quarantine all spam and allow your users to access their spam through a Web console.)

☐ Automatically synchronize system time with NTP server:

☐ **Child Device**

Register to parent device IP address:

< Back Next >

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

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

Also, decide if you want to use EUQ or NTP services.

Step 3: Configuring SMTP Routing

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

Configuration Wizard
Step 3 of 10

SMTP Routing Settings

IMSA will use these settings for **Domain-based delivery** and **Relay Domains**.

Relay Domains

Mails can be delivered from any host to the following domains. We suggest adding all mail servers to your intranet.

Add Domain

For example: example.com (includes all sub-domains)

>>
<<

Domain Based Delivery

0-0 of 0

Page 1

Domain	Delivery Method

15 per page

- Specify the SMTP root domain and default delivery method.

Step 4: Configuring Notification Settings

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

1-9

Configuration Wizard
 Step 4 of 10

Notification Settings

Configure email and SNMP trap notifications for **default system notifications**.

Email Settings

To address(es):*		Use a semicolon ";" to separate multiple addresses
Sender's email address:*	postmaster@imsa.trendmicro.com	
Server name or IP address:*		
SMTP server port:*		
Preferred charset:*	English (us-ascii)	
Message header:		
Message footer:		

SNMP Trap

Server name (IP or FQDN):	
Community:	public

2. Configure the following notification settings, which IMSVA will use for all default system and policy event notifications:
 - **Email Settings**—Type the sender and receiver addresses, the name of the server that IMSVA delivers mail to, the SMTP server port, the language character set, and any additional headers or footers to add to the message.
 - **SNMP Trap**—If you have an SNMP server on your network, type the server name and the community name.

Step 5: Configuring the Update Source

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

Configuration Wizard
Step 5 of 10

Update Source ?

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

Source

☒ Trend Micro ActiveUpdate server

☐ Other Internet source

http://

Proxy Settings

☐ Use a proxy server for pattern, engine, and license updates

Proxy type:* HTTP

Proxy server:*

Port:*

User name:

Password:

< Back Skip Next >

2. Configure the following update settings, which will determine from where IMSVA will receive its component updates and through which proxy (if any) IMSVA needs to connect to access the Internet:
 - **Source:** Click **Trend Micro ActiveUpdate (AU) server** to receive updates directly from Trend Micro. Alternatively, click **Other Internet source** and type the URL of the update source that will check the Trend Micro AU server for updates. You can specify an update source of your choice or type the URL of your Control Manager server, if applicable.
 - **Proxy Settings:** Select the **Use proxy server** check box and configure the proxy type, server name, port, user name, and passwords.

Step 6: Configuring LDAP Settings

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

Configuration Wizard
 Step 6 of 10

?

LDAP Settings

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

LDAP Settings

LDAP server type:* Microsoft Active Directory

☐ Enable **LDAP1**

LDAP server:*
 Example: example.com or 123.123.123.123

Listening port number:* 389

☐ Enable **LDAP2**

LDAP server:*
 Example: example.com or 123.123.123.123

Listening port number:* 389

LDAP cache expiration for policy services and EUQ services

Time to Live in minutes:* 1440

LDAP admin

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

Password:*

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

Authentication method:* ☒ Simple
☐ Advanced: using Kerberos authentication for Active Directory

Kerberos authentication default realm:

Default domain:

KDC and admin server:

KDC port number:

< Back
Skip
Next >

2. Complete the following to enable LDAP settings:
 - a. For **LDAP server type**, select one of the following:
 - **Microsoft Active Directory**

- **Domino**
 - **Sun iPlanet Directory**
- b. To enable one or both LDAP servers, select the check boxes next to **Enable LDAP 1** or **Enable LDAP 2**.
 - c. Type the names of the LDAP servers and the port numbers they listen on.
 - d. Under **LDAP Cache Expiration for Policy Services and EUQ services**, type a number that represents the time to live next to the **TTL in minutes** field.
 - e. Under **LDAP Admin**, type the administrator account, its corresponding password, and the base-distinguished name. See [Table 1-1](#) for a guide on what to specify for the LDAP admin settings.

LDAP SERVER	LDAP ADMIN ACCOUNT (EXAMPLES)	BASE DISTINGUISHED NAME (EXAMPLES)	AUTHENTICATION METHOD
Active Directory	• Without Kerberos: user1@imsstest.com (UPN) or imsstest\user1 • With Kerberos: user1@imsstest.com	dc=imsstest, dc=com	• Simple • Advanced (with Kerberos)
Domino	user1/imsstest	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=imsstest, dc=com	dc=imsstest, dc=com	Simple

TABLE 1-1. LDAP admin settings

- f. For **Authentication method**, click **Simple** or **Advanced** authentication. For Active Directory advanced authentication, configure the Kerberos authentication default realm, Default domain, KDC and admin server, and KDC port number.

Note: Specify LDAP settings only if you will use LDAP for user-group definition, administrator privileges, or Web quarantine authentication. You must enable LDAP to use End-User Quarantine.

Step 7: Configuring Internal Addresses

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

Configuration Wizard
Step 7 of 10

Internal Addresses

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

Internal domains and usergroups

Enter domain

(For example: domain_name or domain_name.com)

Selected	
b.com	X

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 usergroups, 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

1. Click **Next**. The **TCMC Server Settings** screen appears.

Configuration Wizard
Step 8 of 10

TCMC Server Settings

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

TCMC Server Settings

To manage IMSA with Control Manager, enable the TCMC agent and configure all TCMC server settings.

☐ Enable TCMC Agent

Server:*

Communication protocol:*

☒ HTTP Port: 80

☐ HTTPS Port: 443

Web server authentication:

User name: ⓘ

Password: *

☐ Enable proxy

Proxy type:*

HTTP

Proxy server:*

Port:*

User name:

Password:

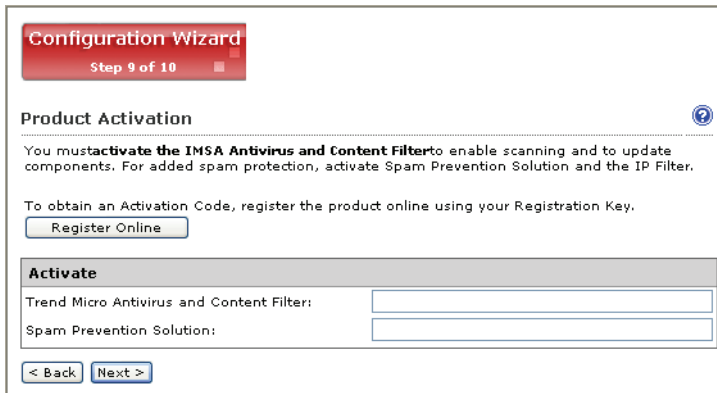
< Back Skip Next >

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

1. Click **Next**. The **Product Activation** screen appears. You must activate the Antivirus and Content Filter to enable scanning and security updates. To obtain an Activation Code, register the product online using the supplied Registration Key.



The screenshot shows the 'Configuration Wizard' window at 'Step 9 of 10'. The title bar is red with the text 'Configuration Wizard' and 'Step 9 of 10'. The main content area is titled 'Product Activation' and includes a help icon. The text reads: 'You must activate the IMSA Antivirus and Content Filter to enable scanning and to update components. For added spam protection, activate Spam Prevention Solution and the IP Filter. To obtain an Activation Code, register the product online using your Registration Key.' Below this is a 'Register Online' button. A section titled 'Activate' contains two input fields: 'Trend Micro Antivirus and Content Filter:' and 'Spam Prevention Solution:'. At the bottom are '< Back' and 'Next >' buttons.

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

Step 10: Verifying Settings Summary

1. Click **Next**. A **Review Settings** screen appears.

Configuration Wizard
Step 10 of 10

Review Settings

You have **finished configuring** the central controller on **imsa.example.com**

Review your settings and click Finish to save and apply them or click Back to make changes.

New Setting:

1. Deployment Settings:

Gateway deployment:	yes
Enable End-User Quarantine:	no
Automatically synchronize system time with NTP server:	no
NTP server address:	

2. Notification Settings

< Back Finish

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.

Setting Up a Child Device

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

To set up a child device:

1. Determine the Internal Communication Port IP address of the child device.

WARNING! Parent and child devices must use their Internal Communication Port to communicate each other. If your parent device or your child devices have multiple network interface cards (NIC), add a host-route entry by Command Line Interface (CLI) following the instructions below.

On the parent device in the CLI:

configure route add <IP address of child device's Internal Communication Port>/32 <next hop> <Internal Communication Port of parent device>

On the child device in the CLI:

configure route add <IP address of parent device's Internal Communication Port >/32 <next hop> <Internal Communication Port of child device>

2. On the **parent** device, do the following:
 - a. After you set up a parent device (see [Viewing the Web Management Console Using Secure Socket Layer on page 1-3](#)), make sure the parent device is operational.
 - b. Log on to the Web console. Make sure that you are logging on the parent device Web console.
 - c. Choose **Administration > IMSVA Configuration > Connections > Child IP**.
 - d. Under **Add IP Address**, add the IP address of the child device.
3. On the **child** device, do the following:
 - e. Just as you did for the parent device, connect a management computer to the child device and log on to the Web console. All IMSVA devices have the same default IP addresses and Web console logon credentials.
 - f. In the Setup Wizard, configure the local system settings and then click **Next>**.
 - g. On the Deployment Settings screen, select **Child Server** and add the Parent device IP address.

- h. Click **Finish**.
4. On the **parent** device, do the following:
 - i. Choose **Summary > System** from the menu.
 - j. 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:
 - k. On the **parent** device, choose **Administration > End-User Quarantine**.
 - l. Choose **Redistribute all** or **Only redistribute to approved senders**. Trend Micro recommends choosing **Redistribute all**.
 - m. 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.

IMSVA Services

The scanner and policy services must be started in order to start protecting your network using IMSVA. You can however, choose whether to install or start the EUQ service.

- **Scanner Services**—Performs scanning of SMTP/POP3 traffic.

- **Policy Services**—Acts as a remote store of rules for the scanner services to enhance rule lookups.
- **EUQ Services**—Hosts a Web-based console to enable end-users to view, delete and release spam messages addressed to them.

For more information on these services, refer to the IMSVA Installation Guide.

Starting or Stopping Services

After you have successfully installed IMSVA and configured the various settings, you have to start the services to begin scanning for malware and other threats. Likewise, you may need to stop IMSVA services prior to performing an upgrade or backup function.

1. Choose **Summary** from the menu. The Real-time Statistics tab appears with the default System tab selected.

Summary 

 **Maintenance for Trend Micro Antivirus and Content Filter will expire in 29 day(s).**
Renewal is necessary to keep your security and product updates current. [More info](#)

 **Maintenance for Spam Prevention Solution (SPS) will expire in 29 day(s).**
Renewal is necessary to keep your security and product updates current. [More info](#)

Real-time Statistics **System**

Enable Connections

☐ Accept POP3 connections ☒ Enable IP Filtering
... ☒ NRS ☒ IP Profiler

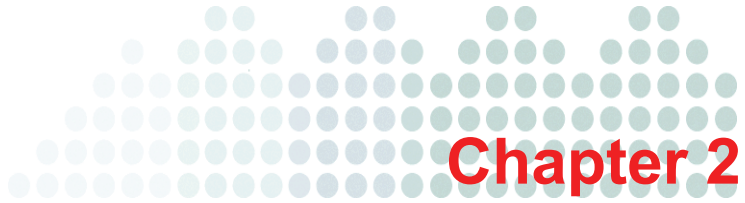
Components Last refresh: Dec 3, 2007 8:35:03 PM  Refresh

☐	Name	Current Version	Availability	Update Schedule
☐	Scan engine	8.500.1001	8.500.1001	15 minutes
☐	Virus pattern	4.857.00	4.857.00	15 minutes
☐	Spyware/grayware pattern	0.557.00	0.557.00	15 minutes
☐	IntelliTrap pattern IntelliTrap exceptions	0.107.00 0.257.00	0.107.00 0.257.00	15 minutes
☐	Anti-spam engine	5.0.1023	5.0.1023	15 minutes
☐	Spam pattern	15582.003	15582.003	15 minutes

Managed Services

Hostname	Connection	Scanner Service	Policy Service	EUQ Service
rd.imsa		 Stop	 Stop	disabled

2. Click the **System** tab.
3. Under the Managed Services section, click the **Start** or **Stop** button for the service(s) that you would like to start or stop.



Configuring IMSVA Settings

This chapter provides general descriptions on the various configuration tasks that you need to perform to get IMSVA up and running. For more details, please refer to the Online Help accessible from the Web management console.

- [IP Filtering Service on page 2-2](#)
- [Scanning SMTP Messages on page 2-19](#)
- [Scanning POP3 Messages on page 2-27](#)
- [Managing Policies on page 2-30](#)
- [Updating Scan Engine and Pattern Files on page 2-85](#)
- [Configuring Log Settings on page 2-91](#)

IP Filtering Service

The IP Filtering service has two individual components: Network Reputation Service and IP Profiler.

- Network Reputation Service filters spam senders at the connection layer.
- IP Profiler helps protect the mail server from attacks with smart profiles (SMTP Intrusion Detection Service (IDS)).

Tip: Trend Micro recommends deploying IP Filtering as the first line of defense in your messaging infrastructure.

Although most email messaging systems have a multi-layer structure that often includes some pre-existing IP blocking, spam filtering, and virus filtering, Trend Micro recommends completely removing other IP blocking techniques from the messaging environment. IP Filtering should act as the precursor to any application filtering you might use.

Using Network Reputation Services

Trend Micro maintains a list of IP addresses belonging to known spam senders in a central database. Network Reputation Services (NRS) filters spam by blocking the IP addresses stored in this database.

Using the SPS Activation Code

IP Filtering Service, which includes NRS and IP Profiler, uses the same license as Spam Prevention Solution (SPS). If you purchase the full SPS service package, you will receive a registration key that will allow you to create a customer account with Trend Micro and upon completion of the registration process, you will receive your Activation Code.

The Activation Code enables you to access the level of services according to your registration. When you activate SPS, the licensing information for IP Filtering will then appear.

For details on configuring NRS, see [Configuring IP Filtering on page 2-5](#).

Preparing Your Message Transfer Agent for Use With Network Reputation Services

To prepare your MTA for use with NRS:

- **RBL+ Service**—Configure the MTA to reject connections that have a **550** level error code (connection refused). This error code indicates that a positive response was received from the RBL+ database. Listings in the RBL+ database are known to be spammers or sources that should not be sending email. Therefore, the standard method for handling these spammers is to reject the connections outright.

For more information, see the following URL:

www.trendmicro.com/en/products/nrs/rbl/use/configure.htm

- **Network Anti-Spam Service**—Configure your MTA to make 2 potential DNS queries, first to the QIL database and then to the RBL+ database.

The QIL (Quick IP Lookup) database is a real-time dynamic database that contains a list of suspicious IP addresses that are sending spam. These IP addresses will be removed from the QIL database once spam stops coming from these addresses. If the QIL database does not receive a positive response, the MTA will need to make a second query to the RBL+ database, which contains a more stable list of blacklisted IP addresses.

The MTA should temporarily deny connections that have a **450** level error code (server temporarily unavailable, please retry), when a positive response is received from the QIL database. The IP listings in this database are occasionally legitimate mail servers that may have compromised hosts behind them temporarily sending spam. If the connection request is from a legitimate mail server, it will re-queue and try sending the message at a later time. This will cause a short delay in mail delivery until the listing expires, but will not permanently block the mail.

For more information, see the following URL:

www.trendmicro.com/en/products/nrs/nas/use/configure.htm

Using the NRS Management Console

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

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

To use the NRS Management Console:

1. Open a Web browser and access the following address:
`https://nrs.nssg.trendmicro.com/`
2. Select **Global Spam Update** from the menu.
3. Click any of the following tabs:
 - **Spam Alert:** Provides a brief overview and discussion of current spamming tactics and the implications for organizations. It also describes how new tactics are deployed, how they evade Trend Micro systems, and what Trend Micro is doing to respond to these new threats.
 - **ISP Spam.x:** The total spam volume from the top 100 ISPs for a specific week. The networks that are producing the most spam are ranked at the top. The ranking of the ISP's will change on a daily basis.
4. To view reports that summarize the query activity between your MTA and the Network Reputation Services database servers, do the following:
 - a. Select **Report** from the menu.
 - b. Click **Percentage queries**, **Queries per hour**, or **Queries per day**.
5. To create or manage Approved Sender IP and Blocked Sender IP lists, choose **Policy** from the menu. You can define your Approved Senders by individual IP address and CIDR by Country, or by ISP.
6. To add an ISP to the list, choose **New ISP** from the menu.
To change your password or Activation Code, choose **Administration** from the menu.

Configuring IP Filtering

To completely configure IP Filtering, perform the following steps:

- Step 1:** Enable NRS and IP Profiler
- Step 2:** Enable IP Profiler Rules
- Step 3:** Configure NRS
- Step 4:** Add IP Addresses to the Approved List
- Step 5:** Add IP Addresses to the Blocked List

Step 1: Enabling NRS and IP Profiler

To enable NRS and IP Profiler:

1. Choose **IP Filtering > Overview** from the menu. The IP Filtering Overview screen appears.

IP Filtering Overview

☒ **Enable IP Filtering** ☐ NRS ☒ IP Profiler

Blocked Domains IP Addresses Last 1 day (Last 24 hours)

DHA Attack

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Bounced Mail

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Virus

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Spam

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

Manual

Domain	IP	Dropped Connections
No malicious domains or IP addresses have been found for the last 1 day(s).		

2. Select the **Enable IP Filtering** check box. This will select both the NRS and IP Profiler check boxes.
3. Clear the **NRS** or **IP Profiler** check box, if you do not require them.
4. Click **Save**.

Step 2: Enabling IP Profiler Rules

WARNING! Before enabling IP Profiler Rules, add all of your email servers' IP addresses (that send outgoing email messages to IMSVA) to the IP Filtering Approved List. To configure the IP Filtering Approved List, see [Step 4: Adding IP Addresses to the Approved List on page 2-15](#).

Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting. Rules can be set for the following:

- Spam
- Viruses
- DHS attacks
- Bounced mail.

Specify IP filtering Spam Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.

The screenshot displays the 'Rules: IP Profiling Settings (IP Behavior Monitor)' window. It features four tabs: Spam, Virus, DHS Attack, and Bounced Mail. The Spam tab is active, showing settings for enabling IP filtering, duration to monitor (20 hours), rate (80%), total mails (1000), and triggering action (Block temporarily). The Virus, DHS Attack, and Bounced Mail tabs are also visible, each with similar settings. The DHS Attack tab includes an additional 'Setting example' section with values for recipients and non-existing recipients. The Bounced Mail tab includes a 'non-existing recipients exceeds' field. Each tab has 'Save', 'Cancel', and 'Restore Defaults' buttons.

Rules: IP Profiling Settings (IP Behavior Monitor)

Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting.

Spam Virus DHS Attack Bounced Mail

☒ Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

Virus Spam DHS Attack Bounced Mail

☐ Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

DHS Attack Spam Virus Bounced Mail

☐ Enable

Setting example

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000 mails

sent to more than: 100 recipients

non-existing recipients exceeds: 0 recipients (if LDAP service is running)

Triggering action: Block temporarily

Save Cancel Restore Defaults

Bounced Mail Spam Virus DHS Attack

☐ Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

2. Click the **Spam** tab. The Spam screen appears.
3. Select the **Enable** check box, to enable blocking for spam.
4. Specify a value for the following:

- **Duration to monitor:** The number of hours that IMSVA monitors email traffic to see if the percentage of spam email messages exceeds the **Threshold** you set below.
- **Threshold:** The maximum percentage of spam email messages that IMSVA will allow during the value you set for **Duration to monitor** above. The threshold is a fraction with a numerator and denominator:
 - **Rate (%):** Type the maximum number of allowable email messages with spam threats (the numerator).
 - **Total mails:** Type the total number of spam email messages out of which the threshold percentage is calculated (the denominator).

Consider the following example. You configure the following:

Duration to monitor: 1 hour at a rate of 20 out of 100

During each one-hour period that spam blocking is active, IMSVA starts blocking IP addresses when more than 20% of the messages it receives contain spam and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
 - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.

6. Click **Save**.

Specify IP filtering Virus Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.

Rules: IP Profiling Settings (IP Behavior Monitor) ?

Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting.

Spam Virus DHA Attack Bounced Mail

☒ **Enable**

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

Spam **Virus** DHA Attack Bounced Mail

☐ **Enable**

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

Spam Virus **DHA Attack** Bounced Mail

☐ **Enable** [Setting example](#)

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000 mails

sent to more than: 100 recipients

non-existing recipients exceeds: 0 recipients (if LDAP service is running)

Triggering action: Block temporarily

Save Cancel Restore Defaults

Spam Virus DHA Attack **Bounced Mail**

☐ **Enable**

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

2. Click the **Virus** tab. The Virus screen appears.
3. Select the **Enable** check box, to enable blocking for virus threats.
4. Configure the following:
 - **Duration to monitor:** The number of hours that IMSVA monitors email traffic to see if the percentage of email messages with virus threats exceeds the Threshold you set below.
 - **Threshold:** The maximum percentage of email messages with virus threats that IMSVA will allow during the value you set for Duration to monitor above. The threshold is a fraction with a numerator and denominator:
 - **Rate (%):** Type the maximum number of allowable email messages with virus threats (the numerator).

- **Total mails:** Type the total number of virus email messages out of which the threshold percentage is calculated (the denominator).

Consider the following example. You configure the following:

Duration to monitor: 1 hour at a rate of 20 out of 100

During each one-hour period that virus blocking is active, IMSVA starts blocking IP addresses when more than 20% of the messages it receives contain virus threats and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
 - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

Specify Direct Harvest Attack (DHA) Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.

Rules: IP Profiling Settings (IP Behavior Monitor)

Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting.

Spam | Virus | DHA Attack | Bounced Mail

☒ Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

Spam | **Virus** | DHA Attack | Bounced Mail

☐ Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

Spam | Virus | **DHA Attack** | Bounced Mail

☐ Enable Setting example

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000 mails

sent to more than: 100 recipients

non-existing recipients exceeds: 0 recipients
(if LDAP service is running)

Triggering action: Block temporarily

Save Cancel Restore Defaults

Spam | Virus | DHA Attack | **Bounced Mail**

☐ Enable

Duration to monitor: 20 hour(s)

Rate (%): 80 %

Total mails: 1000

Triggering action: Block temporarily

Save Cancel Restore Defaults

2. Click the **DHA Attack** tab. The DHA Attack screen appears.
3. Select the **Enable** check box, to enable blocking for directory harvest attacks.
4. Configure the following:
 - **Duration to monitor:** The number of hours that IMSVA monitors email traffic to see if the percentage of email messages signalling a DHA attack exceeds the Threshold you set below.
 - **Threshold:** The maximum percentage of email messages signalling a DHA attack that IMSVA will allow during the value you set for Duration to monitor above. The threshold is a complex expression with the following:
 - **Rate (%):** Type the maximum number of allowable email messages with DHA threats (the numerator).

- **Total mails:** Type the total number of DHA email messages out of which the threshold percentage is calculated (the denominator).
- **Sent to more than:** Type the maximum number of recipients allowed for the threshold value.
- **Non-existing recipients exceeds:** Type the maximum number of nonexistent recipients allowed for the threshold value. DHA attacks often include randomly generated email addresses in the receiver list.

Note: The LDAP service must be running to determine non-existing recipients.

Consider the following example. You configure the following:

Duration to monitor: 1 hour at a rate of 20 out of 100 sent to more than 10 recipients when the number of non-existing recipients exceeds 5.

During each one-hour period that DHA blocking is active, IMSVA starts blocking IP addresses when it receives more than 20% of the messages that were sent to more than 10 recipients (with more than five of the recipients not in your organization) and the total number of messages exceeds 100.

Tip: Technically, the LDAP server is not a must-have. The DHA rule of IMSVA can also obtain the DHA results returned from Postfix, which in turn passes these results to FoxProxy through the LDAP server or other means. FoxProxy then analyzes the results to determine if they are DHA attacks.

LDAP server is only one of the means by which Postfix checks if a user's mailbox exists.

5. Next to **Triggering** action, select one of the following:
 - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

Specify Bounced Mail Settings:

1. Choose **IP Filtering > Rules** from the menu. The Rules screen appears with 4 tabs, one for each type of threat.

The figure displays three sequential screenshots of the 'Rules: IP Profiling Settings (IP Behavior Monitor)' configuration window, illustrating the process of configuring the Bounced Mail tab.

Top Screenshot (Spam tab selected): The window title is 'Rules: IP Profiling Settings (IP Behavior Monitor)'. Below the title bar, there is a description: 'Rules are set to monitor the behavior of all IP addresses and block them according to the threshold setting.' The 'Spam' tab is selected. The settings are: **Enable** (checked), **Duration to monitor:** 20 hour(s), **Rate (%):** 80 %, **Total mails:** 1000, and **Triggering action:** Block temporarily. Buttons at the bottom are Save, Cancel, and Restore Defaults.

Middle Screenshot (Virus tab selected): The 'Virus' tab is selected. The settings are: **Enable** (unchecked), **Duration to monitor:** 20 hour(s), **Rate (%):** 80 %, **Total mails:** 1000, and **Triggering action:** Block temporarily. Buttons at the bottom are Save, Cancel, and Restore Defaults.

Bottom Screenshot (DHA Attack tab selected): The 'DHA Attack' tab is selected. The settings are: **Enable** (unchecked), **Duration to monitor:** 20 hour(s), **Rate (%):** 80 %, **Total mails:** 1000 mails, **sent to more than:** 100 recipients, **non-existing recipients exceeds:** 0 recipients (if LDAP service is running), and **Triggering action:** Block temporarily. Buttons at the bottom are Save, Cancel, and Restore Defaults.

2. Click the **Bounced Mail** tab. The Bounced Mail screen appears.
3. Select the **Enable** check box, to enable blocking for bounced mail.
4. Configure the following:
 - **Duration to monitor:** The number of hours that IMSVA monitors email traffic to see if the percentage of email messages signalling bounced mail exceeds the Threshold you set below.
 - **Threshold:** The maximum percentage of email messages signalling bounced mail that IMSVA will allow during the value you set for Duration to monitor above. The threshold is a fraction with a numerator and denominator:

- **Rate (%):** Type the maximum number of allowable email messages signalling bounced mail (the numerator).
- **Total mails:** Type the total number of bounced email messages out of which the threshold percentage is calculated (the denominator).

Consider the following example. You configure the following:

Duration to monitor: 1 hour at a rate of 20 out of 100

During each one-hour period that blocking for bounced mail is active, IMSVA starts blocking IP addresses when more than 20% of the messages it receives signal bounced mail and the total number of messages exceeds 100.

5. Next to **Triggering action**, select one of the following:
 - **Block temporarily:** Block email messages from the IP address and allow the upstream MTA to try again.
 - **Block permanently:** Never allow another email message from the IP address and do not allow the upstream MTA to try again.
6. Click **Save**.

Step 3: Configuring NRS

To configure NRS:

1. Choose **IP Filtering > NRS** from the menu. The NRS screen appears.

NRS

Network Reputation System Setting

☒ Enable

☒ Default intelligent action

Permanent denial of connection (550) for RBL+ matches

Temporary denial of connection (450) for Zombie matches

☐ Take customized action for all matches

SMTP error code: 450

SMTP error string : (alphanumeric letters)

error message

Save Cancel

2. Select the **Enable** check box.
3. Click a radio button next to one of the following:

- **Default intelligent action**—NRS permanently denies connection (550) for RBL+ matches and temporarily denies connection (450) for Zombie matches.
- **Take customized action for all matches**
 - **SMTP error code**—Reject any connections that have a certain SMTP code. Type an SMTP code.
 - **SMTP error string**—Type the message associated with the SMTP error code.

Note: The above SMTP error code and error string will be sent to the upstream MTA that will then take the necessary preconfigured actions, such as record the error code and error string in a log file.

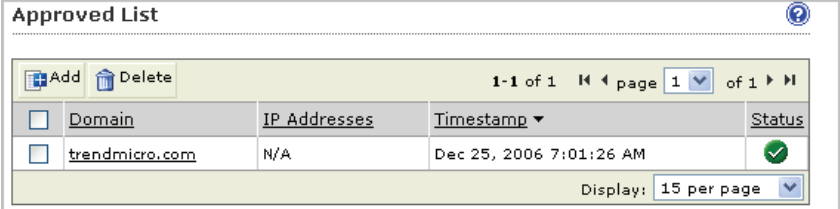
4. Click **Save**.

Step 4: Adding IP Addresses to the Approved List

IMSVA does not filter IP addresses or domains that appear in the Approved List.

To add an IP address to the approved list:

1. Choose **IP Filtering > Approved List** from the menu. The Approved List screen appears.



The screenshot shows the 'Approved List' interface. At the top, there are 'Add' and 'Delete' buttons. Below them is a table with the following data:

	Domain	IP Addresses	Timestamp	Status
☐	trendmicro.com	N/A	Dec 25, 2006 7:01:26 AM	✓

At the bottom right, there is a 'Display: 15 per page' dropdown menu. The top right corner of the interface has a help icon (question mark) and pagination information: '1-1 of 1' and 'page 1 of 1'.

2. Click **Add**. The Add IP/Domain to Approved List screen appears.

Add IP/Domain to Approved List 

☒ **Enable**

☒ Domain:

☐ IP Address:

3. Select the **Enable** check box.
4. Type the domain or IP address that you would like to add to the Approved List.
5. Click **Save**. The domain or IP address appears in the Approved List.

Step 5: Adding IP Addresses to the Blocked List

IMSVA blocks IP addresses that appear in the Blocked List.

To add an IP address to the Blocked List:

1. Choose **IP Filtering > Blocked List** from the menu. The Blocked List screen appears.

Blocked List 

 **Filtered by:**

1-1 of 1  page 1  of 1  

☐	Domain	IP Addresses	Type	Action	Timestamp ▼	Status
☐	trendmicro.com	N/A	manual	Block temporarily	Dec 25, 2006 6:59:54 AM	

15 per page 

2. Click **Add**. The Add IP/Domain to Blocked List screen appears.



The screenshot shows a dialog box titled "Add IP/Domain to Blocked List" with a help icon in the top right corner. Inside the dialog, there is a section with a checked "Enable" checkbox. Below it are two radio buttons: "Domain:" (selected) and "IP Address:". The "Domain:" field contains the text "abc.com". Below these is an "Action:" label followed by a dropdown menu currently set to "Block temporarily". At the bottom of the dialog are "Save" and "Cancel" buttons.

3. Select the **Enable** check box.
4. Type the domain or IP address.
5. Select **Block temporarily** or **Block permanently**.
6. Click **Save**. The domain or IP address is added to the blocked list.

Displaying Suspicious IP Addresses and Domains

IMSVa creates log entries of the IP addresses or domains that have sent email messages violating scanning conditions, but are still not blocked because the total number of messages did not exceed the threshold you set for the given time period.

To display suspicious IP addresses and domains:

1. Click **IP Filtering > Suspicious IP/Domain**.
2. Choose from any of the following conditions:
 - Next to **Type**, select the check boxes next to the type of threat that the IP filter detected.
 - Next to **Dates**, select the date time range within which IMSVa blocked the sender.
 - If you know a specific IP address to query, type it next to **IP**.
 - To display the corresponding domain names of the IP addresses, select the **Show Domain names** check box.
 - Next to **Logs per page**, select the number of log entries to display on the screen at one time.
3. Click **Display Log**.
4. Perform any of the additional actions:
 - To block an IP address temporarily, select the corresponding check box in the list, then click **Block Temporarily**.
 - To block an IP address permanently, select the corresponding check box in the list, then click **Block Permanently**.
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the top of the table.
 - To sort the table, click the column title.

Scanning SMTP Messages

Configuring SMTP Routing

Configuring SMTP routing involves the following four steps:

- Step 1:** Configure SMTP settings
- Step 2:** Configure Connections settings
- Step 3:** Configure Message Rule settings
- Step 4:** Configure Domain-based Delivery settings

Configuring SMTP Settings

Use the SMTP screen to configure SMTP settings for the MTA, such as the SMTP greeting message and the location of the mail processing queue, where IMSVA saves messages before it scans and delivers them.

1. Click **Administration > IMSVA Configuration > SMTP Routing**. The SMTP Routing screen appears.

The screenshot shows the 'SMTP Routing' configuration window. The 'SMTP' tab is active, displaying the 'Greeting Message' section. The text area for the greeting message contains 'ESMTP IMSA'. The 'Save' and 'Cancel' buttons are at the bottom.

2. Specify SMTP server **Greeting Message** (displays when a session is created).
3. Click **Save**.

Configuring Connections Settings

To specify the Connections settings:

1. Choose **Administration > IMSVA Configuration > SMTP Routing** from the menu.
2. Click the **Connections** tab. The Connections screen appears.

SMTP Routing

SMTP | **Connections** | Message Rule | Domain-based Delivery

SMTP Interface

Port:

Disconnect after: minutes of inactivity

Simultaneous connections: ☐ No limit ☒ Allow up to connections

Connection Control

You can either permit or deny computers to connect with the server.

☒ Accept all, except the following list

☐ Single computer

e.g., 123.123.123.123

☐ Group of computers

Subnet address >>>

e.g., 10.123.123.123

Subnet mask

e.g., 255.255.255.0

☐ Deny all, except the following list

Transport Layer Security Setting

☐ Enable Incoming Transport Layer Security

☐ Only accept SMTP connection by TLS

CA certificate:

Private key:

SMTP server certification:

☐ Enable Outgoing Transport Layer Security

3. Specify the **SMTP Interface** settings:
 - **Port:** Type the listening port of the SMTP server.
 - **Disconnect after { } minutes of inactivity:** Type a timeout value.
 - **Simultaneous connections:** Click **No limit** or **Allow up to { } connections** and type the maximum number of connections.
4. Specify the **Connection Control** settings:
 - **Accept all, except the following list:** Configure the list:
 - **Single computer:** Type an IP address, and then click >> to add it to the list.
 - **Group of computers:** Type a subnet address and mask, and then click >> to add the group to the list.
 - **Subnet mask:** Type a subnet mask.
 - **Import from file:** Click to import a deny list from a file. The following shows sample content of an IP list text file:


```
192.168.1.1
192.168.2.0:255.255.255.0
192.168.3.1:255.255.255.128
192.168.4.100
192.168.5.32:255.255.255.192
```
 - **Deny all, except the following list:** Configure the list.
5. Specify the **Transport Layer Security Settings**:
 - a. Select **Enable Incoming Transport Layer Security**.
This causes the IMSVA SMTP Server to provide TLS support to SMTP clients, but does not require that clients use TLS encryption to establish the connection.
 - b. Select **Only accept SMTP connection by TLS** for IMSVA to only accept secure incoming connections.
This causes the IMSVA SMTP Server to accept messages only through a TLS connection.
 - c. Click a **Browse** button next to one of the following:

- **CA certificate:** A CA certificate is usually used for verifying SMTP clients. However, IMSVA does not verify the client and only uses the CA certificate for enabling the TLS connection.

Only upload this file if it is provided to you together with the public key. Otherwise, this file is not mandatory for enabling a TLS connection.

- **Private key:** The SMTP client encrypts a random number using IMSVA SMTP server's public key and an encryption key to generate the session keys.

IMSVA SMTP server then uses the private key to decrypt the random number in order to establish the secure connection.

This key must be uploaded to enable a TLS connection.

- **SMTP server certification:** The IMSVA SMTP server's public key made available to the SMTP clients for generating the session keys.

This key must be uploaded to enable a TLS connection.

d. Click **Upload** to save the file on the IMSVA server.

e. Select **Enable Outgoing Transport Layer Security** to protect outbound messages, if desired.

6. Click **Save**.

Configuring Message Rule Settings

To set limits on the email messages that IMSVA can handle and to control email relay, configure all settings on the messages rules screen.

Email Relay

To prevent spammers from using the IMSVA MTA as a relay for spam, configure relay control. You will add the mail domains on your network to the Relay Domains list. When IMSVA receives an email message, it looks at the final destination of the email and compares it to this list. IMSVA discards the message under the following circumstances:

- The destination domain is not in this list
- The parent domain of the destination domain is not in this list
- The host is not on the **Permitted Senders of Relayed Mail** list

Relay domain settings are different from Domain-based delivery settings.

To specify the Message Rules:

1. Choose **Administration > IMSVA Configuration > SMTP Routing** from the menu.
2. Click the **Message Rule** tab. The Message Rule screen appears.

SMTP Routing ?

SMTP Connections **Message Rule** Domain-based Delivery

Message Limits

Type 0 to remove any limitations.

Maximum message size (1 to unlimited): MB

Maximum number of recipients (1 to unlimited):

Relay Control

☐ Reject unknown sender domains. i

☐ Reject unknown recipients. (by checking LDAP) i

☐ Reject unknown IP address. (Enabling this option might impact IMSA performance.) i

Relay Domains

Mail can be delivered from any host to the following domains. Typically, you add all the mail servers in your intranet.

Add Domain

>>

For example: example.com (includes all sub-domains)

<<

nj-jason-liu.com

Permitted Senders of Relayed Mail

The following hosts can relay mail to all domains and are excluded from the above relay restriction.

☐ Host only

☒ Same subnet as the host

☐ Same IP class as the host

☐ Specified IP addresses:

☒ **Single computer**

e.g., 123.123.123.123

☐ **Group of computers**

Subnet address >>

<<

e.g., 10.123.123.123

Subnet mask

e.g., 255.255.255.0

3. Specify the **Message Limits** settings:
 - **Maximum message size:** Type the number of megabytes.

- **Maximum number of recipients:** Type the number of recipients from 1 to unlimited.
4. Specify the **Relay Control** parameters to have IMSVA reject messages matching the selected condition.
 5. Specify the **Relay Domains**. IMSVA relays the messages to the listed domains.
 6. Specify the **Permitted Senders of Relayed Mail**.
 7. Click **Save**.

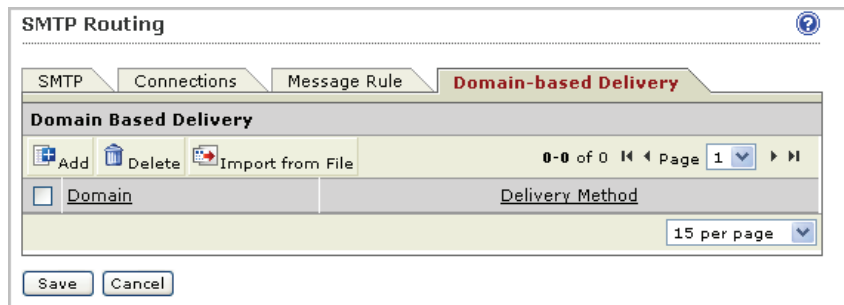
Tip: For security reasons, Trend Micro recommends that you avoid open relay when configuring the message rule settings. For more information on how to avoid open relay, refer to the Online Help and the FAQ section in this manual.

Configuring Domain-based Delivery Settings

Specify settings for the next stage of delivery. IMSVA finds the recipient mail domain and sends the mail to the next SMTP host for the matched domain.

To specify the Domain-based Delivery:

1. Choose **Administration > IMSVA Configuration > SMTP Routing** from the menu.
2. Click the **Domain-based Delivery** tab. The Domain-based Delivery screen appears.



3. Click **Add**, under Domain-Based Delivery. The Destination Domain screen appears.

The screenshot shows a configuration window with two main sections. The first section, titled "Destination Domain", contains a "Name:" label followed by a text input field. The second section, titled "Delivery Method", contains the instruction "Configure the delivery method to use for the destination domain. Forward mail to the following SMTP server:". Below this instruction are two labels, "Server address" and "Port", each followed by a text input field. At the bottom right of the window are two buttons labeled "OK" and "Close".

Destination Domain	
Name:	
Delivery Method	
Configure the delivery method to use for the destination domain. Forward mail to the following SMTP server:	
Server address	Port
OK Close	

4. Specify the **Destination Domain** and **Delivery Method**.
5. Click **OK**.
6. Click **Save**.

Scanning POP3 Messages

In addition to SMTP traffic, IMSVA can scan POP3 messages at the gateway as clients in your network retrieve them. Even if your company does not use POP3 email, your employees might access their personal POP3 email accounts using mail clients on their computers. Hotmail® or Yahoo® accounts are some examples of POP3 email accounts. This can create points of vulnerability on your network if the messages from those accounts are not scanned.

Understanding POP3 Scanning

The IMSVA POP3 scanner acts as a proxy server (positioned between mail clients and POP3 servers) to scan messages as the clients retrieve them.

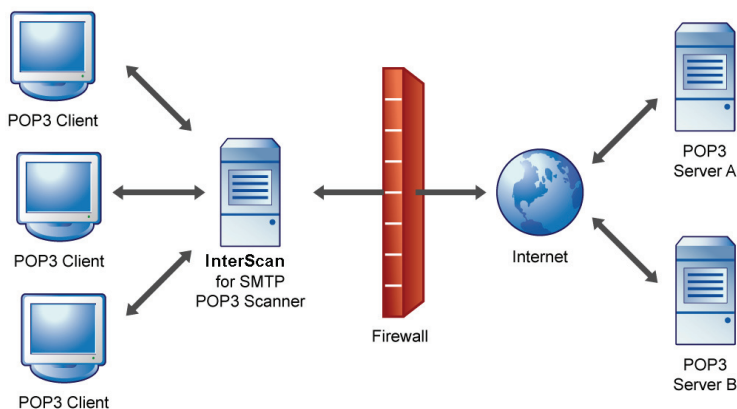


FIGURE 2-1 Scanning POP3 messages

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.

You can set up the following connection types:

- **Generic:** Allows you to access different POP3 servers using the same port, typically 110, the default port for POP3 traffic.

- **Dedicated:** Accesses the POP3 server using a specified port. Use these connections when the POP3 server requires authentication using a secure logon, such as APOP or NTLM.

Requirements

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

Enabling POP3 Scanning

Before IMSVA can begin scanning POP3 traffic, you will need to enable POP3 scanning and configure POP3 settings.

To enable POP3 scanning:

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.
2. Click the **System** tab.

Summary

Maintenance for Trend Micro Antivirus and Content Filter will expire in 28 day(s). Renewal is necessary to keep your security and product updates current. [More info](#)

Maintenance for Spam Prevention Solution (SPS) will expire in 28 day(s). Renewal is necessary to keep your security and product updates current. [More info](#)

Real-time Statistics

System

Enable Connections

☒ Accept POP3 connections
 ☐ Enable IP Filtering
 ☐ NRS
 ☐ IP Profiler

Components

Last refresh: Dec 4, 2007 7:53:43 PM

☐	Name	Current Version	Availability	Update Schedule
☐	Scan engine	8.500.1001	8.500.1001	
☐	Virus pattern	4.859.00	4.859.00	15 minutes
☐	Spyware/grayware pattern	0.557.00	0.557.00	15 minutes
☐	IntelliTrap pattern	0.107.00	0.107.00	
☐	IntelliTrap exceptions	0.259.00	0.259.00	15 minutes
☐	Anti-spam engine	5.0.1023	5.0.1023	15 minutes
☐	Spam pattern	15584.003	15584.003	15 minutes

Managed Services

Hostname	Connection	Scanner Service	Policy Service	EUQ Service
rd.imsa		Stop	Stop	disabled

3. Select the check box next to **Accept POP3 connections**.

4. Click **Save**.

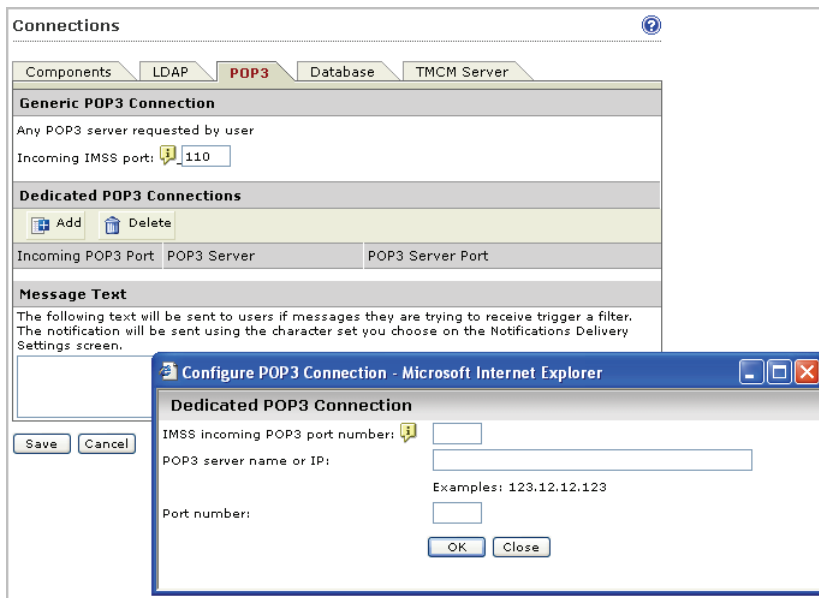
Configuring POP3 Settings

You can specify the IMSVA server ports that clients will use to retrieve POP3 traffic. The default POP3 port is 110. However, if your users need to access a POP3 server through an authenticated connection, (through the APOP command or using NTLM) you may also set up a dedicated connection with a customized port assignment.

To add a POP3 connection:

1. Choose **Administration > IMSVA Configuration > Connections** from the menu. The Components tab appears by default.

2. Click the **POP3** tab.



3. Do one of the following:
 - To accept any POP3 server requested by user, type the incoming IMSVA port number, if it is different from the default port 110.
 - To access the POP3 server using a specific port for authentication purposes, click **Add** to create a new dedicated POP3 connection. Provide the required information and click **OK**.
4. Click **Save**.

Managing Policies

IMSSVA policies are rules that are applied to incoming/outgoing email messages. Create rules to enforce your organization's antivirus and other security goals. By default, IMSSVA includes a Global Antivirus rule to help protect your network from viruses and related Internet threats. Because an antivirus rule addresses the most critical and

potentially damaging types of messages, you should always keep it in the first position on the rule list so IMSVA can analyze traffic for virus content first.

The antivirus rule does not protect against spam. For the best protection against spam, configure a custom rule that includes spam in the scanning conditions, and activate the IP Filtering product.

Note: Before creating a new policy, ensure that you have defined the internal addresses.

How the Policy Manager Works

You can create multiple antivirus and other types of rules to filter and reduce security and productivity threats to your messaging system.

You can create multiple rules for the following two types of policies to filter and reduce security and productivity threats to your messaging system:

- **Antivirus:** Scans messages for viruses and other malware such as spyware and worms.
- **Others:** Scans spam or phishing messages, message content, and other attachment criteria.

An IMSVA policy has the following components:

- The **Route:** A set of sender and recipient email addresses or groups to which the policy is applied. You can use the asterisk (*) to create wildcard expressions and simplify route configuration.
- The **Filter:** A rule or set of rules that apply to a specific route, also known as scanning conditions. IMSVA contains predefined filters that you can use to combat common virus and other threats. You can modify these predefined filters or define your own filters.
- The **Action:** The action that IMSVA should take if the filter conditions are met. Depending on the filter result, a filter action is performed that determines how the message is finally processed.

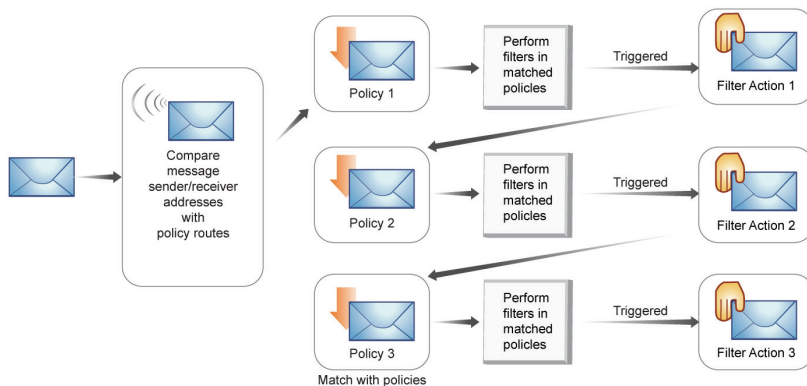


FIGURE 2-2 Simplified policy manager process flow

For more information on how to create a policy, see [Adding Policies on page 2-42](#).

Understanding Address Groups

An address group is a list of email addresses to which your policy applies.

For example, suppose that you have identified three types of content that you want to block from being transmitted through your company’s email system and have defined three filters (in parentheses) to detect these types of content:

- Sensitive company financial data (FINANCIAL)
- Job search messages (JOBSEARCH)
- VBS script viruses (VBSCRIPT)

Now consider the following address groups within your company:

- All Executives
- All HR Department
- All IT Development Staff

The filters that you use in the policies will be applied to these groups as follows:

ADDRESS GROUPS	FINANCIAL	JOBSEARCH	VBSCRIPT
All Executives	Not applied	Applied	Applied
All HR Department	Applied	Not applied	Applied
All IT Development Staff	Applied	Applied	Not applied

Executives, HR staff, and IT developers have legitimate business reasons to send financial information, job search-related correspondence and VBS files, respectively, so you would not apply some filters to those groups.

In IMSVA, email addresses identify the different members of your organization and determine the policies that are applied to them. Defining accurate and complete address groups ensures that the appropriate policies are applied to the individuals in those groups.

Managing Address Groups

Address groups allow you to organize multiple email addresses into a single group and apply the same policy to every address in the group.

Adding an Address Group

You can create an address group when specifying the route during policy creation. You can also add an address group when modifying an existing policy. This can be done by adding email addresses individually or importing them from a text file. The following provides instructions on adding an address group when creating a new policy.

To add an address group:

1. Choose **Policy > Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click on the **Recipients** or **Senders** link. The Select Addresses screen appears.

Incoming Message To ?

Add Rule > Incoming Message To

Select addresses

☐ Anyone

☒ Any of the selected addresses

Enter email address
 Enter email address
 Search for LDAP users or groups
 Select address groups

Selected	

5. Choose **Select Address Groups** from the drop-down list.

Incoming Message To

Add Rule > Incoming Message To

Save Cancel

Select addresses

☐ Anyone

☒ Any of the selected addresses

Select address groups ▼

test

Add >

Selected	

Add Edit Delete

- Click the **Add** button. The Add Address Group screen appears.

Add Address Group

Add Rule > Incoming Message To

Address groups can contain email addresses or wildcarded domains (examples:
*@example.com, *@*.example.com,...)

Save Cancel

Address group name:

Addresses:

Add Import Delete

Save Cancel

- Type a group name, then do any of the following:

- Type an email address and click **Add** to add email addresses individually. You can also use wildcard characters to specify the email address. For example, *@hr.com.
- Click the **Import** button to import a text file containing a list of predefined email addresses.

Note: IMSVA can only import email addresses from a text file. Ensure that the text file contains only one email address per line. You can also use wildcard characters to specify the email address. For example, *@hr.com.

8. Click **Save**.

Editing or Deleting an Address Group

You can edit or delete an address group by editing an existing policy.

To edit or delete an address group:

1. Choose **Policy > Policy List** from the menu.
2. Click the link for an existing policy.
3. Click the **If recipients and senders are** link.
4. Click the **Recipients** or **Senders** link. The Select addresses screen appears.

Incoming Message To 

Default spam rule > Incoming Message To

Select addresses

☐ Anyone
☒ Any of the selected addresses

Enter email address 

Selected	
@	
test@imssrd.com	

- Choose **Select address groups** from the drop-down list.

Incoming Message To 

Default spam rule > Incoming Message To

Select addresses

☐ Anyone
☒ Any of the selected addresses

Select address groups 

test

Selected	
@	
test@imssrd.com	

6. Select the desired address group and click the **Edit** or **Delete** button accordingly.

Searching for an LDAP User or Group

When specifying the route for a policy, instead of entering an individual email address or address group, you can also perform a search for a Lightweight Directory Access Protocol (LDAP) user or group.

IMSVA supports the following three (3) types of LDAP servers:

- Microsoft™ Active Directory 2000 or 2003
- IBM Lotus™ Domino™ 6.0 or above
- SUN™ One LDAP

The following steps provide instructions on adding an LDAP user or group when creating a new policy.

To add an LDAP user or group:

1. Choose **Policy > Policy List** from the menu.
2. Click the **Add** button.
3. Select **Antivirus** or **Other** from the drop-down list to create an antivirus rule or a rule against other threats respectively.
4. Click on the **Recipients** or **Senders** link. The Select Addresses screen appears.

The screenshot shows a web-based configuration window titled "Incoming Message To". At the top, it says "Add Rule > Incoming Message To". Below this are "Save" and "Cancel" buttons. The main section is titled "Select addresses" and contains two radio buttons: "Anyone" (unselected) and "Any of the selected addresses" (selected). Below the radio buttons is a text input field with a dropdown arrow, currently showing "Enter email address". A dropdown menu is open below the input field, listing four options: "Enter email address", "Search for LDAP users or groups" (highlighted in blue), and "Select address groups". To the right of the input field is an "Add >" button. Further right is a table titled "Selected" with a header row and several empty rows, used for displaying selected addresses.

5. Choose **Search for LDAP users or groups** from the drop-down list.

6. Type the LDAP user or group that you are looking for.

Note: 1. You can use the asterisk wildcard when performing a search. See [Using the Asterisk Wildcard on page 2-76](#).

2. You can also search for LDAP groups when adding internal addresses. For more information, see [Configuring Internal Addresses on page 2-40](#).

7. Click the **Search** button.
8. IMSVA displays the LDAP user or group if a matching record exists on the LDAP server.
9. Select the user or group and click the **Add** button to add it to the recipient or sender list.

Configuring Internal Addresses

Internal addresses refer to all the users on your network. IMSVA references the internal address list when it analyzes a rule's route—a specific "To" and "From" combination that includes a recipient and sender address, LDAP users or groups, or address groups.

For reporting and rule creation, IMSVA uses internal addresses to determine which policies and events are Inbound and Outbound.

Any senders and recipients in a rule's route must be on the Internal Addresses list if you selected **incoming messages**, **outgoing messages**, or **both incoming and outgoing messages** when adding a new rule or modifying an existing rule.

If you are configuring an outgoing message, the Internal Address list applies to the senders. If you are configuring an incoming message, the Internal Address list applies to the recipients.

To set internal addresses:

1. Choose **Policy > Internal Addresses** from the menu. The Internal Addresses screen appears.

The screenshot shows the 'Internal Addresses' configuration window. At the top, there is a title bar with a question mark icon. Below the title bar, a note states: 'Note: Please specify a "known" set of users or domains. These shall encompass Incoming and Outgoing addresses for reporting and rule-creation purposes.' The main area is titled 'Internal domains and usergroups'. It contains a text input field labeled 'Enter domain' with a dropdown arrow, an 'Import from File' button, and a '>>' button. To the right of these is a 'Selected' list box with several empty rows. At the bottom of the window are 'Save' and 'Cancel' buttons.

Internal domains and usergroups	
Enter domain	Selected
Import from File	

2. Under **Internal Domains and User Groups**, choose one of the following from the drop-down box:

- **Enter domain:** Type a domain and click >>. Do not type the "@" or user name parts of an email address. For example, domainname or domainname1.domainname2 are valid; user@domainname is invalid.

Note: You can use wildcards for domain names. For example, use *.domain.com to include all sub-domains for "domain.com". However, you cannot use two asterisks in the user name or domain name portion of the address or use the "@" symbol. *.*@domain.com and user@*.* are both invalid.

- **Search for LDAP group:** A screen for searching the LDAP groups appears. Type an LDAP group name (not an individual LDAP user) 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 the LDAP group and, then click >>. For more information, see [Searching for an LDAP User or Group on page 2-38](#).

Note: When selecting an LDAP group for the internal addresses, you can use wildcards in the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, A*, *A, *A* are all allowed.

If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A, *A* are not allowed.

3. To import user groups from a file, click **Import from File** and select the file. The following shows sample content of a domain list text file:

- domain.com
- *.domain.com
- domain.org

Note: The import file must be a text file containing one domain name, domain address, or group per line. You can use wildcards when specifying the domain name or domain address.

4. Click **Save**.

Adding Policies

Before creating a policy, ensure that you have configured the internal addresses. For more information, see [Configuring Internal Addresses on page 2-40](#).

Creating a policy involves four (4) steps:

- Step 1:** [Specifying a Route on page 2-42](#)
- Step 2:** [Specifying Scanning Conditions on page 2-47](#)
- Step 3:** [Specifying Actions on page 2-60](#)
- Step 4:** [Finalizing a Policy on page 2-66](#)

Tip: To prevent a virus leak and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one antivirus rule that applies to **all messages**. Select **all messages** from the drop-down list when specifying the route for an antivirus rule.

Specifying a Route

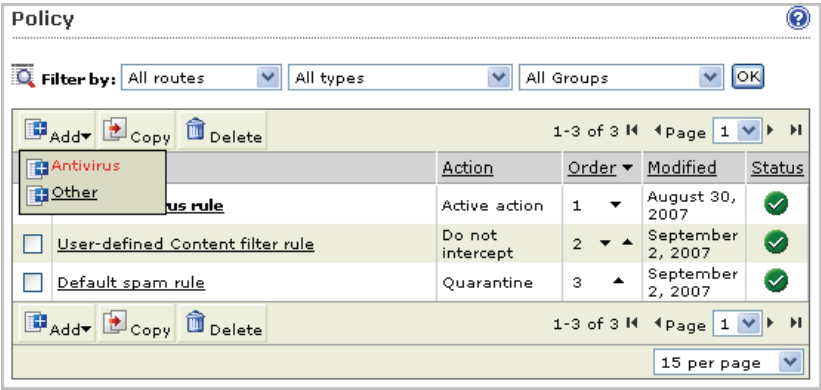
The first step in adding a rule is configuring the following:

- **The route:** A specific "To" and "From" combination that includes a recipient's and sender's email address, LDAP users or groups, or address groups. You can also configure exceptions to a route.
- **Email traffic:** The direction of SMTP traffic or all POP3 traffic.

To add a new policy:

1. Choose **Policy > Policy List** from the menu. The Policy List screen appears.
2. Click **Add**.

3. Select **Antivirus** or **Other** from the drop-down list.



Note: The **Antivirus** rule scans messages for viruses and other malware such as spyware and worms.

The **Other** rule scans spam or phishing messages, message content, and other attachment criteria.

4. The Add Rule screen appears.

Add Rule ?

[Policy List](#) > New Rule

➤ **Step 1: Select Recipients and Senders** >>> Step 2 >>> Step 3 >>> Step 4

This rule will apply to: outgoing messages ▼

< Previous **Next >** Cancel

To	<u>Recipients</u>
From	<u>Senders</u>
Exceptions	<u>Sender to Recipient</u>

If recipients and senders are
 incoming
 to
 AND
 from **Anyone**

Outgoing Message From ?

[Add Rule](#) > Outgoing Message From

Save Cancel

Select addresses

☒ Anyone
☐ Any of the selected addresses

Enter email address: Add >

Selected	

< Previous **Next >** Cancel Save Cancel

5. Select the policy route type from the drop-down list next to **This rule will apply to**.
 - **incoming messages**
 - **outgoing messages**
 - **both incoming and outgoing messages**
 - **POP3**
 - **all messages** (only available when creating an antivirus rule)
6. Select the recipients and senders:
 - For incoming messages, specify the recipient's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid recipients include jim@imsstest.com, bob@imsstest.com)

- For outgoing messages, specify the sender's address, which is in range of the internal addresses. (for example: internal address is imsstest.com, valid senders include jim@imsstest.com, bob@imsstest.com)
- For both incoming and outgoing messages, the rule applies to senders or recipients that match the mail address.

Note:

1. You can use the asterisk wildcard when specifying an email address. For more information, see [Using the Asterisk Wildcard on page 2-76](#).
2. If you selected POP3, you cannot configure the route. The rule applies to all routes.
3. If you selected "all messages" for an antivirus rule, the rule also applies to messages from any sender to any recipient.

7. Click **Next**. The Step 2: Select Scanning Conditions screen appears.

Configuring the Route

A route is a specific "To" and "From" combination that includes a recipients and senders email address, LDAP users or groups, or address groups. You can also configure exceptions to a route.

Senders and recipients must be on the Internal Addresses list if you select incoming messages or outgoing messages when adding a new rule or modifying an existing rule:

If you are configuring an outgoing message, the Internal Address list applies to the senders.

If you are configuring an incoming message, the Internal Address list applies to the recipients.

Examples

Use the asterisk wildcard to include a wide range of email addresses. For example:

- **user@company.com:** Adds only that specific address.
- ***@company.com:** Adds any user at the domain "company.com".
- ***@*.company.com:** Adds any user at any subdomain of "company.com". For example, "user1@accounting.company.com" would be included.

- ***@***: Adds all addresses.

To configure the route:

1. Click one of the following, on the Add Rule screen:
 - **Recipients or Senders:** Appears if you selected incoming messages or outgoing messages.
 - **Users:** Appears if you selected both incoming and outgoing messages.
2. Under **Select addresses**, select one of the following:
 - **Anyone:** Select this option to remove any restriction on the recipients or senders.
 - **Enter address:** Type the email address to add.
 - **Search for LDAP users or groups:** Type the LDAP user or group name and click Search. The results display in the list box.
 - **Select address groups:** All existing address groups appear in the list. If there are a large number of email addresses that you will reuse for routes in several rules, click **Add** to create an address group.
3. If you are adding an email address or email address group, click **Add>**. If you are adding an LDAP or address group, click it in the list box, and then click **Add>**.
4. To remove any email address or email address group from the Selected list, click the trash can icon.
5. Click **Save**.

Note: When selecting an LDAP group as the recipients or senders, you can use wildcards in the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, A*, *A, *A* are all allowed. If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A, *A* are not allowed.

To prevent virus leaks and ensure that all messages are scanned, Trend Micro recommends that you maintain at least one rule that applies to all messages at all times.

Configuring Exceptions for Routes

Do the following to configure a route that applies to a large group of senders or recipients, with the exception of specific users, to whom the rule does not apply.

To configure exceptions for routes:

1. Click the link next to **Exceptions**, on the Add Rule screen. The Exceptions screen appears for the traffic direction (incoming, outgoing, both incoming and outgoing messages, or all messages).
2. Under **Select addresses**, select one of the following for both the **From** and **To** addresses:
 - **Enter email address:** Type the email address to add.
 - **Search for LDAP users or groups:** Type the LDAP user or group name and click **Search**. The results display in the list box.
 - **Select address groups:** All existing address groups appear in the list. If there are a large number of email addresses that you will reuse for routes in a rule, click **Add** to create an address group.
3. If you are adding an email address, click **Add>**. If you are adding an LDAP or address group, click it in the list box, and then click **Add>**.
4. To remove a sender-recipient pair from the list, click the trash can icon.
5. Click **Save**.

Specifying Scanning Conditions

After selecting the senders and recipients for a new rule or modifying the senders and recipients for an existing rule, configure the rules to filter email traffic based on several conditions.

The scanning conditions vary depending on whether Antivirus rules or Other rules are being created.

To specify scanning conditions:

1. Select the check boxes as desired, from the Step 2: Select Scanning Conditions screen. The categories of scanning conditions for the Antivirus and the Other rule types vary as follows:

Add Rule

Policy List > New Rule

Step 1 >>> **Step 2: Select Scanning Conditions** >>> Step 3 >>> Step 4

< Previous
Next >
Cancel

Files to Scan
Select a method to scan viruses, spyware, worms, trojans, and other malicious codes:
☒ All scannable files
☐ IntelliScan: uses "true file type" identification ⓘ
☐ Specific file types

IntelliTrap Settings
☒ IntelliTrap ⓘ
☐ Send the IntelliTrap samples to TrendLab

Spyware/Grayware Scan
☐ Spyware
☐ Dialers
☐ Hacking Tools
☐ Password Cracking Applications
☐ Adware
☐ Joke Programs
☐ Remote Access Tools
☐ Others ⓘ

If recipients and senders are
outgoing
to Anyone
AND
from Anyone

< Previous
Next >
Cancel

Antivirus rule

- a. **Files to Scan:** Set the default method for scanning messages and specific file types containing viruses and other malware.
 - **All scannable files:** Attempt to scan all files.

- **IntelliScan: uses "true file type" identification:** Use IntelliScan to identify malicious code that can be disguised by a harmless extension name.
- **Specific file types:** Select the check box next to one of the following types of file extensions to scan:
 - **Application and executables:** Click the link and select the sub-types to scan.
 - **Documents:** Click the link and select the sub-types to scan.
 - **Compressed files:** Click the link and select the sub-types to scan.
 - **Specified file extensions:** Type the extension in the text box. You do not need to type the period (.) before the extension.
- b. **IntelliTrap Settings:** Scan compressed files for viruses/malware and send samples to TrendLabs for investigation.
 - **IntelliTrap:** Scan email attachments that contain real-time compressed executable files.
 - **Send the IntelliTrap samples to TrendLabs:** IMSVA can automatically send email messages with attachments that IntelliTrap catches to TrendLabs.
- c. **Spyware/Grayware Scan:** Scan for other types of threats such as spyware and adware.

Add Rule 

[Policy List](#) > New Rule

Step 1 >>> **Step 2: Select Scanning Conditions** >>> Step 3 >>> Step 4

Take rule action when: all condition matched (AND) ▼

< Previous Next > Cancel

Spam/phishing emails

☐ [Spam detection settings](#)

☐ [Phishing emails](#)

Attachment

☐ [Name or extension](#)

☐ [MIME content type](#)

☐ [True file type](#)

☐ Size is > ▼ MB ▼

☐ Number of attachments > ▼

Size

☐ Message size is > ▼ MB ▼

Content

☐ [Subject keyword expressions](#)

☐ [Subject is blank](#)

☐ [Body keyword expressions](#)

☐ [Header keyword expressions](#)

☐ [Attachment content keyword expressions](#)

Others

☐ Number of recipients is > ▼

☐ [Received time range](#)

If recipients and senders are

outgoing

to Anyone

AND

from *@test.com

< Previous Next > Cancel

Other rule

- Select one of the following next to **Take rule action when**, which specifies when IMSVA can take action on an email message:

- **all conditions matched (AND):** When an email message matches all of the conditions.
 - **any conditions matched (OR):** When an email message matches any of the conditions.
- b. **Spam/phishing emails:** Scans messages identified as spam and phishing messages. Spam messages are generally unsolicited messages containing mainly advertising content. Phishing messages, on the other hand, originate from senders masquerading as trustworthy entities.
- **Spam detection settings:** Click the link to choose a level of spam protection and configure lists for approved and blocked senders and text exemptions.
 - **Phishing emails**
- c. **Attachment:** Scans messages for file attachments that match the selected criteria, such as attachments with specific extensions or belonging to a certain true file type.
- **Name or extension:** Click the link to configure filter settings for specific file names or extension names.
 - **MIME content type:** Click the link to configure filter settings for MIME content types.
 - **True file type:** Click the link to configure filter settings for common executable, document, image, media, and compressed files.
 - **Size is {>, <, =} {size} {MB, KB, B}:** Choose to filter attachments of a size that is more than, less than, or equal to a certain number of bytes, kilobytes, or megabytes. Type a number that represents the file size.
 - **Number is {>, <, =} {number}:** Choose to filter the number of attachments that is more than, less than, or equal to a certain number. Type a number that represents the total number of attachments for each email message.
- d. **Size:** Scans messages that match the specified message size.
- **Message size is {>, <, =} {size} {MB, KB, B}:** Choose to filter email messages of a size that is more than, less than, or equal to a certain number of bytes, kilobytes, or megabytes. Type a number that represents the email message size.

- e. **Content:** Scans messages containing the keyword expressions that match those expressions specified in the subject, body, header or attachment content keyword expressions links.
 - **Subject keyword expressions:** Click the link to manage your expression lists.
 - **Subject is blank:** Select to filter email messages without a subject. Sometimes spam messages do not contain subject lines.
 - **Body keyword expressions:** Click the link to manage your expression lists.
 - **Header keyword expressions:** Click the link to manage your expression lists. Headers include Subject, To, From, CC, and other headers that you can specify.
 - **Attachment content keyword expressions:** Click the link to manage your expression lists.
- f. **Others:** Scans messages in which the number of recipients match the specified number. Also scans messages that are received within the specified time range.
 - **Recipient number {>, <, =} {number}:** Choose to filter the number of recipients. Type a number that represents the total number of recipients for each email message.
 - **Received time range:** Click the link to choose a day and time within which a message was received.

Selecting Scanning Conditions for Spam

Spam criteria includes a spam catch rate/detection threshold setting and configurable lists for approved and blocked senders and for text exemption rules.

To configure spam scanning conditions:

1. Under **Spam/phishing emails** on the scanning conditions selection screen for the Other rule type, select the check box next to **Spam detection settings**.
2. Click **Spam detection settings**. The Spam detection settings screen appears.
3. To enable spam scanning, select the check box next to Select a spam catch rate or specify a detection threshold. If you do not select this check box, IMSVA will not label any email messages that violate this rule as spam. You can, however, still take actions on any senders in the Blocked Senders list below.

4. Select one of the following spam catch rates or specify a detection threshold.
 - **High:** Catches more spam. Select a high catch rate if too much spam is getting through to your clients.
 - **Medium:** Catches an average amount of spam (the default selection).
 - **Low:** Catches less spam. Select a low catch rate if IMSVA is tagging too many legitimate email messages as spam.
 - **Specify a detection threshold:** Specify a threshold value (between 3.0 and 10.0) that represents how critically IMSVA analyzes email messages to determine if they are spam.

Note: A higher threshold value means that a message must be very "spam-like" for IMSVA to consider it spam. This decreases the spam catch rate, but it also results in a lower number of false positives. If IMSVA is tagging too many legitimate email messages as spam (too many false positives), specify a higher threshold value.

A lower threshold value means that a message only needs to be slightly "spam-like" for IMSVA to consider it spam. This increases the spam catch rate, but it also results in a higher number of false positives. If IMSVA is letting too much spam through to your clients as legitimate email, specify a lower threshold value.

5. Select the check boxes next to any of the following lists to enable them:
 - **Approved sender list:** Prevents IMSVA from identifying email from senders in this list as spam.
 - **Blocked sender list:** Forces IMSVA to identify email from senders in this list as spam.
 - **Text exemption list:** Prevents IMSVA from identifying email that contains any of the text in this list as spam.

Note: For instructions on configuring the lists, see [Configuring Approved and Blocked Sender Lists](#) on page 2-54.

6. Click **Save** to continue selecting scanning conditions.

Configuring Approved and Blocked Sender Lists

To provide added flexibility to spam filtering scanning conditions, IMSVA provides the following lists:

- **Approved sender list:** Prevents IMSVA from identifying email from senders in this list as spam.
- **Blocked sender list:** Forces IMSVA to identify email from senders in this list as spam.

Configure the lists when you select spam scanning conditions.

To configure the approved or blocked sender lists:

1. Select the check box next to **Approved sender list** or **Blocked sender list**.
2. To add addresses manually, do the following:
 - a. Next to **Email address**, type the address. To add multiple addresses, use the asterisk (*) wildcard.
 - b. Click **Add**. The address appears in the list.
3. To import an address group from a file on a local host to the IMSVA server, do the following:
 - a. Click **Import**.
 - b. Click **Browse** and locate the file. A dialog box appears.
 - c. Click **Open**.
 - d. If addresses are already in the list, choose whether to merge them or overwrite them with the imported list.
 - e. Click **Import**.
4. To export an address group as a file on the IMSVA server, do the following:
 - a. Click **Export**. A Save dialog box appears.
 - b. Click **Save**.
 - c. Specify a name for the file and a location to save the file.
 - d. Click **Save**. The file saves to the location and a dialog appears.
 - e. Click **Close**.
5. Click **Save**.

Configuring Spam Text Exemption Rules

IMSVA does not identify any of the text in the text exemption list as spam. Configure rules for this list if you want users to always receive email messages that contain specific keywords.

Use regular expressions to define the conditions. Type a backslash character before any of the following characters:

\ | () { } ^ \$ * + . ?

To configure spam text exemption rules:

1. When configuring the spam scanning conditions, select the **Exclude messages matching text exemption rules** check box under **Text Exemption Rules**.
2. To add a new text exemption rule, click **Add**. To configure an existing rule, click it in the list box, and then click **Edit**. The Text Exemption Rules screen appears.
3. Next to **Name**, type a descriptive name for the text exemption rule.
4. Next to **Scan area**, select a portion of the email message.

Note: If you select **Subject**, **From**, **To**, or **Reply-to** as the scan area and use **Line beginning** to match the header, provide only the header content for **Line beginning**.

Example:

1. Select **From** as the scan area.
2. Under **Strings to match**, provide a message string for **Line beginning**. For example, **test@trendmicro.com**

If you select **All Headers** as the scan area and use **Line beginning** to match the header,, you need to provide the header name as well.

Example:

1. Select **All Headers** as the scan area.
 2. Under **Strings to match**, provide both the header name and a message string for **Line beginning**. For example, **From: test@trendmicro.com**
-

5. Next to **Items are case sensitive**, select the check box to consider the text case as well as the content.

6. Under **Strings to match**, type the text strings in the text boxes. Line beginning means matching regular expressions at the beginning of a line. Line end means matching regular expressions at the end of a line.
7. Click **Save**.

Selecting Scanning Conditions for Attachments

IMSVa can filter email traffic based on the files attached to messages. Attachment scanning conditions includes:

Scanning conditions for attachment names or extensions:

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **Name or extension**.
2. Click **Name or extension**. The Attachment Name or Extension screen appears.
3. Next to **Select**, select one of the following:
 - **Selected attachment names:** IMSVa takes action on email messages with attachments of the selected names.
 - **Not the selected attachment names:** IMSVa takes action on email messages with attachments which are not of the selected names.
4. Select the check boxes next to the attachments to scan or not to scan.
5. To add your own attachment name, do the following:
 - a. Select the check box next to **Attachments named**.
 - b. Click **Import** to import from an existing text file. Another window appears.
Alternatively, type the names in the text box. Use a semicolon (;) to separate values.
 - c. Click **Save**.
6. Click **Save** to continue selecting scanning conditions.

Select MIME content type scanning conditions:

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **MIME content type**.
2. Click **MIME content type**. The Attachment MIME Type screen appears.
3. Next to **Select**, select one of the following:

- **Selected attachment types:** IMSVA takes action on email messages with attachments of the selected types.
 - **Not the selected attachment types:** IMSVA takes action on email messages with attachments which are not of the selected types.
4. Select the check boxes next to the MIME content types to filter.
 5. To add your own MIME types, type them in the text box. Use a semicolon (;) to separate values.
 6. Click **Save** to continue selecting scanning conditions.

Select true file type scanning conditions:

1. Under **Attachment** on the scanning conditions selection screen, select the check box next to **True file type**.
2. Click **True file type**. The Attachment True File Type screen appears.
3. Next to Select, select one of the following:
 - **Selected attachment types:** IMSVA takes action on email messages with attachments of the selected types.
 - **Not the selected attachment types:** IMSVA takes action on email messages with attachments which are not of the selected types.
4. Select the check boxes next to the true file types to filter.
5. Click **Save** to continue selecting scanning conditions.

Select attachment size scanning conditions:

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Size is {>, <, =} {size} {MB, KB, B}**.
2. Choose the comparison symbol (>, <, =).
3. Type a number to represent the size.
4. Choose Megabytes, Kilobytes, or Bytes (**MB, KB, B**).
5. Continue selecting scanning conditions.

Select attachment number scanning conditions:

1. Under **Attachment** on the scanning conditions screen, select the check box next to **Number is {>, <, =} {number}**.
2. Choose the comparison symbol (>, <, =).
3. Type a number to represent the number of attachments.

4. Continue selecting scanning conditions.

Selecting Scanning Conditions for Message Size

IMSVa can take action on an email message based on its total size, including all attachments.

To select message size scanning conditions:

1. Under **Size** on the scanning conditions selection screen, select the check box next to **Message size is {>, <, =} {size} {MB, KB, B}**.
2. Choose the comparison symbol (>, <, =).
3. Type a number to represent the size of the email message.
4. Choose **Megabytes**, **Kilobytes**, or **Bytes (MB, KB, B)**.
5. Continue selecting scanning conditions.

Managing Expression Lists

IMSVa can take action on an email message based on the content in the subject line, body, or header. To filter by message content, add and enable keywords or regular expressions to a keyword expression list. You can configure several expression lists and enable or disable them at any time. To configure a list that is very similar to an existing list, copy a list and then edit the copy.

To select scanning conditions for content:

1. Under **Content** on the scanning conditions selection screen, select the check boxes next to the parts of an email message to which you want the content conditions to apply.
2. Click the link that specifies the part of the email message to which you want to configure content conditions. The Keyword Expressions screen appears with two columns:
 - **Available:** Expressions available for use, but not currently in use.
 - **Selected:** Expressions currently in use.
3. Click **Add**. The screen for managing keyword expressions appears.
4. Configure the expressions.
5. In the **Available** list, click the expression list you want to enable.
6. Click >>. The expressions appear in the Selected list.

To keep an expression list available but temporarily prevent IMSVA from using it, click the expression in the selected list, and then click <<.

7. Click **Save** to continue scanning conditions selection screen.

To copy an expression list:

1. In the **Available** column, click the expression list.
2. Click **Copy**. A copy of the list appears in the **Available** column with the words **Copy of** in front of the original name.

Configuring an Expression

Configure keyword and regular expressions to enable IMSVA to scan email message content. You can add several expressions to a list, and create your own.

To create an expression list and configure expressions:

1. Click **Add** or **Edit** from the Keyword Expressions screen. The configuration screen for keyword expression lists appears.
2. Next to **List name**, type a descriptive name.
3. Next to **Match**, select one of the following that specifies when IMSVA takes action:
 - **Any specified:** Email message content can match any of the expressions in the list.
 - **All specified:** Email message content must match all the expressions in the list.
 - **Not the specified:** Email message content must not match any of the expressions in the list.
 - **Only when combined score exceeds threshold:** Next to **Total message score to trigger action**, type a number that represents the maximum score for allowed keyword expressions. When you add an expression, you can set a score for it.
4. To create an expression, click **Add**. The Add Keyword Expression list appears.
5. Type the keywords. For a partial match, just type the keyword. To specify an exact match, use "\" (without the quotes) before and after the key word.

For example:

- keyword matches "keywords", "keyword", etc.
- \keyword\s matches "keyword" only.

6. If you selected **Only when combined score exceeds threshold**, select a score from the drop down box.
7. Click **Save**. The configuration screen for keyword expression lists reappears with the expression in the list.
8. To instruct IMSVA to consider the capitalization of email content when it uses the filter, select the check box under **Case sensitive**.
9. Click **Save** to continue managing expression lists.

Specifying Actions

The main actions for both the Antivirus and Other rules are similar, although there are minor differences in the options listed. Select the desired action(s) from the following categories:

- **Intercept:** Allows you to choose whether you would like IMSVA to intercept the messages and prevent them from reaching the recipients. Choosing the intercept option allows you to specify an action for IMSVA to take on intercepted messages.
- **Modify:** Instructs IMSVA to make some alterations to the messages or the attachments, such as inserting a stamp or tagging the subject.
- **Monitor:** Instructs IMSVA to send a notification, archive or blind copy the messages if you would like to further analyze them.

To set the actions:

1. Click **Next**. The Step 3: Select Actions screen appears.

Note: The user interface that appears in this step depends on the type of rule that you are creating. The antivirus rule contains two tabs that allow you to configure the main actions and the actions for special viruses.

Specify Main Actions:

Main Actions allow you to specify the default actions that IMSVA takes when messages match the scanning conditions specified in Step 2: Scanning Conditions.

Add Rule

[Policy List](#) > [New Rule](#)

Step 1 >>> Step 2 >>> **Step 3: Select Actions** >>> Step 4

< Previous

Next >

Cancel

Main Actions

Special Viruses

Intercept

☒ Do not intercept messages

☐ Delete entire message

☐ Quarantine to

Default Quarantine

Edit

☐ Change recipient to

☐ Handoff

Host: Port:

Modify

☐ If InterScan MSS finds a virus:

☐ Use ActiveAction - recommended actions by file type

☐ Attempt to clean attachments. If unable to clean:

Delete matching attachment

☐ Delete attachments

Delete matching attachment

☐ Insert stamp in body

Unscanned attachment

Edit

☐ Insert safe stamp for clean mails

Unscanned attachment

Edit

☐ Tag subject

☐ Postpone delivery to

hour of

00

00

If recipients and senders are

outgoing

to Anyone

AND

from Anyone

And scanning conditions match

Virus , IntelliTrap

< Previous

Next >

Cancel

FIGURE 2-3 Antivirus Rule Main Actions

2-61

Add Rule ?

[Policy List](#) > New Rule

Step 1 >>> Step 2 >>> **Step 3: Select Actions** >>> Step 4

< Previous Next > Cancel

IMSS logs all messages that meet rule condition(s).

Intercept

☒ Do not intercept messages

☐ Delete entire message

☐ Quarantine to: Default Quarantine Edit

☐ Change recipient to:

☐ Handoff: Host: Port:

Modify

☐ Delete attachment: Matching attachments Edit

☐ Insert stamp in body: Unscanned attachment Edit

☐ Tag subject

☐ Postpone delivery to: hour of

Monitor

☐ Send notifications

☐ Archive modified to: Default Archive Edit

☐ BCC:

If recipients and senders are
 outgoing
 to: Anyone
 AND
 from: *@test.com
 And scanning conditions match
 Subject is blank

< Previous Next > Cancel

FIGURE 2-4 Other Rule Main Actions

2. Under **Intercept**, click the radio button next to one of the following:
 - **Do not intercept messages:** IMSVA does not intercept the message. Be aware that allowing messages to enter your network without scanning them could expose your network to Internet threats.
 - **Delete entire message:** Deletes the message and all attachments.
 - **Quarantine:** IMSVA puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see [Configuring Quarantine and Archive Settings on page 4-26](#).

- **Change recipient:** IMSVA sends the message to another recipient. Type the recipient email address and separate multiple recipients with a semicolon (;).
- **Handoff:** IMSVA hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
 - Next to **Host**, type the FQDN or IP address of the mail server.
 - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSVA can only track a message before it is handed off. After the handoff, the message is not traceable any more as it is no longer within the control of IMSVA.

3. Under **Modify**, select the check boxes next to any of the following:

Note: Options under **If IMSVA finds a virus** are only available for Antivirus rules.

- **If IMSVA finds a virus:** Select the check box to enable actions if IMSVA finds a virus or other malware, and then click one of the following:
 - **Use ActiveAction:** Enable IMSVA to automatically use preconfigured scan actions for specific types of viruses/malware.
 - **Attempt to clean attachments. If unable to clean:** Select an action for IMSVA to take if it cannot clean the attachment:
 - **Delete matching attachment:** Remove only the attachments with viruses/malware.
 - **Delete all attachments:** Remove all attachments.
 - **Delete attachments:** Select an action for IMSVA to take:
 - **Delete matching attachment:** Remove only the attachment with viruses/malware.
 - **Delete all attachments:** Remove all attachments.
- **Insert stamp in body:** Insert text at the beginning or end of the message. From the drop down box, select the name of the stamp to insert or click Edit to go to the Stamps screen and manage your stamps.

- **Insert safe stamp for clean mails:** Insert text into clean emails signifying that the email is safe. From the drop down box, select the name of the stamp to insert or click Edit to go to the Stamps screen and manage your stamps.

Note: The **Insert safe stamp for clean mails** option is not available on the Special Viruses tab.

- **Tag subject:** Add text to the subject line of the message. Click tag subject to edit the tag.
 - **Postpone delivery time:** Delay delivery until a specified hour of the day. Select the hour of the day and minutes from the drop down boxes.
4. Under **Monitor**, select the check boxes next to any of the following:
- **Send notifications:** Send an email message to one or more recipients. To select a type of notification, click Send notifications. For instructions on creating notifications, see [Managing the Notifications List on page 2-83](#).
 - **Archive modified to:** Archive the message to an archive area. For instructions on creating a new quarantine area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
 - **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.

Specify Special Viruses:

Special Virus settings allow you to specify the actions that IMSVA takes if the messages match any of the following criteria. The actions specified on this screen will override the default actions specified on the Main Actions tab.

Note: These options are only available for Antivirus rules.

- **Mass mailing**—IMSVA takes the actions specified in this section if it detects mass mailing messages.
- **Spyware/grayware**—Allows you to specify the corresponding actions if you have selected any of the Additional Threats Scanning options on the Scanning Conditions screen in step 2. For more information, see [Specifying Scanning Conditions on page 2-47](#). If IMSVA detects spyware/grayware in a message, it takes the actions that are specified here.

Note: IMSVA takes the default action for messages matching the Additional Threats Scanning conditions if you do not select alternative actions.

- **IntelliTrap**—Allows you to specify the corresponding actions if you have selected the IntelliTrap Setting options on the Scanning Conditions screen in step 2. See [Specifying Scanning Conditions on page 2-47](#).

Note: IMSVA takes the default action for messages matching the IntelliTrap conditions if you do not select alternative actions.

Creating a Tag Subject

To notify a recipient that IMSVA took some kind of action on a message's attachment or that the message violated scanning conditions for a rule, add a brief message to the beginning of the subject line. Add a tag only for email that the intended recipients will

eventually receive. If you are configuring a rule to delete messages that violate your scanning conditions, adding a tag is not necessary.

To add a tag:

1. When you are selecting actions, click **Tag subject** under Modify actions. An edit screen appears.
2. Next to Tag, type the text to insert in the subject line.
3. To prevent possible damage to TNEF-encoded messages or digitally signed messages, select **Do not tag digitally signed messages**.
4. Click **Save** to continue selecting actions.
5. To use tag, select the check box next to **Tag subject** under Modify.

Finalizing a Policy

After you select actions for a rule, name and enable the rule. You must also assign an order number that represents its position within the hierarchy of rules. IMSVA allows you to add any notes to the rule that you think are necessary for future reference. You can also modify this information for an existing rule.

When viewing rules, be aware of the following:

-  A green check mark represents active rules.
-  A red X symbol represents rules that are saved but inactive.
-  A gray check mark represents enabled rules but the Activation Code for the product is inactive.
-  A gray X symbol represents that the rules and the Activation Code for the product are inactive.

To finalize a rule:

1. Use one of the following methods to open the screen:
 - When creating a new policy, click **Next** on the Step 3: Select Actions screen. The Step 4: Name and Order screen appears.
 - When finalizing an existing policy, click the name of the policy in the policy list on the **Policy > Policy List** screen

Add Rule

[Policy List](#) > New Rule

Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Name and Order**

< Previous

Finish

Cancel

Rule

Notes

☒ Enable

Rule Name:

Order Number:

Order	Existing Rules	Action	Modified	Status
1	Global antivirus rule	Active action	December 25, 2006	
2	Default spam rule	Quarantine	December 25, 2006	

If recipients and senders are

outgoing

to Anyone

AND

from *@test.com

And scanning conditions match

Subject is blank

Then action is

Quarantine message

< Previous

Finish

Cancel

2. Select the **Enable** check box to activate the rule.
3. Type a name for the rule in the **Rule Name** field.
4. In the **Order Number** field, specify the priority in which IMSVA will perform the scan. IMSVA applies the rule to messages according to the order you specify.
5. Click the **Notes** tab. The Notes screen appears.

Add Rule

Policy List > New Rule

Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Name and Order**

< Previous Finish Cancel

Rule **Notes**

Created:

Last modified:

Notes: Blocks outgoing email messages from test.com

< Previous Finish Cancel

6. Type a note to distinguish the new rule from other rules.
7. If you are creating a new policy, verify that the information on the screen is correct. If any information about the rule is incorrect, click **Previous** and make your changes.
8. Click **Finish** to complete a new rule or **Save** to modify an existing rule.

Policy Example 1

How do I create a rule to delete attachments with specific file names or extensions and then stamp the affected incoming message with an explanation to the recipients?

Step 1: Specify the Route

1. Choose **Policy > Policy List** from the menu.
2. Click **Add**.
3. Select **Other** from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.
5. Click the **Recipients** link. The Select addresses screen appears.

- a. To apply this rule to any recipients, select **Anyone**.
- b. To apply this rule to specific recipients, choose **Any of the selected addresses**, and then specify the target email address or group.
- c. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.

Incoming Message To

Add Rule > Incoming Message To

Save Cancel

Select addresses

☐ Anyone

☒ Any of the selected addresses

Enter email address

Enter email address

Search for LDAP users or groups

Select address groups

Add >

Selected

Step 2: Specify the Scanning Conditions

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Name or extension** condition, select the check box next to it.
4. Click **Name or extension**. The Attachment Name or Extension screen appears.

Attachment Name or Extension

New Rule > Attachment Name or Extension

Save Cancel

Select: Selected attachment names ▼

☐ File extensions to block (recommended)▼

☐ File extensions to consider blocking (more commonly exchanged)▼

☐ Attachments named Import

(Use a semicolon (;) to separate the value)

Save Cancel

5. Select the file extensions to block or consider blocking.
6. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.

Step 3: Specify the Actions

1. Click **Next**. The Step 3: Select Actions screen appears.
2. Under **Modify**, to enable the **Delete attachment** action, select the check box next to it.
3. Select **Matching attachment** from the drop-down list if it is not already selected.
4. Select the check box next to **Insert stamp in body**.
5. If there is no suitable stamp available from the drop-down list, click **Edit**. The Stamps screen appears.

Stamps ?

New Rule > Stamps

Done

Unscanned attachment delete attachment delete bin files	Add Edit Copy Delete

Done

- Click **Add** to create a new stamp. The New Stamp screen appears.

New Stamp ?

New Rule > Stamps > New Stamp

Save Cancel

Name:

Insert at ☒ End of message body
☐ Beginning of message body

Text: Variables list

☒ Do not stamp TNEF-encoded messages or digitally signed messages.

Save Cancel

- Provide the required information.
- Click **Save**. The Stamps screen re-appears.
- Click **Done**. The Select Actions screen re-appears.
- Select the newly created stamp from the drop-down list.

Step 4: Specify the Priority

- Click **Next**. The Step 4: Name and Order screen appears.

2. Type the rule name and order number.
3. Click **Finish**. The newly created rule will appear highlighted in the Policy list screen.

Policy Example 2

How do I create a rule that quarantines messages containing specific keywords in the subject or body and then apply this rule to all recipients except administrators?

Step 1: Specify the Route

1. Choose **Policy > Policy List** from the menu. The Policy List screen appears.
2. Click **Add**.
3. Select **Other** from the drop-down list. The Step 1: Select Recipients and Senders screen appears.
4. Next to **This rule will apply to**, select **incoming messages** from the drop-down list.
5. Click the **Recipients** link. The Select addresses screen appears.
6. Select **Anyone**.
7. Click **Save**. The Step 1: Select Recipients and Senders screen re-appears.
8. Click the **Sender to Recipient link** next to **Exceptions**. The Exceptions screen appears.

Incoming Message Except

Add Rule > Incoming Message Except

Save Cancel

Select addresses

From (sender) To (recipient)

Enter email address Enter email address

Add >

From	To

Save Cancel

9. Under **From (sender)**, type ***@*** to specify any sender.
10. Under **To (recipient)**, type the administrator's email address.
11. Click **Add**. The sender-recipient pair appears in the list.
12. To add other administrators or recipients, repeat steps 9 to 11.
13. Click **Save** after you finish adding all the desired recipients. The Step 1: Select Recipients and Senders screen re-appears.

Step 2: Specify the Scanning Conditions

1. Click **Next**. The Step 2: Select Scanning Conditions screen appears.
2. Next to **Take rule action when**, select **any condition matched (OR)**.
3. To enable the **Subject Keyword Expressions** condition under **Content**, select the check box next to it.
4. Click **Subject Keyword Expressions**. The Keyword Expressions screen appears.

The screenshot shows the 'Keyword Expressions' dialog box. At the top, it says 'New Rule > Keyword Expressions'. Below this are 'Save' and 'Cancel' buttons. The main area is divided into two panes: 'Available' on the left and 'Selected' on the right. The 'Available' pane has buttons for 'Add', 'Edit', 'Copy', and 'Delete'. It contains a list of keywords: Profanity, HOAXES, Chainmail, Sexual Discrimination, Racial Discrimination, HTML and script messages, Credit Card Number, Social Security Number, and Bounce Mail. Between the panes are '>>' and '<<' buttons. The 'Selected' pane is currently empty. At the bottom are 'Save' and 'Cancel' buttons.

5. If the desired keywords are not available from the existing list, click **Add** to create a new keyword list. The New Keyword Expression screen appears.

The screenshot shows the 'New Keyword Expression' dialog box. At the top, it says 'New Rule > Keyword Expressions > New Keyword Expression'. Below this are 'Save' and 'Cancel' buttons. The main area has a 'List name:' text box, a 'Match:' dropdown menu set to 'Any specified', and 'Add' and 'Delete' buttons. Below these is a table with one row: a checkbox, the text 'Keywords/regular expressions', and the text 'Case sensitive'. At the bottom are 'Save' and 'Cancel' buttons.

6. Specify the required information.
7. To add an individual keyword expression, click **Add**. The Add Keyword Expressions screen appears.

Add Keyword Expression

New Rule > Keyword Expressions > Add Keyword Expression

Save Cancel

You may use any combination of keywords and regular expressions to define a keyword expression.

Type a backslash \ immediately before the following characters: . \ | () { } [] ^ \$ * + or ?

joke|

Save Cancel

8. Type the desired keyword expression and click **Save**. The New Keyword Expression screen re-appears.
9. Repeat steps 7 and 8 for additional keyword expressions.
10. After you have added all the required keyword expressions, type the **List name** for the new keyword list and click **Save**. The Keyword Expressions screen re-appears with the newly created keyword list.
11. Select the new list and click >> to insert the list into the Selected box.
12. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears.
13. To enable the **Body Keyword Expression** condition, select the check box next to it.
14. Click **Body Keyword Expression**. The Keyword Expressions screen appears.
15. Select the new keyword list and click >> to insert the list into the Selected box.
16. Click **Save**. The Step 2: Select Scanning Conditions screen re-appears. Ensure that both the Subject keyword and Body keyword expressions are selected.

Content

☒	Subject keyword expressions
☐	Subject is blank
☒	Body keyword expressions
☐	Header keyword expressions
☐	Attachment content keyword expressions

Step 3: Specify the Actions

1. Click **Next**. The Step 3: Select Actions screen appears.
2. Under **Intercept**, select **Quarantine to**.
3. Accept the **Default Quarantine** area or click the drop-down list to select the desired quarantine area.

Step 4: Specify the Priority

1. Click **Next**. The Step 4: Name and Order screen appears.
2. Type the rule name and order number.
3. Click **Finish**. The newly created rule will appear highlighted in the Policy list screen.

Using the Asterisk Wildcard

You can use the asterisk (*) as a wildcard in email addresses when defining routes and in file names.

Wildcards in Email Addresses

Wildcards can appear in the name or domain sections of an email address. The following are valid examples:

- *****—Valid representation of all email addresses.
- ***@domain.tld, name@*.tld**—Valid representation of the whole name or the domain (not the top level domain (TLD)).
- ***@*.tld**—Valid representation of both the name and the domain (not the TLD).

Wildcards cannot appear in a subdomain or the top-level domain. Wildcards also cannot appear with other letters; they must appear alone. The following are invalid examples:

- **name@domain*.tld**—Invalid representation of a subdomain.
- **name@domain.***—Invalid representation of a TLD.
- ***name@domain.tld**—Invalid use in conjunction with a name.

Wildcards in File Names

You can use wildcard characters in file names the same way you can use them in email addresses. Use an asterisk in the name or the extension sections of a filename, but not in conjunction with a partial name or extension. The following are valid examples:

- ***.***—Valid representation of all files.
- ***.extension**—Valid representation of all files of a certain extension.
- **name.***—Valid representation of files with a specific name but with any extension.

The following are invalid examples:

- ***name.***—Invalid representation of a name.
- **name.*extension**—Invalid representation of an extension.

Setting Scan Exceptions

Under certain circumstances, you might want to prevent IMSVA from scanning certain types of email messages that could be part of a DoS attack. For example, messages with extremely large attachments would require significant IMSVA server resources to scan fully. Additionally, messages addressed to hundreds of recipients are most likely spam or some type of attack.

Rather than consuming IMSVA resources to scan these types of email messages, set scan exceptions to bypass scanning and instruct IMSVA to take action on the messages immediately.

WARNING! 1. For the actions specified in Scan Exceptions take effect, verify that the Global antivirus rule is enabled.

2. When a message triggers the scan exception, IMSVA stops scanning and takes the corresponding actions. That means IMSVA will not trigger any policy rules when a scan exception occurs.

To configure scan exceptions:

1. Choose **Policy > Scanning Exceptions** from the menu.
2. To set scan exception conditions for email messages based on several conditions, click the Security settings violations link under Exception. The Security Settings Violations screen appears, where you can configure the settings.
3. To set an action for an exception type, click the corresponding link under Action:
 - [Setting Scan Actions for Security Setting Violations on page 2-78](#)
 - [Setting Scan Actions for Encrypted Messages on page 2-79](#)

- [Setting Scan Actions for Password Protected Zip Files on page 2-80](#)
- [Setting Scan Actions for Other Scanning Exceptions on page 2-82](#)

Configuring Exceptions for Security Settings Violations

The scan exceptions for the security settings violations on this screen apply to all senders and receivers.

To configure security settings violations:

1. On the Scanning Exceptions screen, click **Security settings violations** under **Exception**. The Security Settings Violations screen appears.
2. To set limits on the types of email messages IMSVA can scan, configure the following:
 - **Total message size exceeds { } MB:** Type the maximum number of megabytes.
 - **Total # recipients exceeds { } recipients:** Type the maximum number of recipients.
 - **Total # embedded layers in compressed file exceeds { } layers:** Select the maximum number of layers.
 - **Total decompressed size of any single file exceeds { } MB:** Type the maximum number of megabytes.
 - **Total # files in compressed file exceeds { } files:** Type the maximum number of files.
3. Click **Save**. The Scanning Exceptions screen reappears.

Setting Scan Actions for Security Setting Violations

To set scan actions for security settings violations:

1. On the Scanning Exceptions screen, click the **Quarantine and Notify** link under **Actions for Security Settings Violations**. The screen for configuring actions appears.
2. Under **Intercept**, click the radio button next to one of the following:
 - **Do not intercept messages:** IMSVA does not take action on the message.
 - **Delete entire message:** Deletes the message and all attachments.

- **Quarantine to:** IMSVA puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
- **Handoff:** IMSVA hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
 - Next to **Host**, type the FQDN or IP address of the mail server.
 - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSVA can only track a message before it is handed off. After the handoff, the message is not traceable any more as it is no longer within the control of IMSVA.

3. Under **Monitor**, select the check boxes next to any of the following:
 - **Send notification:** Send a notification message to one or more recipients. To select a type of notification, click **Send notifications**. For instructions on creating notifications, see [Managing the Notifications List on page 2-83](#).
 - **Archive:** Archive the message to an archive area. For instructions on creating a new archive area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
 - **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.
4. Click **Save**.

Setting Scan Actions for Encrypted Messages

To set scan actions for encrypted messages:

1. On the Scanning Exceptions screen, click the **Quarantine and Notify** link under **Actions for Encrypted messages**. The screen for configuring actions appears.
2. Under **Intercept**, click the radio button next to one of the following:
 - **Do not intercept messages:** IMSVA does not process the message.
 - **Delete entire message:** Deletes the message and all attachments.

- **Quarantine to:** IMSVA puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
- **Handoff:** IMSVA hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
 - Next to **Host**, type the FQDN or IP address of the mail server.
 - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSVA can only track a message before it is handed off. After the handoff, the message is not traceable any more as it is no longer within the control of IMSVA.

3. Under **Monitor**, select the check boxes next to any of the following:
 - **Send notification:** Send an email message to one or more recipients. To select a type of notification, click Send notifications. For instructions on creating notifications, see [Managing the Notifications List on page 2-83](#).
 - **Archive:** Archive the message to an archive area. For instructions on creating a new archive area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
 - **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.
4. Click **Save**.

Setting Scan Actions for Password Protected Zip Files

To set scan actions for password protected zip files:

1. On the Scanning Exceptions screen, click the **Stamp** link under **Actions** for **Messages with password protected zip files**. The screen for configuring actions appears.
2. Under **Intercept**, click the radio button next to one of the following:
 - **Do not intercept messages:** IMSVA does not process the message.

- **Delete entire message:** Deletes the message and all attachments.
- **Quarantine to:** IMSVA puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
- **Handoff:** IMSVA hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
 - Next to **Host**, type the FQDN or IP address of the mail server.
 - Next to **Port**, type the port number through which the mail server receives email traffic.

Note: IMSVA can only track a message before it is handed off. After the handoff, the message is not traceable as it is no longer within the control of IMSVA.

3. Under **Modify**, select the check boxes next to any of the following:
 - **Delete attachment:** Strip the attachments from the message. To strip only the attachments that match the scanning conditions you selected for a rule, select Matching attachments from the drop down box. To remove all attachments, select All attachments.
 - **Insert stamp in body:** Insert text at the beginning or end of the message. From the drop down box, select the name of the stamp to insert or click Edit to go to the Stamps screen and manage your stamps.
 - **Tag subject:** Add text to the subject line of the message. Click Tag subject to edit the tag.
 - **Postpone delivery time:** Delay delivery until a specified hour of the day. Select the hour of the day and minutes from the drop down boxes.
4. Under **Monitor**, select the check boxes next to any of the following:
 - **Send notifications:** Send an email message to one or more recipients. To select a type of notification, click Send notifications. For instructions on creating notifications, see [Managing the Notifications List on page 2-83](#).
 - **Archive:** Archive the message to an archive area. For instructions on creating a new archive area, see [Configuring Quarantine and Archive Settings on page 4-26](#).

- **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.
5. Click **Save**.

Setting Scan Actions for Other Scanning Exceptions

To set scan actions for other scanning exceptions:

1. On the Scanning Exceptions screen, click the **Quarantine and Notify** link under **Actions** for **Other scanning exceptions**. The screen for configuring actions appears.
 2. Under **Intercept**, click the radio button next to one of the following:
 - **Do not intercept messages:** IMSVA does not take action on the message.
 - **Delete entire message:** Deletes the message and all attachments.
 - **Quarantine to:** IMSVA puts the message and its attachments into the quarantine area that you select from the drop down box. For instructions on creating a new quarantine area, see [Configuring Quarantine and Archive Settings on page 4-26](#).
 - **Handoff:** IMSVA hands off the message to a specific mail server. Select Handoff if you have a secure messaging server on your network that can process or handle the message. Configure the following:
 - Next to **Host**, type the FQDN or IP address of the mail server.
 - Next to **Port**, type the port number through which the mail server receives email traffic.
-
- Note:** IMSVA can only track a message before it is handed off. After the handoff, the message is not traceable as it is no longer within the control of IMSVA.
-
3. Under **Monitor**, select the check boxes next to any of the following:
 - **Send notifications:** Send an email message to one or more recipients. To select a type of notification, click Send notifications. For instructions on creating notifications, see [Managing the Notifications List on page 2-83](#).
 - **Archive:** Archive the message to an archive area. For instructions on creating a new archive area, see [Configuring Quarantine and Archive Settings on page 4-26](#).

- **BCC:** Blind carbon copy the message to another recipient. Type the recipient's email address and separate multiple addresses with a semicolon (;). Select the BCC option to prevent the intended recipients from seeing the new recipient.
4. Click **Save**.

Managing the Notifications List

To notify a recipient or an email administrator that IMSVA took some kind of action on a message's attachment or that the message violated IMSVA rule scanning conditions, send a notification.

To send notifications:

1. When you are selecting actions, click **Send notifications** under Monitor actions. The Notifications screen appears with two columns:
 - **Available:** Notification messages available for use, but not currently in use.
 - **Selected:** Notification messages currently in use.
2. Add or modify a notification.
3. In the **Available** list, click the notifications you want to enable.
4. Click >>. The notifications appear in the **Selected** list.

To keep a notification available but temporarily prevent IMSVA from using it, click the notification in the selected list, and then click <<.
5. Click **Save** to continue selecting actions.

Adding or Modifying a Policy Notification

To add or modify a policy notification:

1. When you are selecting actions for a policy, click **Send notifications** under Monitor actions. The Notifications screen appears with two columns:
 - **Available:** Notification messages available for use, but not currently in use.
 - **Selected:** Notification messages currently in use.
2. Click **Add** or **Edit**. The configuration screen for the notification appears.
3. To send an email notification, configure the following:
 - **Name:** Type a descriptive name for the notification.

- **From:** Type a sender email address.
 - **To:** Type the receiver email addresses and select the check boxes next to Original Mail Sender and/or Original Mail Recipient. Separate each address with a semicolon (;).
 - **Subject:** Type the subject line of the notification.
 - **Message:** Type the notification message.
4. To send the message as an attachment, select the check box next to **Attach the message**.
 5. To see the types of variables you can include in the message, click **Variables list**.
 6. To send an SNMP trap, configure the following:
 - a. Click one of the following:
 - **Disable (first radio button):** Avoid sending any trap IDs.
 - **Second radio button:** Select one of the default SNMP traps.
 - **Third radio button:** Type a custom trap ID.
 - b. **Message:** Type the notification message.
 7. Click **Save** to return to continue managing the notifications list.
 8. To copy a notification:
 - a. In the Available column, click a notification.
 - b. Click **Copy**.
 - c. A copy of the list appears in the Available column with the words **Copy of** in front of the original name.

Updating Scan Engine and Pattern Files

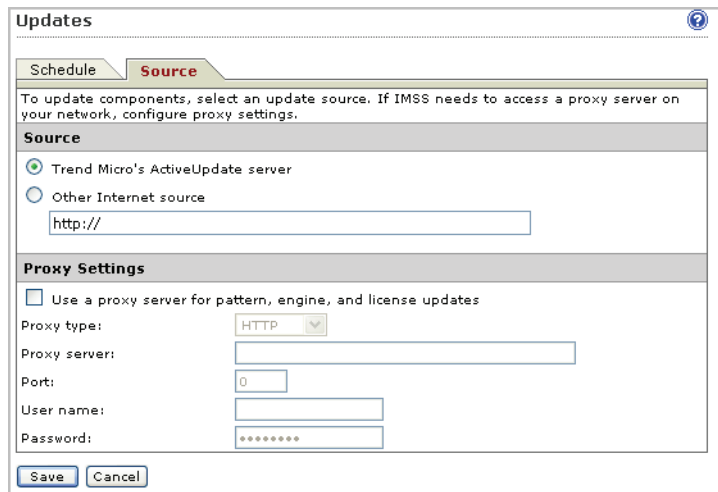
To ensure that your network is constantly well-protected against the latest malware, ensure that you update IMSVA components such as the scan engine and virus pattern files on a regular basis. You can choose to perform a manual or scheduled update of the components.

Specifying an Update Source

Before you can update the IMSVA scan engine and pattern files, you need to specify the update source. By default, IMSVA downloads components from the Trend Micro ActiveUpdate server, which is the only source for up-to-date components. However, if you are using Trend Micro Control Manager (TMCM) to manage IMSVA, you can update the components from the Control Manager server.

If you did not specify the Update Source when configuring IMSVA using the Configuration Wizard, enter the update source and/or any proxy settings as follows:

1. Choose **Administration > Updates > Components** from the menu. The Updates screen appears.
2. Click the **Source** tab.



The screenshot shows the 'Updates' configuration window with the 'Source' tab selected. The window has a title bar with a question mark icon. Below the title bar are two tabs: 'Schedule' and 'Source'. The 'Source' tab is active. The main content area has a header 'To update components, select an update source. If IMSS needs to access a proxy server on your network, configure proxy settings.' Below this is a section titled 'Source' with two radio buttons: 'Trend Micro's ActiveUpdate server' (selected) and 'Other Internet source'. Below the 'Other Internet source' radio button is a text input field containing 'http://'. Below the 'Source' section is a section titled 'Proxy Settings' with a checkbox 'Use a proxy server for pattern, engine, and license updates' (unchecked). Below the checkbox are four input fields: 'Proxy type:' with a dropdown menu showing 'HTTP', 'Proxy server:', 'Port:' with a value of '0', 'User name:', and 'Password:' with a masked password '*****'. At the bottom of the window are two buttons: 'Save' and 'Cancel'.

3. Under **Source**, select one of the following:
 - **Trend Micro ActiveUpdate server:** The default source for up-to-date components.
 - **Other Internet source:** Type the URL or IP address of the Control Manager server.
4. If connection to Active Update and Product Registration Server must pass through a proxy server to get to the Internet, select **Use a proxy server for pattern file, engine, and license updates** and configure the following:
 - **Proxy type:** Select **HTTP**, **SOCKS4**, or **SOCKS5**.
 - **Proxy server:** Type the host name or IP address of the proxy server.
 - **Port:** Type the port the proxy server uses to communicate.
 - **User name:** Type the username you need for administrative access to the proxy server.
 - **Password:** Type the corresponding password.
5. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

Performing a Manual Update

You may perform a manual update of IMSVA components under the following circumstances:

- If you have just deployed or upgraded IMSVA.
- If you suspect that your network's security is compromised by new malware and would like to update the components immediately.

To perform a manual update:

1. Click **Summary** from the menu. The Summary screen appears with the Real-time Statistics tab selected by default.
2. Click the **System** tab.

Summary 

 **Maintenance for Trend Micro Antivirus and Content Filter will expire in 28 day(s).**
Renewal is necessary to keep your security and product updates current. [More info](#)

 **Maintenance for Spam Prevention Solution (SPS) will expire in 28 day(s).**
Renewal is necessary to keep your security and product updates current. [More info](#)

Real-time Statistics **System**

Enable Connections

☐ Accept POP3 connections ☒ Enable IP Filtering
... ☒ NRS ☒ IP Profiler

Components Last refresh: Dec 4, 2007 8:17:18 PM  Refresh

☐	Name	Current Version	Availability	Update Schedule
☒	Scan engine	8.500.1001	8.500.1001	
☐	Virus pattern	4.859.00	4.859.00	15 minutes
☐	Spyware/grayware pattern	0.557.00	0.557.00	15 minutes
☐	IntelliTrap pattern	0.107.00	0.107.00	15 minutes
☐	IntelliTrap exceptions	0.259.00	0.259.00	15 minutes
☐	Anti-spam engine	5.0.1023	5.0.1023	15 minutes
☐	Spam pattern	15584.003	15584.003	15 minutes

Managed Services

Hostname	Connection	Scanner Service	Policy Service	EUQ Service
rd.imsa		Stop	Stop	disabled

- Under **Components**, verify the version numbers of the antivirus, anti-spyware, and anti-spam components that IMSVA uses to protect your network.
- To update all components, select the first check box on the column header next to the **Name** field. Otherwise, to update specific component(s), select the check box next to the desired component.
- Click **Update**.

Rolling Back a Component Update

If you encounter any system issues after updating IMSVA components, you can roll back to the previous version.

To roll back a component update:

1. Choose **Summary** from the menu. The Summary screen appears with the Real-time Statistics tab selected by default.
2. Click the **System** tab.
3. To roll back all components to the previous versions, select the first check box on the column header next to the **Name** field. Otherwise, to roll back specific component(s), select the check box next to the desired component.
4. Click the **Rollback** button.

Configuring Scheduled Update

If you forget to regularly download antivirus and anti-spam components, your network will be at risk from Internet threats. To automate the update process, configure an update schedule on this screen. If your network has limited Internet bandwidth, schedule updates for off-peak hours.

To configure a scheduled update:

1. Click **Administration > Updates > Components** from the menu. The Updates screen appears with the Schedule tab selected by default.

Updates

Schedule | Source

☐ Enable scheduled update

Update Component

☐ Scan engine

☒ Virus pattern

☐ Spyware/grayware pattern file

☐ IntelliTrap pattern
IntelliTrap exceptions

☐ Anti-spam engine

☐ Spam pattern

Update Schedule

☐ Minutes intervals: 15

☐ hourly: 00

☒ daily: 7 : 00

☐ weekly: Sunday 0 : 00

Save Cancel

2. Select the **Enable Scheduled Update** check box.
3. Under **Update Component**, select the components to update. Trend Micro recommends updating all components.
4. Under **Update Schedule**, select the update frequency:
 - **Minute intervals:** Updates every { } minutes per hour. Select the minute interval. For example, if you select 15, the update is triggered four times an hour: at 00, 15, 30, 45 mins. If you select 30, the update will be triggered twice an hour: at 00 and 30 mins.
 - **Hourly at minute:** Updates every hour at { } minutes. Select the number of minutes after the hour. For example, if you select 15, the update is triggered at 15 minutes after the hour, every hour.
 - **Daily at time:** Updates every day at the time you choose. Select the time of day.
 - **Weekly at day and time:** Updates once a week at the specified day and time. Select a day of the week and the time of day.
5. Click **Save**.

Updating the System and Application Files

When new operating system and application files become available from Trend Micro, upload them to a parent IMSVA device and all of its child devices. By default, child devices will be updated before the parent device.

Updating devices is a two-step process:

- Upload the file to the IMSVA parent device.
- Deploy the file to selected devices.

To upload a new system or application file:

1. Click **Administration > Updates > System & Applications** from the menu.
2. Under **Upload**, click **Browse** and locate the file.
3. Click **Upload**. After the file finishes uploading, the package type, build number, and title appear under **Latest uploaded package**.

To deploy the system or application file:

1. Select the check boxes next to the devices to which you want to deploy the update.
2. Click **Update**.
3. Accept the license agreement. After the update is complete, a summary page appears.
4. Click **OK**.

WARNING! During the update, do not modify any other settings. To stop the update, click **Cancel**.

If a device check box is grayed out, you cannot deploy the update to the device because the device:

- Already has the updated files.
- Has more up-to-date files than the ones you are trying to deploy.
- Is a child device and you have not yet uploaded the files to the parent device.

To view update history for any device or to roll back an update:

1. Under **Host Name**, click the name of the device you want to view. A summary screen appears showing the updates and related log information.

- 2. To remove an update, click **Rollback**. You can only roll back the latest application updates.
- 3. To view details of the patch update, click **Download patch log**.
- 4. To go back to the main screen, click **OK**.

Configuring Log Settings

You can configure the level of detail IMSVA will write to the logs and the length of time it will store them. In addition, you can set the update period that controls how frequently the scanner services write their local logs to the InterScan admin database.

To configure log settings:

- 1. Choose **Logs > Settings** from the menu. The Log Settings screen appears.

Log Settings

Reporting Logs (Stored in Database)

Database log update interval: 01 minutes

Number of days to keep logs for query: days

Log Files

Application log detail level: Normal

☐ Number of days to keep log files: days

☐ Maximum log file size for each service: MB

Save

Cancel

- 2. Under **Reporting Logs**, configure the following:
 - **Database log update interval:** IMSVA updates the logs regularly at every interval. Select a number between 1 and 60 for the interval. Selecting 60 means that IMSVA updates the logs once every hour.

Tip:

Trend Micro recommends setting a value below 5 to ensure timely update of the traffic summary data.

- **Number of days to keep logs for query:** Type a value between 1 and 60 that represents the number of days IMSVA will preserve the logs for query in the IMSVA admin database.

3. Under **Log Files**, configure the following:

- **Application log detail level:** The level of log detail. Select one of the following:
- **Normal:** The standard level of detail. This level provides the basic information needed by an administrator for daily monitoring and maintenance.
- **Detailed:** A high level of detail. All IMSVA processes write detailed information to the logs, including: telnet session information, the policy matched, the filter executed, and the action taken.
- **Diagnostic:** Comprehensive information on each event or action. Diagnostic level logs include all information from the detailed level, plus SMTP routing information, and the route match information that determined which policy was applied.
- **Debug:** The most complete and verbose level of detail. Debug logs are only recommended when troubleshooting.

Note: Diagnostic or Debug logs might consume excessive resources and could lower system performance.

- **Number of days to keep log files:** Select the check box and type a number between 1 and 150 that represents the number of days IMSVA will keep the local log files. To prevent IMSVA from deleting the log files, clear the check box.
- **Maximum log file size for each service:** Select the check box and type a number between 100 and 99999 that represents the size in MB for local log files for each type of process or service. To remove any size restriction, clear the check box.

-
- Note:**
1. IMSVA log files are stored in the folder /opt/trend/IMSA/logs. IP Profiler log files are stored in the folder /opt/trend/ipprofiler/logs.
 2. Daily log files for each event type are created at midnight and have the suffix of "<Date>.<Count>". The <Count> suffix is incremented if there is more than one (1) log file per day.
 3. If the log file size exceeds the maximum log file size for each service, IMSVA will delete the oldest file.
-

4. Click **Save**.



Backing Up, Restoring, and Replicating Settings

This chapter provides instructions on how you can back up and restore IMSVA configuration settings as a precaution against system failure. If you have deployed multiple IMSVA scanners and are using Trend Micro Control Manager simultaneously, you can also replicate IMSVA settings without having to reconfigure settings for each new scanner.

Topics include:

- [Import/Export Notes on page 3-2](#)
- [Restoring IMSVA on page 3-4](#)
- [Replicating Settings on page 3-5](#)

Import/Export Notes

To back up IMSVA settings, export the settings from the Web management console. In the event of system failure, you can restore the settings by importing the configuration file that you have backed up previously. Note the following when importing/exporting settings:

- You cannot import or export the component list and child device registration information.
- When exporting/importing your settings, the database will be locked. Therefore, all IMSVA actions that depend on database access, such as performing a mail trace, will not function.
- SMTP Routing Settings that were exported from IMSA 1.0 or IMSVA 7.0, and subsequently imported into IMSVA 7.0, will overwrite existing settings in the current IMSVA version.

Trend Micro strongly suggests that you:

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

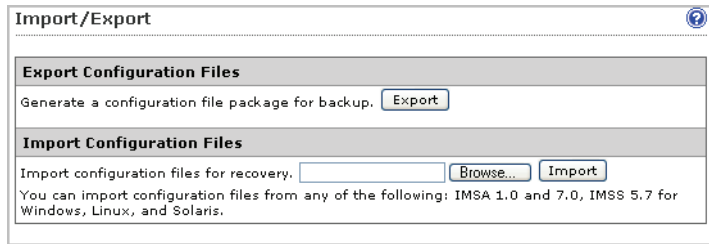
Backing Up IMSVA

Trend Micro recommends exporting your settings to:

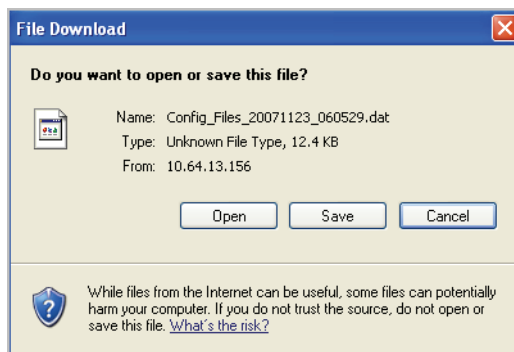
- **Keep a backup**—In case a problem occurs with the IMSVA application file and you need to rescue the application. Importing your configuration backup will prevent you from having to configure all settings again.
- **Replicate settings across several devices**—If you have several devices on your network, you do not need to configure most settings on each of them separately.

To export settings:

1. Choose **Administration > Import/Export** from the menu.



2. Click **Export**.
3. When the File Download dialogue box appears, click **OK** to save the configuration file to your computer.



4. To return to the Import/Export screen, click **Return**.

During export, do not:

- Access other Web console screens or modify any settings
- Perform any database operations
- Start/stop any services on the device or in the group to which the device belongs
- Register/unregister any child devices into/from the group to which the device belongs
- Launch other export or import tasks

Restoring IMSVA

To restore IMSVA settings, import the configuration files that you have backed up previously.

To import settings:

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.
2. Click the **System** tab.
3. Verify that no services are starting or stopping. If services are starting or stopping, wait until they are stable.
4. Choose **Administration > Import/Export** from the menu.
5. Under **Import Configuration Files**, click **Browse...** and locate the file.
6. Click **Import**. The original settings and rules, such as domain-based delivery settings, will be deleted and replaced by the imported settings and rules. All services on each device in the group will be restarted to apply the imported settings and rules. Wait until all services are restarted.

During import, do not:

- Access other Web console screens or modify any settings.
- Perform any database operations.
- Start/stop any services on the device or in the group to which the device belongs.
- Register/unregister any child devices into/from the group to which the device belongs.
- Launch other export or import tasks.

Settings That Cannot Be Restored

- Control Manager Settings
- EUQ approved senders
- Administrator Accounts & Password
- Activation Code & license information
- ActiveUpdate server information
- IP and network settings
- Group member list

Replicating Settings

If you have installed multiple IMSVA scanners that do not share the same admin database, you can use Trend Micro Control Manager to replicate settings across these scanners without having to configure each scanner separately. If the scanners share the same admin database, it is not necessary to replicate settings.

Do the following if you intend to replicate settings using Control Manager:

Step 1: Back up IMSVA settings. For details, see [Backing Up IMSVA on page 3-3](#).

Step 2: Enable the Control Manager agent.

Step 3: Replicate settings from the Control Manager Web console.

Enabling Control Manager Agent

IMSVA automatically installs the Trend Micro Control Manager agent during installation. To integrate with Control Manager, all you need to do is provide the Control Manager server details and enable the agent from the Web management console.

To configure Control Manager Server settings:

1. Choose **Administration > IMSVA Configuration > Connections** from the menu. The Components tab appears by default.
2. Click the **TCCM Server** tab. The TCCM Server Settings screen appears.

Connections

Components | LDAP | POP3 | Database | **TCM Server**

TCM Server Settings

To manage IMSS with Control Manager, enable the TCM agent and configure all TCM server settings.

[Un-register All Agents](#)

☒ **Enable TCMC Agent**

Server:

Communication protocol: ☒ HTTP Port: ☐ HTTPS Port:

Web server authentication:

User name: ⓘ

Password:

Proxy Settings

☐ **Enable proxy**

Proxy type: ▼

Proxy server:

Port:

User name:

Password:

[Save](#) [Cancel](#)

3. Provide the required information.
4. Select the check box next to **Enable TCMC Agent**.
5. Click **Save**.

Replicating Settings from Control Manager

After enabling the Control Manager agent from the IMSVA Web management console, you can start to replicate IMSVA settings by logging on to the Control Manager Web console.

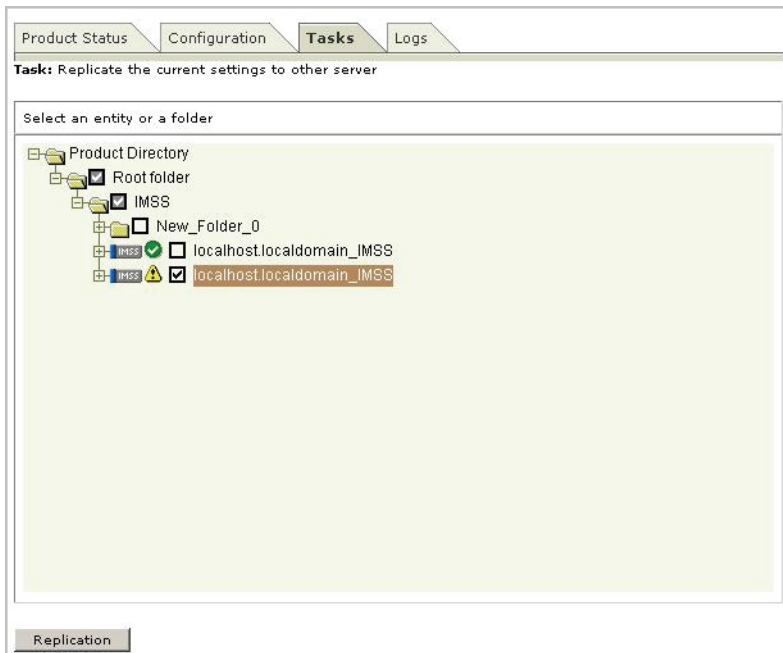
To replicate IMSVA settings:

1. Choose **Products** from the Control Manager menu.
2. Locate the source IMSVA scanner from the Product Directory on the left of the user interface.
3. Click the **Tasks** tab.

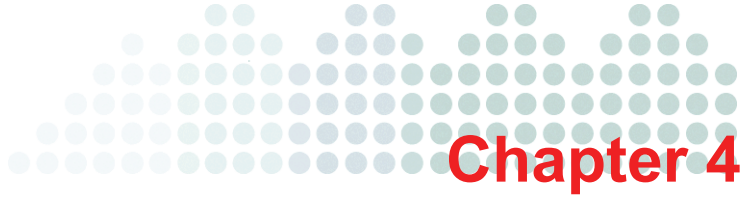
4. Select **Configuration Replication** from the drop-down list.



5. Click **Next**.
6. Select the check box next to the target server.



7. Click the **Replication** button.



Maintenance

This chapter provides you with general instructions on the tasks that you need to perform for the day-to-day maintenance of IMSVA. For more information on each field on the Web management console, please refer to the Online Help.

Topics include:

- [Monitoring Your Network on page 4-2](#)
- [Logs on page 4-18](#)
- [Quarantine and Archive on page 4-26](#)
- [Event Notifications on page 4-41](#)
- [Managing Administrator Accounts on page 4-49](#)
- [Configuring Connection Settings on page 4-53](#)

Monitoring Your Network

IMSVA provides a complete set of tools that enable you to monitor your network traffic. You can obtain useful information such as the statistics on the performance of IMSVA components, or generate reports that display a breakdown of messages matching various scanning conditions.

Viewing the Real-time Statistics

You can obtain up to the last 24 hours' of statistics on the performances of IMSVA scanners and IP profilers. These statistics provide useful information to help you better manage your IMSVA policies and enhance the security of your network.

The Real-time Statistics Summary screen shows the following information:

- **System Overview:** Device CPU and memory usage, the number of mails in the delivery queue and deferred queue, and the data partition size in use.
- **IMSVA Scan Performance**
 - **Messages Processed:** The incoming, outgoing, and total number of messages that IMSVA processed. The processing speed is also displayed in messages per minute.
 - **Scanning Conditions:** The scanning conditions that were violated. Message counts will overlap. The percentage in column refers to the total number of messages.
- **IP Filtering Performance:** The type of threat IMSVA blocked using the IP filtering product.

Note: If you use Internet Explorer 7.0 to browse Web management console, Internet Explorer 7.0 might block the access. Please click the **Continue to this website (not recommended)** link to view the management console.

To view the statistics:

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.
2. Select the device from the **Host** drop-down list.
3. Select the desired last # minutes/hours from the **Show** drop-down list.

Note: IMSVA automatically updates these statistics in its database every 5 minutes.

Interpreting the Real-time Statistics

IMSVa presents performance statistics in both graphical and table formats. This section explains how the values in the System Overview, IMSVA Scan Performance, and IP Filtering Performance sections on the Real-time Statistics tab are derived.

Note: In the table, the total number of messages matching each scanning condition or IP filtering type consists of overlaps. For example, if a message matches more than one scanning condition, such as spam and attachment, this message will be counted twice, once in the total number for spam and a second time in the total number for attachment. Values in the chart, however, do not include such overlaps.

System Overview

This section shows the system information of the devices that you select from the **Host** drop-down list. If you select **All servers**, IMSVA will display the system information for all the devices within a group.

Note:

1. The data partition stores IMSVA logs and databases.
2. The queue partition stores messages in the delivery, quarantined, postponed, and deferred queues.

Summary 



Trend Micro Antivirus and Content Filter has not been activated.
You must activate your product to enable scanning and security updates.[More info](#)



Spam Prevention Solution (SPS) has not been activated.
You must activate your product to enable scanning and security updates.[More info](#)

Real-time Statistics

System

Host: Show: 

System Overview

Host	CPU Usage	Memory Usage	Mails in Delivery Queue	Mails in Deferred Queue	Queue Partition in Use (MB)	Data Partition in Use (MB)
rd.imsa	0.41%	72.24%	0	0	76(0%)	527(0%)

IMSVA Scan Performance

This section shows a breakdown of the total number of messages processed in terms of the following:

- Number of incoming and outgoing messages, and their corresponding values in percentages of the total.
- Number of messages matching various types of scanning conditions specified in the policy rules, and their corresponding values in percentages of the total.

The chart and table are interpreted as follows:

- **Chart**

IMSVA displays a maximum of 12 bars in the chart. The duration represented by each bar depends on the period you select from the **Show** drop-down list. For example, if you choose to view the scan performance of the **Last 60 minutes**, each bar represents 5 minutes' worth of messages scanned.

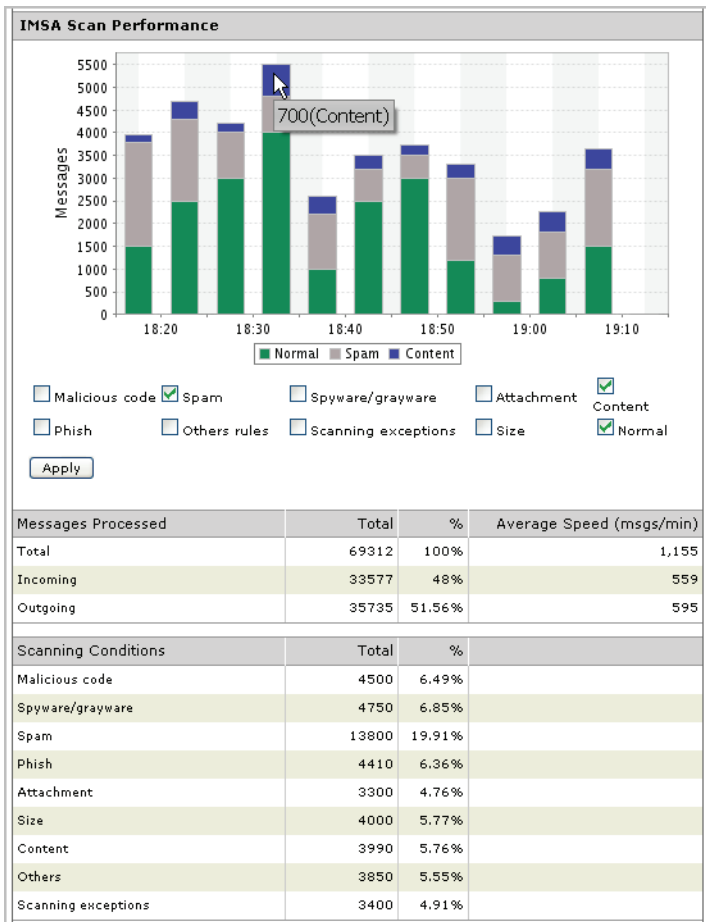
You can choose to view the statistics for messages matching all the scanning conditions, or for messages matching only selected conditions.

To view the statistics for messages matching only specific scanning conditions:

- Select the check box(es) next to the desired scanning condition(s).
- Click **Apply**.

- **Table**

Numbers in the table show the messages matching each scanning condition.



Viewing System Summary Statistics

These statistics provide useful information to help you better manage your IMSVA policies and enhance the security of your network.

To view the statistics:

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.

2. Click the **Systems** tab.

From the System Summary screen, you can manage the following:

- **Enable Connections:** The connections currently enabled (POP3, NRS and IP Profiler).

To enable or disable connections:

- a. Select or clear the check box next to a connection item.
- b. Click **Save**.

- **Components:** The version numbers of the antivirus, anti-spyware, and anti-spam components that IMSVA uses to protect your network.

To manually update components:

- a. Select the check box next to the component to update.
- b. Click **Update**.

To roll back to the previous version of the components:

- a. Select the check box next to the component to roll back.
- b. Click **Rollback**.

To refresh the page:

- Click **Refresh** to connect to the update source and display the latest component versions in the Availability column.
- **Managed services:** Other IMSVA servers registered to this IMSVA admin database.

To start or stop managed server services:

- Click **Start** or **Stop** under the service to change.

To unregister managed server services:

- When a managed server is inactive (it is disconnected from the IMSVA server), the Unregister button will appear in the Connection column next to the specific server. To unregister the managed server from this IMSVA server, click **Unregister**.
- A managed server could become disconnected for any of the following reasons:
 - You removed the scanner.
 - The IMSVA manager service stopped.

- The scanner server is shut down.

IP Filtering Performance

This section shows the number of connections blocked by the following:

- The four types of IP Filtering rules, namely, spam, virus, DHA attack, and bounced mail
- IP addresses that you have manually entered
- NRS

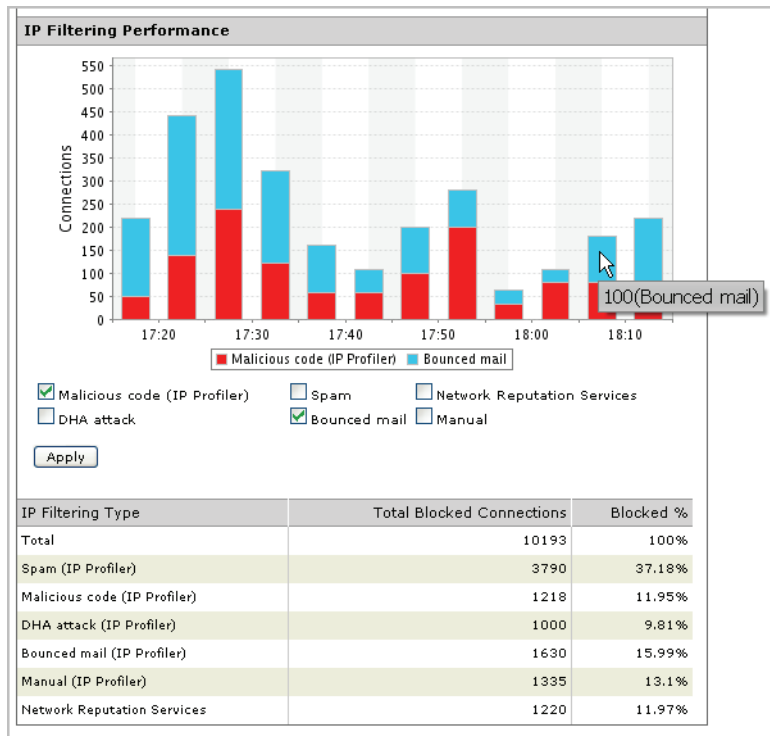
Values in the chart and table are computed as follows:

Value = Number of messages matching the specific IP filtering rule divided by the total number of messages blocked by IP Profiler and NRS.

Example:

Total number of messages blocked by IP Profiler and NRS = 360

Percentage of spam messages: $22\% = 80 / 360$



Generating Reports

Depending on your needs, you can choose to generate a one-time report on demand or schedule a report to be run at specific intervals. IMSVA offers you the flexibility of specifying the content for each report and the option of viewing or saving the result in HTML or CSV format.

Types of Report Content

You can choose from the following types of content to be included in the report:

TABLE 4-1. Report content descriptions

REPORT CONTENT	DESCRIPTIONS
Policy and traffic summary	Shows the total number and size of incoming and outgoing messages. Also shows the number of messages matching specific scanning conditions.
Virus and malicious code summary	Shows a summary of the virus message count by actions.
Spam summary	Shows a summary of the total spam message count by anti-spam engine, NRS, IP Profiler, and actions.
Sender IP address blocking summary	Includes "IP Profiler Blocking Summary" and "NRS Blocking Summary". The former shows a summary of the total number of sender connections that reached IP Profiler and are blocked by the different IP Filtering rules. The latter shows the total sender connections that reached NRS and are blocked by NRS.
Top 10 traffic email addresses	Shows the top 10 email addresses ranked by the total sent and received message count.
Top 10 virus names	Shows the top 10 virus names ranked by their detected count.
Top 10 IP addresses for DHA attack addresses	Shows the top 10 IP addresses ranked by the blocked count for DHA attack.
Top 10 IP addresses for bounced mail attack addresses	Shows the top 10 IP addresses ranked by the blocked count for bounced mail attack.

TABLE 4-1. Report content descriptions

REPORT CONTENT	DESCRIPTIONS
Top 10 virus recipients and senders	Shows the top 10 virus recipients and senders ranked by their total received and sent virus message count respectively.
Top 10 most frequently triggered rule names	Shows the top 10 rule names ranked by the number of messages that triggered each rule.
Top 10 spam recipients	Shows the top 10 spam recipient addresses ranked by their total received spam message count.
Top 10 IP addresses blocked by NRS	Top 10 blocked IP addresses ranked by the number of connections dropped by NRS.
Top 10 IP addresses blocked by spam	Top 10 IP addresses ranked by the blocked count for spam.
Top 10 IP addresses blocked by viruses or malicious code	Top 10 IP addresses ranked by the blocked count for viruses.

Managing One-time Reports

Generate a one-time report for an at-a-glance summary of IMSVA protection as it is now. For future reference, IMSVA retains all one-time reports on this screen.

You can also enable IMSVA to automatically generate daily, weekly, or monthly reports.

To manage one-time reports:

1. Choose **Reports > One-time Report** from the menu. The One-time Reports screen appears with a list of the one-time reports that you previously generated.
2. To change the display, do any of the following:
 - To sort the table, click any of the column headings.
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select a number from the drop down box that represents which page to view.
 - To change the number of items that appear in the list at one time, select a new display value from the drop down box on the bottom of the table.

3. To generate a report, click **Add**. The report takes several minutes to generate. In progress appears in the Output column if the report is not finished generating.
4. To view the report, click one of the following formats under **Output**:
 - **HTML**: Opens the report in another browser window.
 - **CSV**: Saves the report as a comma separated value file that you can open with a spreadsheet application.
5. To delete a report, select the check box next to it and click **Delete**.

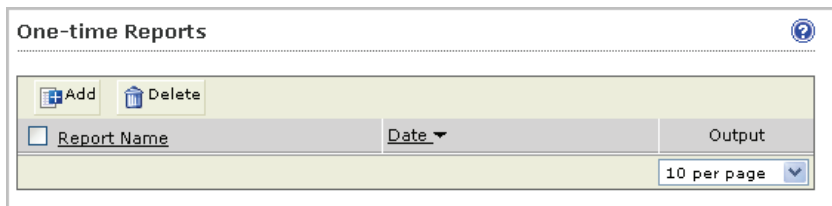
Note: NRS and IP Profiler report content is not available unless you activate those products. For more information on activating NRS and IP Profiler, see [Managing Product Licenses on page 4-60](#).

Adding One-time Reports

You can generate one-time reports on demand to help monitor the traffic on your network.

To create a one-time report:

1. Choose **Reports > One-time Report** from the menu.



The screenshot shows the 'One-time Reports' interface. At the top, there is a title bar with a question mark icon. Below the title bar, there are two buttons: 'Add' (with a plus icon) and 'Delete' (with a trash icon). Below these buttons is a table with three columns: 'Report Name', 'Date', and 'Output'. The 'Report Name' column has a checkbox next to it. The 'Date' column has a dropdown arrow. The 'Output' column is currently empty. At the bottom right of the table, there is a '10 per page' dropdown menu.

2. Click **Add**. The Add One-time Report screen appears.

Add one-time Report

Name:

Dates: to:
mm/dd/yyyy hh mm/dd/yyyy hh

☐ **Report Content**

- ☒ Policy and traffic summary
- ☐ Virus and malicious code summary
- ☐ Spam summary
- ☐ Sender IP address blocking summary
- ☐ Top 10 traffic email addresses
- ☐ Top 10 virus names
- ☐ Top 10 IP addresses for DHA attack addresses
- ☐ Top 10 IP addresses for bounced mail attack addresses
- ☐ Top 10 virus recipients and senders
- ☐ Top 10 most frequently triggered rule names
- ☐ Top 10 spam recipients
- ☐ Top 10 IP addresses blocked by NRS
- ☐ Top 10 IP addresses blocked for spam
- ☐ Top 10 IP addresses blocked for viruses or malicious code

3. Next to **Name**, type a descriptive name.
4. Next to **Dates**, select the time span that the report will cover.
5. Under **Report Content**, select the content to include in the report.
6. Click **Save**. The report takes several minutes to generate. The message **In progress** appears in the report table.

One-time Reports

1-1 of 1 Page 1

☐ Report Name	Date	Output
☐ Policy & traffic summary	December 25, 2006 9:11:58 AM	In progress

10 per page

After the report generates, the hyperlinks **HTML** and **CSV** display in the report table.

One-time Reports 

 Add  Delete

1-3 of 3   Page

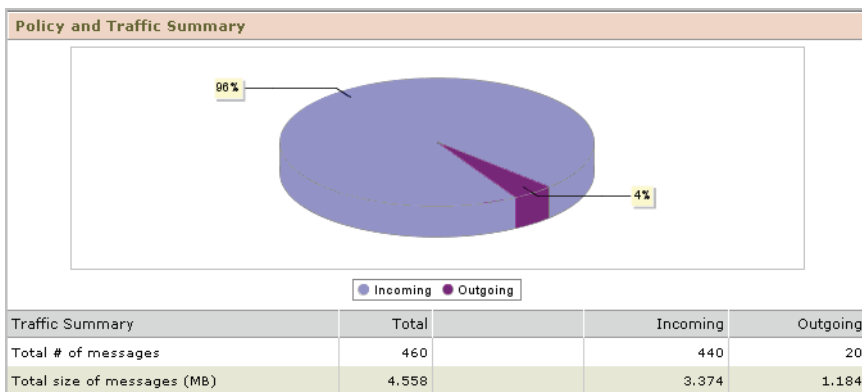
1 

☐ Report Name	Date 	Output	
☐ Top 10 traffic email addr	December 25, 2006 9:17:30 AM	HTML	CSV
☐ Virus and malicious code	December 25, 2006 9:17:05 AM	HTML	CSV
☐ Policy and traffic summary	December 25, 2006 9:15:47 AM	HTML	CSV

10 per page 

7. Click **HTML** to display the report in HTML format.
8. Click **CSV** to export the report data to a csv file.



Note: Report generation occurs once every five minutes. This means that report generation could require as much as five minutes in addition to the time required to aggregate reporting data and make the necessary calculations.

Using Scheduled Reports

Schedule reports to automate report generation. IMSVA offers daily, weekly, and monthly reports.

To manage scheduled reports:

1. Click **Reports > Scheduled Reports** from the menu. The Schedule Reports screen appears with the **Daily** tab displayed.
2. Click the **Weekly** or **Monthly** tab to view the corresponding reports.
3. To view the report, click one of the following formats under **Output**:
 - **HTML**: Opens the report in another browser window.
 - **CSV**: Saves the report as a comma separated value file that you can open with a spreadsheet application.
4. To change the display, do one of the following:
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page.
 - To change the number of items that appears in the list at one time, select a new display value from the drop-down box on the bottom of the table.
5. To delete a report, select the check box next to it and click **Delete**.

Configuring Scheduled Reports

Scheduled reports generate automatically according to the intervals you configure.

To create a scheduled report:

1. Choose **Reports > Settings** from the menu. The Scheduled Report Settings screen appears.

Scheduled Report Settings

Report Type	Status	Schedule	Configure	# to Save
Daily reports		2:00	Settings	60
Weekly reports		Sunday at 2:00	Settings	20
Monthly reports		Date 0at 2:00	Settings	5

Save

Cancel

2. Click the **Settings** link for one of the following report types:

- Daily reports
- Weekly reports
- Monthly reports

The Report Settings screen appears.

Daily Report Settings

[Scheduled Report Settings](#) > Daily Report Settings

☒ **Generate daily reports**

Start time: 14
hh

☐ **Report Content**

- ☒ Policy and traffic summary
- ☒ Virus and malicious code summary
- ☐ Spam summary
- ☒ Sender IP address blocking summary
- ☐ Top 10 traffic email addresses
- ☐ Top 10 virus names
- ☐ Top 10 IP addresses for DHA attack addresses
- ☐ Top 10 IP addresses for bounced mail attack addresses
- ☐ Top 10 virus recipients and senders
- ☐ Top 10 most frequently triggered rule names
- ☐ Top 10 spam recipients
- ☐ Top 10 IP addresses blocked by NRS
- ☐ Top 10 IP addresses blocked for spam
- ☐ Top 10 IP addresses blocked for viruses or malicious code

3. Specify your settings for the report.

Note: When configuring monthly report settings, if you choose to generate the report on the 29th, 30th, or 31st day, IMSVA will generate the report on the last day of the month for months with fewer days. For example, if you select 31, IMSVA will generate the report on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

4. Click **Save**. The report status changes.

Scheduled Report Settings


Report Type	Status	Schedule	Configure	# to Save
Daily reports		12:00	Settings	60
Weekly reports		Sunday at 2:00	Settings	20
Monthly reports		Date 0 at 2:00	Settings	5

5. Specify the number for each type of report that you would like to retain. Click **Save**.
6. Choose **Reports > Scheduled Reports** from the menu. The Scheduled Reports screen appears.

Note: The report has not generated yet.

Archived Scheduled Reports


Daily
Weekly
Monthly

 Delete

☐ Archived Reports

Output

10 per page


7. After the report generates, you can click **HTML** or **CSV** to view the report.

Archived Scheduled Reports	
Daily Weekly Monthly	
Delete	1-6 of 6
1-6 of 6 Page 1	
Archived Reports	Output
☐ December 3, 2007	HTML CSV
☐ December 2, 2007	HTML CSV
☐ December 1, 2007	HTML CSV
☐ November 30, 2007	HTML CSV
☐ November 27, 2007	HTML CSV
☐ November 26, 2007	HTML CSV
15 per page	

Logs

Logs are a useful means of enabling you to monitor various types of events and information flow within IMSVA. They also serve as an important resource for troubleshooting purposes.

To enable logs and benefit from the information, do the following:

- Step 1:** Configure the log settings. For details, see [Configuring Log Settings on page 4-24](#).
- Step 2:** Perform log query.

Querying Logs

You can perform queries on five types of events or information:

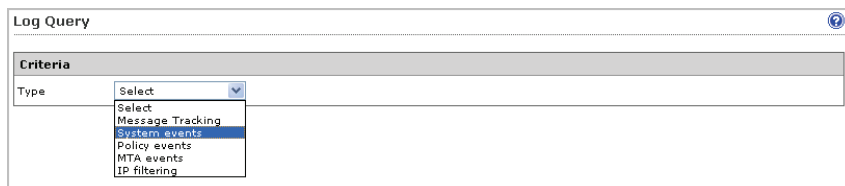
- **Message tracking:** Records message details such as the sender, recipient(s), message size, and the final action that IMSVA has taken. In the case of quarantined messages, the query result will also indicate the name and type of the policy rule that was triggered.
- **System events:** Tracks the time of system events such as user access, modification of rules, registration of Control Manager agent and so on.
- **Policy events:** Provides details on the policy rules that were triggered, the actions taken, and the message details.

- **MTA logs:** Provides connection details of Postfix on the local computer where the central controller is installed.
- **IP Filtering:** Provides the time when IMSVA started and stopped blocking email messages from the queried IP address.

For most log queries, IMSVA supports wildcards (*) and exact matches (for example, to view mail recipients whose name includes A or B, set the recipient(s) to “*A*; *B*”). IMSVA uses exact matching by default. Leaving the search condition blank displays all logs. For multiple-conditions items, use semicolons (;) to separate the entries for recipient(s) and attachment(s).

To query message tracking logs:

1. Choose **Logs > Query** from the menu. The Log Query screen appears.



The screenshot shows a web interface titled "Log Query". Under the "Criteria" section, there is a "Type" label followed by a dropdown menu. The dropdown menu is open, displaying a list of options: "Select", "Message Tracking", "System events", "Policy events", "MTA events", and "IP filtering". The "Message Tracking" option is currently selected and highlighted in blue.

2. Next to **Type**, select **Message tracking**. The query screen for message event logs appears.
3. Next to **Dates**, select a date and time range.
4. Type any of the following additional information:
 - **Subject**
 - **Message ID**
 - **Sender**
 - **Recipient(s):**

Note: Use the asterisk wildcard for partial searches on any field.

5. Click **Display Log**. A timestamp, sender, recipient, subject, and last known action appear for each event.
6. Click the timestamp link to see the following information:

- **Timestamp**
- **Sender**
- **Recipient**
- **Subject**
- **Message size in MB**
- **Message ID**
- **Internal ID**
- **Scanner that detected the message**
- **Final action that IMSVA took on the message**
- **Action details**

7. Perform any of the additional actions:

- To change the number of items that appears in the list at one time, select a new display value from the drop-down box on the top of the table.
- To print the query results, click **Print current page**.
- To save the query result to a comma separated value file, click **Export to CSV**.

To query system event logs:

1. Choose **Logs > Query** from the menu.
2. Next to **Type**, select **System events**. The query screen for system event logs appears.
3. In the second drop down box next to **Type**, select one of the following:
 - **All events:** Displays the timestamp and descriptions for all system events.
 - **Updates:** Displays the timestamp of successful scan engine and pattern file updates from the ActiveUpdate server to the IMSVA admin database.
 - **Service Status:** Displays the timestamp and descriptions when the scanner service is started or stopped.
 - **Admin activity:** Displays the timestamp and descriptions for major admin activities such as changing IMSVA settings, admin account logons and logoffs.
 - **Errors:** Displays the timestamp and descriptions for all errors that IMSVA encountered, such as unsuccessful update of the scan engine and pattern files.
4. In the third drop down box next to **Type**, select the server to view.
5. Next to **Dates**, select a date and time range.

6. Next to **Keyword in description**, type any special words to search for.
7. Click **Display Log**. A timestamp, component, and description appear for each event.
8. Perform any of the additional actions:
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the top of the table.
 - To sort the table, click the column title.
 - To print the query results, click **Print current page**.
 - To save the query result to a comma separated value file, click **Export to CSV**.

To view policy event logs:

1. Choose **Logs > Query** from the menu.
2. Next to **Type**, select **Policy events**. The query screen for policy event logs appears.
3. In the second drop down box next to **Type**, select one of the following items related to the policy and the rules you configured for the policy:
 - **All**
 - **Virus and malicious code**
 - **Spam**
 - **Attachment name or type**
 - **Size**
 - **Content**
 - **Others**
 - **Scanning exceptions**
4. Type any of the following additional information:
 - **Senders**
 - **Recipient(s)**
 - **Rule**
 - **Subject**
 - **Attachment(s)**
 - **Message ID**

Note: If you leave any text box blank, all results for that item appear.

5. Click **Display Log**. A timestamp, action, rule, and message ID appear for each event.
6. Click the timestamp link to see the following information:
 - **Timestamp**
 - **Sender**
 - **Recipient**
 - **Subject**
 - **Message size in MB**
 - **Violating attachment**
 - **Rule type**
 - **Rule(s)**
 - **Action details**
 - **Message ID**
 - **Internal ID**
 - **Scanner that detected the message**
7. Perform any of the additional actions:
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the top of the table.
 - To sort the table, click the column title.
 - To print the query results, click **Print current page**.
 - To save the query result to a comma separated value file, click **Export to CSV**.

Note:

- “*A*;*B*” means a string that has A or B.
- “A*;*B” means a string that starts with A or ends with B.
- “;” represents the OR operation.

To query MTA event logs:

1. Choose **Logs > Query** from the menu.
2. Next to **Type**, select **MTA events**. The query screen for MTA event logs appears.
3. Next to **Dates**, select a date and time range.
4. Next to **Keyword in Description**, type the keyword to search for.
5. Click **Display Log**. A timestamp and MTA event description appears.
6. Perform any of the additional actions:
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the top of the table.
 - To print the query results, click **Print current page**
 - To save the query result to a comma separated value file, click **Export to CSV**.

To view IP filtering logs:

1. Choose **Logs > Query** from the menu.
2. In the second drop down box next to **Type**, select one of the following items related to IP Filtering:
 - **NRS**
 - **DHA attack**
 - **Bounced mail**
 - **Virus**
 - **Spam**
 - **Manual:** Refers to the IP addresses that you have manually entered into the blocked list.
 - **All**
3. Next to **Dates**, select a date and time range.
4. Next to **IP**, provide any IP address or domain name to search for.
5. Click **Display Log**. Information appears for the time that InterScan both started and stopped blocking each IP address or domain.
6. Perform any of the additional actions:
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the top of the table.
 - To print the query results, click **Print current page**.

- To save the query result to a comma separated value file, click **Export to CSV**.

Configuring Log Settings

You can configure the level of detail that IMSVA writes to the logs and the length of time it stores them. In addition, you can set the update period that controls how frequently the scanner services write their local logs to the IMSVA admin database.

To configure log settings:

1. Choose **Logs > Settings** from the menu.
2. Under **Reporting Logs**, configure the following:
 - **Database log update interval:** IMSVA updates the logs regularly at every interval. Select a number between 1 and 60 for the interval. Selecting 60 means that IMSVA updates the logs once every hour.
 - **Number of days to keep reporting logs:** Type a value between 1 and 60 that represents the number of days IMSVA preserves the report logs in the IMSVA admin database.
3. Under **Log Files**, configure the following:
 - **Application log detail level:** The level of log detail. Select one of the following:
 - **Normal:** The standard level of detail. This level provides the basic information needed by an administrator for daily monitoring and maintenance.
 - **Detailed:** A high level of detail. All IMSVA processes write detailed information to the logs, including: telnet session information, the policy matched, the filter executed, and the action taken.
 - **Diagnostic:** Comprehensive information on each event or action. Diagnostic level logs include all information from the detailed level, plus SMTP routing information, and the route match information that determined which policy was applied.
 - **Debug:** The most complete and verbose level of detail. Debug logs are only recommended when troubleshooting.

Note: Diagnostic or Debug logs might consume excessive IMSVA resources and could lower system performance.

- **Number of days to keep log files:** Select the check box and type a number between 1 and 99999 that represents the number of days IMSVA keeps the local log files. To prevent IMSVA from deleting the log files, clear the check box.
 - **Maximum log file size for each service:** Select the check box and type a number between 100 and 2048 that represents the size in MB for local log files for each type of process or service. To remove any size restriction, clear the check box.
-

Note: - IMSVA log files are stored in the folder /opt/trend/imss/logs. IP Profiler log files are stored in the folder /opt/trend/ipprofiler/logs.

- Daily log files for each event type are created at midnight and have the suffix of "<Date>.<Count>". The <Count> suffix is incremented if there is more than one (1) log file per day.

- If the log file size exceeds the maximum log file size for each service, IMSVA will delete the oldest file.

4. Click **Save**.

Quarantine and Archive

IMSVA stores messages matching specific policy rule actions in the following areas and queues:

- **Quarantine Area:** Stores messages that you would like to analyze before deciding whether to delete or release to the intended recipient(s).
- **Archive Area:** Stores messages for future reference.
- **Postponed Queue:** Stores messages that will be delivered at a specified time.
- **Deferred Queue:** Stores messages that IMSVA is unable to deliver to the next MTA. IMSVA will try to resend the message every 1000 seconds. If IMSVA is still unable to deliver the message within 24 hours, the message will be returned to the sender.

Configuring Quarantine and Archive Settings

Quarantine and archive settings allow you to manage these areas and allocate the amount of disk space per scanner for storing quarantined or archived messages.

To configure quarantine and archive settings:

1. Choose **Mail Areas & Queues > Settings** from the menu. The Quarantine and Archive Settings screen appears.

Area	Expiration	Size	Items
☐ Default Quarantine	15 day(s)	0MB	0

2. To configure a quarantine area or an archive area, click the **Quarantine** tab (default) or **Archive** tab respectively. The list of areas appears in the table below.
3. To modify the total disk size allowed for all quarantine areas or archive areas for each scanner service, type the size of the area next to **Disk quota (per scanner)**, and then select **MB** or **GB** from the drop down box.

4. To add a quarantine or archive area, click **Add** and do the following:
5. Next to **Name**, type a descriptive name.
6. Next to **Delete messages older than**, type the number of days after which InterScan deletes the quarantined or archived messages. The value is exclusive. For example, if you type 15, IMSVA deletes the quarantined messages on the 16th day.
7. Click **Save**. The Quarantine and Archive Settings screen reappears.
8. To view or modify a quarantine or archive area, click the name of the area and configure the settings above.
9. To delete a quarantine or archive area, select the check box next to it and click **Delete**.
10. After modifying any settings, click **Save**.

Managing Quarantine Areas

IMSVa can quarantine messages on the server in the
\$IMSVa_HOME\queue\quarantine directory.

Tip: Trend Micro recommends quarantining messages that you think you might want to analyze and possibly send to the intended recipient later. Create different types of quarantine areas for different types of email, such as email that violates spam scanning conditions or email that violates message content conditions.

You can get to a screen to modify quarantine areas from one of the following screens:

From the Actions screen of a policy rule:

If you are configuring the actions for a rule, do the following:

1. Click **Edit** next to **Quarantine to** under **Intercept** actions. The Quarantines screen appears showing the available quarantine areas.
2. To add a new quarantine area, click **Add**. To modify an existing quarantine area, click the area name and then click **Edit**. An edit screen appears.
3. Next to **Name**, type the name of the quarantine area.
4. To automatically delete quarantined email after a certain number of days, next to **Delete messages older than**, type the number of days from 1 to 60. This number represents the number of days after which IMSVA deletes the quarantined messages.

The value is exclusive. For example, if you type 15, IMSVA deletes the quarantined messages on the 16th day.

5. Click **Save** to return to the Quarantines screen.
6. Click **Done** to continue selecting actions.
7. To quarantine messages, select the radio button next to **Quarantine to** under **Intercept** and select the desired quarantine area from the drop down box.

From Mail Areas & Queues > Settings:

1. Click **Mail Areas & Queues > Settings**. The Quarantine and Archive settings screen appears with the **Quarantine** tab displayed by default.
2. Next to **Disk quota per scanner service**, do the following:
 - a. Type the maximum size for the area.
 - b. Select **MB** or **GB**.

Note: When the total disk size for all the quarantined email messages exceed the quota on a scanner, the oldest quarantined messages are deleted first to keep the size under the quota.

3. To add a new quarantine area, click **Add**. To modify an existing quarantine area, click the area name. An edit screen appears.
4. Next to **Name**, type the name of the quarantine area.
5. To automatically delete quarantined email after a certain number of days, next to **Delete messages older than**, type the number of days from 1 to 60. This number represents the number of days after which IMSVA deletes the quarantined messages. The value is exclusive. For example, if you type 15, IMSVA deletes the quarantined messages on the 16th day.
6. Click **Save** to return to the Quarantine and Archive Settings screen.
7. Click **Save**.

Querying Messages

You can perform a query on quarantined and archived messages before deciding on the action to be taken. After viewing the message details, you can choose to release or delete the quarantined messages, or delete archived messages from IMSVA.

Tip: Trend Micro recommends quarantining items that could pose a risk to your network, such as messages and attachments that violate antivirus rules. Before you resend any quarantined message, make sure that it does not pose a threat to your network.

Trend Micro recommends archiving only items that you want to reference later. You should quarantine items that could pose a threat to your network, such as email messages and attachments that violated an antivirus rule.

To query quarantine areas:

1. Choose **Mail Areas & Queues > Query** from the menu. The Quarantine and Archive Query screen appears. The **Quarantine** tab displays by default. If it does not display, click **Quarantine**.

Mail Areas & Queues Management

Quarantine Archive Postpone Deferred

Criteria

Search: Any quarantine Any reason All System

Dates: 11/21/2007 08:11 to 11/21/2007 09:11
mm/dd/yyyy hh mm mm/dd/yyyy hh mm

Sender: Subject:

Recipient(s): Attachment(s):

Rule: Message ID:

Display Log

2. Under **Criteria**, configure the following:
 - **Search:** Select the quarantine area, the reason the email was quarantined, and the scanner that scanned the email.
 - **Dates:** Select a date and time range.
3. Type values for the following:
 - **Sender**
 - **Subject**
 - **Recipient**

- **Attachment**
 - **Rule**
 - **Message ID**
-

Note: When querying an email containing multiple recipients or attachments, type *string* (where string is the name of one of the recipients or attachments).

4. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject and reason for quarantining the message.
 5. To change the display, do any of the following:
 - To sort the table, click any of the column headings (except reason).
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select the desired page to view from the drop-down list.
 - To change the number of items that appears in the list at one time, select a new display value from the drop-down list on the bottom of the table.
 6. To view details about any quarantined message, click the timestamp for the item. The Quarantine Query screen appears showing the email message and all of its details.
 7. To resend any message, click the check box next to it in the query result table, and then click **Release**.
-

Tip: Trend Micro does not recommend resending email messages that violated antivirus filters. Doing so could put your network at risk.

8. To delete any message, click the check box next to it in the query result table, and then click **Delete**.
-

Note: IMSVA only records and shows names of attachments if you have specified Attachment as a scanning condition. However, if the number of attachments in the email exceeds the maximum number specified in the condition, the attachment name will not be shown.

To query archive areas:

1. Choose **Mail Areas & Queues > Query** from the menu. The **Quarantine** tab displays by default.
2. Click the **Archive** tab.
3. Under **Criteria**, configure the following:
 - **Search:** Select the archive area, the reason the email was archived, and the scanner that scans the email.
 - **Dates:** Select a time range.
4. Type values for the following:
 - **Sender**
 - **Subject**
 - **Recipient**
 - **Attachment**
 - **Rule**
 - **Message ID**

Note: When querying an email containing multiple recipients or attachments, type `*string*` (where string is the name of one of the recipients or attachments).

5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject and reason for archiving the message.
6. To change the display, do any of the following:
 - To sort the table, click any of the column headings (except reason).
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select the desired page to view from the drop-down list.
 - To change the number of items that appears in the list at one time, select a new display value from the drop-down list on the bottom of the table.
7. To view details about any archived message, click the timestamp for the item. The Archive Query screen appears showing the email message and all of its details.
8. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

Note: IMSVA only records and shows names of attachments if you have specified Attachment as a scanning condition. However, if the number of attachments in the email exceeds the maximum number specified in the condition, the attachment name will not be shown.

To query postponed messages:

1. Choose **Mail Areas & Queues > Query** from the menu. The Quarantine tab displays by default.
2. Click the **Postpone** tab.
3. Under **Criteria**, configure the following:
 - **Search:** Select the reason and device.
 - **Dates:** Select a date and time range.
4. Type values for the following:
 - **Sender**
 - **Subject**
 - **Recipient(s)**
 - **Attachment(s)**
 - **Rule**
 - **Message ID**
5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, subject, and reason for postponing the message.
6. To change the display, do any of the following:
 - To sort the table, click any of the column headings (except reason).
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select that number from the drop down box that represents which page to view.
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the bottom of the table.
7. To view details about any postponed message, click the **Timestamp** for the item. The email message and all of its details appears.
8. To resend any message, click the check box next to it in the query result table, and then click **Release**.

9. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

To query deferred messages:

1. Choose **Mail Areas & Queues > Query** from the menu. The **Quarantine** tab displays by default.
2. Click the **Deferred** tab.
3. Under **Criteria**, configure the following:
 - **Search:** Select the device.
 - **Dates:** Select a date and time range.
4. Type values for the following:
 - **Sender**
 - **Recipient(s)**
 - **Reason**
5. Click **Display Log**. The results appear at the bottom of the screen showing the timestamp, sender, recipient, size, the reason for deferring the message, and the host (or device).
6. To change the display, do any of the following:
 - To sort the table, click any of the column headings.
 - If too many items appear on the list, click the arrow buttons on top of the list to move to the next page or select a number from the drop down box that represents which page to view.
 - To change the number of items that appears in the list at one time, select a new display value from the drop down box on the bottom of the table.
7. To view details about any deferred message, click the **Timestamp** for the item. The email message and all of its details appears.
8. To resend any message, click the check box next to it in the query result table, and then click **Release**.
9. To delete any message, click the check box next to it in the query result table, and then click **Delete**.

Note: If you reconfigure a device as a child device and it has deferred messages in its deferred queue, then you register it to a parent device, you will not be able to view any of the original deferred messages on the child device from the parent device Web console. Handle all deferred messages before changing device roles.

Viewing a Quarantined Message

To view a quarantined message:

1. After you perform a query for quarantined messages, click the timestamp for the quarantined item in the query result table. The Quarantine Query screen appears showing the following information:
 - **Timestamp**
 - **Message ID**
 - **Sender**
 - **Reason**
 - **Recipient**
 - **Rules**
 - **Subject**
 - **Scanner**
 - **Size**
 - **Internal ID**
 - **Attachments**
2. Next to **Message view**, click either **Header** or **Message**.
3. Click any of the following buttons:
 - **Back to List:** Return to the query screen.
 - **Release:** Resend the message to its original recipients.
 - **Delete:** Delete the message.
 - **Download:** Save the message to your computer.

Tip: Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Viewing Archived Messages

To view archived messages:

1. After you perform a query for archived messages, click the timestamp for the quarantined item in the query result table. The Archive Query screen appears showing the following information:
 - **Timestamp**
 - **Message ID**
 - **Sender**
 - **Reason**
 - **Recipient**
 - **Rules**
 - **Subject**
 - **Scanner**
 - **Size**
 - **Internal ID**
 - **Attachments**
2. Next to **Message view**, click either **Header** or **Message**.
3. Click any of the following buttons:
 - **Back to List:** Return to the query screen.
 - **Delete:** Delete the message.
 - **Download:** Save the message to your computer.

Tip: Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Viewing Postponed Messages

To view a postponed message:

1. After you perform a query for postponed messages, click the **Timestamp** for the postponed item in the query result table. The query screen appears showing the following information:
 - **Timestamp**
 - **Message ID**
 - **Sender**
 - **Reason**
 - **Recipient**
 - **Rules**
 - **Subject**
 - **Scanner**
 - **Size**
2. Next to **Message view**, click either **Header** or **Message**.
3. Click any of the following buttons:
 - **Back to List:** Return to the query screen.
 - **Release:** Resend the message to its original recipients.
 - **Delete:** Delete the message.
 - **Download:** Save the message to your computer.

Tip: Trend Micro does not recommend saving messages or attachments that violated an antivirus rule.

Viewing Deferred Messages

To view a deferred message:

1. After you perform a query for deferred messages, click the **Timestamp** for the item in the query result table. The query screen appears showing the following information:
 - **Arrival Time**

- **Sender**
- **Host**
- **Size**
- **Message ID**

Each recipient and corresponding reason appear at the bottom of the screen.

2. Perform any of the additional actions:

- To change the number of items that appears on a page at one time, select a new display value from the **Display** drop down box on the upper right of the list.
- To move to another page, select a number from the drop down box to the right, or click one of the arrow icons.

3. Click any of the following buttons:

- **Back to List:** Return to the query screen.
- **Release:** Resend the message to its original recipients.
- **Delete:** Delete the message.

Configuring User Quarantine Access

You can grant all users or selected end-users access to the EUQ Web console so that they can manage the spam messages addressed to them by visiting `https://<target server IP address>:8447`.

To configure user quarantine access:

1. Click **Administration > End-User Quarantine**. The End-User Quarantine screen appears.
2. Click the **User Quarantine Access** tab. The User Quarantine Access screen appears.

User Quarantine Access ?

These groups can access quarantined spam items and will use LDAP authentication with the designated IMSS server.

☒ Enable access ⓘ

Keep quarantined spam for: 7 days ▾

Set maximum number of approved senders

Maximum approved senders per end-user: 50 ▾

Specify login page greeting

Enter the greeting displayed to the user after logon. Specify a new line using
. Optionally use HTML to specify the greeting text format.

Select LDAP groups to enable access

☒ Enable All

Select groups from LDAP Search below.

Search LDAP groups ▾

Search

Selected Groups

>> <<

Save Cancel

3. Select **Enable access**.
4. Select the number of days to keep quarantined spam.

5. Select the maximum number of senders each end-user can approve when sifting through the quarantined email messages.
6. Type a log on page message that appears on your user's browser when he/she starts to access the quarantined email messages.
7. Under **Select LDAP groups**, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.
8. To add individual LDAP groups, clear the **Enable all** check box and do either of the following:

Search for groups:

- a. From the drop down list, select Search LDAP groups.
- b. Type the group name.
- c. Click **Search**. The groups appear in the table below.
- d. Click the LDAP groups to add.
- e. Click >>. The groups appear in the **Selected Groups** table.

Browse existing groups:

- a. From the drop down list, select **Browse LDAP groups**. The groups appear in the table below.
 - b. Click the LDAP groups to add.
 - c. Click >>. The groups appear in the **Selected Groups** table.
9. Click **Save**.

Note: When enabling user quarantine access for an LDAP group, you can use wildcards in the beginning and/or at the end of the LDAP group if you have specified Microsoft Active Directory or Sun iPlanet Directory as the LDAP server. For example, A*, *A, *A* are all allowed. If you have selected Domino as the LDAP server, you can only use wildcards at the end. For example, *A, *A* are not allowed.

Using EUQ

To use EUQ, you must enable and configure LDAP.

To start using EUQ:

1. Choose **Administration > End-User Quarantine**. The EUQ Management tab displays by default.
2. Do the following:
 - **Enable EUQ:** To enable EUQ, select the check box next to **Enable End-User Quarantine**, and then click **Save**.
 - **Clear the EUQ database:** To remove all data (including spam and approved sender information) from all EUQ services in a group, click **Remove**.
 - **Redistribute EUQ data:** If there are multiple devices with EUQ enabled on your network, you can redistribute EUQ data across all devices to improve EUQ performance. Redistribute data after you start or stop an EUQ service on a device or add a new device that has an EUQ service. Also redistribute data before you use the command line interface to remove a device with an EUQ service.

To redistribute data:

Tip: 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.
-

1. Under **Redistribute EUQ Data**, click one of the following:
 - **Only redistribute approved senders**
 - **Redistribute all (approved senders and spam)**
 2. Click **Redistribute**.
-

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

Event Notifications

You can configure IMSVA to send an email or SNMP notification to you or specific email users upon the occurrence of the following categories of event:

- **System Status**—Informs you when certain IMSVA performances fall below the desired level. For example, when a scanner service stops working, or when the number of messages in the delivery queue exceeds the desired quantity.
- **Scheduled Update Event**—Alerts you when IMSVA is able or unable to perform a scheduled update of the scan engine or pattern files from the update source onto the admin database.
- **Scanner Update Result**—Alerts you when IMSVA is unable to update the engine or pattern files on any scanner.

Note: Component update is a 2-step process:

1. At the scheduled time, the IMSVA admin database will first check the update source for new engine or pattern files.

2. IMSVA scanners will then check the admin database at regular intervals for updated components. The default interval is three minutes.

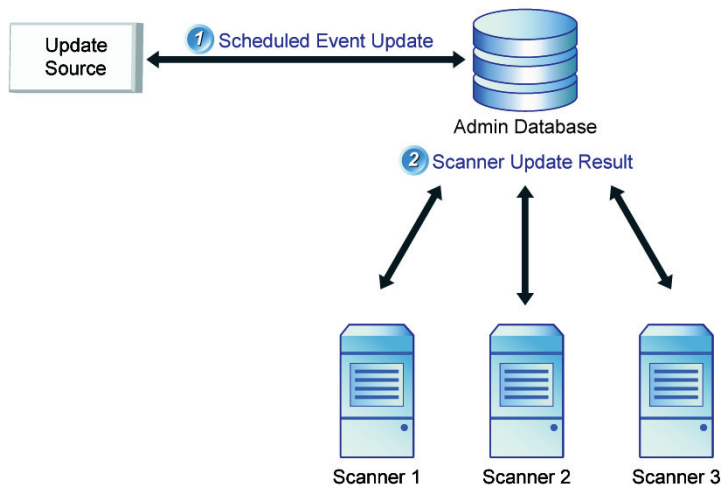


FIGURE 4-1 Scan engine and pattern file updates

Configuring Delivery Settings

The delivery settings allow you to specify the sender, recipient(s) and other settings required for delivering the notification message when certain events are triggered.

To configure the delivery settings:

1. Choose **Administration > Notifications** from the menu. The Events tab appears by default.
2. Click the **Delivery Settings** tab.

Notifications

Events **Delivery Settings** Web EUQ Digest

Email Settings

To address(es): postmaster@glory.co.jp
Use a semicolon ";" to separate multiple addresses

Sender's email address: "InterScan MSS Notification" <postmaster@glory.co.jp>

Server name or IP address:

SMTP server port: 25

Preferred charset: Japanese (iso-2022-jp)

Message header:

Message footer:

SNMP Trap

Server name (IP or FQDN):

Community: public

Save Cancel

3. Under **Email Settings**, configure the following:
 - **To address(es):** Type the recipient email addresses.
 - **Sender's email address:** Type the email address to appear as the sender.
 - **Server name or IP address:** Type the Fully Qualified Domain Name (FQDN) or IP address of the SMTP server that delivers email on your network.
 - **SMTP server port:** Type the port number that IMSVA uses to connect to the SMTP Server.
 - **Preferred charset:** IMSVA will use this setting to encode the notification messages.
 - **Message header:** Type the text to appear at the top of the notification.
 - **Message footer:** Type the text to appear at the bottom of the notification.
4. Under **SNMP Trap**, configure the following:

Note: **SNMP Trap:** The notification message sent to the Simple Network Management Protocol (SNMP) server when events that require administrative attention occur.

- **Server name:** Type the FQDN or IP address of the SNMP server.
- **Community:** Type the SNMP server community name.

Note: **Community:** The group that devices and management stations running SNMP belong to. To send the alert message to all SNMP management stations, type 'public' as the community name. For more information, refer to the official SNMP documentation.

5. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

Configuring Event Criteria and Notification Message

You can set the criteria under which IMSVA will trigger a notification message and also customize the message content for each event.

To configure the criteria and message content:

1. Choose **Administration > Notifications** from the menu. The Events tab appears by default.

Notifications



Events	Delivery Settings	Web EUQ Digest
System Events Notification		
System Status	Email	SNMP
Notify every 10 minutes		
Service on any scanner stops for more than 10 minutes	☒	☐
Data partition free space on any host is less than 10240 MB	☒	☐
MTA queue free space on any host is less than 2048 MB	☒	☐
Delivery queue contains more messages than 20000 messages	☒	☐
Retry queue folder contains more messages than 10000 messages	☒	☐
Scheduled Update Event	Email	SNMP
Scheduled virus, spyware/grayware or IntelliTrap pattern and exceptions update is:		
Unsuccessful	☒	☐
Successful	☐	☐
Scheduled scan engine update is:		
Unsuccessful	☒	☐
Successful	☐	☐
Scheduled spam engine or pattern update is:		
Unsuccessful	☒	☐
Successful	☐	☐
Scanner Update Result	Email	SNMP
Applying engine or pattern update fails on any scanner	☒	☐

2. Under System Status, configure the following:

- **Notify every { } minutes:** Type the notification frequency for all performance notifications.

To edit each of the following notifications, click the link.

- **Service on any scanner stops for more than:** Type the number of minutes.
- **Data partition free space on any host is less than:** Type the number of MB.
- **MTA queue free space on any host is less than:** Type the number of MB.
- **Delivery queue contains more messages than:** Type the number of messages.
- **Retry queue folder contains more messages than:** Type the number of messages.

3. Under **Scheduled Update Event**, click the **Unsuccessful** and **Successful** links to edit notifications for component updates.

Note: **Scheduled Update Event:** The event in which the latest engine and pattern files from the Update Source are updated onto the IMSVA admin database.

4. Under **Scanner Update Results**, click the **Applying engine or pattern update fails on any scanner** link to edit the notification.

Note: **Scanner Update Results:** The result of updating the latest engine and pattern files from the IMSVA admin database onto the scanners.

5. Select the **Email** and/or **SNMP** check boxes according to how you would like to receive the notification.
6. Click **Save**.

Configuring Web EUQ Digest Settings

The EUQ digest is a notification that IMSVA sends to users telling them how many of their email messages are in the End-User Quarantine.

To configure Web EUQ Digest settings:

1. Choose **Administration > Notifications** from the menu. The Events tab displays by default.
2. Click **Web EUQ Digest**.
3. Select the check box next to **Enable EUQ Digest**.
4. Under **Digest Schedule**, click the radio button next to one of the following frequencies:
 - **Daily:** Select the time of day from the drop down boxes.
 - **Weekly:** Select the day and time of day from the drop down boxes.
5. Under **Digest Mail Template**, type the subject and notification content.
To see a list of variables to include in the notification, click **Variables List**.
6. Click **Save**.

Editing Notifications

To edit notifications:

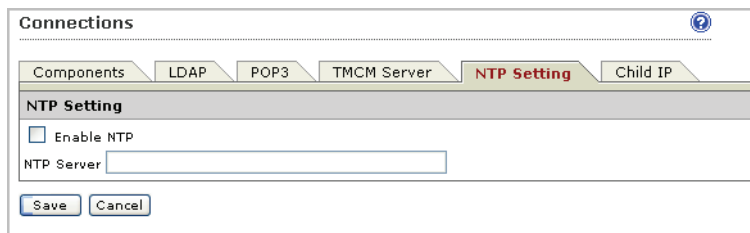
1. Choose **Administration > Notifications** from the menu.
2. Click the notification to edit. The edit screen for that notification appears.
3. Type the email subject and message, or SNMP message.
To see a list of variables to include in the notification, click Variables List.
4. Click **Save**.

Configuring NTP Settings

The Network Time Protocol (NTP) synchronizes the clocks of computer systems across the Internet. To synchronize the computer clock of an IMSVA device with the clock of an NTP server, configure the NTP setting.

To configure NTP setting:

1. Choose **Administration > IMSVA Configuration > Connections** from the menu. The Components tab appears by default.
2. Click the **NTP Setting** tab.



The screenshot shows a web-based configuration window titled "Connections" with a help icon in the top right corner. Below the title bar is a tabbed interface with six tabs: "Components", "LDAP", "POP3", "TMC Server", "NTP Setting" (which is highlighted in red), and "Child IP". The "NTP Setting" tab is active, displaying a section with the title "NTP Setting". Inside this section, there is a checkbox labeled "Enable NTP" which is currently unchecked. Below the checkbox is a text input field labeled "NTP Server". At the bottom of the window, there are two buttons: "Save" and "Cancel".

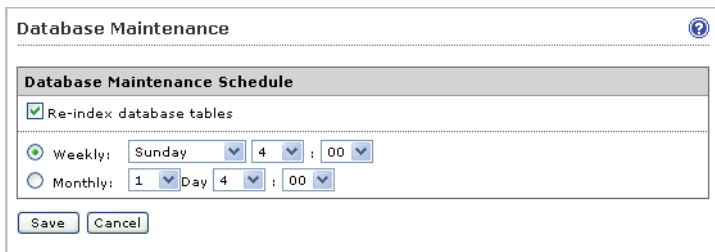
3. Select the **Enable NTP** check box.
4. Type the domain name or IP address of the NTP server.
5. Click **Save**.

Configuring Database Maintenance Schedule

You may want to re-index the IMSVA database tables if you encounter slow performance when performing queries. As re-indexing can impact the scanner performance, Trend Micro recommends that you do this during off-peak hours.

To re-index database tables:

1. Choose **Administration > Database Maintenance** from the menu. The Database Maintenance Schedule screen appears.



The screenshot shows a web-based configuration window titled "Database Maintenance" with a help icon in the top right corner. Inside the window is a section titled "Database Maintenance Schedule". Within this section, there is a checked checkbox labeled "Re-index database tables". Below this, there are two radio button options for scheduling: "Weekly" and "Monthly". The "Weekly" option is selected, and its configuration shows "Sunday" for the day, "4" for the day of the month, and "00" for the hour. The "Monthly" option is unselected, and its configuration shows "1" for the day of the month, "4" for the day of the month, and "00" for the hour. At the bottom of the window are "Save" and "Cancel" buttons.

2. Select the **Re-index database tables** check box.
3. Select the weekly or monthly schedule from the drop-down boxes.
4. Click **Save**.

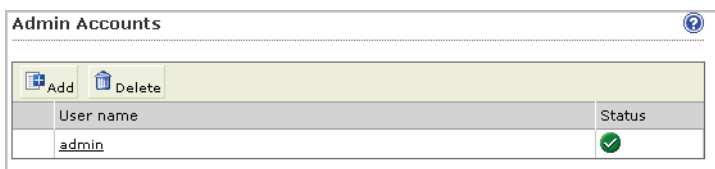
Managing Administrator Accounts

To reduce bottlenecks in administering IMSVA, you can delegate administrative tasks to other staff by creating new administrator accounts and assigning the desired permissions to the various areas of the Web management console.

Adding Administrator Accounts

To add administrator accounts:

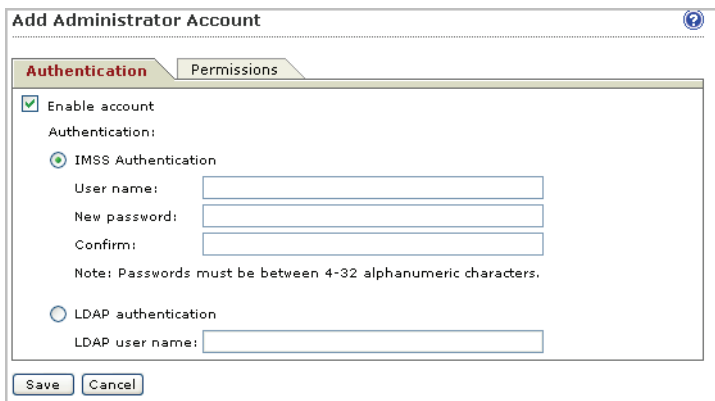
1. Choose **Administration > Admin Accounts** from the menu. The Admin Accounts screen appears.



The screenshot shows the 'Admin Accounts' interface. At the top, there are 'Add' and 'Delete' buttons. Below them is a table with two columns: 'User name' and 'Status'. The table contains one entry with the username 'admin' and a green checkmark in the status column.

User name	Status
admin	✓

2. Click **Add**. The Add Administrator Account screen appears with the **Authentication** tab displaying.



The screenshot shows the 'Add Administrator Account' screen. The 'Authentication' tab is selected. It features a checkbox for 'Enable account' which is checked. Under 'Authentication', there are two radio buttons: 'IMSS Authentication' (selected) and 'LDAP authentication'. The IMSS section includes fields for 'User name:', 'New password:', and 'Confirm:', along with a note: 'Note: Passwords must be between 4-32 alphanumeric characters.' The LDAP section has a field for 'LDAP user name:'. At the bottom are 'Save' and 'Cancel' buttons.

3. Specify Authentication settings:
 - a. Select **Enable account**.

- b. Select an authentication type:
 - **IMSPA Authentication:** Type the username, new password, and the new password confirmation.
The password must be between 4 and 32 alphanumeric characters.
 - **LDAP authentication:** Type the LDAP username.
 - c. Click **Save**.
 4. Click the **Permissions** tab. The Permissions screen appears.

Access Areas	Full	Read	None
Summary	☐	☐	☒
Policy	☐	☐	☒
IP Filtering	☐	☐	☒
Reports	☐	☐	☒
Logs	☐	☐	☒
Quarantine & Archive	☐	☐	☒
Administration	☐	☐	☒

Save Cancel

5. Specify Permissions settings:
 - a. Select **Full**, **Read**, or **None** for each of the following access areas that appear on the IMSVA Web management console menu:
 - **Summary**
 - **Policy**
 - **IP Filtering**
 - **Reports**
 - **Logs**
 - **Quarantine & Archive**
 - **Administration**
 - **Command Line Interface**
 - b. Click **Save**.

-
- Note:**
1. Only the default IMSVA administrator account can add new administrator accounts. Delegate administrator accounts cannot do so even if you assign full permission to the Administration area.
 2. Delegate administrator accounts with full administration rights can only change their own IMSVA passwords. If you forget the default administrator account password, please contact Trend Micro's technical support to reset the password.
-

Editing or Deleting Administrator Accounts

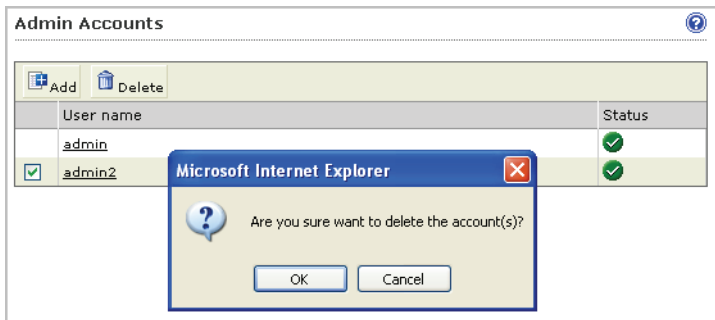
You can change or delete the permissions of a delegate whenever there is a revision of roles or other organizational changes.

To edit an administrator account:

1. Choose **Administration > Admin Accounts** from the menu. The Admin Accounts screen appears.
2. To edit an administrator account, click the account name hyperlink.
3. Make the required changes.
4. Click **Save**.

To delete an administrator account:

1. To delete an administrator account, select the check box next to the account to be removed.
2. Click **Delete**.
3. Click **OK** to confirm the deletion or **Cancel** to withdraw.



Note: You can only delete the delegate administrator account but not the default IMSVA administrator account.

Configuring Connection Settings

To enable the scanner to receive messages , configure the connection settings.

To configure scanner and policy connections:

1. Choose **Administration > IMSVA Configuration > Connections** from the menu. The Components tab appears by default.

The screenshot shows a window titled "Connections" with a help icon in the top right. Below the title bar are several tabs: "Components" (highlighted in red), "LDAP", "POP3", "TMC Server", "NTP Setting", and "Child IP". Under the "Components" tab, there is a section titled "Settings for All Policy Services". This section contains three configuration items: "Protocol:" with a dropdown menu currently set to "HTTP"; "Keep-alive:" with an unchecked checkbox labeled "Enable"; and "Maximum number of backlogged requests:" with a text input field containing the value "100". At the bottom of the window are two buttons: "Save" and "Cancel".

2. Under **Settings for All Policy Services**, configure the following:
 - **Protocol:** Select the type of protocol the scanner uses to communicate with the policy service (HTTP or HTTPS).
 - **Keep-alive:** Select the check box to enhance policy retrieval by maintaining a constantly active connection between the scanner and policy services.
 - **Maximum number of backlogged requests:** Type a number that represents the maximum number of requests IMSVA will preserve until it can process them later.
3. Click **Save**.

Configuring LDAP Settings

Configure LDAP settings for user-group definition, administrator privileges, or end-user quarantine authentication. You can enable up to two LDAP servers for each InterScan group.

To provide a backup LDAP server, configure two LDAP servers.

To configure LDAP settings:

1. Choose **Administration > IMSVA Configuration > Connections**. The **Components** tab displays by default.
2. Click the **LDAP** tab.
3. Next to **LDAP server type**, choose the type of LDAP servers on your network:
 - **Microsoft Active Directory**
 - **Domino**
 - **Sun iPlanet Directory**
4. Next to **Enable LDAP 1**, select the check box.
5. Next to **LDAP server**, type the server name or IP address.
6. Next to **Listening port number**, type the port number that the LDAP server uses to listen to access requests.
7. Configure the settings under **LDAP 2** if necessary.
8. Under **LDAP cache expiration for policy services and EUQ services**, type the **Time to live** in minutes.

Note: **Time To Live:** Duration that determines how long IMSVA retains the LDAP query results in the cache. Specifying a longer duration enhances LDAP query during policy execution. However, the policy server will be less responsive to changes in the LDAP server. A shorter duration means that IMSVA has to perform the LDAP query more often, thus lowering the performance.

9. Under **LDAP admin**, type the administrator account, the corresponding password and the base distinguished name. Refer to the table below for assistance on what to specify under this section according to the LDAP server type:

TABLE 4-2. LDAP Server Types

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)
Domino	user1/domain	Not applicable	Simple
Sun iPlanet Directory	uid=user1, ou=people, dc=domain, dc=com	dc=domain, dc=com	Simple

10. Select an authentication method:

- **Simple**
- **Advanced:** Uses Kerberos authentication for Active Directory. Configure the following:
 - **Kerberos authentication default realm:** Default Kerberos realm for the client. For Active Directory it must be the Windows domain name in upper case (Kerberos is case-sensitive).
 - **Default domain:** The Internet domain name equivalent to the realm.
 - **KDC and admin server:** Hostname or IP address of the Key Distribution Center for this realm. For Active Directory, it is usually the domain controller.
 - **KDC port number:** The associated port number.

11. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

Note: IBM Domino only supports Simple Authentication method.

If the domain name in LDAP administrator account can be resolved by DNS, the

Kerberos authentication will succeed no matter what value you type in the default realm.

If the domain name in LDAP administrator account cannot be resolved, Kerberos will use the default realm to check.

Configuring POP3 Settings

In addition to SMTP traffic, IMSVA can scan POP3 messages at the gateway as your clients retrieve them.

Tip: To use the POP3 message filter, enable **Accept POP3 connection** from **Summary > System** screen. This option is not selected by default.

To configure POP3 settings:

1. Choose **Administration > IMSVA Configuration > Connections**. The **Components** tab displays by default.
2. Click the **POP3** tab.
3. To configure a connection from unknown POP3 servers on the Internet, type the port number IMSVA uses for incoming POP3 connections under **Generic POP3 Connection**.
4. To configure connections from specific POP3 servers, do the following:
 - a. Click **Add** under **Dedicated POP3 Connections**. The Dedicated POP3 Connection window appears.
 - b. Type the port IMSVA uses for incoming POP3 connections, the POP3 server IP address, and the POP3 server port number.
 - c. Click **OK**.
 - d. To modify an existing connection, click the connection name.
5. Under **Message Text**, modify the message that IMSVA will send to users if email messages that they are trying to receive trigger a filter and are quarantined or deleted.
6. Click **Save**.

Note: The incoming port on your scanners must be idle or the IMSVA daemon might not function properly.

Configuring POP3 generic services

For a generic POP3 service, the POP3 client logs on using the USER command and specifies the actual POP3 server and optional port number along with the user's name using the UserServerSeparator character to separate the values.

Example 1: To connect user "User1" to server "Server1", and the UserServerSeparator character is "#", the client issues the following USER command:

```
USER User1#Server1
```

Example 2: To connect to port 2000 on Server1, the following command would be used:

```
USER User1#Server1#2000
```

Note: If you do not specify a port number, IMSVA uses the default value of 110.

The following example shows how to configure generic POP3 settings for Outlook:

1. Specify the POP3 server address with IMSVA scanner IP 192.168.11.147.
2. Type user name **test123#192.168.11.252**.
3. Set POP3 port to 110.

Configuring POP3 dedicated services

For a POP3 dedicated service, the POP3 service always connects to a specific POP3 server. IMSVA uses this service for a POP log on and for any type of log on using the AUTH command. For this service, a separate port on the proxy has to be set up for each specific POP3 server that any client might want to connect to.

The following example shows how to configure dedicated POP3 settings in Outlook:

1. Specify the POP3 server address with IMSVA scanner IP 192.168.11.147.
2. Type user name **test123**.
3. Set the POP3 port to 1100 which is the port that IMSVA dedicated POP3 service is listening on.

Configuring TCMC Settings

To use Trend Micro Control Manager (TCMC) 3.5 or above to manage IMSVA, enable the TCMC agent on the IMSVA server and configure TCMC server settings. If a proxy server is between the TCMC server and IMSVA, configure proxy settings. If a firewall is between the TCMC server and IMSVA, configure port forwarding to work with the firewall's port-forwarding functionality.

To configure TCMC settings:

1. Choose **Administration > IMSVA Configuration > Connections**. The **Components** tab displays by default.
2. Click the **TCMC Server** tab.
3. Select the **Enable TCMC Agent** check box.
4. Next to **Server**, type the TCMC IP address or FQDN.
5. 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.
6. Under **Web server authentication**, type the access credentials to access the TCMC Web server.
7. Select **Enable proxy** under Proxy Settings.
8. Next to **Proxy Type**, select the protocol the proxy server uses: **HTTP**, **SOCKS4**, or **SOCKS5**.
9. Type the proxy server FQDN or IP address, port number, and the username and password.
10. Click **Save**.

If you are using the Configuration Wizard, click **Next**.

If you enabled the agent, it will soon register to the TCMC server. If you disabled the agent, IMSVA will soon log off from the TCMC server. Verify the change on the TCMC management console.

For additional information about Control Manager, see your TCMC documentation.

To unregister from Control Manager:

1. Choose **Administration > IMSVA Configuration > Connections**. The **Components** tab displays by default.

2. Click the **TMC Server** tab.
3. Click the **Un-register All Agents** button.

Configuring Child IP Settings

Devices in the Child IP address list can access each other for internal communications in a group. Add all IP addresses of child devices in the current group to this list before you register these child devices to the parent.

To configure child IP address settings:

1. Choose **Administration > IMSVA Configuration > Connections**. The Components tab displays by default.
2. Click the **Child IP** tab.
3. Under **Add IP Address**, type the child device IP address.
4. Click **>>**. The address appears in the table.
5. Click **Save**.

Changing the Web Console Password

Trend Micro recommends periodically changing the password you use to access the Web management console.

To change the Web management console password:

1. Choose **Administration > Password**.
2. Type the current password, the new password, and the new password confirmation. The password must be between 4 and 32 alphanumeric characters
3. Click **Save**.

WARNING! If you are still using the default administration password, Trend Micro strongly recommends that you change the password immediately.

Managing Product Licenses

InterScan can use the following components:

- **Antivirus and Content Filter:** Basic scanning and filtering functionality. You can think of this product as the IMSVA program itself.
- **Spam Prevention Solution (SPS):** A built-in filter to help IMSVA identify content typically found in spam.
- **IP Filtering Service:** Automatic blocking of known spam senders. IP Filtering includes the following:
 - **NRS:** Trend Micro Network Reputation Services (NRS) are designed to be used to identify and block spam before it enters a computer network by routing Internet Protocol (IP) addresses of incoming mail connections to Trend Micro Threat Protection Network for verification against an extensive Reputation Database.
 - **IP Profiler:** IP Profiler allows you to configure threshold settings and determine what action IMSVA will take when it detects any of the four potential Internet threats:
 - **Spam:** Email with unwanted advertising content.
 - **Viruses:** Various virus threats, including Trojan programs.
 - **Directed Harvest Attack (DHA):** Programs that could add your user's email addresses to spam databases.
 - **Bounced Mail:** Email messages returned to you because the messages were sent with your domain in the sender address.

You can activate IMSVA products through the Web management console. If a product license expires, you must renew the license, obtain a new Activation Code, and enter the code through the Web management console. If the product remains inactive, its features are disabled.

Viewing Your Product Licenses

To view your existing licenses:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears:
 - **Product**

- **Version**

- **Full:** Indicates that you have purchased the full licensed product.
- **Evaluation:** Indicates that you are using an evaluation product that expires after an elapsed time. The evaluation period varies according to the activation code you have obtained.

Fourteen (14) days prior to the expiration of the evaluation period, you will see a warning message on the Web management console.

To continue using IMSVA to protect your network after the evaluation period, purchase a licensed version of IMSVA and enter the new activation code.

- **Activation Code:** A 31 alphanumeric character code in the format **xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx**. Trend Micro will send you an activation code via email when you register a product online. You can then copy and paste this activation code on the Product License page.
- **Seats:** The number of licenses you have purchased.
- **Status:** Indicates whether the product has expired or has been activated.
- **Maintenance expiration:** The date when you will no longer be able to download the latest scan engine and virus pattern files from the Trend Micro ActiveUpdate server. To ensure that your network is well-protected against the latest Web threats, contact your sales representative to renew your license.

2. For the license you want to view, click **View detailed license online**.

3. To check the status of your license agreement on the Trend Micro Web site, click **Check Status Online**.

Renewing or Activating a License

There are two ways to renew a license:

- **Obtain a new Activation Code:** Contact your sales representative to obtain a new Activation Code, and then enter the code on the Product Licenses screen.
- **Extend the life of an existing Activation Code:** Contact your sales representative to extend the lifetime of your Activation Code, and then either manually update the license status or wait until IMSVA automatically updates it.

To renew with a new Activation Code:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears.
2. Next to **Activation Code**, click **Enter a new code**. The Enter a New Code screen appears.
3. Next to **New Activation Code**, type the new code.
4. Click **Activate**. The Web management console might access the Trend Micro Web site to activate the license. If you are unable to reach the Trend Micro Web site, verify your network settings and try again.

To renew with an existing Activation Code:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears.
2. For the license you want to renew, click **View detailed license online**.
3. Click **Check Status Online**. The Web management console accesses the Trend Micro Web site to activate the license. If you are unable to reach the Trend Micro Web site, verify your network settings and try again.

90, 60, 30, and 0 days before the expiration of the current license, and every day after the expiration of the current license, IMSVA will automatically check the status of your license and update it if you have extended the valid period.

Tip: You can wait for IMSVA to update the license status automatically. However, Trend Micro recommends that you manually update it as soon as you extend the lifetime of the Activation Code.

Activating Products

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

You can activate products from one of the following screens:

- From step 9 of the Configuration Wizard.
- From Administration > Product Licenses

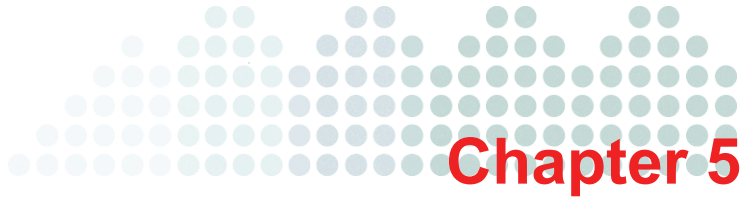
From step 9 of the Configuration Wizard:

1. If you do not have an Activation Code, click **Register Online**. Upon successful registration, Trend Micro will send you the Activation Code through email.
2. Type the Activation Code to activate any of the following:
 - Trend Micro Antivirus and Content Filter
 - Spam Prevention Solution
3. Click **Next**.

Note: The Activation Code comes in the format xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx.

From Administration > Product Licenses:

1. Choose **Administration > Product Licenses**. A brief summary of each license appears.
2. Next to Activation Code, click **Enter a new code**. The Enter a New Code screen appears.
3. Next to New Activation Code, type the new code.
4. Click **Activate**. The Web console might access the Trend Micro Web site to activate the license. If you are unable to reach the Trend Micro Web site, verify your network settings and try again.



Using End User Quarantine

This chapter explains how to use End-User Quarantine (EUQ).

Topics include:

- [About EUQ on page 5-2](#)
- [Step 1: Configuring and Enabling LDAP on page 5-2](#)
- [Step 2: Enabling EUQ on page 5-5](#)
- [Step 3: Starting the EUQ Service on page 5-7](#)
- [Step 4: Enabling End-User Access on page 5-8](#)
- [Step 5: Opening the End-User Quarantine Console on page 5-10](#)
- [Disabling EUQ on page 5-11](#)

About 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 are determined 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, delete, or approve for delivery.

To use EUQ, you must do the following:

[Step 1: Configuring and Enabling LDAP on page 5-2](#)

[Step 2: Enabling EUQ on page 5-5](#)

[Step 3: Starting the EUQ Service on page 5-7](#)

[Step 4: Enabling End-User Access on page 5-8](#)

[Step 5: Opening the End-User Quarantine Console on page 5-10](#)

Step 1: Configuring and Enabling LDAP

To use EUQ, you must configure and enable LDAP.

To enable and configure LDAP:

1. You can configure and enable LDAP settings in 2 ways:
 - Choose **Administration > IMSVa Configuration > Connections** from the menu, then click the **LDAP** tab.

Connections

Components
LDAP
POP3
TMC Server
NTP Setting
Child IP

LDAP Settings
Enter LDAP settings if you wish to use them for user-group definition, administrator privileges, or end-user quarantine authentication.

LDAP server type:
Microsoft Active Directory

☒ Enable **LDAP1**
LDAP server:
Example: example.com or 123.123.123.123
Listening port number:
389
Note: Please use the global catalog port 3268 if the LDAP server type is Microsoft Active Directory.

☐ Enable **LDAP2**
LDAP server:
Example: example.com or 123.123.123.123
Listening port number:
389
Note: Please use the global catalog port 3268 if the LDAP server type is Microsoft Active Directory.

LDAP cache expiration for policy services and EUQ services
Time to Live in minutes:
1440

LDAP admin
LDAP admin account:
Example: Domain_NameAccount_Name or Account_Name@Domain_Name
Password:
.....
Base distinguished name:
Example: DC=foo, DC=foonet, DC=org
Authentication method:
☒ Simple
☐ Advanced: using Kerberos authentication for Active Directory
Kerberos authentication default realm:
Default domain:
KDC and admin server:
KDC port number:

Save
Cancel

- Choose **Administration > IMSVA Configuration > Configuration Wizard** from the menu.

Configuration Wizard
 Step 6 of 10

?

LDAP Settings

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

LDAP Settings

LDAP server type:* Microsoft Active Directory

☐ Enable **LDAP1**

LDAP server:*
 Example: example.com or 123.123.123.123

Listening port number:* 389

☐ Enable **LDAP2**

LDAP server:*
 Example: example.com or 123.123.123.123

Listening port number:* 389

LDAP cache expiration for policy services and EUQ services

Time to Live in minutes:* 1440

LDAP admin

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

Password:*

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

Authentication method:* Simple

Advanced: using Kerberos authentication for Active Directory

Kerberos authentication default realm:

Default domain:

KDC and admin server:

KDC port number:

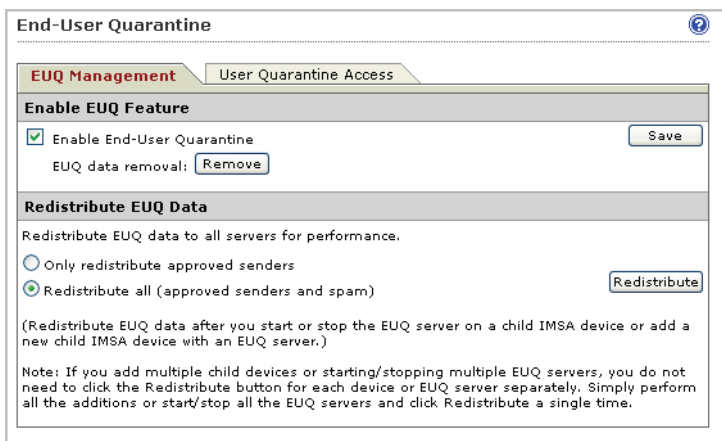
< Back
Skip
Next >

2. Configure all LDAP settings.

Step 2: Enabling EUQ

To enable EUQ:

1. You can enable EUQ in two ways:
 - Choose **Administration > End-User Quarantine** from the menu.



The screenshot shows the 'End-User Quarantine' configuration window. It has two tabs: 'EUQ Management' (selected) and 'User Quarantine Access'. Under 'EUQ Management', there are two sections. The first section, 'Enable EUQ Feature', contains a checked checkbox for 'Enable End-User Quarantine' with a 'Save' button to its right. Below this is a label 'EUQ data removal:' followed by a 'Remove' button. The second section, 'Redistribute EUQ Data', contains the text 'Redistribute EUQ data to all servers for performance.' followed by two radio button options: 'Only redistribute approved senders' and 'Redistribute all (approved senders and spam)'. A 'Redistribute' button is to the right of the second option. At the bottom, there is a note: '(Redistribute EUQ data after you start or stop the EUQ server on a child IMSA device or add a new child IMSA device with an EUQ server.)' and another note: 'Note: If you add multiple child devices or starting/stopping multiple EUQ servers, you do not need to click the Redistribute button for each device or EUQ server separately. Simply perform all the additions or start/stop all the EUQ servers and click Redistribute a single time.'

- Choose **Administration > IMSVA Configuration > Configuration Wizard** from the menu, then go to **Step 2: Deployment Settings**.

Configuration Wizard
Step 2 of 10

Deployment Settings

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

imsa.example.com deployment type:

☒ **Parent Device**

Import Settings...

☒ Gateway deployment
(To use IP Filtering, you must deploy IMSA at the gateway.)

☐ Enable End-User Quarantine
(Quarantine all spam and allow your users to access their spam through a Web console.)

☐ Automatically synchronize system time with NTP server:

☐ **Child Device**

Register to parent device IP address:

< Back Next >

2. Select the **Enable End-User Quarantine** check box.
3. Click **Save** at the EUQ Management tab. If you are using the wizard, progress through the wizard screens and click **Finish**.
4. At the EUQ Management tab, click **Redistribute** to redistribute the EUQ data among the devices in the group.

Note: Any time you enable EUQ in a group, you should redistribute EUQ data.

Step 3: Starting the EUQ Service

To start the EUQ service:

1. Choose **Summary** from the menu. The Real-time Statistics tab appears.
2. Click the **System** tab.
3. In the **Managed Services** table, click **Start** under **EUQ Service**.

Summary 

Real-time Statistics **System**

Enable Connections

☐ Accept POP3 connections
 ☒ Enable IP Filtering
 ☒ NRS
 ☒ IP Profiler

Components Last refresh: Nov 23, 2007 5:07:19 AM

☐	Name	Current Version	Availability	Update Schedule
☐	Scan engine	8.500.1001	8.500.1001	15 minutes
☐	Virus pattern	4.843.00	4.843.00	15 minutes
☐	Spyware/grayware pattern	0.555.00	0.555.00	15 minutes
☐	IntelliTrap pattern IntelliTrap exceptions	0.107.00 0.255.00	0.107.00 0.255.00	15 minutes
☐	Anti-spam engine	5.0.1023	5.0.1023	15 minutes
☐	Spam pattern	15562.002	15562.002	15 minutes

Managed Services

Hostname	Connection	Scanner Service	Policy Service	EUQ Service
rd.imsa.com		 Stop	 Stop	 Start

4. Choose **Administration > End-User Quarantine** from the menu. The EUQ Management tab appears.
5. Click **Redistribute** to redistribute the EUQ data among the devices in the group.
6. Choose **Summary > System** from the menu and verify that the EUQ service is active (or inactive).

Step 4: Enabling End-User Access

Enable end-user access to allow your users to access quarantined spam items that IMSVA might have misidentified as spam. The clients use LDAP authentication to access the IMSVA EUQ service.

To configure and enable end-user access:

1. Choose **Administration > End-User Quarantine** from the menu. The EUQ Management tab appears.
2. Click the **User Quarantine Access** tab.

End-User Quarantine

These groups can access quarantined spam items and will use LDAP authentication with the designated IMSA server.

EUQ Management **User Quarantine Access**

☒ Enable access ⓘ

Keep quarantined spam for: 7 days ▼

Set maximum number of approved senders

Maximum approved senders per end-user: 50 ▼

Specify login page greeting

Enter the greeting displayed to the user after logon. Specify a new line using
. Optionally use HTML to specify the greeting text format.

Select LDAP groups to enable access

☒ Enable All

Select groups from LDAP Search below.

Search LDAP groups ▼

Search

Selected Groups

>> <<

Save Cancel

3. Select **Enable access**.
4. Select the number of days to keep quarantined spam.
5. Select the maximum number of approved senders per end-user.
6. Type a log on page message that appears on your user's browser when he/she starts to access the quarantined email messages.
7. Under Select LDAP groups, select the check box next to **Enable all** to allow all LDAP group users to access quarantined spam.
8. To add individual LDAP groups, clear the **Enable all** check box and do either of the following:

Search for groups:

- a. From the drop-down list, select **Search LDAP groups**.
- b. Type the group name.
- c. Click **Search**. The groups appear in the table below.
- d. Click the LDAP groups to add.
- e. Click **>>**. The groups appear in the Selected Groups table.

Browse existing groups:

- a. From the drop-down list, select **Browse LDAP groups**. The groups appear in the table below.
- b. Click the LDAP groups to add.
- c. Click **>>**. The groups appear in the Selected Groups table.
- d. Click **Save**.

Step 5: Opening the End-User Quarantine Console

You can view the EUQ Web console from the computer where the program was deployed or you can view the EUQ Web console remotely across the network.

To view the console from another computer on the network, go to:

- Primary EUQ service—`https://<target server IP address>:8447`
- Secondary EUQ service—`https://<target server IP address>:8446`

WARNING! To successfully access all Web consoles on secondary EUQ services, you must synchronize the system time of all EUQ services on your network.

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN).

Logon Name Format

The format of the user logon name for accessing the EUQ Web console differs according to the LDAP server type you have selected when configuring LDAP settings. Following are some examples of the logon name format for the three types of supported LDAP servers:

- **Microsoft Active Directory**
 - Without Kerberos—`user1@domain.com` (UPN) or `domain\user1`
 - With Kerberos—`user1@domain.com`
- **Domino**—`user1/domain`
- **Sun iPlanet Directory**—`uid=user1, ou=people, dc=domain, dc=com`

Disabling EUQ

Before disabling EUQ, inform your users that they should handle their quarantined spam.

To disable EUQ:

1. To access the EUQ configuration screen, do one of the following:
 - Choose **Administration > End-User Quarantine** from the menu. The EUQ Management tab appears.
 - Choose **Administration > IMSVA Configuration > Configuration Wizard** from the menu, then go to **Step 2: Deployment Settings**.
2. Clear the **Enable End-User Quarantine** check box.
3. To save disk space on each device, you have the option of removing all EUQ data from each device. To do so, click **Remove** on the EUQ Management tab.
4. Click **Save** at the EUQ Management tab. If you are using the wizard, progress through the wizard screens and click **Finish**.
5. Choose **Summary** from the menu.
6. Click the **System** tab and verify that the EUQ service is inactive.



Using the Command Line Interface

This chapter describes the Command Line Interface (CLI) commands that you can use in the InterScan Messaging Security Virtual Appliance (IMSVa) product to perform monitoring, debugging, troubleshooting, and configuration tasks.

Topics include:

- [Using the CLI on page 6-2](#)
- [Entering the CLI on page 6-2](#)
- [CLI Overview on page 6-3](#)
- [Entering the OS Shell on page 6-3](#)
- [Command Line Interface Commands on page 6-4](#)

Using the CLI

Use the CLI to do the following:

- Configure initial settings, such as the device IP address and host name
- Restart the device
- Rescue the application
- View device status
- Debug and troubleshoot the device

Note: Do not enable scroll lock on your keyboard when using HyperTerminal. If scroll lock is enabled, you cannot enter data.

Entering the CLI

If the IMSVA becomes a child device, the passwords for admin and enable that were set during installation are not available. Use the password for the parent device.

To enter the CLI:

1. Verify the computer you are using can ping IMSVA's IP address.
2. Use a SSH client to connect to IMSVA's IP address and TCP port 22.
3. Log on with the following:
 - User name: **admin**
 - Password: The password used for the CLI when installing the product
4. Type **logout** and press ENTER to terminate the SSH session.

CLI Overview

After you open the CLI menu, it displays the following:

```
Trend Micro IMSVA - InterScan Messaging Security Virtual Appliance

To manage the IMSVA software appliance through its Web interface, open a
browser window and enter the following URL:

    http://192.168.159.57:8445

You will be prompted for your administrator account and password.
Please have your administrator account and password ready for authentication.
Please refer to the user guide for the factory default account and password.

To manage the IMSVA appliance through the Command Line (CLI) Shell, please
login using the Login prompt below. Please refer to the user guide
for the factory default account and password.

InterScan-Virtual-Appliance-01 login: process 'named' is using obsolete setsocke
pt SO_BSDCOMPAT
B_
```

Entering the OS Shell

WARNING! Enter the shell environment only if your support provider instructs you to perform debugging operations.

To enter the OS shell:

1. Verify the computer you are using can ping IMSVA's IP address.
2. Use a SSH client to connect to IMSVA's IP address and TCP port 22.
3. Log on with the following:
 - User name: **root**
 - Password: The password used for the OS shell when installing the product

Command Line Interface Commands

IMSVA's CLI commands are separated into two categories—root and privileged commands. Root commands are basic commands that allow the administrator to obtain specific low security risk information and to perform simple tasks. Privileged commands provide full configuration control and advanced monitoring and debugging features. Privileged commands are protected by an additional layer of credentials—the Enable account and password.

To enter privileged mode:

1. Enter CLI.
 - a. Verify the computer you are using can ping IMSVA's IP address.
 - b. Use a SSH client to connect to IMSVA's IP address and TCP port 22.
 - c. Log on with the following:
 - User name: **admin**
 - Password: The password used for the CLI when installing the product
2. At the prompt **>** type **enable** and press ENTER. The prompt changes from **>** to **#**.
3. Type the password used for the CLI when installing the product and press ENTER.

configure adminUI disable	
Disables the IMSVA Web console on all network interface cards (NIC).	
SYNTAX: <code>configure adminUI disable</code>	
VIEW	Privileged
PARAMETERS	None
EXAMPLES:	
To disable the IMSVA Web console on all NICs: <code>configure adminUI disable</code>	

configure adminUI enable

Enables the IMSVA Web console on one specific network interface card (NIC).

SYNTAX:

```
configure adminUI enable <interface>
```

VIEW

Privileged

PARAMETERS

<interface>: Name of the NIC

EXAMPLES:

To enable the IMSVA Web console for the NIC **eth0**:

```
configure adminUI enable eth0
```

configure adminUI enable all

Enables the IMSVA Web console on all network interface cards (NIC).

SYNTAX:

```
configure adminUI enable all
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To enable the IMSVA Web console for all NICs:

```
configure adminUI enable all
```

configure date

Configures the time and date and saves the data in CMOS.

SYNTAX:

```
configure date <date> <time>
```

VIEW

Privileged

PARAMETERS

<date>: Set the date using the following format: **yyyy-mm-dd**

<time>: Set the time with the following format: **hh:mm:ss**

EXAMPLES:

To set the date to August 12, 2008 and the time to 3:40 PM:

```
configure date 2008-08-12 15:40:00
```

configure dns

Configures DNS settings for the IMSVA device.

SYNTAX:

```
configure dns <dns1> <dns2>
```

VIEW

Privileged

PARAMETERS

<dns1>: Primary DNS server

<dns2>: Secondary DNS server

Note: Use a space to separate the primary and secondary DNS value.

EXAMPLES:

To configure the primary DNS with an IP address of 192.168.10.21:

```
configure dns 192.168.10.21
```

To configure the primary and secondary DNS with the following values:

- Primary DNS: 192.168.10.21
- Secondary DNS: 192.168.10.22

```
configure dns 192.168.10.21 192.168.10.22
```

configure hostname

Configures the host name for the IMSVA device.

SYNTAX:

```
configure hostname <hostname>
```

VIEW

Privileged

PARAMETERS

<hostname>: The host name or fully qualified domain name (FQDN) for the IMSVA device

EXAMPLES:

To change the host name of the IMSVA device to **test.imsva.com**:

```
configure hostname test.imsva.com
```

configure interface

Configures the IP address for the network interface card (NIC).

SYNTAX:

```
configure interface <interface> <ip> <mask>
```

VIEW

Privileged

PARAMETERS

<interface>: NIC name

<ip>: specify IP address for the interface

<mask>: specify network mask for the NIC

EXAMPLES:

To configure an NIC with the following values:

- **IP address:** 192.168.10.10
- **Subnet mask:** 255.255.255.0

```
configure interface 192.168.10.10 255.255.255.0
```

configure password enable

To change the password required to enter Privileged mode.

SYNTAX:

```
configure password enable
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To change the password required to enter Privileged mode

```
configure password enable
```

configure role change-parent

Changes the role of an IMSVA device from child to parent.

SYNTAX:

```
configure role change-parent <new_parent_ip>
```

VIEW

Privileged

PARAMETERS

<new_parent_ip>: IP address for a new parent server

EXAMPLES:

To change an IMSVA device's role from child to parent using the IP address 192.168.10.24:

```
configure role change-parent 192.168.10.24
```


configure role unregister

Unregisters a child IMSVA device from a parent IMSVA device.

SYNTAX:

```
configure role unregister
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To unregister a child IMSVA device from a parent IMSVA device:

```
configure role unregister
```

configure route add

Adds a new route entry

SYNTAX:

```
configure route add <ip_prefixlen> <via> <dev>
```

VIEW

Privileged

PARAMETERS

<ip_prefixlen>: destination network ID with format
IP_Address/Prefixlen

<via>: The address of the next hop

<dev>: The device name

EXAMPLES:

To add a new route entry:

```
configure route add 172.10.10.0/24 192.168.10.1 eth1
```

configure route default

Sets the default route for IMSVA device.

SYNTAX:

```
configure route default <gateway>
```

VIEW

Privileged

PARAMETERS

<gateway>: IP address of default gateway

EXAMPLES:

To set the default route for an IMSVA device:

```
configure route default 192.168.10.1
```

configure route del

Deletes a route for IMSVA device.

SYNTAX:

```
configure route del <ip_prefixlen> <via> <dev>
```

VIEW

Privileged

PARAMETERS

<ip_prefixlen>: destination network ID with format
IP_Address/Prefixlen

<via>: The address of the next hop

<dev>: The device name

EXAMPLES:

To delete a route for an IMSVA device:

```
configure route del 172.10.10.0/24 192.168.10.1 eth1
```

configure ssh disable

Disables SSH on all network interface cards (NIC).

SYNTAX:

```
configure ssh disable
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To disable SSH on all NICs:

```
configure ssh disable
```

configure ssh enable

Enables SSH on one specific network interface card (NIC).

SYNTAX:

```
configure ssh enable <interface>
```

VIEW

Privileged

PARAMETERS

<interface>: The name of the NIC

EXAMPLES:

To enable SSH on NIC **eth0**:

```
configure ssh enable eth0
```

configure ssh enable all

Enables SSH on all network interface cards (NIC).

SYNTAX:

```
configure ssh enable all
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To enable SSH on all NICs:

```
configure ssh enable all
```

configure timezone

Configures the time zone used by the IMSVA device.

SYNTAX:

```
configure timezone <region> <city>
```

VIEW

Privileged

PARAMETERS

<region>: Region name

<city>: City name

EXAMPLES:

To configure the IMSVA device to use the time zone for the following location:

Region: America

City: New York

```
configure timezone America New_York
```

enable

Enters privileged mode so privileged commands can be provided.

SYNTAX:

`enable`

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To enter privileged mode:

`enable`

exit

Exits privileged mode.

Exits the session for those not in privileged mode.

SYNTAX:

`exit`

VIEW

Root/Privileged

PARAMETERS

None

EXAMPLES:

To exit privileged mode or to exit the session when not in privileged mode:

`exit`

help

Displays the CLI help information.

SYNTAX:

```
hlep
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the CLI help information:

```
help
```

history

Displays the current session's command line history.

SYNTAX:

```
history [limit]
```

VIEW

Privileged

PARAMETERS

[limit]: Specifies the number of previous commands to display

EXAMPLES:

To display the last six commands used in the current session:

```
history 6
```

logout

Logs out of the current CLI session.

SYNTAX:

```
logout
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To logout from the current session:

```
logout
```

ping

Pings a specified host.

SYNTAX:

```
ping [-c num_echos] [-i interval] <dest>
```

VIEW

Root

PARAMETERS

[-c num_echos]: Specifies the number of echo requests to be sent. Default value is 5.

[-i interval]: Specifies the delay interval in seconds between each packet. Default value is 1 second.

<dest>: Specifies the destination hostname or IP address

EXAMPLES:

To ping the IP address 192.168.1.1:

```
ping 192.168.1.1
```

To ping the host remote.imsva.com:

```
ping remote.imsva.com
```

postfix drop

Deletes a specified message or all messages in the email message queue.

SYNTAX:

```
postfix drop { <mail_id> | all }
```

VIEW	Privileged
PARAMETERS	<mail_id>: Specifies the message ID in the postfix queue to delete
EXAMPLES:	
To delete email message D10D4478A5 from the email message queue: postfix drop D10D4478A5	
To delete all email messages from the email message queue: postfix drop all	

postfix flush

Attempts to deliver all queued email messages.

SYNTAX:

```
postfix flush
```

EXAMPLES:

To deliver all queued email messages:

```
postfix flush
```


postfix queue

Displays all email messages queued in postfix.

SYNTAX:

```
postfix queue
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To display all postfix queued email messages:

```
postfix queue
```

postfix start

Starts the postfix mail system

SYNTAX:

```
postfix start
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To start the postfix mail system:

```
postfix start
```

postfix stop

Stops the postfix mail system.

SYNTAX:

```
postfix stop
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To stop the postfix mail system:

```
postfix stop
```

reboot

Reboots the IMSVA device immediately or after a specified delay.

SYNTAX:

```
reboot [time]
```

VIEW

Privileged

PARAMETERS

[time]: Specifies the delay, in minutes, to reboot the IMSVA device

EXAMPLES:

To reboot the IMSVA device immediately:

```
reboot
```

To reboot the IMSVA device after 5 minutes:

```
reboot 5
```

rescue

Rescues the application software.

SYNTAX:

```
rescue
```

VIEW

Privileged

PARAMETERS

None

EXAMPLES:

To rescue the application software:

```
rescue
```

resolve

Resolves an IP address from a hostname or resolves a hostname from an IP address.

SYNTAX:

```
resolve <dest>
```

VIEW

Privileged

PARAMETERS

<dest>: Specifies the IP address or hostname to resolve

EXAMPLES:

To resolve the hostname from IP address 192.168.10.1:

```
resolve 192.168.10.1
```

To resolve the IP address from hostname parent.imsva.com:

```
resolve parent.imsva.com
```

service Starts, stops, or restarts all IMSVA application services. Displays the current status of all IMSVA application services.	
SYNTAX: service {start stop restart status}	
VIEW	Privileged
PARAMETERS	start: Starts all IMSVA services stop: Stops all IMSVA services restart: Restarts all IMSVA services status: Displays the current status for all IMSVA services
EXAMPLES:	
To start all IMSVA services: service start	
To stop all IMSVA services: service stop	
To restart all IMSVA services: service restart	
To display the status for all IMSVA services: service status	

show arp

Displays the Address Resolution Protocol (ARP) tables.

SYNTAX:

```
show arp
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the ARP tables:

```
show arp
```

show connections

Displays the IMSVA device's current network connections.

SYNTAX:

```
show connections
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the IMSVA device's current network connections:

```
show connections
```

show date

Displays the current time and date.

SYNTAX:

```
show date
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the current time and date of the IMSVA device:

```
show date
```

show disk partition

Displays the file system disk space usage.

SYNTAX:

```
show disk partition
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the file system disk space usage of the IMSVA device:

```
show disk partition
```

show firewall

Displays firewall's configuration.

SYNTAX:

```
show firewall
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the firewall configuration settings of the IMSVA device:

```
show firewall
```

show hostname

Displays the IMSVA device's hostname.

SYNTAX:

```
show hostname
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the hostname of the IMSVA device:

```
show hostname
```

show ip dns

Displays the IMSVA device's IP address.

SYNTAX:

```
show ip dns
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the DNS configuration:

```
show ip dns
```

show ip interface

Displays the network interface card (NIC) status and configuration.

SYNTAX:

```
show ip interface
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the NIC status and configuration:

```
show ip interface
```


show ip route

Displays the IP address route table.

SYNTAX:

```
show ip route
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the IP address route table:

```
show ip route
```

show kernel

Displays the IMSVA device's OS kernel information.

SYNTAX:

```
show kernel {messages | modules | parameters}
```

VIEW

Root

PARAMETERS

messages: Displays kernel messages

modules: Displays kernel modules

parameters: Displays kernel parameters

EXAMPLES:

To display the OS kernel's messages:

```
show kernel messages
```

To display the OS kernel's modules:

```
show kernel modules
```

To display the OS kernel's parameters:

```
show kernel parameters
```

show log

Displays various IMSVA log data.

SYNTAX:

```
show log {imssd | imssmgr | imssps | postfix} [num]
```

VIEW

Root

PARAMETERS

imssd: Displays IMSVA scanner logs

imssmgr: Displays IMSVA manager logs

imssps: Displays IMSVA policy server logs

postfix: Displays postfix logs

[num]: Displays the specified number of latest log entries.
Default value is 25

EXAMPLES:

To display the latest 25 IMSVA scanner logs:

```
show imssd
```

To display the latest 50 IMSVA policy server logs:

```
show imssps 50
```

show ntp

Displays the NTP service status.

SYNTAX:

```
show ntp
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the NTP service status:

```
show ntp
```

show open-ports

Displays the listening ports on the IMSVA device.

SYNTAX:

```
show open-ports
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the NTP service status:

```
show open-ports
```

show process

Displays the status of IMSVA processes currently running.

SYNTAX:

```
show process [top]
```

VIEW

Root

PARAMETERS

[top]: Displays the status of IMSVA processes currently running and system resource usage

EXAMPLES:

To display the status of IMSVA processes currently running:

```
show process
```

show role

Displays the role (parent or child) of the IMSVA device in a group.

SYNTAX:

```
show role
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the role of the IMSVA device:

```
show role
```

show statistics

Displays the IMSVA device's system statistics information.

SYNTAX:

```
show statistics {io | vm}
```

VIEW

Root

PARAMETERS

io: Displays CPU statistics and I/O statistics for devices and partitions

vm: Displays virtual memory statistics

EXAMPLES:

To display IMSVA device CPU statistics and I/O statistics:

```
show statistics io
```

To display IMSVA device virtual memory statistics:

```
show statistics vm
```

show status

Displays the status of the IMSVA Web console and SSH.

SYNTAX:

```
show status [adminUI | ssh]
```

VIEW

Root

PARAMETERS

adminUI: Displays the status of adminUI.

ssh: Displays the status of SSH.

EXAMPLES:

To display status for both the IMSVA Web console and SSH:

```
show status
```

To display the IMSVA Web status

```
show status adminUI
```

To display the SSH status:

```
show status ssh
```

show timezone

Displays the IMSVA device's timezone settings.

SYNTAX:

```
show timezone
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display the IMSVA device's timezone settings:

```
show timezone
```

show uptime

Displays how long the IMSVA device has been running.

SYNTAX:

```
show uptime
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display how long IMSVA has been running:

```
show uptime
```

show version

Displays version number for the IMSVA device.

SYNTAX:

```
show version
```

VIEW

Root

PARAMETERS

None

EXAMPLES:

To display IMSVA's version number:

```
show version
```

shutdown

Specifies shutting down the IMSVA device immediately or after a specified delay.

SYNTAX:

```
shutdown
```

VIEW

Privileged

PARAMETERS

[time]: Shuts down the IMSVA device after a specified delay in minutes

EXAMPLES:

To shut down the IMSVA device immediately:

```
shutdown
```

To shut down the IMSVA device after a 5 minute delay:

```
shutdown 5
```

stop process

Stops a specific IMSVA process.

Note: Use the command [show process on page 6-27](#) to display the <pid> for each process.

SYNTAX:

```
stop process [core] <pid>
```

VIEW

Privileged

PARAMETERS

[core]: Stops a specific process and generates a core file
<pid>: Specifies the process to stop

EXAMPLES:

To stop the IMSVA process 2988:

```
stop process 2988
```

traceroute	
Displays the tracking route to a specified destination.	
SYNTAX:	
traceroute [-h hops] <dest>	
VIEW	Root
PARAMETERS	[-h hops]: Specifies the maximum number of hops to the destination. The minimum number is 6. <dest>: Specifies the remote system to trace
EXAMPLES:	
To display the route to IP address 172.10.10.1 with a maximum of 6 hops:	
traceroute 172.10.10.1	
To display the route to IP address 172.10.10.1 with a maximum of 30 hops:	
traceroute -h 30 172.10.10.1	

TABLE 6-1. Time Zone Setting Examples

REGION/COUNTRY	CITY
Africa	Cairo
	Harare
	Nairobi

TABLE 6-1. Time Zone Setting Examples

REGION/COUNTRY	CITY
America	Anchorage
	Bogota
	Buenos_Aires
	Caracas
	Chicago
	Chihuahua
	Denver
	Godthab
	Lima
	Los_Angeles
	Mexico_City
	New_York
	Noronha
	Phoenix
	Santiago
	St_Johns
	Tegucigalpa

TABLE 6-1. Time Zone Setting Examples

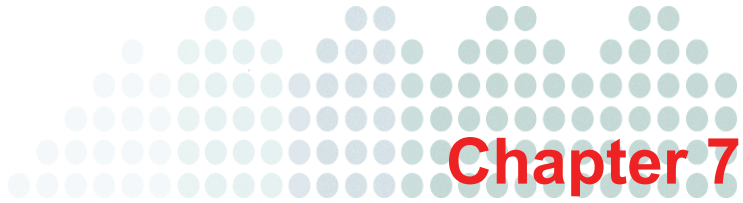
REGION/COUNTRY	CITY
Asia	Almaty
	Baghdad
	Baku
	Bangkok
	Calcutta
	Colombo
	Dhaka
	Hong_Kong
	Irkutsk
	Jerusalem
	Kabul
	Karachi
	Katmandu
	Krasnoyarsk
	Kuala_Lumpur
	Kuwait
	Magadan
	Manila
	Muscat
	Rangoon
	Seoul
	Shanghai
	Singapore
	Taipei
	Tehran
	Tokyo
	Yakutsk

TABLE 6-1. Time Zone Setting Examples

REGION/COUNTRY	CITY
Atlantic	Azores
Australia	Adelaide
	Brisbane
	Darwin
	Hobart
	Melbourne
	Perth
Europe	Amsterdam
	Athens
	Belgrade
	Berlin
	Brussels
	Bucharest
	Dublin
	Moscow
	Paris
Pacific	Auckland
	Fiji
	Guam
	Honolulu
	Kwajalein
	Midway

TABLE 6-1. Time Zone Setting Examples

REGION/COUNTRY	CITY
US	Alaska
	Arizona
	Central
	East-Indiana
	Eastern
	Hawaii
	Mountain
	Pacific



Modifying IMSVA Deployment

This chapter explains how to perform important maintenance tasks, such as changing the device role (parent to child or child to parent), changing a device IP address, and using the backup data port.

Topics include:

- [Internal Communication Port on page 7-2](#)
- [Adding and Removing Devices on page 7-3](#)
- [Changing Device Roles on page 7-4](#)
- [Changing the Deployment on page 7-5](#)
- [Changing IP Addresses on page 7-7](#)
- [on page 7-8](#)

Internal Communication Port

IMSVA supports multiple network interface cards (NIC) as data ports, which means one IMSVA device can have several IP addresses. In a group scenario, for communication to occur between an IMSVA parent device and child devices, each IMSVA device must specify a single IP address. The single IP address is as a means to identify each IMSVA device. With each device capable of having multiple IP address, this creates a problem for communication.

In order to resolve this issue, the concept of Internal Communication Port has been introduced. Once an Internal Communication Port is specified on an IMSVA device, the IP address of the port identifies the IMSVA device.

For example:

A parent device has two NIC installed with the following IP addresses:

- **eth0:** 192.168.10.1
- **eth1:** 192.168.20.1

With **eth0** specified as the Internal Communication Port, a child IMSVA device registering to the parent must specify the parent IP address as 192.168.10.1.

Child devices also have an Internal Communication Port. Both parent and child devices must communicate each other through their Internal Communication Port.

Note: The default Internal Communication Port for all IMSVA devices is **eth0**.

Adding and Removing Devices

This section explains how to add or remove a device from a group.

Adding a Child Device to a Group

To add a child device to a group:

1. Determine the device settings for the new device (IP address, net mask, gateway IP address, DNS server IP address, NTP server IP address if necessary).
2. Follow the instructions in [Setting Up a Child Device on page 1-17](#).

Removing a Child Device from a Group

This section explains how to remove a device from a group. If the device is active, you must first stop all services running on it. If it is inactive, you can unregister it directly.

Note: When you remove a device that has EUQ enabled, all email messages in the EUQ quarantine area are deleted. Trend Micro suggests notifying your users to handle the email messages in the EUQ quarantine area before you remove the device.

To remove a child device from a group:

1. Choose **Summary** from the menu. The Real-time Statistics tab appears by default.
2. On the top of the screen next to **Host**, verify that there are no email messages in the delivery queue or deferred queue for the device you want to remove. If there are messages in the delivery queue or deferred queue, wait momentarily for IMSVA to process them.
3. Click the **System** tab. The System Summary appears.
4. Under **Managed Services**, stop all services on the device you want to remove. When the services stop, the **Unregister** button appears.

Note: If the device was using EUQ, redistribute the data across the remaining EUQ databases before you unregister the child device:

- a. Choose **Administration > End-User Quarantine**.
- b. Click **Redistribute**.

5. Click **Unregister**. The child will be automatically removed from the group.

Tip: Trend Micro recommends that you notify your users to not add members to the EUQ approved list while you are adding a child device and redistributing EUQ data.

Resetting Child Devices When the Parent-Child Connection is Broken

If the parent device is broken, you must reset all child devices and choose one of them as parent. Then register all other devices to the parent.

To reset child devices:

1. Connect to the child devices through an SSH connection.
2. Log on to the OS shell as **root**.
3. Back up the folder `opt/trend/imss/queue` to other machine so that all messages quarantined or archived will not be deleted during rescue.
4. Exit the OS shell.
5. Log on to the CLI as **admin**.
6. Use the **enable** command to enter privilege mode.
7. Use the **postfix flush** command to flush postfix queue.
8. Use the **rescue** command to rescue the IMSVA application. The child device then changes to a parent automatically.

Changing Device Roles

This section explains how to change device roles.

Changing the Device Role from Parent to Child

To change the device role from parent to child:

1. Remove all child devices from the group (see [Removing a Child Device from a Group on page 7-3](#)).

2. Register the former parent devices to another parent device (see [Setting Up a Child Device on page 1-17](#)).

Changing the Device Role from Child to Parent

To change a device from a child to a parent, simply unregister it from its parent. The device automatically becomes a parent.

To change the device role from child to parent:

1. Unregister the child from the parent by doing one of the following:
 - Use the Web console (see [Removing a Child Device from a Group on page 7-3](#)).
 - Use the CLI:
 - a. Connect to the child device through an SSH connection.
 - b. Log on to the CLI as **admin**.
 - c. Use the **enable** command to enter privilege mode.
 - d. Use the **configure role unregister** command to unregister from the parent.
2. Register other child devices to this device if necessary.

Changing the Deployment

This section explains how to change the deployment to and from a gateway/non-gateway setup.

Changing the Deployment from Gateway to Non-Gateway

Note: IMSVA cannot use IP Filtering in a non-gateway setup.

To change the deployment from gateway to non-gateway:

1. On the Web console, choose **Administration > IMSVA Configuration > Configuration Wizard** from the menu.
2. Go to **Step 2: Deployment Settings**.

3. Clear the **Gateway deployment** check box.
4. Skip the rest of the wizard steps.
5. On the last wizard screen, click **Finish**.

Changing the Deployment from Non-Gateway to Gateway

Note: IMSVA can use IP Filtering in a gateway setup only.

To change the deployment from non-gateway to gateway:

1. On the Web console, choose **Administration > IMSVA Configuration > Configuration Wizard** from the menu.
2. Go to **Step 2: Deployment Settings**.
3. Select the **Gateway deployment** check box.
4. Skip the rest of the wizard steps.
5. On the last wizard screen, click **Finish**.

Changing IP Addresses

This section explains how to change the IP address of parent and child devices.

Note: When changing IP addresses in the Command Line Interface (CLI) through Secure Shell (SSH), do not close the SSH client until connection times out. Otherwise, the IP change script may not execute completely, causing inconsistencies in the settings.

Changing the Parent's Internal Communication Port IP Address

To change the parent's Internal Communication Port IP address:

1. Connect to the **parent** device through an SSH connection and do the following from the CLI:
 - a. Log on to the CLI as **admin**.
 - b. Use the **enable** command to enter privilege mode.
 - c. Change the IP address using the **configure interface** command.
2. Connect to each **child** device through an SSH connection and do the following:
 - a. Log on to the OS shell as **root**.
 - b. Use the **clish** command to enter the CLI.
 - c. Use the **enable** command to enter privilege mode.
 - d. Use the **configure role change-parent** command to change the parent IP to the updated one.

Changing the Child Internal Communication Port IP Address

If the parent or child devices have multiple network interface cards (NIC), check the route table on the parent and child device using the command `show ip route` in the CLI. Verify that parent-child communication uses the Internal Communication Port.

To change the child's Internal Communication Port IP address:

1. On the parent device, do the following from the IMSVA Web management console:

- a. Choose **Administration > IMSVA Configuration > Connections** from the menu.
 - b. Click the **Child IP** tab.
 - c. Under **Add IP Address**, add the new IP address.
2. Connect to the child device through an SSH connection and do the following from the CLI:
 - a. Log on to the CLI as **admin**.
 - b. Use the **enable** command to enter privilege mode.
 - c. Change the IP address using the **configure interface** command.
3. On the parent device, do the following:
 - a. Choose **Administration > IMSVA Configuration > Connections** from the menu.
 - b. Click the **Child IP** tab.
 - c. Under **Add IP Address**, remove the old child IP address.



Updating and Rescuing the System and Application

This chapter explains how to update and rescue the system and application files when Trend Micro releases patches, service packs, and other updates.

Topics include:

- [Updating the System and Application on page 8-2](#)
- [Rescuing IMSVA on page 8-4](#)

Updating the System and Application

When new operating system and application files become available from Trend Micro, deploy them to a parent IMSVA device and all of its child devices. By default, child devices will be updated before the parent device.

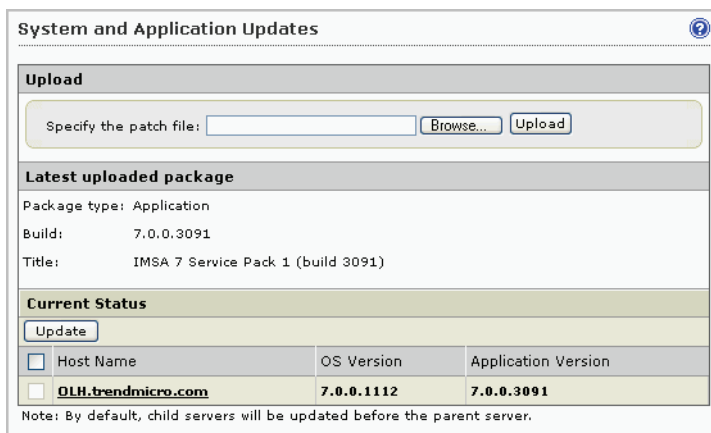
Updating devices is a two-step process:

Step 1: Upload the file to the IMSVA parent device.

Step 2: Deploy the file to selected devices.

To upload a new system or application file:

1. Choose **Administration > Updates > System & Applications** from the menu.



System and Application Updates

Upload

Specify the patch file:

Latest uploaded package

Package type: Application
 Build: 7.0.0.3091
 Title: IMSA 7 Service Pack 1 (build 3091)

Current Status

☐	Host Name	OS Version	Application Version
☐	OLH.trendmicro.com	7.0.0.1112	7.0.0.3091

Note: By default, child servers will be updated before the parent server.

2. Under **Upload**, click **Browse** and locate the file.
3. Click **Upload**. After the file finishes uploading, the package type, build number, and title appear under Latest uploaded package.

To deploy the system or application file:

1. Select the check boxes next to the devices to which you want to deploy the update.
2. Click **Update**.
3. Accept the license agreement.

After an operating system update or upgrade, IMSVA reboots. An application upgrade might force IMSVA to automatically reboot.

4. If IMSVA rebooted, wait for it to start up and log on again.
5. Choose **Administration > Updates > System and Applications** to view the summary screen.

-
- Note:**
1. During an update, do not modify any other settings. If you are updating several devices, you can click **Cancel** to stop the update of the next device.
 2. If you have applied some patches on a child device, and later unregister this child device from the parent device, IMSVA automatically rescues the system and application files, then re-applies the patches during unregistration. Due to the re-application of the patches, it might take some time before the Web management console for the new parent device (unregistered child device) becomes available.
-

If a device check box is grayed out, you cannot deploy the files to the device because the device:

- Already has the updated files.
- Has more up-to-date files than the ones you are trying to deploy.
- Is a child device and the patch requires you to upload the files and deploy them to the parent first, or vice versa.

To view update history for any device or to roll back an update:

1. Under **Host Name**, click the name of the device you want to view. A summary screen appears showing the updates and related log information.
2. To remove an update, click **Rollback**. You can only roll back the latest application updates.
3. To go back to the main screen, click **OK**.

Rescuing IMSVA

Rescuing IMSVA means that you reinstall the application.

Application Rescue Overview

You might need to rescue the application if application files become corrupt. Rescuing the application reinstalls the IMSVA application that instructs IMSVA to scan traffic, carry out filter actions, and create logs.

Rescuing the application is not the same as applying a patch.

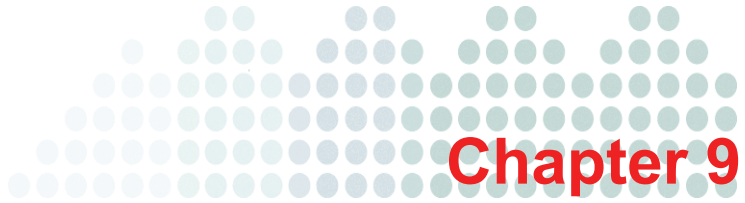
- Rescuing—Replaces all application files and deletes all settings.
- Applying a patch—Updates the existing application files to enhance features.

WARNING! All settings you configure through the Web console are deleted when you rescue the application. Before rescuing the application, create a backup of your settings.

Rescuing the Application

To rescue the application:

1. Log on to the IMSVA Web console as **admin** and export your current settings.
2. Enter the CLI as admin (see [Using the CLI on page 6-2](#)).
3. Type `enable` and provide the password to enter privileged mode.
4. Type `rescue`.
5. Type `y` to confirm. IMSVA rescue begins, and will take several minutes.
6. After the rescue process completes, log on to the IMSVA Web console and import your saved settings.
7. Re-activate **Trend Micro Antivirus and Content Filter** and **Spam Prevention Solution (SPS)** using the Activation Code.



Troubleshooting, FAQ, and Support

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

Topics include:

- [Troubleshooting on page 9-2](#)
- [Frequently Asked Questions on page 9-14](#)
- [Using the Knowledge Base on page 9-22](#)
- [Contacting Support on page 9-22](#)

Troubleshooting

Table 9-1 shows common troubleshooting issues that you might encounter when installing configuring, or administering IMSVA. Read through the solutions below. If you have additional problems, check the Trend Micro Knowledge Base.

For troubleshooting and FAQ information pertaining to the deployment of IMSVA, refer to the *IMSVa Installation Guide*.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
General	
Unable to access the Web console or other components.	The target port is not in the firewall approved list. Open the ports as shown in Table 9-2 on page 9-11 in the firewall. If you are unable to access the Web console, do the following: 1. Start the database process, <code>dbctl.sh</code>, before starting the Central Controller process, <code>S99ADMINUI</code>. 2. If you are still unable to access the Web console, restart the Central Controller process, <code>S99ADMINUI</code>. For more details, refer to Using IMSVA Scripts on page A-2.
Unable to access IMSVA through an SSH connection to the Data port	Do either of the following: • Verify that SSH is enabled on IMSVA. By default, SSH access to the Data port is disabled. To enable SSH access: 1. Connect to the device's Console (serial connection) or Management (SSH connection) port. 2. Enter your user name and password. 3. Select (4) Utility. 4. Select (6) Enable SSH access. • Verify that the application on your computer is running SSH2, not SSH1. IMSVA only supports SSH2.
No access to the Web console	The Web console URL is not a trusted site in Internet Explorer. Add the URL to the trusted sites.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Unable to activate products	If a proxy server is on your network, verify your proxy settings. To activate NRS, IMSVA needs to connect to Trend Micro. This process requires a DNS query. Therefore, if a DNS server is not available or has connection problems, activation will fail. Verify your DNS server settings. To verify your DNS settings from the CLI: 1. Enter the command line interface through a serial or SSH connection. 2. Use the command show ip dns to verify the current DNS setting. 3. Use the command configure dns <dns IP address> to modify the IP address of your DNS server if necessary. To verify your DNS settings from the Web console: 1. On the Web console menu, choose Administration > Configuration Wizard > Local System Settings > Network Settings. 2. Modify the IP address of your DNS server if necessary.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Unable to update components	IMSVa uses the HTTP protocol to connect to the update source (by default, the Trend Micro ActiveUpdate server). If a firewall is located between IMSVa and the Internet and IMSVa must use a proxy server, verify that your proxy settings are correct. To verify your proxy settings: 1. On the Web console menu, choose one of the following: • Administration > Configuration Wizard > Update Source > Proxy Setting • Administration > Update > Components > Source > Proxy Settings 2. Modify the proxy server settings if necessary. If you update the components manually and Unknown appears under Availability on the Update Now screen, IMSVa is unable to connect to the update source. Verify your network settings and connections and try again.
Email notifications do not display properly.	If your computer is running a non-English operating system and the notification message was not written in English, it may appear distorted. Modify the character set through the Web console. To modify the character set: 1. On the Web console menu, choose Administration > Notifications > Delivery Settings. 2. Next to Preferred Charset, select the language in which the messages will be encoded.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Unable to export configuration files	You will not be able to export configuration files if: • Your computer is running Windows 2003 SP1 or Windows XP SP2 • Internet Explorer (IE) 6.0 or 7.0 has default security settings You must change the default security settings on Internet Explorer. To change the IE security settings: 1. On the Internet Explorer menu, choose Tools > Internet Options. 2. Click the Security tab. 3. Click Custom Level. 4. Under Downloads > Automatic prompting for file downloads, select Enable. 5. Click OK and save your settings.
Cannot query message logs in IMSVA.	IMSVA scanner records the log with local time. To query message logs, synchronize the date/time for all machines with IMSVA.
Server displays as disconnected in the Summary screen.	A managed server could become disconnected for any of the following reasons: • The scanner was removed from your network. • The IMSVA manager service has stopped. • Network connection issue. Check your firewall settings for the Manager Service listening port. Click Administration > IMSVA Configuration > Connections > Components > IMSVA Manager Port.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
When viewing detailed information for quarantined or archived email, attachment information is sometimes not available	IMSVa records attachment information only when the scanning conditions for a policy is set to attachment. This issue occurs under the following circumstances: 1. When there is no attachment in the quarantined or archived email. 2. When attachment is not specified as a scanning condition. 3. Even when you have selected attachment as one of the scanning conditions, this issue will also occur if the number of attachments in the quarantined or archived email has exceeded the maximum number specified in the conditions.
Cannot enable LDAP with Kerberos authentication	Synchronize the date/time for all IMSVa devices.
End-User Quarantine Issues	
Unable to access the EUQ Web console	Do the following: • Verify that you are using the correct URL and port number. To view the console from another computer on the network, go to <pre>https://<target server IP address>:8447</pre>

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
Users are unable to log on to EUQ Web console	Do the following: 1. On the LDAP server, verify that the user accounts are in the correct group. Only user accounts in the approved group can access EUQ. 2. Verify LDAP and User Quarantine Access settings through the IMSVA Web console: a. Choose Administration > IMSS Configuration > Connections > LDAP from the menu. b. Verify all settings, especially the LDAP type and server information. If you are using Kerberos authentication, ensure that the time for all IMSVA computers and the LDAP server is synchronized. c. Choose Administration > User Quarantine Access from the menu. d. Enable User Quarantine Access. e. Verify that the correct LDAP groups appear under Selected Groups and that the user account belongs to the selected groups. 3. Verify that your users are using the correct log on name and password. Logon Name Format on page 5-10
The EUQ Web digest does not display quarantined email information correctly	Verify that the correct character set is selected: 1. Choose Administration > Notifications > Delivery Settings. 2. Next to Preferred charset, choose the character set that will properly display the digest information.
Some quarantined email messages are not appearing on the EUQ Web console	The EUQ Web console can only access email that IMSVA identifies as spam or phishing attempts. From the EUQ Web console, you cannot view quarantined email that violated other rules, such as the antivirus rule.
Cannot enable LDAP with Kerberos authentication.	Kerberos protocol requires time synchronization between the Kerberos server and IMSVA. Synchronize the date/time for all computers with IMSVA.
IP Filtering Issues	

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
FoxProxy cannot start up	There are several reasons why FoxProxy might not start. To find out the reason, view the IP Profiler logs. To view IP Profiler logs: 1. Go to the directory where IP Profiler is installed (by default: <code>/opt/trend</code>). 2. Open <code>foxproxy.ini</code>. 3. Change the value for <code>log_level</code> to 4. 4. Restart FoxProxy by typing the following: <code>/opt/trend/ipprofiler/script/foxproxyd restart</code> 5. Open the log file by typing the following: <code>/opt/trend/ipprofiler/logs/foxproxy-general.****</code>
Unable to connect to FoxProxy	Verify that FoxProxy is running and that it is binding on port 25.
FoxProxy processes email messages slowly	When FoxProxy receives email, it performs a DNS query on FoxDNS. If Bind is not running, FoxProxy continues to wait until the DNS query times out. Verify that the bind service is running on the computer where FoxDNS is installed: 1. Type the following command: <code>ps -ef grep named</code> 2. Start the service if it is not running.
Unable to view connections that FoxProxy is blocking	Every five (5) minutes, FoxProxy sends information about blocked connections to the IMSVA server. Wait for at least five minutes before viewing the connection information. To change this time value: 1. Open <code>foxproxy.ini</code>. 2. Modify the value for <code>report_send_interval</code>.
FoxDNS is not functioning	Verify that BIND service is running: 1. Type the following command: <code>ps -ef grep named</code> 2. Start the service if it is not running.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
No IP Profiler log information exists	The following IP Profiler-related log files are in the IMSVA admin database: • foxmsg.*** • foxnullmsg.*** • foxreport.*** Verify that the log files exist: 1. Go to the log directory on the where IMSVA is installed (by default: /opt/trend/imss/log/). 2. If the files are not present, use the following command to check if imssmgr is running: ps -ef grep imssmgr 3. Check if FoxProxy is running: ps -ef grep foxproxy 4. Verify that IP Profiler is enabled. In table 't_foxhuntersetting', the following should exist: record: 'Type' = 1 and 'enable' = TRUE
NRS does not work after being enabled from the Web console.	NRS may not work due to the following reasons: • Spam Prevention Solution (SPS) was not activated. NRS shares the same Activation Code (AC) with SPS. If SPS has not been activated, please activate SPS and then activate NRS. • The computer on which the scanning service is installed cannot access the Internet. MTA cannot get a response for the DNS query for AC validation. Please confirm that the computer where the scanner service is installed has access to the Internet. Please activate SPS and confirm that the computer with SPS installed can access the Internet.

TABLE 9-1. Troubleshooting issues

ISSUE	SUGGESTED RESOLUTION
The MTA settings on the SMTP Routing Web console screen are not being written into the Postfix configuration files	By default, the settings on the SMTP routing screen cannot be written to Postfix. Enable this function using the following steps: Go to the IMSVA configuration directory (by default: <code>/opt/trend/imss/config</code>). Open the IMSVA configuration file <code>imss.ini</code> Change the value for <code>enable_postset_thd</code> to <code>yes</code> or leave the value empty. Restart IMSVA manager using the following command: <code>/opt/trend/imss/script/S99MANAGER restart</code>
IP profiler does not block IP addresses in the Blocked List.	The changes required about one (1) minute to take effect. Please wait one (1) minute.
Blocked IP address does not display in the Overview page	The Overview page displays the top 10 blocked IP addresses by type for the last 24 complete hours. For example, at 16:12 today the Overview page displays data from 16:00 yesterday to 16:00 today. Please view the Overview page after an hour.

IMSVA Ports

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

TABLE 9-2. IMSVA Ports

Port Number	Component and Role	Configuration Location
8015	Tomcat management port that can handle Tomcat management command.	{IMSVa}\UI\euqUI\conf\server.xml: Server\port
8445	Admin UI listening port. You need to open this port to log on to the Web management console using a Web browser.	Tomcat listen port: {IMSVa}\UI\adminUI\conf\server.xml: Server\Service\Connector\port
8446	EUQ service listening port.	{IMSVa}\UI\euqUI\conf\server.xml: Server\Service\Connector\port
8447	EUQ service listening port with load balance.	{IMSVa}\UI\euqUI\conf\EUQ.conf: Listen\VirtualHost\ServerName
10024	IMSVa scanner reprocessing port. Messages released from the central quarantine area in the admin database and from the EUQ database will be sent to this port for reprocessing.	imss.ini[Socket_3]\proxy_port

TABLE 9-2. IMSVa Ports

Port Number	Component and Role	Configuration Location
10026	The IMSVA "passthrough" SMTP port for internal use (such as the delivery of notification messages generated by IMSVA.) All messages sent to this port will not be scanned by IMSVA. Due to security considerations, the port is only bound at IMSVA server's loopback interface (127.0.0.1). It is therefore not accessible from other computers. You are not required to open this port at the firewall.	tsmtpd.ini
15505	IMSVA Manager listening port. The manager uses this port to accept management commands (such as service start/stop) from the Web management console. The manager also provides quarantine/archive query results to the Web management console and the EUQ Web console through this port.	From the Web management console, click Administration > IMSVA Configuration > Connections > Components on the menu.
IMSVA uses the following ports when you enable related service:		
389	LDAP server listening port.	From the Web management console, click Administration > IMSVA Configuration > Connections > LDAP on the menu.

TABLE 9-2. IMSVA Ports

Port Number	Component and Role	Configuration Location
80	Microsoft IIS http listening port. You would need this port if you are using Control Manager to manage IMSVA, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click Administration > IMSVA Configuration > Connections > TCM Server on the menu.
443	Microsoft IIS https listening port. You would need this port if you are using Control Manager to manage IMSVA, as the Control Manager Server depends on Microsoft IIS.	From the Web management console, click Administration > IMSVA Configuration > Connections > TCM Server on the menu
88	KDC port for Kerberos realm.	Not configurable on the IMSVA server.
53	The Bind service listening port. Please do not change the port.	Not configurable on the IMSVA server.

TABLE 9-2. IMSVA Ports

Frequently Asked Questions

Postfix MTA Settings

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

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

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

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

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

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

WARNING! Use extreme caution when modifying the configuration file.

Network Reputation Services

How do I configure Network Reputation Services (NRS) to not block certain IP addresses or domains?

Add the IP addresses / domains to the NRS approved list by doing the following:

- Log on to the Web console.
- Click **IP Filtering > Approved List**.
- Add the IP addresses or domains that you do not want blocked to the Approved List.

Note: If the domain cannot be resolved by the DNS service, the domain will not work in the approved list.

IP Profiler

Why is the domain name of an IP address that was added to the blocked/approved list always N/A?

IMSVA does not determine the domain name of an IP address that was added to the blocked/approved list (IMSVA does resolve the IP address of an added domain name).

Why does the IP Filtering Suspicious IP screen also display the connection information of blocked IP addresses?

The **IP Filtering > Suspicious IP** screen shows all information for successful connections. Therefore, although an IP address is now in the blocked list, the previous connections for this IP address, which have not been blocked, are shown.

How does IP Profiler process email?

The IP Filter decides if the source IP address is a safe IP address. IMSVA scanner service queries matched policies from the IMSVA policy service. The policies are applied to the email in the required order. If a policy specifies that an email should be quarantined, deleted or delivered, then the action is taken and the remaining policies are not applied.

Is the LDAP service mandatory for analyzing whether an incoming traffic is a form of DHA attack?

Technically, LDAP service is not a must-have. The DHA rule of IMSVA 7.0 relies on the result returned from Postfix, which in turn passes the result to FoxProxy, a sub-module of IP Profiler, for analysis. The LDAP server is just one of the many means by which Postfix checks for the existence of a recipient's mailbox.

Quarantine and Archive

Can I use special characters to perform queries?

Yes, you can use the following special characters to perform queries:

- **Asterisk (*)** — Used as a wildcard character to search for zero or more characters. You can use asterisk (*) to search for email addresses or file names.

To search for email addresses, see the following examples:

***** — Valid representation of all email addresses.

***@domain.tld, name@*.tld** — Valid representation of the whole name or the domain (not the top level domain (TLD)).

***@*.tld** — Valid representation of both the name and the domain (not the TLD).

To search for file names, see the following examples:

. — Valid representation of all files.

***.extension** — Valid representation of all files of a certain extension.

- name.*** —Valid representation of files with a specific name but of any extension.
- **Semicolon (;)** — Used as a separator when searching for multiple recipients or attachments.

End-User Quarantine

If I am using Kerberos, why are users unable to log on to the EUQ console with a short name: "domain\user_name"?

Kerberos servers cannot accept user names in the format: Domain\user_name.
Kerberos requires the format user_name@domain.xxx

If I installed Microsoft Exchange Server, and have set multiple mail addresses for each user, how do I enable EUQ to check multiple mail addresses for one user?

If you installed one Microsoft Exchange Server together with the Active Directory, you can do the following:

- a. Open the table `tb_global_setting` in IMSVA administrator database and replace the value of `LDAP-->mail_attr` from "mail" to "proxyAddresses".
- b. Restart all IMSVA services.

How can I speed up my LDAP access if the LDAP server is Active Directory?

There are two methods to speed up your access. The method you use depends on the port number you can use: port 389 or port 3268.

Active Directory uses 3268 for the Global Catalog. LDAP queries that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

Tip: Trend Micro recommends using port 3268 for LDAP queries.

Active Directory uses port 389 for LDAP query. If one item cannot be queried in one domain controller, it uses the LDAP referral mechanism to query another domain controller. Use port 389 if your company has only one domain or if port 3268 is unavailable.

To use port 3268 for LDAP queries:

- a. Click **Administration >IMSS Configuration > Connections**. The Connections screen appears.
- b. Click the **LDAP** tab.
- c. Configure the LDAP listening port as 3268.

To use port 389 for LDAP queries:

- a. Click **Administration >IMSS Configuration > Connections**. The Connections screen appears.
- b. Click the **LDAP** tab.
- c. Configure the LDAP listening port:
 - To use port 3268, configure the LDAP listening port as 3268.
 - To use port 389, configure the LDAP listening port as 389.

What user logon name formats does IMSVA support for Active Directory?

Active Directory supports the following log on name formats:

- Example 1: bob@imsstest.com

Note: The log on name is not email address (though it appears as one).

- Example 2 (pre-Windows 2000): IMSSTEST\bob

Note: The pre-Windows 2000 format is not supported by Kerberos authentication.

Transport Layer Security (TLS)

What do I have to do to use Transport Layer Security (TLS)?

Upload the certificate for TLS and enable it on the **Administration > IMSVA Configuration > SMTP Routing > Connections** screen. IMSVA 7.0 uses the Postfix TLS function. All settings are written to the configuration file `main.cf`. For more information, see [Transport Layer Security on page C-1](#).

Spam Protection Service

How is the spam catch rate determined?

Specify a threshold value between 3.0 and 10.0 for IMSVA classification of an email message as spam. A high threshold value means that a message must be very "spam-like" to be classified as spam (this decreases the spam catch rate but reduces the likelihood of false positives). A lower threshold value means that a message only needs to be slightly "spam-like" to be classified as spam (this increases the spam catch rate and may lead to more false positives).

How do I simplify SPS rules after migration?

In order to retain all SPS filter settings for all policies of IMSVA 1.0 or InterScan Messaging Security Suite 5.7, IMSVA 7.0 migrates each SPS filter to one SPS rule (or several SPS rules depending on the Routes and Filter Actions). If you want to reduce the number of SPS rules after migration, do the following:

- Create a new SPS rule after migration.
- Delete all migrated SPS rules.

ActiveUpdate

How do I roll back a pattern file?

Click the **Rollback** button on the Summary page.

Others

How does IMSVA process a partial email?

IMSVa rejects partial email as a malformed message if `BypassMessagePartial=no` in the `imss.ini` file (default setting).

If the key is set to `yes`, IMSVA will bypass the partial mails. Trend Micro does not recommend changing the item "BypassMessagePartial" to `yes` as this may cause virus leak.

Why can't newly created administrator accounts access the User Quarantine Access, Admin Accounts and Product License pages?

Only the default IMSVA admin account has the permission to access the User Quarantine Access, Admin Accounts and Product License pages. Delegated admin accounts cannot access these pages.

Why are changes to the IMSVA configuration settings not effective immediately?

There is a lapse between the time you modify the configuration settings from the Web management console and the time modifications are actually updated on the IMSVA server.

Policy settings will be reloaded in no longer than three (3) minutes. If you want the settings to load faster, please modify the

`policy_server=>dbChangePollIntervalInSecs` setting in the `tb_global_setting` table of the IMSVA administrator database as desired.

For other general settings, `imssmgr` will take no longer than one (1) minute to reload the new settings modified from the Web management console.

Trend Micro recommends that you do not send mail to IMSVA immediately after modifying the configuration settings from the Web management console.

Is there any limit on the maximum number of the following items?

- Senders and recipients for each rule
- Mail addresses in one address group
- Approved/Block Senders for SPS rule

Technically, there is one limitation on the total size of each rule, which is 640KB. The total size includes the rule route (senders/recipients), rule filter (scanning condition), and rule action. Assuming that each email address/LDAP account consists of 20 characters, IMSVA can support at least 10,000 senders/recipients for the rule route.

The maximum number of mail addresses for one address group is 10,000.

The maximum number of Approved/Block Senders for SPS rule is 5000.

Mails from some senders are always received as attachments. The mail body is also replaced by the disclaimer or stamp. Why is that so?

When the charset of the stamp is different from the charset of the mail content, IMSVA will encounter issues inserting the stamp into the mail body after scanning the mail. In this situation, IMSVA will create a new mail, insert the stamp into the mail body and attach the original message. The mail content, however, will not be changed.

How can I specify a keyword expression to represent a blank header for matching fields such as “from”, “to”, or “subject” when creating rules with content filter?

If you are going to use a regular keyword expression to represent a blank header, Trend Micro recommends that you use “^ (\s) *\$” (without the quotation marks). The expression “^ (\s) *\$” (without the quotation marks) represents a blank header or whitespace characters.

For example, if you want to check if a mail’s “**from**” header is blank, you can edit a rule’s scanning condition as follows:

- a. On the Web management console, click **Policy>Policy List**.
- b. Click the link for an existing rule to edit the rule.
- c. Click **And scanning conditions match**.
- d. Click **Header keyword expressions** under the **Content** section.
- e. Click **Add** to create a new keyword expression.
- f. Add the content as “^ (\s) *\$” (without the quotation marks).

Using the Knowledge Base

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

<http://esupport.trendmicro.com>

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

Contacting Support

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

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

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

Get the latest Trend Micro product documentation:

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

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

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

TrendLabs

TrendLabs is the global antivirus research and support center of Trend Micro. It is located on three continents, with a staff of more than 250 researchers and engineers who operate around the clock to provide you, and every Trend Micro customer, with service and support.

You can rely on the following post-sales service:

- Regular virus pattern updates for all known "zoo" and "in-the-wild" computer viruses and malicious codes
- Emergency virus outbreak support
- Email access to antivirus engineers
- Knowledge Base, the Trend Micro online database of technical support issues

TrendLabs has achieved ISO 9002 quality assurance certification.

Security Information Center

Comprehensive security information is available at the Trend Micro Web site:
<http://www.trendmicro.com/vinfo/>

At the top of the Web console, click the Help drop-down box, then Security Info. Information available:

- List of viruses and malicious mobile code currently "in the wild," or active

- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Security advisories
- Scams and hoaxes
- Joke programs
- Spyware/Grayware
- Phishing Encyclopedia

Staying Up to Date

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

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

The Update Center screen displays. Select your product from the links on this screen. Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

Send Trend Micro Your Viruses

If you have a file you think is infected but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

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

Please include in the message text a brief description of the symptoms you are experiencing. The team of antivirus engineers will analyze the file to identify and characterize any virus(es) it may contain, usually the same day it is received.

You can also send an email to: virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject.



Appendix A

IMSVA Scripts

This appendix provides you with a list of IMSVA scripts and their respective parameters that you can invoke from the command line.

Topics include:

- [Using IMSVA Scripts on page A-2](#)

Using IMSVA Scripts

IMSPA scripts provide a convenient and alternative means of performing administrative tasks from the command line.

See [Table A-1](#) for a list of the scripts, their respective parameters and the functions they perform.

Note: All scripts listed in the table are located in `/opt/trend/imss/script`, except `foxproxyd`, which is located in `/opt/trend/imss/ipprofiler/script`.

SCRIPTS	PARAMETERS	DESCRIPTIONS
foxproxyd	start / stop / restart	IP Profiler service
dbctl.sh	start / stop / restart	Postgres database service
imsstop.sh		Forces all IMSS services to stop.
postfixctl.sh	start / stop / reload / restart	Postfix daemon
regipro.sh	reg / unreg	Register or unregister IP Profiler to or from the admin database.
S99ADMINUI	start / stop / restart	Central Controller
S99CLEANEUQ		Removes expired quarantined data from the EUQ and admin databases as configured under the Administration > User Quarantine Access area of the Web management console.
S99CLEANEXPIRE		Removes expired quarantined and archived data from the EUQ and admin databases as configured under the Quarantine & Archive > Settings area of the Web management console.
S99CMAGENT	start / stop / restart	CMAgent service
S99DIGEST		Sends the EUQ digest message

TABLE A-1. IMSVA scripts

SCRIPTS	PARAMETERS	DESCRIPTIONS
S99EUQ	start / stop / restart	EUQ service
S99FOXDNS	start / stop / restart	Foxdns service
S99IMSS	start / stop / restart	IMSS scanner service
S99MANAGER	start / stop / restart	Manager service
S99MONITOR	start / stop / restart	Manager monitor service
S99POLICY	start / stop / restart	Policy service
S99REPORT	[option] start / stop / restart [option]: • -s—generates centralized reports (covers all one-time and scheduled reports configured on the Web management console) • -h—generates hourly individual traffic data • -t—generates hourly traffic data • -d—performs database log maintenance	Used by S99SCHEDULED to generate related reports. Note: Do not run this script on its own.
S99UPDATE	start / stop	Used by S99SCHEDULED to run the scheduled update. Note: Do not run this script on its own.
S99SCHEDULED		Starts the scheduled task.
forceUpdate.sh	DBDSN username password	Notifies the policy server to reload the policy settings
euqtrans		Transfers EUQ database data

TABLE A-1. IMSVA scripts



Appendix B

Default Directory Locations

This appendix provides information on the default directory locations that IMSVA uses for mail processing.

Topics include:

- [Default Mail Queues on page B-2](#)
- [eManager, Virus and Program Logs on page B-3](#)
- [Temporary Folder on page B-3](#)
- [Notification Pickup Folder on page B-4](#)

Default Mail Queues

Table B-1 shows the various mail directories that store the mail messages managed by IMSVA.

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
queue_malform=/opt/trend/imss/queue/malform		Stores malformed messages.
queue_archive=/opt/trend/imss/queue/archive		Stores archived messages.
queue_quarantine = /opt/trend/imss/queue/quarantine		Stores quarantined messages.
queue_notify=/opt/trend/imss/queue/notify	queue_notify_big=/opt/trend/imss/queue/notifybig	Stores notification messages.
queue_postpone=/opt/trend/imss/queue/postpone	queue_postpone_big=/opt/trend/imss/queue/postponebig	Stores postponed messages.
queue_deliver=/opt/trend/imss/queue/deliver	queue_deliver_big=/opt/trend/imss/queue/deliverbig	Stores messages for final delivery.
queue_reprocess=/opt/trend/imss/queue/reprocess	queue_reprocess_big=/opt/trend/imss/queue/reprocessbig	Stores messages pending reprocessing.
queue_handoff=/opt/trend/imss/queue/handoff	queue_handoff_big=/opt/trend/imss/queue/handoffbig	Stores messages pending handoff.
queue_undeliverable=/opt/trend/imss/queue/undeliverable		Stores undeliverable messages.
queue_unnotify=/opt/trend/imss/queue/unnotify		Stores undeliverable notification messages.
/var/spool/postfix/incoming		Stores incoming mail from the network, or from the /var/spool/postfix/maildrop directory.

TABLE B-1. Default Mail Locations

QUEUES FOR REGULAR MAILS	QUEUES FOR LARGE MAILS	DESCRIPTIONS
/var/spool/postfix/active		Stores messages that the queue manager has opened for delivery.
/var/spool/postfix/deferred		Stores messages that could not be delivered on the first attempt.
/var/spool/postfix/corrupt		Unreadable or damaged queue files are moved here for inspection.
/var/spool/postfix/hold		Stores messages that are kept "on hold" until someone releases them.

TABLE B-1. Default Mail Locations

eManager, Virus and Program Logs

Many modules in IMSVA write log information for troubleshooting purposes to the following folder:

/opt/trend/imss/log

and

/var/log

Temporary Folder

IMSVa stores all application-generated temporary files in the temporary folder:

/opt/trend/imss/temp/

and

/tmp

Note: This directory is not configurable.

Notification Pickup Folder

IMSVa stores all notification messages and picks them up from the following folders, then delivers them to a specified SMTP notification server:

/opt/trend/imss/queue/notify/

and

/opt/trend/imss/queue/notifybig

To configure the SMTP notification server:

Choose **Administration > Notifications > Delivery Settings** from the menu.

Note: The queue_notify_big queue is for large mail messages.



Appendix C

Transport Layer Security

This appendix provides you with an introduction to Transport Layer Security (TLS), and includes additional information on configuring TLS settings.

Topics include:

- [How Transport Layer Security Works on page C-2](#)
- [Transport Layer Security Related Terms on page C-2](#)
- [Prerequisites to Using Transport Layer Security with IMSVA on page C-3](#)
- [Configuring Transport Layer Security Settings on page C-4](#)

How Transport Layer Security Works

Transport Layer Security (TLS) provides a secure communication channel between client and server applications over the internet, ensuring the privacy and integrity of the data during transmission.

A client and server establish a TLS connection through a handshaking procedure as described below:

1. The handshake begins when the client requests a secure connection with the server by sending a list of ciphers.
2. The server then selects one cipher presented by the client and replies with its digital certificate that may have been signed by a Certificate Authority (CA).
3. The client verifies the server's identity with the trusted CA certificate. If the verification fails, the client may choose to stop the TLS handshake.
4. Upon verifying the server's identity, the client proceeds to generate the session keys by encrypting a message using the server's public key.
5. This message can only be decrypted using the corresponding private key. The server's identity is thus authenticated when the server is able to decrypt the message successfully using the private key.
6. The handshake completes and the secure connection is established after the client and server have created the material required for encryption and decryption.

Transport Layer Security Related Terms

- **TLS handshake**—The process by which the client and server applications establish the TLS secure connection.
- **Certificate Authority (CA)**—A CA is an entity that issues digital certificates to applicants after verifying the applicants' credentials. A CA acts as a trusted third-party and attests that the public key contained in the certificate belongs to the party specified in the certificate.
- **Certificate**—A digital certificate owned by a client or server that is used to verify the client or server's identity. A valid certificate is signed by a trusted CA that verifies the party specified in the certificate is indeed the owner of the public key contained therein.
- **Public key**—A recipient's public key used to encrypt a message.

- **Private key**—The only key that can decrypt a message encrypted using the recipient's public key.

Prerequisites to Using Transport Layer Security with IMSVA

Check the following before you configure a TLS connection in IMSVA:

- Obtain a digital certificate

You may obtain a digital certificate through one of the following methods:

- Generate the certificate and public/private key pairs using some certificate generator or key generator tools, then request a certificate authority to sign the certificate.
- Apply for the certificate and public/private key pairs from a certificate authority.
- Ensure that the certificate format is valid
 - IMSVA only supports .pem certificate format.
 - Ensure that the signed certificate contains both the private key and certificate information.
- **Upload the certificate**
 - a. Click **Administration > IMSVA Configuration > SMTP Routing** on the menu.
 - b. Click the **Connections** tab.
 - c. Under **Transport Layer Security Setting**, click the **Browse** button next to **CA certificate**.
 - d. Select the signed certificate.
 - e. Click **Upload**.

Configuring Transport Layer Security Settings

You can enable global Transport Layer Security (TLS) settings for incoming and outgoing messages using the Web management console. When implementing TLS with IMSVA acting as the server, you enable incoming TLS, but when implementing TLS with IMSVA acting as the client, enable outgoing TLS.

While the Web management console provides a convenient means to enable global TLS settings, it does not provide the option to configure specific TLS settings per site. To configure site-specific TLS settings, refer to the scenario below.

Scenario on Configuring Site-Specific TLS Settings

This example is based on the assumptions that you would like to:

- disable incoming TLS globally
- enforce TLS and set the TLS level to `verify` for messages received from 192.168.1.1
- disable outgoing TLS globally
- enforce TLS and set the TLS level to `verify` for messages sent to `example.com`. It is assumed that you have configured the relay method through domain-based delivery with the next hop set to 192.168.2.2, port 25.
- enforce TLS and set the TLS level to `encrypt` for messages sent to `example1.com` (relay by querying DNS server).

To configure site-specific TLS settings for the above scenario, do the following:

1. Edit `/opt/trend/imss/config/imss.ini` as follows:
`detach_key_postfix=smtpd_use_tls:smtpd_enforce_tls:smtpd_tls_CAfile:smtpd_tls_cert_file:smtpd_tls_key_file:smtp_use_tls`
2. Restart `imssmgr` using the command `/opt/trend/imss/script/S99MANAGER restart`.
3. Copy the CA certificate file, public key file and private key file to the `/opt/trend/imss/postfix/etc/postfix` folder.
4. Add the following in `/opt/trend/imss/postfix/etc/postfix/main.cf`:
`smtpd_tls_security_level = none`
`smtpd_tls_CAfile = /opt/trend/imss/postfix/etc/postfix/ca.pem`

```

smtpd_tls_cert_file = /opt/trend/imss/postfix/etc/postfix/public.pem
smtpd_tls_key_file = /opt/trend/imss/postfix/etc/postfix/private.pem
smtpd_tls_policy_maps =
hash:/opt/trend/imss/postfix/etc/postfix/smtpd_tls_policy
smtpd_tls_policy:
192.168.1.1 verify

```

```

smtp_tls_security_level = none
smtp_tls_CAfile = /opt/trend/imss/postfix/etc/postfix/ca1.key
smtp_tls_cert_file = /opt/trend/imss/postfix/etc/postfix/public1.key
smtp_tls_key_file = /opt/trend/imss/postfix/etc/postfix/private1.key
smtp_tls_policy_maps =
hash:/opt/trend/imss/postfix/etc/postfix/smtp_tls_policy
smtp_tls_policy:
[192.168.2.2]:25 verify
example1.com encrypt

```

5. Create two files `smtpd_tls_policy` and `smtp_tls_policy` under the folder `/opt/trend/imss/postfix/etc/postfix`.

Content of `smtpd_tls_policy`:

```
192.168.1.1 verify
```

Content of `smtp_tls_policy`:

```
[192.168.2.2]:25 verify
```

```
example1.com encrypt
```

6. Generate the database files using the commands:

```
postmap smtpd_tls_policy
postmap smtp_tls_policy
```
7. Reload Postfix using the command `postfix reload`.

Incoming Transport Layer Security Levels

The `smtpd_tls_security_level` parameter controls the global TLS settings for incoming messages. To configure specific incoming TLS settings per site, you need to define the security levels for each site by editing the `smtpd_tls_policy_maps` and `smtpd_tls_policy` parameters in `main.cf`.

Table C-1 lists the incoming TLS security levels in order of increasing security. For more information on each security level, visit http://www.postfix.org/TLS_README.html#server_tls

SECURITY LEVELS	DESCRIPTIONS
none	No TLS.
may	Opportunistic TLS.
encrypt	Mandatory TLS encryption.
verify	Mandatory TLS verification.

TABLE C-1. Incoming TLS levels

Scenario on Configuring Incoming Transport Layer Security Settings

Assuming that you would like to disable TLS globally but apply TLS settings only to specific IP addresses, for example, 10.28.148.1, configure `main.cf` as follows:

```
smtpd_tls_security_level=none
smtpd_tls_policy_maps= hash:/opt/trend/imss/postfix/etc/postfix/smtpd_tls_policy
smtpd_tls_policy:
10.28.148.1 may
```

Client whose IP address is not in the `smtpd_tls_policy` list will communicate with the Postfix server without TLS.

You can change the security level from 'may' to 'encrypt' or 'verify' if desired.

Outgoing Transport Layer Security Levels

The `smtp_tls_security_level` parameter controls the global TLS settings for outgoing messages. To configure specific outgoing TLS settings per site, you need to define the security levels for each site by editing the `smtp_tls_policy_maps` and `smtp_tls_policy` parameters in `main.cf`.

Table C-2 lists the outgoing TLS security levels in order of increasing security. For more information on each security level, visit

http://www.postfix.org/TLS_README.html#client_tls

SECURITY LEVELS	DESCRIPTIONS
none	No TLS
may	Opportunistic TLS
encrypt	Mandatory TLS encryption
verify	Mandatory TLS verification
secure	Secure-channel TLS

TABLE C-2. Outgoing TLS levels

Scenario on Configuring Outgoing Transport Layer Security Settings

Assuming that you would like to disable TLS globally but apply TLS settings only to specific outgoing connections, for example, 10.28.148.1, configure `main.cf` as follows:

```
smtp_tls_security_level=none
```

```
smtp_tls_policy_maps= hash:/opt/trend/imss/postfix/etc/postfix/smtp_tls_policy
```

```
smtp_tls_policy:
```

```
[10.28.148.1]:25 may
```

Server whose IP address is not in the `smtp_tls_policy` list will communicate with Postfix client without TLS.

You can change the security level from 'may' to 'encrypt' or 'verify' if desired.



Appendix D

Creating a New Virtual Machine Under VMware ESX for IMSVA

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

Topics include:

- [Creating a New Virtual Machine on page D-2](#)

Creating a New Virtual Machine

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

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

To create the virtual machine:

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

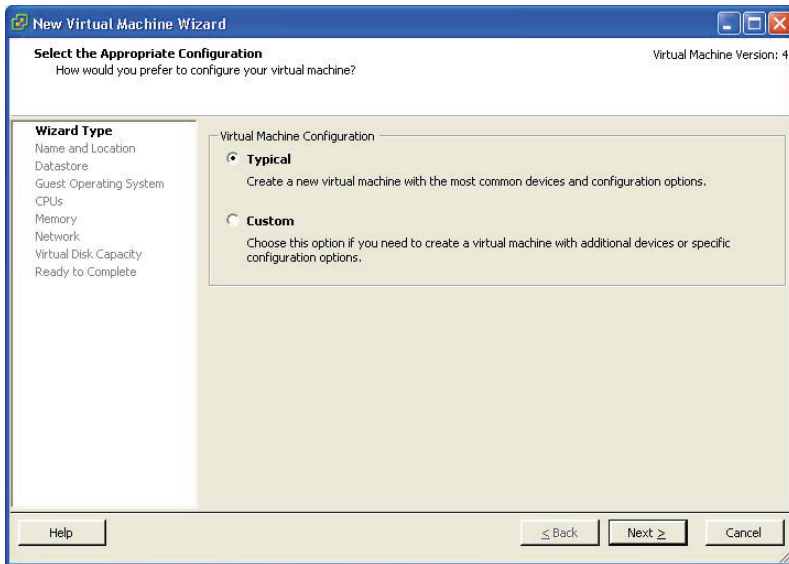


FIGURE D-1 Virtual Machine Configuration

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

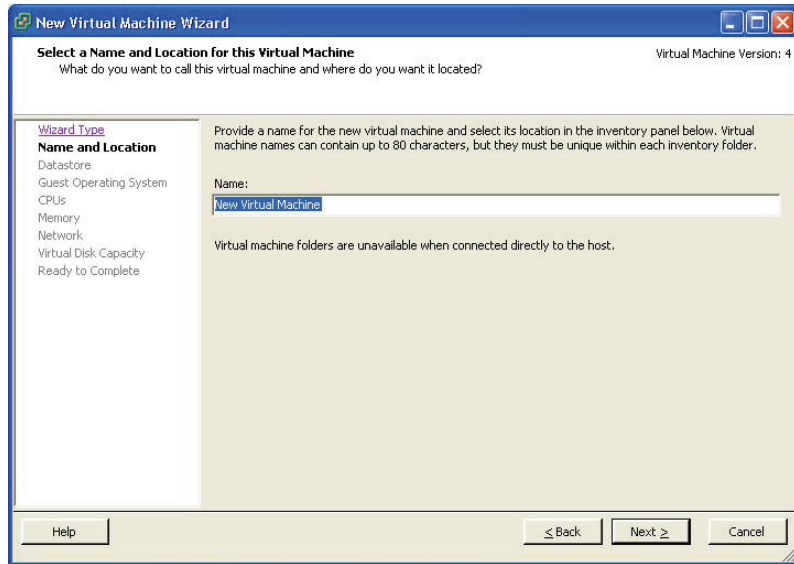
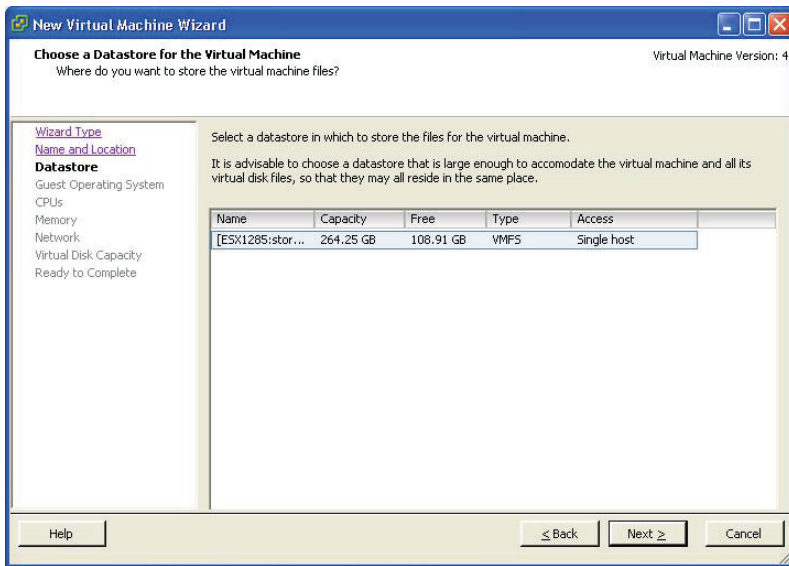


FIGURE D-2 **Select a Name and Location for this Virtual Machine**

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

**FIGURE D-3 Virtual Machine Datastore**

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

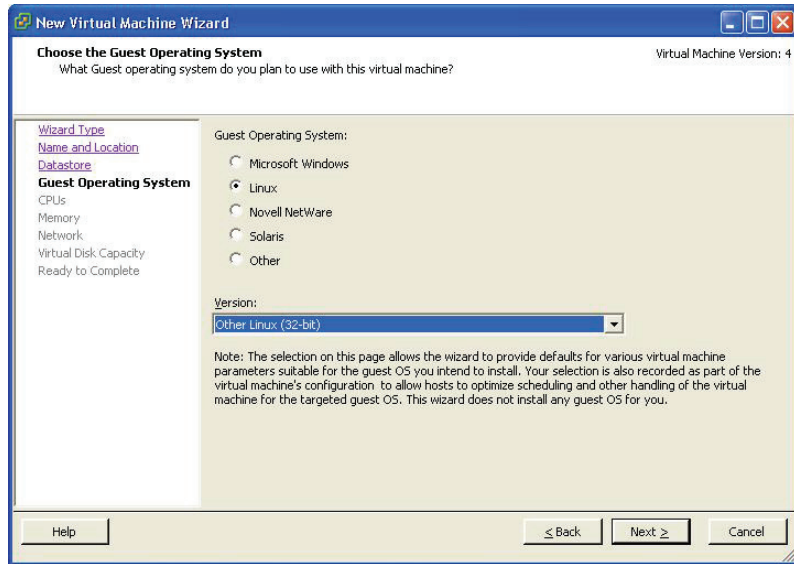


FIGURE D-4 Virtual Machine Guest Operating System

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

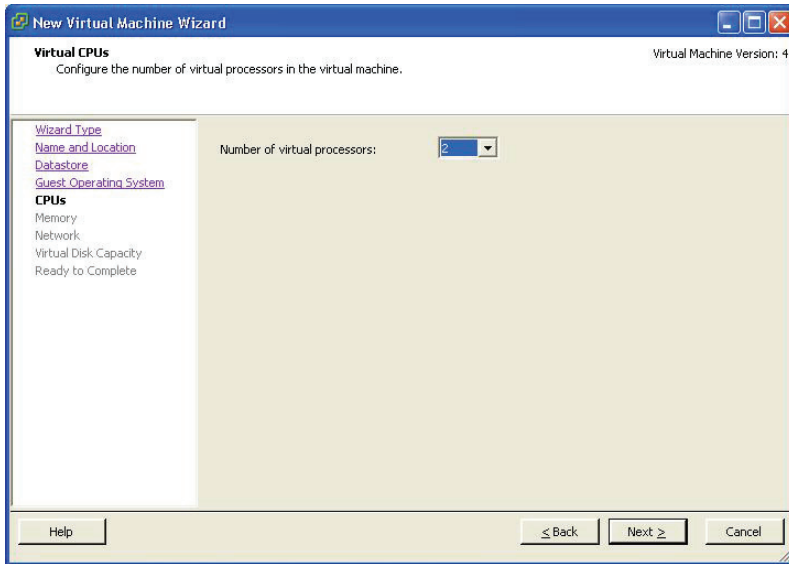


FIGURE D-5 Virtual Machine CPU

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

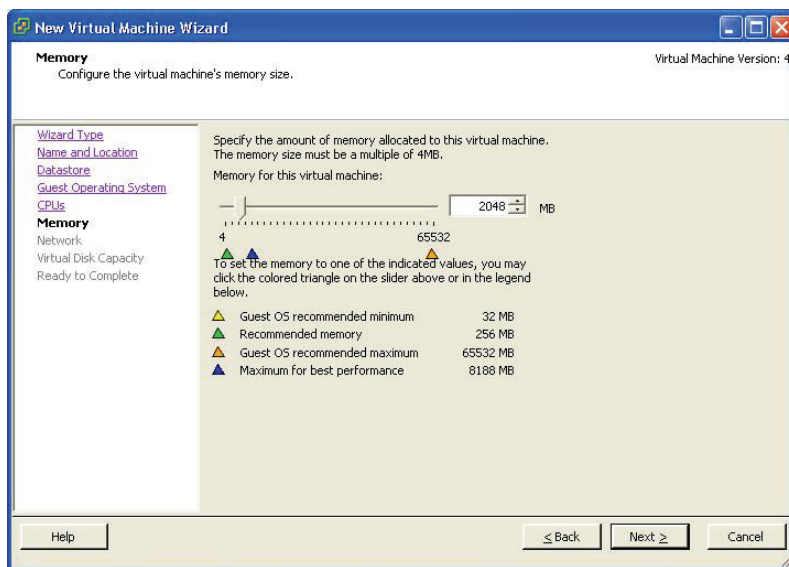


FIGURE D-6 Virtual Machine Memory

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

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

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

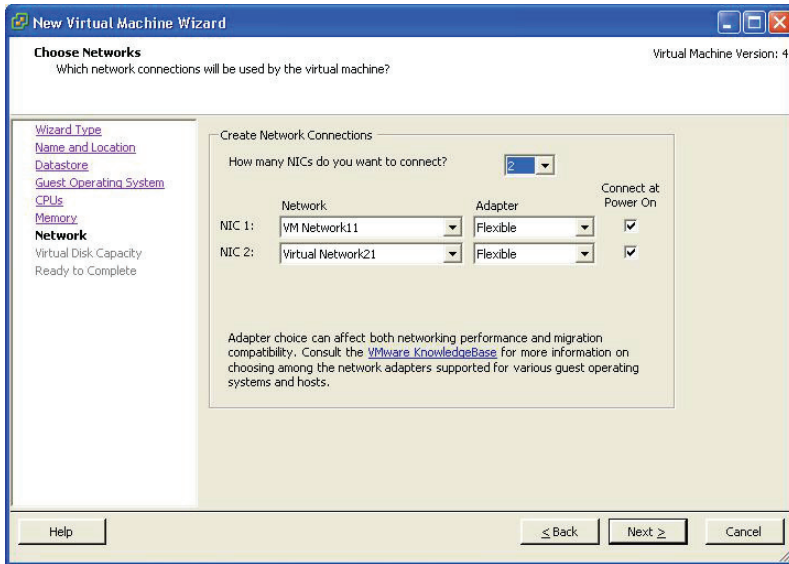


FIGURE D-7 Virtual Machine Network

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

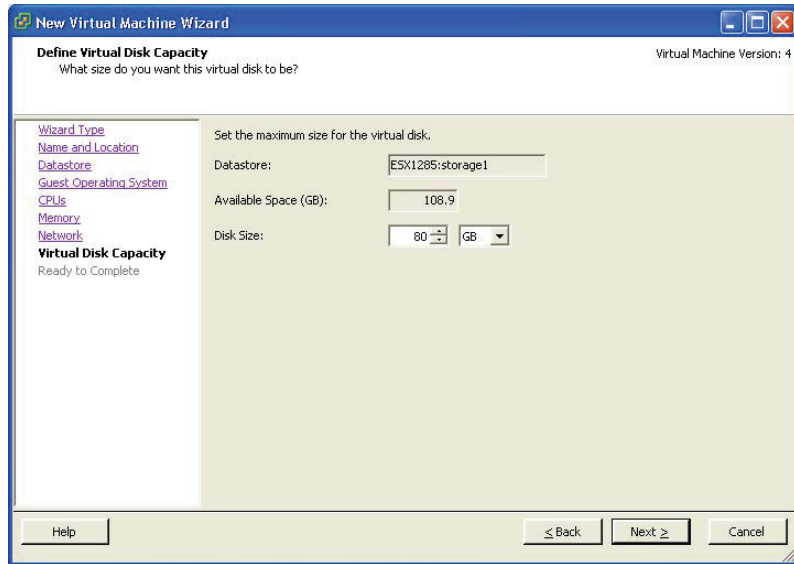


FIGURE D-8 Virtual Disk Capacity

14. IMSVA requires at least 80GB disk space. See [IP Filtering Service](#) on page 2-2 for more information on disk space allocation.

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

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

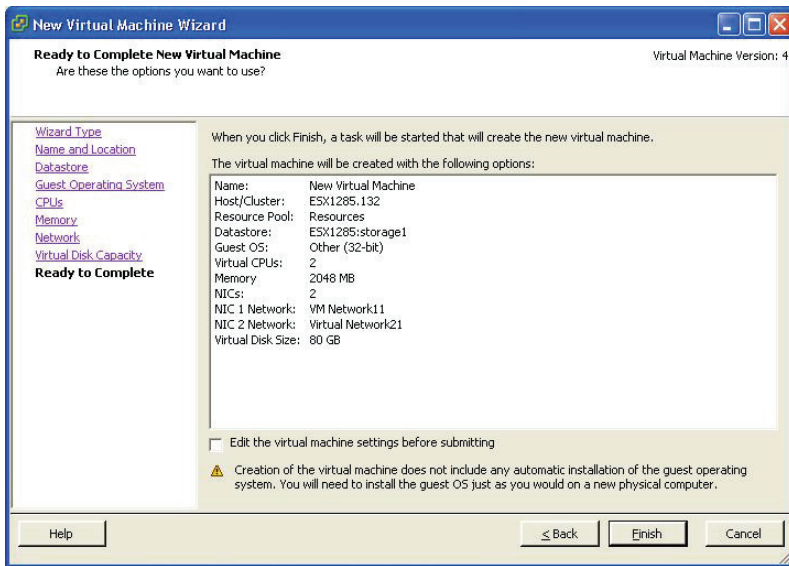


FIGURE D-9 Ready to Complete

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

Index

A

- activate
 - IMSV A 1-16
 - license 4-61
 - product 4-62
- add
 - administrator accounts 4-49
 - one-time reports 4-12
- address group
 - add 2-34
 - delete 2-36
 - edit 2-36
- address groups
 - examples of 2-33
 - manage 2-34
 - understand 2-33
- administrator accounts
 - add 4-49
 - delete 4-51
 - edit 4-51
 - manage 4-49
- antivirus rule 2-48
- APOP 2-29
- application
 - rescuing 8-4
- approved list
 - add IP addresses 2-15
- approved senders list
 - configure 2-54
- archived messages
 - view 4-35
- asterisk wildcard
 - use 2-76
- attachment size
 - scanning conditions 2-57
- audience **X**

B

- back up
 - IMSV A 3-3
- basic configuration 1-5
- blocked list

- add IP addresses 2-16
- blocked senders list
 - configure 2-54
- bounced mail settings
 - configure 2-13

C

- change
 - device roles 7-4
 - web console password 4-59
- child
 - add to group 7-3
 - change to parent 7-5
 - configure IP Settings 4-59
 - Internal Communication Port 7-7
 - remove from group 7-3
 - reset when connection broken 7-4
- child device
 - set up 1-17
- command line interface
 - accessing 6-2
 - entering the shell environment 6-3
 - overview 6-3
 - using 6-2
- commands A-2
- Configuration Wizard
 - accessing 1-5
- configure 2-47
 - approved senders list 2-54
 - blocked senders list 2-54
 - child IP settings 4-59
 - Connection settings 2-20
 - connection settings 4-53
 - Control Manager Server Settings 1-15
 - database maintenance schedule 4-48
 - delivery settings 4-42
 - Deployment Settings 1-7
 - Direct Harvest Attack (DHA) settings 2-10
 - Domain-based Delivery settings 2-25
 - encrypted message scan actions 2-78–2-79
 - expressions 2-59
 - Internal Addresses 1-14

- internal addresses 2-40
- IP Filtering 2-5
- IP Filtering bounced mail settings 2-13
- IP Filtering spam settings 2-7
- IP Filtering virus settings 2-8
- LDAP Settings 1-11
- LDAP settings 4-53
- log settings 2-91, 4-24
- Message Rule settings 2-22
- notification messages 4-44
- Notification Settings 1-9
- NRS 2-14
- password protected zip file scan actions 2-80
- POP3 settings 2-29, 4-56
- quarantine and archive settings 4-26
- route 2-45
- scan exceptions 2-77
- scheduled reports 4-15
- security setting violation scan actions 2-78
- security settings violation exceptions 2-78
- SMTP Routing 1-8
- SMTP routing 2-19
- SMTP settings 2-19
- spam text exemption rules 2-55
- System Settings 1-6
- TMCM settings 4-58
- Update Source 1-10
- User Quarantine Access 4-38
- Web EUQ Digest settings 4-46

- configure event criteria 4-44

- configure other scanning exceptions scan actions 2-82

- Connection settings

- configure 2-20

- connection settings

- configure 4-53

- contact

- support 9-22

- Control Manager

- enable agent 3-5

- replicate settings 3-6

- Control Manager Server Settings

- configure 1-15

D

- database

- configure maintenance schedule 4-48

- deferred messages

- view 4-36

- delete

- address group 2-36

- administrator accounts 4-51

- delivery settings

- configure 4-42

- Deployment Settings

- configure 1-7

- device

- rescuing 8-4

- application 8-4

- device role

- change child to parent 7-5

- parent to child 7-4

- device roles

- change 7-4

- Direct Harvest Attack (DHA) settings

- configure 2-10

- display

- domains 2-18

- suspicious IP addresses 2-18

- Documentation **X**

- domain-based delivery 2-25

- Domain-based Delivery settings

- configure 2-25

- domains

- display 2-18

E

- edit

- address group 2-36

- administrator accounts 4-51

- email relay 2-22

- enable

- Control Manager agent 3-5

- End-User Access 5-8

- EUQ 5-5

- IP Profiler 2-5

- IP Profiler rules 2-6

- NRS 2-5

- POP3 scanning 2-28

- End-User Access

- enable 5-8

- EUQ 4-39, 5-2
 - disable 5-11
 - enable 5-5
 - open the console 5-10
 - start 5-7
 - Web console 5-10
- event criteria
 - configure 4-44
- event notifications 4-41
- export notes 3-2
- expression lists
 - manage 2-58
- expressions
 - configure 2-59

F

- FAQ
 - EUQ 9-17
 - IP Profiler 9-15
- filters
 - examples of 2-33

G

- generate
 - reports 4-10

I

- import notes 3-2
- IMSVa
 - backing up 3-3
 - rescue 8-4
 - restore 3-4
 - scripts A-2
 - services 1-19
 - start/stop services 1-21
- installing
 - using SSL 1-3
- Internal Addresses
 - configure 1-14
- internal addresses
 - configure 2-40
- Internal Communication Port 7-2
 - child 7-7
 - parent 7-7
- IP Filtering
 - configure 2-5

- configure bounced mail settings 2-13
- configure Direct Harvest Attack (DHA) settings 2-10
- configure spam settings 2-7
- configure virus settings 2-8
- IP Filtering Service
 - about 2-2
- IP Profiler
 - enable 2-5
 - enable rules 2-6

K

- Knowledge Base 9-22

L

- LDAP
 - configure and enable 5-2
- LDAP Settings
 - configure 1-11
- LDAP settings
 - configure 4-53
- LDAP User or Group
 - search for 2-38
- license 4-61
 - activate 4-61
- log settings
 - configure 2-91
- logs 4-18
 - configure settings 4-24
 - query 4-18
 - query message tracking 4-19
 - query MTA event 4-23
 - query policy event 4-21
 - query system event 4-20

M

- Main Actions
 - specify 2-60
- manage
 - address groups 2-34
 - administrator accounts 4-49
 - expression lists 2-58
 - notifications list 2-83
 - one-time reports 4-11
 - product licenses 4-60
- managing

- policies 2-30
- manual update 2-86
- Message Rule settings
 - configure 2-22
- message size
 - scanning conditions 2-58
- MIME content type
 - scanning conditions 2-56
- MTA
 - with NRS 2-3

N

- Network Anti-Spam Service 2-3
- notes
 - export 3-2
 - import 3-2
- notification messages
 - configure 4-44
- Notification Settings
 - configure 1-9
- notifications
 - event 4-41
- notifications list
 - manage 2-83
- NRS
 - Activation Code 2-2
 - Administration Console 2-4
 - configure 2-14
 - enable 2-5
 - MTA settings 2-3
 - using 2-2

O

- one-time reports
 - add 4-12
 - manage 4-11
- Online Help **X**
- online help
 - accessing 1-3
- other rule 2-50

P

- parent
 - change role 7-4
 - Internal Communication Port 7-7
- password

- InterScan Web console default 1-2
- web console 4-59
- pattern files
 - update 2-85
- permitted senders 2-25
- policies
 - add 2-42
 - example 1 2-68
 - example 2 2-72
 - finalize 2-66
 - managing 2-30
- policy notification
 - add 2-83
 - edit 2-83
- POP3 messages
 - scan 2-27
- POP3 scanning
 - enable 2-28
- POP3 settings
 - configure 2-29, 4-56
- postponed messages
 - view 4-36
- product licenses
 - manage 4-60
 - view 4-60

Q

- quarantine and archive 4-26
 - configure settings 4-26
- quarantine areas
 - manage 4-27
- quarantined messages
 - view 4-34
- query
 - archive areas 4-31
 - deferred messages 4-33
 - message tracking logs 4-19
 - messages 4-29
 - MTA event logs 4-23
 - policy event logs 4-21
 - postponed messages 4-32
 - quarantine areas 4-29
 - system event logs 4-20
- query logs 4-18

R

- RBL+ Service 2-3
- Readme File **X**
- Real-time Statistics
 - interpreting 4-3
 - view 4-2
- renew 4-61
 - license 4-61
- replicating settings 3-5
- reports
 - add one-time 4-12
 - content 4-10
 - generate 4-10
 - manage one-time 4-11
- rescue
 - IMSVa 8-4
- rescue mode 8-4
- rescuing the application 8-4
- rescuing the device 8-4
- restore
 - IMSVa 3-4
- roll back
 - components 2-87
- route
 - configure 2-45
 - configure exceptions 2-47
 - specify 2-42
- route exceptions 2-47

S

- scan
 - POP3 messages 2-27
 - SMTP messages 2-19
- scan actions
 - configure encrypted message settings 2-78–2-79
 - configure other scanning exceptions settings 2-82
 - configure password protected zip file settings 2-80
- scan engine
 - update 2-85
- scan exceptions
 - configure 2-77
- scanning conditions 2-57
 - attachment names 2-56
 - attachment number 2-57
 - attachment size 2-57
 - attachments 2-56
 - extensions 2-56
 - message size 2-58
 - MIME content type 2-56
 - spam 2-52
 - specify 2-47
 - true file type 2-57
- scheduled reports
 - configure 4-15
 - use 4-15
- scheduled updates 2-88
- security setting violations
 - configure scan actions 2-78
- security settings violations
 - configure exceptions 2-78
- services
 - IP Filtering Service 2-2
- set up
 - child device 1-17
- settings
 - that cannot be restored 3-5
- setup wizard 1-5
- shell environment 6-3
- SMTP messages
 - scan 2-19
- SMTP Routing
 - configure 1-8
- SMTP routing 2-19
 - configure 2-19
- SMTP settings
 - configure 2-19
- Spam Prevention Solution (SPS)
 - Activation Code 2-2
- spam settings
 - configure 2-7
- spam text exemption rules
 - configure 2-55
- Special Viruses
 - specify 2-64
- specify
 - actions 2-60
 - Main Actions 2-60
 - route 2-42
 - scanning conditions 2-47
 - Special Viruses 2-64

- update source 2-85

SSL

- create certificate 1-3

- using 1-3

- SSL certificate 1-3

- start

- EUQ 5-7

- support 9-22

- suspicious IP addresses

- display 2-18

- System Settings

- configure 1-6

T

- tag subject

- add 2-65

- TMCN settings

- configure 4-58

- transport layer 2-21

- Trend Micro Knowledge Base 9-22

- troubleshooting 9-2

- email notifications 9-4

- EUQ quarantined messages 9-7

- EUQ Web console access 9-7

- EUQ Web digest 9-7

- IP Filtering 9-7

- true file type 2-57

U

- update

- application files 2-90

- automatically 2-88

- manually 2-86

- pattern files 2-85

- scan engine 2-85

- system and application 8-2

- system files 2-90

- Update Source

- configure 1-10

- update source

- specify 2-85

- user name

- InterScan Web console default 1-2

- User Quarantine Access

- configure 4-38

V

- view

- archived messages 4-35

- deferred messages 4-36

- postponed messages 4-36

- product licenses 4-60

- quarantined messages 4-34

- Real-time Statistics 4-2

- virtual machine

- create D-2

- virus settings

- configure 2-8

W

- Web console 1-2

- web console password

- change 4-59

- Web EUQ Digest

- configure settings 4-46

- wizard 1-5

- Works C-2